J. H. van Lint R. M. Wilson

Un corso di combinatoria

Traduzione italiana della seconda edizione

Edizione di lavoro per lettura e studio

Novembre 2026

Nota editoriale

Traduzione italiana di *A Course in Combinatorics*, seconda edizione, di J. H. van Lint e R. M. Wilson (Cambridge University Press, 2001), dal PDF fornito per questo lavoro. Si conserva la struttura del testo, con la numerazione originale di teoremi, formule, esempi, problemi e figure. I riferimenti marginali «Orig.» indicano le pagine dell'edizione di partenza; la paginazione della traduzione è autonoma.

La terminologia segue le definizioni degli autori. In particolare, *walk* è reso con «passeggiata», *path* con «cammino» (senza spigoli ripetuti), *simple path* con «cammino semplice» (senza vertici ripetuti, salvo la coincidenza degli estremi nel caso chiuso). Questa convenzione va tenuta presente anche quando differisce dall'uso di altri manuali.

Le figure riprese dall'originale mantengono le loro etichette simboliche; le didascalie sono in italiano. I riferimenti bibliografici conservano i titoli delle pubblicazioni. Le affermazioni storiche e lo stato dei problemi aperti appartengono all'epoca dell'edizione originale.

Le eventuali osservazioni del traduttore sono esplicitamente indicate come note redazionali, distinte dalla voce degli autori. La traduzione non costituisce un'edizione italiana ufficiale.

Indice

Nota editoriale **i**

Prefazione alla prima edizione **iv**

Prefazione alla seconda edizione **v**

1 Grafi **1**

2 Alberi **7**

3 Colorazioni dei grafi e teorema di Ramsey **14**

4 Teorema di Turán e grafi estremali **22**

5 Sistemi di rappresentanti distinti **25**

6 Teorema di Dilworth e teoria estremale degli insiemi **30**

7 Flussi nelle reti **35**

8 Successioni di De Bruijn **40**

9 Due problemi su $(0, 1, *)$: indirizzamento dei grafi e uno schema di codifica hash **44**

10 Il principio di inclusione ed esclusione; formule di inversione **51**

11 Permanenti **57**

12 La congettura di Van der Waerden **64**

13 Conteggio elementare; numeri di Stirling **69**

14 Ricorrenze e funzioni generatrici **75**

15 Partizioni **87**

16 Matrici a elementi 0 e 1 **96**

17 Quadrati latini **103**

18 Matrici di Hadamard, codici di Reed–Muller **112**

19 Disegni combinatori **122**

20 Codici e disegni **137**

21 Grafi fortemente regolari e geometrie parziali **146**

22 Quadrati latini ortogonali **159**

23 Geometrie proiettive e combinatorie **171**

24 Numeri gaussiani e q-analoghi **184**

25 Reticoli e inversione di Möbius **189**

26 Disegni combinatori e geometrie proiettive **199**

27 Insiemi di differenze e automorfismi **209**

28 Insiemi di differenze e anello di gruppo **217**

29 Codici e disegni simmetrici **224**

30 Schemi di associazione **229**

31 (Altre) tecniche algebriche nella teoria dei grafi **243**

32 Connessione dei grafi **253**

33 Planarità e colorazione **257**

34 Dualità di Whitney **264**

35 Immersioni di grafi sulle superfici **274**

36 Reti elettriche e quadrati suddivisi in quadrati **283**

37 La teoria enumerativa di Pólya **291**

38 Il teorema di Baranyai **300**

Appendice 1. Suggerimenti e commenti sui problemi **304**

Appendice 2. Serie formali di potenze **324**

Indice dei nomi **328**

Indice analitico **334**

Prefazione alla prima edizione

Uno dei corsi avanzati di matematica più apprezzati al Caltech per molti anni fu il corso di H. J. Ryser, *Combinatorial Analysis*, Math 121. Uno degli obiettivi principali di Ryser era mostrare eleganza e semplicità. Inoltre, in quel corso che teneva così bene, cercava di mettere in luce l'unità della combinatoria. Dedichiamo questo libro alla memoria di Herb Ryser, nostro amico, che ammiravamo e dal quale abbiamo imparato molto.

Il lavoro a questo libro iniziò nell'anno accademico 1988–89, quando tenemmo insieme il corso Math 121. Volevamo non soltanto proseguire nello stile di Ryser, mostrando i molti legami fra settori della combinatoria apparentemente estranei, ma anche tentare di offrire una panoramica della disciplina. Pensavamo che, dopo un corso di questo tipo, gli studenti che avessero poi partecipato a un convegno di «Combinatoria» non avrebbero dovuto ascoltare alcuna conferenza nella quale si sentissero completamente smarriti per mancanza di familiarità con l'argomento. O almeno avrebbero dovuto avere già sentito molte delle parole. Crediamo fermamente che chi studia combinatoria debba conoscerne il maggior numero possibile di rami.

Naturalmente nessun capitolo può trattare in modo completo l'argomento indicato nel titolo. Ne presentiamo invece alcuni aspetti salienti, insistendo però sul fatto di sviluppare qualcosa di sostanziale o non banale per ciascun tema. A nostro avviso, un buon modo di imparare la combinatoria è ritornare sugli argomenti a intervalli. Perciò diversi settori sono affrontati in più parti del libro: per esempio, gli insiemi parzialmente ordinati e i codici ricompaiono più volte. I problemi enumerativi e la teoria dei grafi percorrono l'intero volume. Alcuni argomenti sono trattati più a fondo perché ci piacciono; alcuni materiali, come la nostra dimostrazione della congettura di Van der Waerden sul permanente, compaiono qui per la prima volta in un libro di testo.

Un corso di algebra moderna costituisce una preparazione sufficiente, ma non è assolutamente indispensabile: molte parti si possono comprendere con un certo grado di maturità matematica. La combinatoria è infatti ben nota per essere «accessibile». Il lettore dovrebbe tuttavia trovare il libro impegnativo e dovrà completare dettagli che speriamo siano istruttivi e non troppo difficili. Osserviamo di passaggio che, nell'apprendimento di una disciplina, riteniamo insostituibile un insegnante in carne e ossa. Per alcuni argomenti sarà necessaria familiarità con il calcolo infinitesimale, i gruppi, i campi finiti, la teoria elementare dei numeri e, soprattutto, l'algebra lineare. Al Caltech il corso è seguito sia da studenti dei primi anni universitari sia da studenti di livello avanzato. Il materiale di ogni capitolo è stato presentato a lezione, ma non siamo mai riusciti a svolgere tutti i capitoli in un solo anno.

Le note al termine dei capitoli contengono spesso osservazioni biografiche sui matematici. Abbiamo scelto di non includere notizie biografiche sui matematici viventi, salvo quelli già ritirati dall'attività, con l'eccezione di P. Erdős.

Gli esercizi hanno difficoltà variabile. Per alcuni può essere necessario consultare i suggerimenti dell'appendice 1. Nell'appendice 2 includiamo una breve trattazione delle serie formali di potenze.

Il manoscritto è stato composto tipograficamente dagli autori in AMS-TEX.

J. H. v. L., R. M. W.
Eindhoven e Pasadena, 1992

Prefazione alla seconda edizione

La favorevole accoglienza del libro e il suo impiego in vari corsi di matematica combinatoria presso numerosi istituti universitari ci hanno incoraggiati a preparare questa seconda edizione. Abbiamo aggiunto nuovo materiale e aggiornato i riferimenti bibliografici. Sono stati corretti diversi errori tipografici e di altro genere. In più punti abbiamo dovuto sostituire «questo secolo» con «il secolo scorso».

Il nuovo materiale è stato perlopiù inserito in capitoli che mantengono i titoli della prima edizione. Fa eccezione il materiale degli ultimi capitoli di teoria dei grafi, che è stato riorganizzato in quattro capitoli anziché due. Fra le aggiunte figurano, per esempio, il crivello di Lovász, i disegni a blocchi associativi e le colorazioni per liste dei grafi.

Sono stati aggiunti molti nuovi problemi e speriamo che soprattutto questa modifica accresca il valore didattico del libro. Abbiamo deciso di non cercare di indicare il grado di difficoltà dei singoli problemi, ma ribadiamo che esso può variare molto. La difficoltà dipende spesso dall'esperienza e dalla preparazione del lettore; spetterà al docente decidere quali esercizi siano adatti ai propri studenti. Ci piace enunciare i problemi nel punto in cui sono più pertinenti al testo, ma ne abbiamo aggiunti alcuni anche alla fine dei capitoli. I problemi che compaiono più avanti non sono necessariamente più difficili di quelli all'inizio di un capitolo. Diversi suggerimenti e commenti dell'appendice 1 sono stati migliorati.

La seconda edizione è stata preparata durante una visita di sei mesi del primo autore al California Institute of Technology in qualità di Moore Distinguished Scholar. Egli ringrazia la Moore Foundation per il sostegno ricevuto.

Capitolo 1

Grafi

Orig. 1

Un *grafo* G è costituito da un insieme V (o $V(G)$) di *vertici*, da un insieme E (o $E(G)$) di *spigoli* e da un'applicazione che associa a ogni spigolo $e \in E(G)$ una coppia non ordinata x, y di vertici, detti *estremi* di e. Diciamo che uno spigolo è *incidente* con i suoi estremi e che li *congiunge*. Ammettiamo che $x = y$; in tal caso lo spigolo si chiama *cappio*. Un vertice è *isolato* se non è incidente con alcuno spigolo.

È consuetudine rappresentare un grafo mediante un disegno, rappresentando ciascun vertice con un punto del piano e gli spigoli con segmenti o archi che congiungono alcune coppie di punti. Si può pensare, per esempio, a una rete di strade fra città. Un grafo si dice *planare* se può essere disegnato nel piano in modo che due spigoli distinti, ossia i segmenti o gli archi che li rappresentano, non si incrocino. La planarità sarà trattata nel capitolo 33; per il momento intendiamo occuparci dei grafi da un punto di vista più strettamente combinatorio.

spigolo	estremi
a	x, z
b	y, w
c	x, z
d	z, w
e	z, w
f	x, y
g	z, w

Figura 1.1

Un grafo è dunque descritto da una tabella come quella della figura 1.1, che elenca gli estremi di ciascuno spigolo. Il grafo qui descritto ha insieme dei vertici $V = \{x, y, z, w\}$ e insieme degli spigoli $E = \{a, b, c, d, e, f, g\}$; un suo disegno compare nella figura 1.2(iv). Orig. 2

Un grafo si dice *semplice* se non ha cappi e se due spigoli distinti non hanno mai esattamente la stessa coppia di estremi. Due spigoli che non siano cappi si dicono *paralleli* se hanno gli stessi estremi; alcuni autori chiamano *multigrafi* i grafi che li contengono, oppure dicono che tali grafi hanno «spigoli multipli».

Se a ogni spigolo si associa una coppia *ordinata* di vertici, si ottiene un *grafo orientato*, o *digrafo*. Nel disegno di un digrafo usiamo una freccia diretta dal primo vertice (la *coda*) al secondo (la *testa*) incidente con uno spigolo. In un digrafo semplice escludiamo i cappi e richiediamo che due spigoli distinti non abbiano la stessa coppia ordinata di estremi.

Quando si considerano grafi semplici, è spesso comodo identificare gli spigoli con le coppie non ordinate dei vertici che congiungono; uno spigolo che congiunge x e y può quindi essere indicato con $\{x, y\}$. Analogamente, gli spigoli di un digrafo semplice possono essere identificati con coppie ordinate (x, y) di vertici distinti.

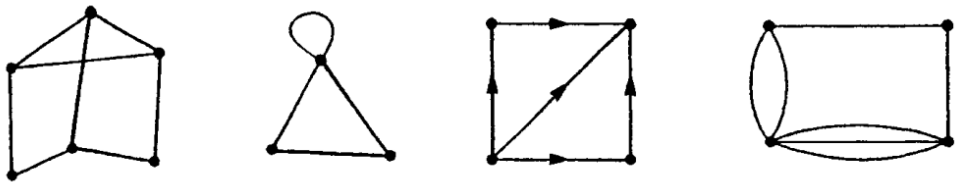


Figura 1.2. (i) Grafo; (ii) grafo con cappio; (iii) digrafo; (iv) spigoli multipli.

Vi sono diversi modi di disegnare uno stesso grafo. Per esempio, i due grafi della figura 1.3 sono essenzialmente lo stesso grafo.

Precisiamo questa affermazione; per evitare definizioni inutilmente tecniche a questo punto, nelle prossime due definizioni supponiamo che tutti i grafi siano non orientati e semplici.

Due grafi si dicono *isomorfi* se esiste una corrispondenza biunivoca fra i loro insiemi di vertici tale che, se due vertici sono congiunti da uno spigolo in un grafo, allora i vertici corrispondenti sono congiunti da uno spigolo nell'altro.[1] Per mostrare che i due grafi della figura 1.3 sono lo stesso grafo, trovate una numerazione opportuna dei vertici di entrambi (usando $1, 2, 3, 4, 5, 6$) e osservate che gli insiemi degli spigoli sono gli stessi insiemi di coppie non ordinate. Orig. 3

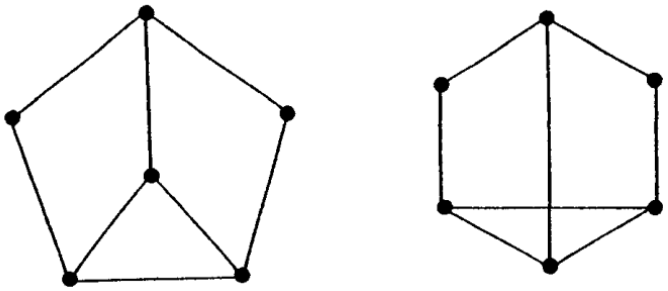


Figura 1.3

Una permutazione σ dell'insieme dei vertici di un grafo G tale che $\{a, b\}$ è uno spigolo se e solo se $\{\sigma(a), \sigma(b)\}$ è uno spigolo si chiama *automorfismo* di G.

Problema 1A. (i) Mostrate che i disegni della figura 1.4 rappresentano lo stesso grafo (ossia grafi isomorfi).

(ii) Determinate il gruppo degli automorfismi del grafo della figura 1.4.

Osservazione. Non esiste un modo rapido o facile per farlo, a meno di essere fortunati; dovrete sperimentare e fare tentativi.

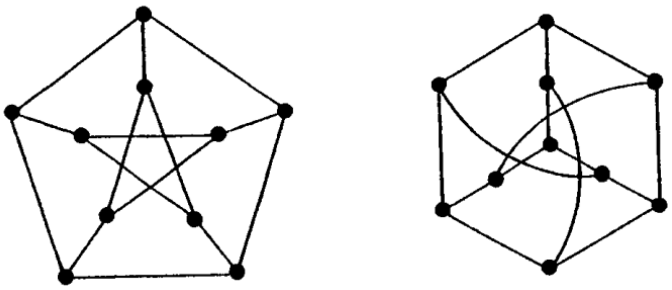


Figura 1.4

Il *grafo completo* K_n su n vertici è il grafo semplice che possiede tutti i $\binom{n}{2}$ spigoli possibili.

Due vertici a e b di un grafo G si dicono *adiacenti* se sono distinti e congiunti da uno spigolo. Indicheremo con $\Gamma(x)$ l'insieme di tutti i vertici adiacenti a un dato vertice x; tali vertici sono detti anche *vicini* di x. Il numero di spigoli incidenti con un vertice x è detto *grado*, o *valenza*, di x. Si considera Orig. 4

[1] Nota di traduzione: la corrispondenza deve preservare l'adiacenza in entrambi i sensi; nell'originale la condizione è formulata con il solo «se».

che ciascun cappio contribuisca 2 alla valenza, come suggeriscono i disegni. Se tutti i vertici di un grafo hanno lo stesso grado, il grafo si dice *regolare*.

Uno degli strumenti importanti della combinatoria è il metodo di contare certi oggetti in due modi diversi. È ben noto che, se non si commettono errori, le due risposte coincidono. Ne diamo un primo esempio elementare. Un grafo si dice *finito* quando $E(G)$ e $V(G)$ sono entrambi insiemi finiti. Ci occuperemo principalmente di grafi finiti, al punto che potremmo aver talvolta dimenticato di specificare questa condizione fra le ipotesi di qualche affermazione.

Teorema 1.1. Un grafo finito G ha un numero pari di vertici di valenza dispari.

Dimostrazione. Consideriamo una tabella che elenchi gli estremi degli spigoli, come nella figura 1.1. Il numero di elementi nella colonna di destra è il doppio del numero degli spigoli. D'altra parte, il grado di un vertice x è, per definizione, il numero di volte in cui esso compare nella tabella. Il numero di elementi nella colonna di destra è dunque

$$\sum_{x \in V(G)} \deg(x) = 2|E(G)|. \tag{1.1}$$

L'affermazione segue immediatamente. □

L'equazione (1.1) è semplice, ma importante. La si potrebbe chiamare il «primo teorema della teoria dei grafi», e il nostro teorema 1.1 ne è il primo corollario.

Un *sottografo* di un grafo G è un grafo H tale che $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$ e gli estremi di uno spigolo $e \in E(H)$ sono gli stessi che esso ha in G. Il sottografo H si dice *ricoprente* se $V(H) = V(G)$. Il sottografo di G *indotto* da un sottoinsieme S dei vertici di G è il sottografo il cui insieme dei vertici è S e i cui spigoli sono tutti gli spigoli di G aventi entrambi gli estremi in S.

Una *passeggiata* in un grafo G consiste in una successione alternata

$$x_0, e_1, x_1, e_2, x_2, \ldots, x_{k-1}, e_k, x_k$$

di vertici x_i, non necessariamente distinti, e di spigoli e_i, tale che gli estremi di e_i siano precisamente x_{i-1} e x_i, per $i = 1, 2, \ldots, k$. Una tale passeggiata ha *lunghezza* k. Se il grafo è semplice, una passeggiata è determinata dalla sua successione di vertici, nella quale due elementi consecutivi qualsiasi sono adiacenti. Orig. 5

Se gli spigoli $e_1, \ldots, e_k$ sono distinti, la passeggiata si chiama *cammino* da x_0 a x_k. Se $x_0 = x_k$, una passeggiata (o un cammino) si dice *chiusa*. Un *cammino semplice* è un cammino nel quale anche i vertici $x_0, x_1, \ldots, x_k$ sono distinti; si parla però di *cammino semplice chiuso* quando $k \geq 1$ e tutti i vertici sono distinti tranne $x_0 = x_k$.

Se per ogni coppia di vertici x, y di G esiste un cammino da x a y, il grafo G si dice *connesso*. Altrimenti G è costituito da un certo numero di *componenti connesse* (sottografi connessi massimali). Converremo, per comodità, che il grafo nullo, privo di vertici e spigoli, non sia connesso.

Problema 1B. Sia G un grafo semplice su 10 vertici non connesso. Dimostrate che G ha al più 36 spigoli. Può verificarsi l'uguaglianza?

La lunghezza della passeggiata più breve da a a b, se tali passeggiate esistono, si chiama *distanza* $d(a, b)$ fra questi vertici. Una passeggiata di lunghezza minima è necessariamente un cammino semplice.

Esempio 1.1. Un grafo ben noto ha come vertici i matematici di tutto il mondo. Due vertici sono adiacenti se e solo se hanno pubblicato un articolo in comune. La distanza, in questo grafo, fra un matematico e il vertice P. Erdős è nota come il suo *numero di Erdős*.

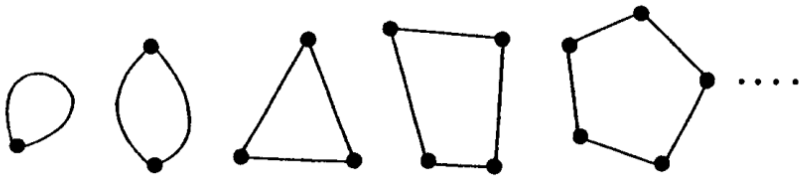


Figura 1.5

Un *poligono* è il «grafo di» un cammino semplice chiuso; più precisamente, lo si può definire come un grafo finito connesso regolare di grado 2. Per ogni intero positivo n esiste, a meno di isomorfismo, esattamente

un poligono P_n con n vertici (spesso detto *n-gono*). La successione dei poligoni è mostrata nella figura 1.5. Orig. 6

Un grafo connesso che non contiene cammini semplici chiusi, ossia che non ha poligoni come sottografi, si chiama *albero*.

Problema 1C. Mostrate che un grafo connesso su n vertici è un albero se e solo se ha $n-1$ spigoli.

Problema 1D. Il *grafo bipartito completo* $K_{n,m}$ ha $n+m$ vertici $a_1,\ldots,a_n$ e $b_1,\ldots,b_m$ e, come spigoli, tutte le mn coppie $\{a_i,b_j\}$. Mostrate che $K_{3,3}$ non è planare.

Nessuna introduzione alla teoria dei grafi può tralasciare il problema dei ponti di Königsberg (un tempo città della Prussia). Il fiume Pregel attraversava la città e si divideva in due rami. Nel fiume si trovava l'isola di Kneiphof. Sette ponti collegavano diverse parti della città, come mostra lo schema della figura 1.6.

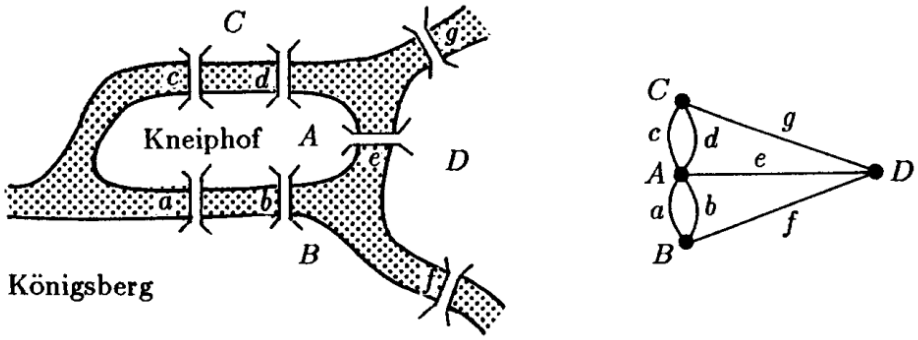


Figura 1.6

In un articolo scritto nel 1736 da L. Euler, considerato il primo articolo di teoria dei grafi, l'autore afferma che si riteneva difficile la seguente domanda: è possibile fare una passeggiata attraverso la città, tornare al punto di partenza e attraversare ogni ponte esattamente una volta? Questo articolo ha condotto alla definizione seguente. Un cammino chiuso in un grafo che utilizza ogni spigolo una volta si chiama *circuito euleriano*; un grafo che ammette un tale cammino si dice *grafo euleriano*.

Teorema 1.2. Un grafo finito G senza vertici isolati (ma eventualmente con spigoli multipli) è euleriano se e solo se è connesso e ogni suo vertice ha grado pari. Orig. 7

Dimostrazione. È evidente che G deve essere connesso. Poiché il cammino entra in un vertice lungo uno spigolo e ne esce lungo un altro, è chiaro che tutti i gradi devono essere pari. Per mostrare che le condizioni sono sufficienti, partiamo da un vertice x e iniziamo a costruire un cammino. Proseguiamo senza mai usare due volte lo stesso spigolo, finché non possiamo andare oltre. Poiché ogni vertice ha grado pari, ciò può accadere soltanto quando siamo tornati a x e tutti gli spigoli uscenti da x sono stati utilizzati. Se rimangono spigoli inutilizzati, consideriamo il sottografo formato da essi. Applichiamo lo stesso procedimento a una sua componente, ottenendo un secondo cammino chiuso. Se facciamo partire questo secondo cammino da un punto del primo, i due cammini possono essere combinati in un cammino chiuso più lungo da x a x. Pertanto, il più lungo di questi cammini utilizza tutti gli spigoli. □

Il problema dei ponti di Königsberg è descritto dal grafo della figura 1.6. Nessun vertice ha grado pari, quindi non esiste un circuito euleriano.

Si può considerare un problema analogo per i digrafi. La condizione necessaria e sufficiente per l'esistenza di un circuito euleriano orientato è che il grafo sia connesso e che ogni vertice abbia lo stesso «grado entrante» e «grado uscente».

Esempio 1.2. Un rompicapo chiamato *Instant Insanity* riguarda quattro cubi con le facce colorate di rosso, blu, verde e giallo, in modo che ogni cubo abbia almeno una faccia di ciascun colore. Si chiede di impilare i cubi in modo che tutti e quattro i colori compaiano su ciascuno dei quattro lati della pila. Nella figura 1.7 sono descritti quattro possibili cubi mediante i loro sviluppi piani.

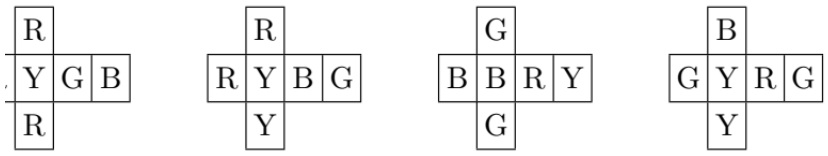


Figura 1.7. Cubi 1, 2, 3 e 4. Le lettere originali R, B, G, Y indicano rispettivamente rosso, blu, verde e giallo.

Non è una buona idea provare tutte le possibilità. Un approccio sistematico è il seguente. Le informazioni essenziali sui cubi sono contenute nei quattro grafi della figura 1.8.

Orig. 8

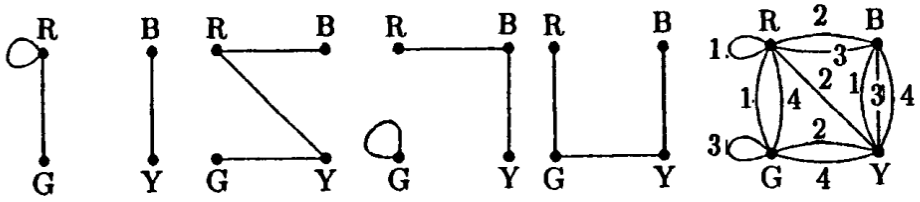


Figura 1.8. Da sinistra: cubi 1–4 e grafo G.

Uno spigolo indica che i due colori adiacenti compaiono su facce opposte del cubo. Sovrapponendo i quattro grafi otteniamo un grafo G e numeriamo gli spigoli secondo il cubo da cui provengono. Non è difficile vedere che dobbiamo trovare in G due sottografi regolari di grado 2, con spigoli numerati $1, 2, 3, 4$, privi di spigoli comuni. Uno dei sottografi indica quali coppie di colori disporre sul lato sinistro e sul lato destro della pila. L'altro descrive i colori sul davanti e sul retro. È naturalmente facile ruotare i cubi in modo da portare i colori nelle posizioni desiderate. Il punto dell'esempio è che basta un minuto per trovare due sottografi con le proprietà appena descritte. In questo esempio la soluzione è unica.

Accenniamo a un concetto che sembra simile a quello di circuito euleriano, ma che in realtà è molto diverso. Un *circuito hamiltoniano* in un grafo G è un cammino semplice chiuso che passa per ciascun vertice esattamente una volta (anziché per ciascuno spigolo). Un grafo ammette quindi un circuito hamiltoniano se e solo se contiene un poligono come sottografo ricoprente. A metà del XIX secolo, Sir William Rowan Hamilton cercò di rendere popolare il problema di trovare un tale cammino chiuso nel grafo del dodecaedro (figura 1.9).

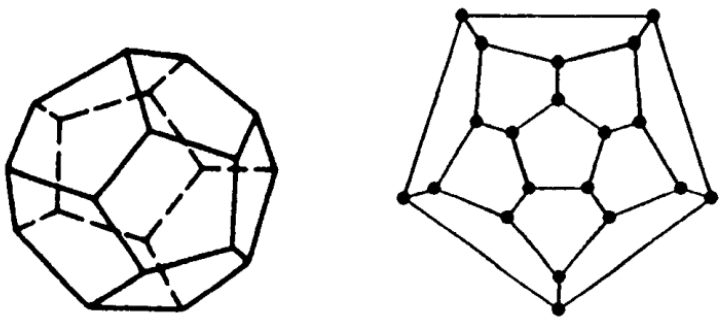


Figura 1.9

Orig. 9

Il grafo della figura 1.4 si chiama *grafo di Petersen* (cfr. capitolo 21); una delle ragioni della sua notorietà è che non è «hamiltoniano»: contiene n-goni soltanto per $n = 5, 6, 8, 9$, e non per $n = 7$ o $n = 10$.

Per il teorema 1.2 è facile decidere se un grafo ammette un circuito euleriano. Si può facilmente programmare un calcolatore per controllare se i gradi di un grafo sono pari e se il grafo è connesso, e persino per produrre un circuito euleriano quando esiste. Al contrario, il problema di decidere se un grafo arbitrario ammetta un circuito hamiltoniano è verosimilmente «intrattabile». Più precisamente, è stato dimostrato che è NP-completo: si veda Garey e Johnson (1979).

Problema 1E. Siano $A_1, \ldots, A_n$ sottoinsiemi distinti dell'insieme di n elementi $N := \{1, \ldots, n\}$. Mostrate che esiste un elemento $x \in N$ tale che gli insiemi $A_i \setminus \{x\}$, $1 \le i \le n$, siano tutti distinti. A tale scopo, costruite un grafo G con vertici A_i, ponendo uno spigolo di «colore» x fra A_i e A_j se e solo se la differenza simmetrica di A_i e A_j è $\{x\}$. Considerate i colori degli spigoli di un poligono. Mostrate che

si possono eliminare spigoli da G in modo che non rimangano poligoni e che il numero dei colori distinti rimanga invariato. Usate poi il problema 1C. (Questa idea è dovuta a J. A. Bondy (1972).)

Problema 1F. La *maglia* di un grafo è la lunghezza del suo poligono più corto. Sia G un grafo di maglia 5 in cui tutti i vertici abbiano grado $\geq d$. Mostrate che G ha almeno $d^2 + 1$ vertici. Può valere l'uguaglianza?

Problema 1G. Mostrate che un grafo semplice finito con più di un vertice ha almeno due vertici dello stesso grado.

Problema 1H. Un grafo sull'insieme di vertici $\{1, 2, \ldots, n\}$ è spesso descritto da una matrice A di ordine n, nella quale a_{ij} e a_{ji} sono uguali al numero di spigoli con estremi i e j. Qual è l'interpretazione combinatoria degli elementi della matrice A^2?

Problema 1I. Sia $Q := \{1, 2, \ldots, q\}$. Sia G il grafo avente come vertici gli elementi di Q^n, con uno spigolo fra $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ se e solo se $a_i \neq b_i$ per esattamente un valore di i. Mostrate che G è hamiltoniano.

Orig. 10

Problema 1J. Sia G un grafo semplice su n vertici, con $n > 3$, privo di vertici di grado $n-1$. Supponete che, per ogni coppia di vertici di G, esista un unico vertice congiunto a entrambi.

(i) Se x e y non sono adiacenti, dimostrate che hanno lo stesso grado.

(ii) Mostrate ora che G è regolare.

Note

Paul Erdős (1913–1996), cfr. esempio 1.1, è stato probabilmente il matematico più prolifico del XX secolo, con ben oltre 1400 articoli pubblicati. I suoi contributi alla combinatoria, alla teoria dei numeri, alla teoria degli insiemi e ad altri campi comprendono molti risultati importanti. Collaborò con numerosi matematici di tutto il mondo, tutti orgogliosi di avere numero di Erdős 1, fra cui gli autori di questo libro; si veda J. W. Grossman (1997).

Leonhard Euler (1707–1783) fu un matematico svizzero che trascorse gran parte della vita a San Pietroburgo. Fu probabilmente il matematico più produttivo di tutti i tempi. Anche dopo essere diventato cieco nel 1766, continuò a lavorare allo stesso ritmo. La celebrazione, nel 1986, del duecentocinquantesimo anniversario della teoria dei grafi si basava sull'articolo di Euler sul problema dei ponti di Königsberg. Königsberg è oggi la città russa di Kaliningrad.

Per un'introduzione elementare alla teoria dei grafi consigliamo R. J. Wilson (1979) e J. J. Watkins e R. J. Wilson (1990).

Sir William Rowan Hamilton (1805–1865) fu un matematico irlandese. Era considerato un genio: conosceva tredici lingue a dodici anni e fu nominato professore di astronomia al Trinity College di Dublino a ventidue anni, prima di conseguire la laurea. I suoi lavori più importanti riguardavano la fisica matematica.

Riferimenti bibliografici

M. Garey e D. S. Johnson (1979)
Computers and Intractability; A Guide to the Theory of NP-completeness, W. H. Freeman and Co.

J. W. Grossman (1997)
Paul Erdős: The Master of Collaboration, pp. 467–475 in *The Mathematics of Paul Erdős*, R. L. Graham e J. Nešetřil (a cura di), Springer-Verlag.

Orig. 11

J. J. Watkins e R. J. Wilson (1990)
Graphs (An Introductory Approach), J. Wiley & Sons.

R. J. Wilson (1979)
Introduction to Graph Theory, Longman.

Capitolo 2

Alberi

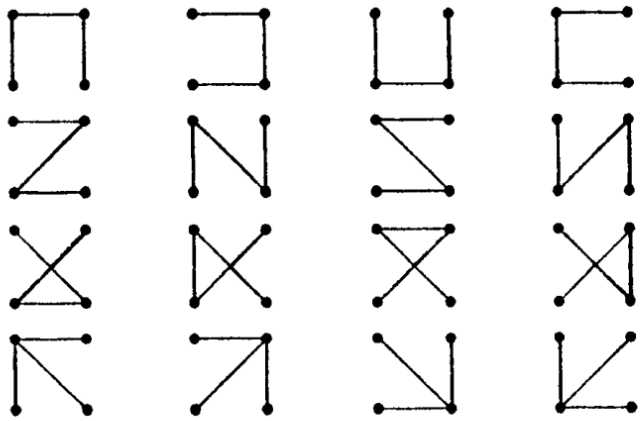
Orig. 12

Arriviamo al primo teorema non del tutto facile. È dovuto ad A. Cayley (1889). Ne daremo qui tre dimostrazioni diverse. Altre due compariranno in capitoli successivi: si vedano gli esempi 14.14 e 38.2. Le prime due dimostrazioni illustrano un metodo molto frequente in combinatoria: per contare oggetti che sembrano difficili da enumerare, si trova una corrispondenza biunivoca con un insieme di altri oggetti il cui numero sia più facile da determinare.

Teorema 2.1. Esistono n^{n-2} alberi etichettati distinti su n vertici.

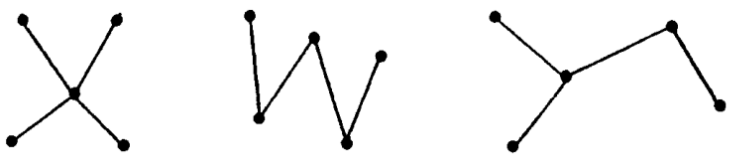
Il termine *etichettati* sottolinea che non identifichiamo grafi isomorfi. Abbiamo fissato l'insieme dei vertici e contiamo due alberi come lo stesso albero se e solo se sono adiacenti esattamente le stesse coppie di vertici. Un *albero ricoprente* di un grafo connesso G è un sottografo ricoprente di G che sia un albero. Il teorema si sarebbe potuto enunciare così: il grafo completo K_n ha n^{n-2} alberi ricoprenti.

Esempio 2.1. Ecco i 16 alberi etichettati su quattro vertici:



Orig. 13

Esempio 2.2. Esistono tre alberi a due a due non isomorfi su cinque vertici:



Il numero di alberi ricoprenti di K_5 isomorfi a un dato albero T su cinque vertici è 5! diviso per l'ordine del gruppo degli automorfismi di T (perché?). Vi sono quindi $5!/4! = 5$ alberi in K_5 isomorfi al primo albero della figura e $5!/2 = 60$ alberi isomorfi a ciascuno degli altri due, per un totale di 125 alberi ricoprenti.

Problema 2A. Trovate i sei alberi a due a due non isomorfi su 6 vertici e, per ciascuno, calcolate il numero di alberi ricoprenti distinti di K_6 a esso isomorfi.

Prima di iniziare le dimostrazioni facciamo alcune osservazioni. (Probabilmente il lettore le avrà già notate risolvendo il problema 1C.) Anzitutto, ogni albero con $n \geq 2$ vertici ha almeno due vertici *monovalenti*, cioè di grado 1. Ciò segue immediatamente, per esempio, dal problema 1C e dall'equazione (1.1): la somma dei gradi $d_1, d_2, \ldots, d_n$, tutti almeno uguali a 1, è $2n-2$. In secondo luogo, eliminando da un albero un vertice monovalente e lo spigolo a esso incidente, il grafo risultante è ancora un albero. Infine, dato un albero T, se introduciamo un nuovo vertice x e un nuovo spigolo che congiunge x a un vertice qualsiasi di T, otteniamo ancora un albero.

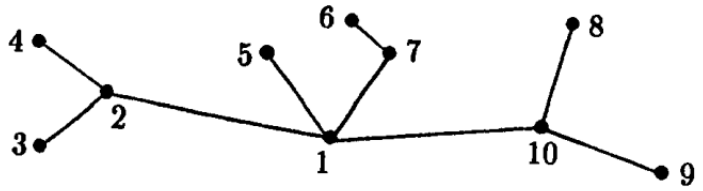


Figura 2.1

Dimostrazione 1. La prima dimostrazione, dovuta a H. Prüfer (1918), usa un algoritmo che associa a ogni albero T un «nome» $P(T)$, detto *codice di Prüfer*, che caratterizza l'albero. Come vertici di K_n prendiamo l'insieme ordinato $V = \{1, 2, 3, \ldots, n\}$. Dato un albero ricoprente T di K_n, poniamo $T_1 = T$ e generiamo una successione di alberi $T_1, T_2, \ldots, T_{n-1}$ e due successioni di vertici nel modo seguente. Dato l'albero T_i con $n-i+1$ vertici, per $i = 1, 2, \ldots, n-1$, sia x_i il suo vertice monovalente minimo; eliminiamo da T_i il vertice x_i e lo spigolo incidente $\{x_i, y_i\}$, ottenendo un albero T_{i+1} su $n-i$ vertici. Il nome di T sarà

$$P(T) = (y_1, y_2, \ldots, y_{n-2}).$$

Orig. 14

Affermiamo che l'applicazione P, dall'insieme di tutti gli alberi ricoprenti di K_n all'insieme V^{n-2} di tutti i possibili nomi, è iniettiva e suriettiva, cioè biiettiva. Questo dimostrerà che il numero degli alberi ricoprenti di K_n è n^{n-2}.

Per l'albero della figura 2.1, in cui $n = 10$, abbiamo $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (4, 2)$, $(x_3, y_3) = (2, 1)$, …, $(x_9, y_9) = (9, 10)$; questi spigoli sono le colonne della matrice seguente:

$$\begin{pmatrix} 3 & 4 & 2 & 5 & 6 & 7 & 1 & 8 & 9 \\ 2 & 2 & 1 & 1 & 7 & 1 & 10 & 10 & 10 \end{pmatrix}.$$

Quindi $P(T) = (2, 2, 1, 1, 7, 1, 10, 10)$. Non includete $y_9 = 10$.

Per capire perché P è biiettiva, osserviamo anzitutto alcuni semplici fatti sugli x_i e sugli y_i. Primo: si ha sempre $y_{n-1} = n$. Infatti ogni albero con almeno due vertici ha almeno due vertici monovalenti, quindi n non sarà mai il vertice monovalente minimo. Secondo: $x_k, x_{k+1}, \ldots, x_{n-1}$ e n sono i vertici dell'albero T_k. Terzo: $\{x_i, y_i\}$, con $k \leq i \leq n-1$, sono precisamente gli spigoli di T_k, in un certo ordine.

Il numero di volte in cui un vertice v compare fra $y_1, y_2, \ldots, y_{n-2}$ è $\deg_T(v) - 1$. Infatti v compare $\deg_T(v)$ volte fra gli spigoli $\{x_i, y_i\}$, $1 \leq i \leq n-1$, ed esattamente una volta fra $x_1, x_2, \ldots, x_{n-1}, y_{n-1}$.

Analogamente, il numero di volte in cui un vertice v di T_k compare fra $y_k, y_{k+1}, \ldots, y_{n-2}$ è il suo grado in T_k meno 1. In particolare, i vertici monovalenti di T_k sono quegli elementi di V che non appartengono a

$$\{x_1, x_2, \ldots, x_{k-1}\} \cup \{y_k, y_{k+1}, \ldots, y_{n-1}\},$$

e ciò significa che x_k, il minimo vertice monovalente di T_k, è il minimo elemento di $\{1, 2, \ldots, n\}$ non appartenente all'insieme precedente.[1] In particolare, x_1 è il minimo elemento di V che non compare nel nome $P(T)$, e possiamo determinare univocamente x_k a partire da $P(T)$ e da $x_1, \ldots, x_{k-1}$. □

Orig. 15

Problema 2B. Quanti alberi T esistono sull'insieme di vertici $\{1, 2, 3, 4, 5, 6, 7\}$ nei quali i vertici 2 e 3 abbiano grado 3, il vertice 5 abbia grado 2 e quindi tutti gli altri abbiano grado 1? Non limitatevi a disegnare figure: considerate i possibili codici di Prüfer di questi alberi.

[1] Nota redazionale: l'insieme scritto nell'originale termina con $y_{n-1} = n$ e quindi esclude anche n, che può essere monovalente. La caratterizzazione di *tutti* i vertici monovalenti richiede di fermarsi a y_{n-2}; l'individuazione del minimo x_k rimane valida.

Dimostrazione 2. Diamo un'altra dimostrazione, ancora mediante un algoritmo reversibile. Consideriamo una qualunque applicazione f da $\{2, 3, \dots, n-1\}$ a $\{1, 2, \dots, n\}$. Esistono n^{n-2} tali applicazioni. Costruiamo un digrafo D sui vertici da 1 a n, prendendo come spigoli $(i, f(i))$, per $i = 2, \dots, n-1$. La figura 2.2 mostra un esempio con $n = 21$.

Il digrafo D è costituito da due alberi «radicati» in 1 e in n e da un certo numero, diciamo k, di circuiti (poligoni orientati) ai quali sono attaccati degli alberi. (Gli alberi orientati in cui tutti gli spigoli puntano verso uno stesso vertice, detto *radice*, si chiamano *arborescenze*.) Disponiamo questi circuiti come nella figura 2.2: il vertice più a destra dell'i-esima componente, indicato con r_i, è il suo elemento minimo, mentre l_i è il vertice a sinistra. I circuiti sono ordinati dalla condizione $r_1 < r_2 < \cdots < r_k$. A D associamo l'albero ottenuto aggiungendo gli spigoli $\{1, l_1\}$, $\{r_1, l_2\}$, …, $\{r_{k-1}, l_k\}$, $\{r_k, n\}$ ed eliminando gli spigoli $\{r_i, l_i\}$, come nella figura 2.3.

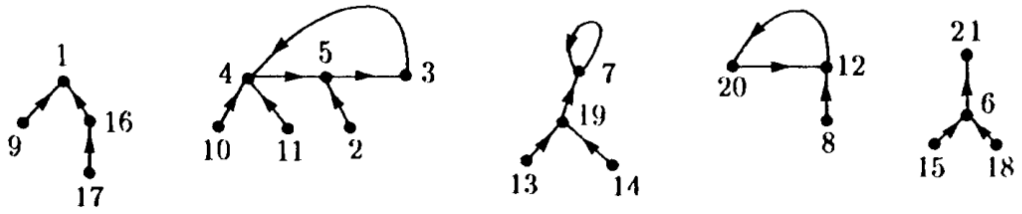


Figura 2.2

Dato l'albero della figura 2.3, consideriamo il cammino da 1 a n (= 21). Poniamo $r_0 := 1$. Definiamo r_1 come il numero minimo su questo cammino, escluso $r_0 = 1$, e in generale r_i come il numero minimo sul cammino da r_{i-1} a n. Si vede facilmente che in questo modo si ricostruisce la funzione f. □ Orig. 16

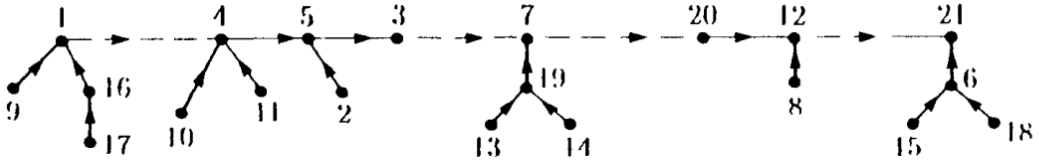


Figura 2.3

Generalizzazioni di questa dimostrazione si trovano in Eğecioğlu e Remmel (1986).

Problema 2C. Sia G un grafo orientato con vertici $x_1, \dots, x_n$ che ammetta un circuito euleriano orientato. Un'*arborescenza ricoprente* con radice x_i è un albero ricoprente T di G, con radice x_i, tale che per ogni $j \neq i$ esista in T un cammino orientato da x_j a x_i. Mostrate che il numero delle arborescenze ricoprenti di G con radice x_i non dipende da i. (È difficile: consultate i suggerimenti.)

Dimostrazione 3. Diamo ora una dimostrazione per conteggio, perché è utile aver visto questo metodo. Ricordiamo la definizione di *coefficiente multinomiale*. Siano $r_1, r_2, \dots, r_k$ interi non negativi di somma n. Allora $\binom{n}{r_1,\dots,r_k}$ è definito da

$$(x_1 + x_2 + \cdots + x_k)^n = \sum \binom{n}{r_1, \dots, r_k} x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}, \tag{2.1}$$

dove la somma è estesa a tutte le k-uple $(r_1, \dots, r_k)$ di somma n. Poiché $(x_1 + \cdots + x_k)^n = (x_1 + \cdots + x_k)^{n-1}(x_1 + \cdots + x_k)$, si ha

$$\binom{n}{r_1, \dots, r_k} = \sum_{i=1}^{k} \binom{n-1}{r_1, \dots, r_i - 1, \dots, r_k}. \tag{2.2}$$

Indichiamo con $t(n; d_1, d_2, \dots, d_n)$ il numero degli alberi etichettati con n vertici aventi gradi $d_1, d_2, \dots, d_n$. Questo numero è chiaramente 0 se uno dei d_i è 0. Il suo valore dipende soltanto dal multiinsieme dei numeri d_i, non dal loro ordine. Possiamo supporre, senza perdita di generalità, che $d_1 \geq d_2 \geq \cdots \geq d_n$,

cosicché $d_n = 1$. Consideriamo il vertice v_n corrispondente a d_n: esso è congiunto a un vertice v_i di grado $d_i \geq 2$, e ciascuno degli altri vertici è un possibile candidato. Pertanto Orig. 17

$$t(n; d_1, \ldots, d_n) = \sum_{i=1}^{n-1} t(n-1; d_1, \ldots, d_i - 1, \ldots, d_{n-1}). \tag{2.3}$$

È immediato verificare direttamente che

$$t(n; d_1, \ldots, d_n) = \binom{n-2}{d_1 - 1, \ldots, d_n - 1} \tag{2.4}$$

per $n = 3$. Poiché i numeri al primo e al secondo membro della (2.4) soddisfano la stessa relazione di ricorrenza, rispettivamente (2.3) e (2.2), per induzione la (2.4) vale per ogni n.

Nella (2.1) sostituiamo n con $n-2$, k con n, r_i con $d_i - 1$ e x_i con 1. Troviamo

$$n^{n-2} = \sum t(n; d_1, d_2, \ldots, d_n).$$

□

Confrontate la (2.4) con il problema 2B.

È facile costruire un albero ricoprente partendo da un vertice qualsiasi, prendendo gli spigoli che conducono ai vertici a distanza 1, poi uno spigolo per ciascun vertice a distanza 2, e così via. Sono possibili diverse altre costruzioni, per esempio partendo da G ed eliminando spigoli opportuni.

Un grafo privo di poligoni come sottografi si chiama *foresta*. Ogni componente $C_1, C_2, \ldots, C_k$ di una foresta G è un albero; quindi una foresta con n vertici e k componenti ha

$$(|V(C_1)| - 1) + (|V(C_2)| - 1) + \cdots + (|V(C_k)| - 1) = n - k$$

spigoli.

Un *grafo pesato* è un grafo G dotato di una funzione che associa a ogni spigolo e un numero reale $c(e)$, di solito non negativo, detto, secondo il contesto, *lunghezza* o *costo*. Qui useremo il termine «costo». Dato un grafo pesato connesso G, definiamo il costo di un albero ricoprente T di G come

$$c(T) := \sum_{e \in E(T)} c(e).$$

Il grafo può rappresentare una rete di città, dove $c(\{x, y\})$ è il costo di installazione di una linea telefonica fra le città x e y; è dunque chiaro che trovare un albero ricoprente di costo minimo in G è un problema di importanza pratica. Orig. 18

Il metodo seguente è spesso chiamato *algoritmo greedy*. In realtà è soltanto uno dei molti algoritmi che possono essere detti greedy: non si pianifica in anticipo, ma si prende ogni volta l'alternativa che sembra migliore, senza tornare indietro. È sorprendente che un procedimento così semplice produca effettivamente un albero ricoprente di costo minimo, ma lo dimostreremo nel teorema 2.2.

Diremo che un insieme S di spigoli di un grafo G è *indipendente* se il sottografo ricoprente con insieme degli spigoli S, indicato con $G : S$, è una foresta.

Algoritmo greedy. Sia G un grafo pesato connesso con n vertici. A ogni passo avremo un insieme $\{e_1, e_2, \ldots, e_i\}$ di i spigoli indipendenti (all'inizio $i = 0$), cosicché $G : \{e_1, e_2, \ldots, e_i\}$ ha $n - i$ componenti. Se $i < n - 1$, sia e_{i+1} uno spigolo con estremi in componenti diverse di $G : \{e_1, e_2, \ldots, e_i\}$ e di costo minimo fra quelli con questa proprietà. Ci fermiamo dopo aver scelto $n - 1$ spigoli.

Teorema 2.2. Scelti $e_1, \ldots, e_{n-1}$ come sopra, l'albero ricoprente $T_0 := G : \{e_1, \ldots, e_{n-1}\}$ soddisfa $c(T_0) \leq c(T)$ per ogni albero ricoprente T.

Dimostrazione. Sia $\{a_1, a_2, \ldots, a_{n-1}\}$ l'insieme degli spigoli di un albero T, numerati in modo che $c(a_1) \leq c(a_2) \leq \cdots \leq c(a_{n-1})$. Affermiamo qualcosa di molto più forte di $c(T_0) \leq c(T)$: precisamente, $c(e_i) \leq c(a_i)$ per ogni $i = 1, 2, \ldots, n-1$. Se non fosse così, per qualche k avremmo

$$c(e_k) > c(a_k) \geq c(a_{k-1}) \geq \cdots \geq c(a_1).$$

Poiché nessuno fra $a_1, a_2, \ldots, a_k$ è stato scelto al passo in cui è stato scelto e_k, ciascuno di questi k spigoli ha entrambi gli estremi nella stessa componente di $G : \{e_1, e_2, \ldots, e_{k-1}\}$.[2] Il numero di componenti di $G : \{a_1, a_2, \ldots, a_k\}$ è allora almeno il numero $n - k + 1$ di componenti di $G : \{e_1, e_2, \ldots, e_{k-1}\}$, in contraddizione con l'indipendenza di $\{a_1, a_2, \ldots, a_k\}$. □

Problema 2D. Ecco una variante dell'algoritmo greedy precedente. Sia x_1 un vertice qualsiasi di un grafo pesato connesso G con n vertici e sia T_1 il sottografo con il solo vertice x_1 e senza spigoli. Definito un albero T_k, con $k < n$, sia e_k uno spigolo di costo minimo fra quelli con un estremo in $V(T_k)$ e l'altro fuori da $V(T_k)$; sia T_{k+1} l'albero ottenuto aggiungendo a T_k quello spigolo e il suo altro estremo. Dimostrate che T_n è un albero ricoprente di costo minimo in G. Orig. 19

In molte situazioni pratiche è necessario esplorare un albero partendo da un vertice particolare. (Un albero con un vertice distinto, la *radice*, si chiama *albero radicato*.) Due metodi ben noti sono la *ricerca in profondità* e la *ricerca in ampiezza*. Spieghiamo questa terminologia mediante l'esempio della figura 2.4.

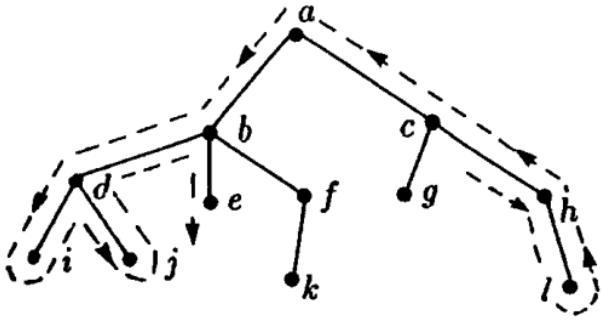


Figura 2.4

In una ricerca in profondità che parte da a, si considera essenzialmente l'albero come una recinzione e gli si cammina intorno tenendolo a sinistra, cioè seguendo la passeggiata $abdidjdbebfk \ldots lhca$. Numerando i vertici secondo l'ordine della ricerca, si ottiene $a = 1$, $b = 2$, $d = 3$, $i = 4$, …, $l = 12$. Questa descrizione si basa su un disegno planare dell'albero; si veda però quanto segue.

In una ricerca in ampiezza si procede come nella costruzione di un albero ricoprente descritta sopra. I vertici vengono allora numerati nell'ordine della figura 2.4, cioè in ordine alfabetico.

Queste idee si applicano più in generale all'esplorazione dei vertici di un grafo connesso.

Dato un grafo finito connesso G, possiamo ottenere una numerazione dei suoi vertici e un suo albero ricoprente T, detto *albero di ricerca in profondità*, come segue. Scegliamo un vertice v_0 e partiamo dall'albero T_0 con vertice v_0 e senza spigoli. Procediamo per induzione: scelti i vertici $v_0, v_1, v_2, \ldots, v_k$ e un albero T_k avente esattamente questi vertici e alcuni degli spigoli di G, sia ℓ il massimo indice $\le k$ tale che v_ℓ sia adiacente a un vertice non ancora in T_k. Un tale vertice esiste se T_k non è ancora ricoprente; altrimenti ci fermiamo e poniamo $T = T_k$. Chiamiamo v_{k+1} quel nuovo vertice e aggiungiamo a T_k sia esso sia lo spigolo $\{v_\ell, v_{k+1}\}$, ottenendo l'albero T_{k+1}. Consideriamo T radicato in v_0. Orig. 20

Diamo due proprietà degli alberi di ricerca in profondità e le usiamo per ottenere una semplice dimostrazione costruttiva di un teorema sugli orientamenti dei grafi.

Dato un vertice x di un albero radicato in v_0, gli *antenati* di x sono i vertici attraversati dall'unico cammino da x alla radice v_0. Il primo vertice diverso da x su questo cammino è il *padre* di x. Se x è un antenato di y, diciamo anche che y è un *discendente* di x. Consideriamo x sia discendente sia antenato di se stesso.

Proposizione 2.3. Se i vertici x e y sono adiacenti in G, allora uno dei due è discendente dell'altro in ogni albero di ricerca in profondità T di G.

Dimostrazione. Supponiamo che nella ricerca in profondità x riceva un indice minore di y, e scriviamo $x = v_k$.

Al passo in cui sono stati scelti $v_0, v_1, v_2, \ldots, v_k$, il massimo indice ℓ tale che v_ℓ sia adiacente a un vertice non ancora numerato è chiaramente $\ell = k$. Quindi v_{k+1} è congiunto a v_k, non a un v_i con $i < k$,

[2] Nota redazionale: «nessuno è stato scelto» va inteso qui come «nessuno è stato scelto al passo k»: alcuni degli a_i possono già appartenere alla foresta costruita. Anche in tal caso i loro estremi appartengono alla stessa componente, che è la proprietà usata nel seguito.

in T. Se $v_{k+1} = y$, abbiamo finito: y è discendente di v_k. Altrimenti, poiché v_k è ancora adiacente a un vertice non numerato, cioè y, la scelta di ℓ sarà k oppure $k+1$, e v_{k+2} sarà adiacente in T a v_k oppure a v_{k+1}. Se $v_{k+2} = y$, abbiamo finito: y è discendente di v_k.

Induttivamente, finché y rimane non numerato, $v_k, v_{k+1}, \ldots, v_{k+j}$ sono discendenti di v_k e la scelta successiva di ℓ sarà uno fra $k, k+1, \ldots, k+j$. Il nuovo vertice v_{k+j+1} sarà pertanto adiacente a uno fra $v_k, v_{k+1}, \ldots, v_{k+j}$, e quindi discendente di v_k. Poiché il grafo è finito, prima o poi questo nuovo vertice deve essere y. □

Un *istmo* di un grafo connesso G è uno spigolo la cui eliminazione rende il grafo sconnesso. (Alcuni autori lo chiamano *ponte*.)

Proposizione 2.4. Sia $\{x, y\}$ uno spigolo di T che non sia un istmo di G; supponiamo che x sia il padre di y. Allora esiste uno spigolo di G non appartenente a T che congiunge un discendente a di y a un antenato b di x. Orig. 21

Dimostrazione. Sia D l'insieme dei discendenti di y. Si ha $y \in D$ e $x \notin D$. Poiché G rimane connesso dopo l'eliminazione di $\{x, y\}$, esiste uno spigolo $\{a, b\} \neq \{x, y\}$ con un estremo $a \in D$ e l'altro $b \notin D$. Tale spigolo non appartiene certamente a T e, per la proposizione 2.3, b è un antenato di a: non può infatti esserne un discendente, perché allora sarebbe anche discendente di y, e quindi apparterrebbe a D. L'unico cammino in T da a a v_0 passa per y, antenato di a, e poi per x, padre di y. Ma b deve trovarsi su questo cammino, essendo antenato di a, e deve quindi essere anche antenato di x. □

Ogni grafo orientato ottenuto da un grafo non orientato G assegnando una direzione a ciascuno spigolo si chiama *orientamento* di G. Una passeggiata in un digrafo D si può dire *forte* se percorre ogni spigolo nel suo verso, cioè dalla coda alla testa; il digrafo D è *fortemente connesso* se, per ogni coppia di vertici x, y, esiste una passeggiata forte da x a y.

Teorema 2.5. Sia G un grafo finito connesso senza istmi. Allora G ammette un orientamento forte, cioè un orientamento che sia un digrafo fortemente connesso.

Dimostrazione. Costruiremo un digrafo D da G scegliendo una direzione per ogni spigolo. Troviamo un albero di ricerca in profondità T e una numerazione $v_0, v_1, \ldots$ dei vertici di G. Sia $\{v_i, v_j\}$ uno spigolo di G, con $i < j$. Se appartiene a T, lo orientiamo da v_i a v_j, cosicché (v_i, v_j) è uno spigolo di D. Se non appartiene a T, lo orientiamo da v_j a v_i, cosicché (v_j, v_i) è uno spigolo di D.

Resta da mostrare che D è fortemente connesso. Da v_0 esiste una passeggiata forte a ogni vertice x di G, usando soltanto spigoli di T; basterà quindi mostrare che da ogni vertice x possiamo trovare una passeggiata forte a v_0.

Dato un vertice v_k, $k > 0$, la proposizione 2.4 assicura che uno spigolo $\{a, b\}$ di G, non appartenente a T, congiunge un discendente a di v_k a un suo antenato proprio $b = v_i$.[3] Otteniamo una passeggiata forte in D da v_k a v_i aggiungendo lo spigolo orientato (a, v_i) a una passeggiata forte in T da v_k al suo discendente a. Naturalmente $i < k$, poiché v_i è un antenato proprio di v_k. Se $i = 0$, abbiamo finito. Altrimenti ripetiamo l'argomento per trovare una passeggiata forte da v_i a un v_j con $j < i$ e concateniamo le passeggiate, ottenendone una forte da v_k a v_j. Continuiamo così fino a raggiungere v_0. □ Orig. 22

Problema 2E. Un'*etichettatura graziosa* di un albero T su n vertici è un'applicazione $f : V(T) \to \{1, 2, \ldots, n\}$ tale che i numeri $|f(x) - f(y)|$, calcolati sugli spigoli $\{x, y\}$, siano tutti distinti. Mostrate che i grafi-cammino, cioè gli alberi con esattamente due vertici monovalenti, ammettono etichettature graziose. (Si congettura che tutti gli alberi le ammettano.)

Problema 2F. Supponete che un albero G abbia esattamente un vertice di grado i per $2 \leq i \leq m$ e che tutti gli altri vertici abbiano grado 1. Quanti vertici ha G?

Problema 2G. Sia G un grafo con esattamente un vertice di grado i per $2 \leq i \leq m$ e altri k vertici, tutti di grado 1. Dimostrate che $k \geq \lfloor (m+3)/2 \rfloor$. Date una costruzione di un tale grafo.

Problema 2H. Considerate alberi radicati trivalenti etichettati T con $2n$ vertici, contando anche la radice etichettata $2n$; si veda la figura 14.3. Le etichette sono scelte in modo che il procedimento che conduce a $P(T)$ abbia $1, 2, 3, \ldots, 2n-1$ come prima riga. Quanti codici $P(T)$ sono possibili?

[3] Nota redazionale: in questo punto l'originale presenta le lettere x_k e y senza coerenza con la notazione del paragrafo. Si esplicita qui l'applicazione della proposizione 2.4 allo spigolo che congiunge v_k al suo padre.

Note

A. Cayley (1821–1895), professore a Cambridge dal 1863 fino alla morte, fu uno dei grandi matematici del XIX secolo. Il suo lavoro comprende importanti contributi alla teoria delle funzioni ellittiche, alla geometria analitica e all'algebra, per esempio alla teoria degli invarianti. Il suo articolo sugli alberi apparve nel 1889, ma non conteneva ciò che oggi considereremmo una dimostrazione. Fra le molte dimostrazioni, cinque delle quali sono trattate in questo libro, quella di Prüfer è la più nota.

H. Prüfer (1896–1934) fu uno dei numerosi allievi di I. Schur. Fu professore a Münster.

Riferimenti bibliografici

A. Cayley (1889)
A theorem on trees, *Quart. J. Pure and App. Math.* **23**, 376–378.

Orig. 23

Ö. Eğecioğlu e J. B. Remmel (1986)
Bijections for Cayley trees, spanning trees, and their q-analogues, *J. Combinatorial Theory (A)* **42**, 15–30.

H. Prüfer (1918)
Neuer Beweis eines Satzes über Permutationen, *Archiv der Math. und Phys.* (3) **27**, 142–144.

Capitolo 3

Colorazioni dei grafi e teorema di Ramsey

Orig. 24

Consideriamo dapprima alcuni cosiddetti problemi di colorazione dei grafi. Una *colorazione propria* di un grafo G è una funzione dai vertici a un insieme C di «colori», per esempio $C = \{1, 2, 3, 4\}$, tale che gli estremi di ogni spigolo abbiano colori distinti. (Un grafo con un cappio non ammette quindi colorazioni proprie.) Se $|C| = k$, diciamo che G è *k-colorato*.

Il *numero cromatico* $\chi(G)$ di un grafo G è il numero minimo di colori per il quale esiste una colorazione propria.

Se $\chi(G) = 2$, oppure $\chi(G) = 1$, il che accade se e solo se G non ha spigoli, allora G si dice *bipartito*. Un grafo senza poligoni di lunghezza dispari, o equivalentemente senza cammini chiusi di lunghezza dispari, è bipartito, come il lettore dovrebbe verificare.

Il celebre «teorema dei quattro colori» (K. Appel e W. Haken, 1977) afferma che, se G è planare, allora $\chi(G) \leq 4$.

Chiaramente $\chi(K_n) = n$. Se k è dispari, $\chi(P_k) = 3$. Nel teorema seguente mostriamo che, tranne questi esempi, il numero cromatico è al più uguale al grado massimo (R. L. Brooks, 1941).

Teorema 3.1. Sia $d \geq 3$ e sia G un grafo in cui tutti i vertici abbiano grado $\leq d$ e tale che K_{d+1} non sia un sottografo di G. Allora $\chi(G) \leq d$.[1]

Dimostrazione 1. Come per molti teoremi di analisi combinatoria, si può procedere supponendo falso il risultato, considerando un controesempio minimo, qui un grafo con il minor numero possibile di vertici, e arrivando a una contraddizione. Useremo la tecnica della *ricolorazione*: è possibile cambiare i colori di certi vertici per passare da una colorazione propria a un'altra. Per esempio, sia S un sottoinsieme dell'insieme C dei colori. In una qualsiasi componente connessa del sottografo indotto dai vertici con colori in S, permutiamo arbitrariamente i colori, senza cambiare quelli dei vertici colorati con elementi di $C \setminus S$. Otteniamo chiaramente ancora una colorazione propria.

Orig. 25

Sia dunque G un controesempio con il minimo numero di vertici. Sia $x \in G$ e sia $\Gamma(x) = \{x_1, \ldots, x_l\}$, con $l \leq d$. Per la minimalità di G, il grafo H ottenuto eliminando x e gli spigoli a esso incidenti ammette una d-colorazione, diciamo con i colori $1, 2, \ldots, d$. Se uno di questi colori non compare su $\Gamma(x)$, possiamo assegnarlo a x e ottenere una d-colorazione di G. Ne segue che $l = d$ e che ogni d-colorazione di H deve usare tutti i colori su $\Gamma(x)$. Supponiamo che x_i abbia colore i, per $i = 1, 2, \ldots, d$.

Consideriamo ora x_i e x_j e il sottografo H_{ij} di H indotto dai colori i e j. Se x_i e x_j appartenessero a componenti connesse diverse di H_{ij}, potremmo scambiare i colori in una di esse: allora x_i e x_j avrebbero lo stesso colore, il che è impossibile. Appartengono quindi alla stessa componente, diciamo C_{ij}, di H_{ij}. Mostriamo che questa componente è il grafo di un cammino semplice da x_i a x_j, con colori alternati i e j. Se due vicini di x_i in H avessero colore j, i vicini di x_i in H avrebbero al più $d - 2$ colori distinti. Potremmo allora ricolorare x_i, il che è impossibile. Sia y il primo vertice di grado almeno 3 lungo un cammino da x_i a x_j in C_{ij}. I vicini di y in H hanno al più $d - 2$ colori, perciò possiamo ricolorare y con

[1] Nota redazionale: il teorema di colorazione è inteso per grafi semplici; in particolare i cappi devono essere esclusi, come mostra la definizione di colorazione propria.

un colore fuori da $\{i, j\}$; allora x_i e x_j non sono più connessi in H_{ij}, cosa che sappiamo impossibile. Un tale y non esiste, e C_{ij} è dunque un cammino.

Supponiamo che un vertice $z \neq x_i$ appartenga sia a C_{ij} sia a C_{ik}. Allora z ha due vicini di colore j e due di colore k. Ancora una volta i vicini di z in H hanno al più $d-2$ colori, e possiamo ricolorare z con un colore fuori da $\{i, j, k\}$, ottenendo un'altra contraddizione. Quindi $C_{ij} \cap C_{ik} = \{x_i\}$.

L'ipotesi $K_{d+1} \not\subseteq G$ implica che in $\Gamma(x)$ vi siano due vertici, diciamo x_1 e x_2, non congiunti da uno spigolo. Siamo nella situazione della figura 3.1. Il vertice a è il vicino di x_1 di colore 2 su C_{12}. Ricoloriamo H scambiando i colori 1 e 3 sul sottografo C_{13}. Per la nuova colorazione abbiamo nuovi cammini, che indichiamo con C'_{ij}. Chiaramente $a \in C'_{23}$, poiché x_1 ora ha colore 3. Tuttavia su C_{12} nessun punto tranne x_1 ha cambiato colore, quindi $a \in C'_{12}$. Ne segue $C'_{12} \cap C'_{23} \neq \{x_2\}$, contro quanto dimostrato. La contraddizione mostra che l'ipotesi dell'esistenza di un controesempio minimo è falsa. □

Orig. 26

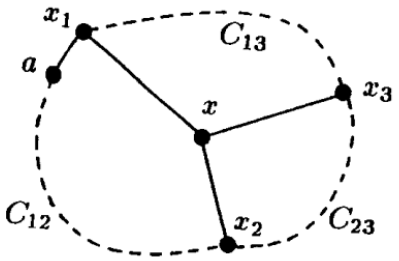


Figura 3.1

In preparazione a una seconda dimostrazione del teorema di Brooks, il lettore dovrebbe risolvere il problema seguente senza applicare il teorema.

Problema 3A. Fissate un intero $d \geq 3$. Sia H un grafo semplice con tutti i gradi $\leq d$, non d-colorabile e minimo, cioè con il minor numero di vertici, fra i grafi con queste proprietà. (Affermiamo che H è completo su $d+1$ vertici, ma ancora non lo sappiamo.) (i) Mostrate che H è *non separabile*: ogni grafo ottenuto da H eliminando un vertice è connesso. (ii) Mostrate poi che, se $V(H)$ è partizionato in insiemi X e Y, con $|Y| \geq 3$, esistono almeno tre vertici $a, b, c \in Y$ ciascuno adiacente ad almeno un vertice di X.[2]

Dimostrazione 2. Siano d e H come nel problema 3A. Se H non è completo, esistono vertici x_1, x_{n-1}, x_n tali che x_1 sia adiacente a x_{n-1} e a x_n, mentre questi ultimi non siano adiacenti fra loro. Vogliamo numerare gli altri $n-3$ vertici in modo che la successione

$$x_1, x_2, \ldots, x_{n-1}, x_n$$

abbia la proprietà che ogni x_k, $k \geq 2$, sia adiacente ad almeno un vertice x_i che lo precede, cioè con $i < k$. È semplice: scelti $x_1, x_2, \ldots, x_k$, con $k < n-2$, scegliamo come x_{k+1} un vertice qualsiasi diverso da x_{n-1} e x_n, adiacente a uno fra $x_1, x_2, \ldots, x_k$; poiché esistono almeno tre vertici di questo tipo, la scelta è sempre possibile.

Orig. 27

Ora coloriamo i vertici con d colori partendo dalla fine della successione. Assegniamo a x_{n-1} e a x_n lo stesso colore. Dopo aver colorato i vertici $x_{k+1}, \ldots, x_{n-1}, x_n$, con $k \geq 2$, rimane un colore disponibile per x_k, perché esso è adiacente ad al più $d-1$ vertici già colorati. Infine rimane un colore disponibile per x_1, perché due dei suoi vicini hanno ricevuto lo stesso colore. □

Consideriamo ora un problema di colorazione di natura completamente diversa, che introduce un teorema molto importante della combinatoria: il teorema di Ramsey. Prima di proseguire, il lettore dovrebbe provare a risolvere il problema seguente.

Problema 3B. Colorate gli spigoli di K_7 di rosso e blu. Mostrate che vi sono almeno quattro sottografi K_3 con tutti e tre gli spigoli dello stesso colore, cioè *triangoli monocromatici*. Mostrate anche che l'uguaglianza è possibile.

L'esempio sempre usato per introdurre l'argomento è K_6 con gli spigoli colorati di rosso o blu. Mostriamo che esiste almeno un triangolo monocromatico. Sia a un vertice qualsiasi. Poiché ha grado 5,

[2] Nota redazionale: in (ii) si sottintende $X \neq \varnothing$; per $X = \varnothing$ l'affermazione non sarebbe vera.

è incidente con almeno tre spigoli dello stesso colore, diciamo rossi, verso i vertici b, c, d. Se uno degli spigoli fra questi tre vertici è rosso, abbiamo un triangolo rosso; altrimenti essi formano un triangolo blu.

L'idea della dimostrazione è la stessa che si usa nella situazione più difficile del teorema di Ramsey. Tuttavia essa dimostra meno del seguente argomento di conteggio.

Teorema 3.2. Se gli spigoli di K_n sono colorati di rosso o blu, r_i, per $i = 1, 2, \ldots, n$, è il numero di spigoli rossi aventi il vertice i come estremo e Δ è il numero di triangoli monocromatici, allora

$$\Delta = \binom{n}{3} - \frac{1}{2}\sum_{i=1}^{n} r_i(n-1-r_i). \tag{3.1}$$

DIMOSTRAZIONE. Ogni triangolo non monocromatico in K_n ha esattamente due vertici nei quali si incontrano uno spigolo rosso e uno blu. Al vertice i, una coppia di tali spigoli può essere scelta in $r_i(n-1-r_i)$ modi. La somma nella (3.1) conta quindi due volte i triangoli bicromatici. □ Orig. 28

Corollario.

$$\Delta \geq \binom{n}{3} - \left\lfloor \frac{n}{2}\left\lfloor \left(\frac{n-1}{2}\right)^2 \right\rfloor \right\rfloor. \tag{3.2}$$

DIMOSTRAZIONE. Dalla (3.1) vediamo che Δ è minimo se $r_i = n-1-r_i$ per ogni i quando n è dispari, oppure se $r_i = n/2$ o $r_i = n/2-1$ per ogni i quando n è pari. Poiché Δ è intero, la prima situazione non può sempre verificarsi. È facile mostrare che la (3.2) non può essere migliorata. □

Questo argomento mostra che una colorazione rosso-blu di K_6 deve sempre avere almeno due triangoli monocromatici.

Passiamo ora al teorema di Ramsey (Ramsey, 1930).

Teorema 3.3. Siano assegnati $r \geq 1$ e $q_i \geq r$, per $i = 1, 2, \ldots, s$. Esiste un minimo intero positivo $N(q_1, q_2, \ldots, q_s; r)$ con la seguente proprietà. Sia S un insieme di n elementi e si suddividano tutti i suoi $\binom{n}{r}$ sottoinsiemi di r elementi in s famiglie disgiunte $T_1, \ldots, T_s$, dette «colori». Se $n \geq N(q_1, q_2, \ldots, q_s; r)$, esistono un indice i, con $1 \leq i \leq s$, e un sottoinsieme di S di q_i elementi i cui sottoinsiemi di r elementi appartengono tutti a T_i.

(Il lettore dovrebbe confrontare questo enunciato con l'esempio introduttivo e mostrare che $N(3, 3; 2) = 6$.)

DIMOSTRAZIONE. Diamo la dimostrazione soltanto per $s = 2$. Il caso generale richiede soltanto una gestione un po' più laboriosa degli indici.

(a) Per $r = 1$ il teorema è ovvio e $N(p, q; 1) = p + q - 1$.

(b) Per ogni r e $p \geq r$ è anche evidente che $N(p, r; r) = p$ e, analogamente, $N(r, q; r) = q$ per $q \geq r$.

(c) Procediamo per induzione su r, supponendo dunque vero il teorema per $r-1$. Usiamo ora l'induzione su $p+q$, con (b) come base. Possiamo quindi definire $p_1 = N(p-1, q; r)$ e $q_1 = N(p, q-1; r)$. Sia S un insieme di n elementi, con $n \geq 1 + N(p_1, q_1; r-1)$. Coloriamo i sottoinsiemi di r elementi di S con due colori, diciamo rosso e blu. Come nella dimostrazione per K_6, scegliamo un elemento arbitrario $a \in S$. Definiamo una colorazione dei sottoinsiemi di $r-1$ elementi di $S' := S \setminus \{a\}$, assegnando a $X \subseteq S'$ lo stesso colore di $X \cup \{a\}$. Per induzione, S' contiene o un sottoinsieme A di cardinalità p_1 con tutti i suoi sottoinsiemi di $r-1$ elementi rossi, oppure un sottoinsieme B di cardinalità q_1 con tutti i suoi sottoinsiemi di $r-1$ elementi blu. Senza perdita di generalità supponiamo che si verifichi il primo caso. Poiché A ha $N(p-1, q; r)$ elementi, vi sono due possibilità. La prima è che A contenga un sottoinsieme di q elementi con tutti i suoi sottoinsiemi di r elementi blu, e allora abbiamo finito. L'altra è che A contenga un sottoinsieme A' di $p-1$ elementi con tutti i suoi sottoinsiemi di r elementi rossi. Anche $A' \cup \{a\}$ ha questa proprietà, perché $A' \subseteq A$. Il teorema è dimostrato; inoltre abbiamo mostrato che Orig. 29

$$N(p, q; r) \leq N\big(N(p-1, q; r), N(p, q-1; r); r-1\big) + 1. \tag{3.3}$$

□

Un caso particolare della (3.3) si ottiene tornando alla colorazione degli spigoli, $r = 2$, di un grafo con due colori. Usando (a) della dimostrazione, troviamo

$$N(p, q; 2) \leq N(p-1, q; 2) + N(p, q-1; 2). \tag{3.4}$$

Problema 3C. Mostrate che nella (3.4) non può valere l'uguaglianza se entrambi i termini del secondo membro sono pari.

Teorema 3.4.

$$N(p,q;2) \le \binom{p+q-2}{p-1}.$$

DIMOSTRAZIONE. Poiché $N(p,2;2) = p$, il risultato segue dalla (3.4), dato che i coefficienti binomiali soddisfano la stessa relazione con l'uguaglianza. □

Vediamo che cosa sappiamo ora di $N(p,q;2)$. Per il problema 3C, $N(3,4;2) \le 9$. Per dimostrare l'uguaglianza dobbiamo colorare K_8 senza triangoli rossi né K_4 blu. Procediamo così: numeriamo i vertici con gli elementi di $\mathbb{Z}_8$ e coloriamo lo spigolo $\{i,j\}$ di rosso se e solo se $i-j \equiv \pm 3$ oppure $i-j \equiv 4 \pmod 8$. Si verifica facilmente che questa colorazione ha le proprietà richieste.

Problema 3D. Usate lo stesso metodo per mostrare che $N(4,4;2) = 18$ e $N(3,5;2) = 14$.

Con un lavoro molto maggiore è stato dimostrato che

$$N(3,6;2) = 18, \quad N(3,7;2) = 23, \quad N(3,8;2) = 28, \quad N(3,9;2) = 36,$$

$$N(4,5;2) = 25.$$

Orig. 30

Non sono noti altri valori di $N(p,q;2)$.

Un problema interessante di quest'area, nel quale per trent'anni non si sono avuti praticamente progressi, è il comportamento asintotico di $N(p,p;2)$. Dal teorema 3.4 sappiamo che

$$N(p,p;2) \le \binom{2p-2}{p-1} \le 2^{2p-2}. \tag{3.5}$$

Mostriamo ora che $N(p,p;2)$ cresce esponenzialmente, mediante un metodo usato molto spesso in combinatoria. Lo si chiama spesso «probabilistico», perché stima la probabilità che una colorazione casuale contenga un K_p monocromatico. Consideriamo un K_n. Esistono $2^{\binom{n}{2}}$ modi diversi di colorarne gli spigoli di rosso o blu. Fissiamo un sottografo K_p: vi sono $2^{\binom{n}{2}-\binom{p}{2}+1}$ colorazioni nelle quali quel K_p è monocromatico. Il numero delle colorazioni nelle quali almeno un K_p è monocromatico è al più $\binom{n}{p}$ volte questo numero, perché potremmo contare alcune colorazioni più di una volta. Se il risultato è minore del numero totale delle colorazioni, esistono colorazioni senza K_p monocromatici. Usando $\binom{n}{p} < n^p/p!$, troviamo che una tale colorazione esiste certamente se $n < 2^{p/2}$, salvo il caso $p = 2$. Questo dimostra il teorema seguente.

Teorema 3.5. $N(p,p;2) \ge 2^{p/2}$.

Dalla (3.5) e dal teorema 3.5 sappiamo che

$$\sqrt{2} \le \sqrt[p]{N(p,p;2)} \le 4 \qquad (p \ge 2).$$

Sarebbe molto bello riuscire a dimostrare che questa radice p-esima ha un limite per $p \to \infty$.

Per migliorare considerevolmente il teorema 3.5, discutiamo un metodo probabilistico utile in molte parti della combinatoria. Consideriamo eventi $A_1, A_2, \ldots, A_n$ in uno spazio di probabilità. Indichiamo con $\Pr[A_i]$ la probabilità di A_i e, come al solito, con $\overline{A_i}$ il suo complementare, ossia il non verificarsi di A_i. Ci interessano applicazioni nelle quali gli A_i rappresentano situazioni indesiderate e vogliamo affermare che vi è probabilità positiva che non si verifichi *nessuno* degli eventi A_i. In alcuni semplici problemi di conteggio si può usare

Orig. 31

$$\sum_{i=1}^{n} \Pr[A_i] < 1 \quad \Longrightarrow \quad \bigcap_i \overline{A_i} \neq \varnothing.$$

Si confronti il problema 5F.[3] In generale, però, la dipendenza fra gli eventi indesiderati comporta conteggi multipli, producendo una somma molto maggiore di 1. Naturalmente, se gli eventi A_i sono indipendenti, basta che ciascuno abbia probabilità minore di 1 perché il non verificarsi di tutti abbia probabilità positiva.

[3] Nota di traduzione: il rinvio originale a 5E è un refuso; l'applicazione probabilistica pertinente è il problema 5F.

Il *crivello di Lovász* tratta situazioni in cui vi sono alcune dipendenze, ma contemporaneamente molte combinazioni di eventi palesemente indipendenti.

Definiamo quello che chiameremo un *grafo di dipendenza* per gli eventi $A_1, \dots, A_n$: è un grafo G sull'insieme di indici $\{1, 2, \dots, n\}$ tale che, per ogni i, l'evento A_i sia indipendente da ogni sottofamiglia di $\{A_j : \{i, j\} \notin E(G)\}$. Notate che richiediamo molto più della sola indipendenza di A_i da ciascuno degli A_j di tale famiglia.[4]

Teorema 3.6. Sia G un grafo di dipendenza per gli eventi $A_1, \dots, A_n$. Supponiamo che $\Pr[A_i] \le p$, per $i = 1, \dots, n$, e che ogni vertice di G abbia grado $\le d$. Se $4dp < 1$, allora $\bigcap_i \overline{A_i} \neq \varnothing$.[5]

Dimostrazione. Mostriamo dapprima che, per ogni sottoinsieme $\{i_1, i_2, \dots, i_m\}$ dell'insieme degli indici,

$$\Pr[A_{i_1} \mid \overline{A_{i_2}} \cdots \overline{A_{i_m}}] \le \frac{1}{2d}. \tag{3.6}$$

Il caso $m = 1$ è immediato e, per $m = 2$, abbiamo

$$\Pr[A_1 \mid \overline{A_2}] \le \frac{p_1}{1 - p_2} \le \frac{1}{4d - 1} < \frac{1}{2d},$$

dove, per comodità, abbiamo preso $i_j = j$ e posto $p_i := \Pr[A_i]$. Procediamo per induzione.

Supponiamo che in G il vertice 1 sia adiacente a $2, 3, \dots, q$ e non adiacente a $q + 1, \dots, m$. Abbiamo

$$\Pr[A_1 \mid \overline{A_2} \cdots \overline{A_m}] = \frac{\Pr[A_1 \overline{A_2} \cdots \overline{A_q} \mid \overline{A_{q+1}} \cdots \overline{A_m}]}{\Pr[\overline{A_2} \cdots \overline{A_q} \mid \overline{A_{q+1}} \cdots \overline{A_m}]}.$$

Per definizione di G, il numeratore è al più

Orig. 32

$$\Pr[A_1 \mid \overline{A_{q+1}} \cdots \overline{A_m}] = \Pr[A_1] \le \frac{1}{4d}.$$

Dall'ipotesi induttiva, il denominatore è almeno

$$1 - \sum_{i=2}^{q} \Pr[A_i \mid \overline{A_{q+1}} \cdots \overline{A_m}] \ge 1 - \frac{q-1}{2d} \ge \frac{1}{2}.$$

[6] Questo dimostra la (3.6). Ora

$$\Pr[\overline{A_1} \cdots \overline{A_n}] = \prod_{i=1}^{n} \Pr[\overline{A_i} \mid \overline{A_1} \cdots \overline{A_{i-1}}] \ge \left(1 - \frac{1}{2d}\right)^n > 0,$$

dove abbiamo usato la (3.6) per ciascun fattore. □

Applichiamo questo metodo per ottenere un limite inferiore per $N(p, p; 2)$.

Teorema 3.7. $N(p, p; 2) \ge c\, p\, 2^{p/2}$, dove c è una costante.

Dimostrazione. Consideriamo K_n e coloriamone casualmente gli spigoli con due colori. Per ogni insieme S di k vertici, sia A_S l'evento che il sottografo su S sia monocromatico. Vogliamo affermare che fra le colorazioni casuali ve n'è almeno una senza sottografi monocromatici su k vertici. Definiamo un grafo di dipendenza rendendo S e T adiacenti se e solo se $|S \cap T| \ge 2$, cioè se i sottografi su S e T hanno uno spigolo in comune. Il grado d di G è chiaramente al più $\binom{k}{2}\binom{n}{k-2}$. Tutti gli eventi A_S hanno probabilità $2^{1-\binom{k}{2}}$. Dal teorema 3.6, dalla formula di Stirling e da qualche manipolazione si ottiene il risultato e, volendo, una stima di c. □

Abbiamo dato alcuni esempi di un'area della combinatoria nota come *teoria di Ramsey*. Citiamo ancora un esempio, un teorema dovuto a B. L. van der Waerden (1927): esiste un numero $N(r)$ tale che, se $N \ge N(r)$ e gli interi da 1 a N sono colorati di rosso o blu, l'insieme contiene una progressione aritmetica monocromatica di lunghezza r. Per una dimostrazione breve, ma non facile, si veda Graham e Rothschild (1974). Un riferimento generale per quest'area è il libro *Ramsey Theory* di R. L. Graham,

Orig. 33

[4] Nota redazionale: nella famiglia si intende $j \neq i$; l'indipendenza richiesta è dalla famiglia congiuntamente, non soltanto a coppie.

[5] Nota redazionale: la formulazione e la dimostrazione usano $d \ge 1$. Se $d = 0$, gli eventi sono indipendenti e occorre inoltre $p < 1$; la sola condizione $4dp < 1$ non esclude un evento certo.

[6] Nota redazionale: nella somma l'originale stampa A_1 al posto di A_i; si corregge il refuso nell'indice.

B. L. Rothschild e J. L. Spencer (1980).

Un'interessante applicazione del teorema di Ramsey è il seguente teorema di Erdős e Szekeres (1935).

Teorema 3.8. Per ogni n esiste un intero $N(n)$ tale che ogni insieme di $N \geq N(n)$ punti del piano, senza tre punti allineati, contenga un sottoinsieme di n punti che formano un n-gono convesso.

DIMOSTRAZIONE. (i) Osserviamo dapprima che n punti, nessuna terna dei quali è allineata, formano un n-gono convesso se e solo se ogni quadrilatero formato da quattro di essi è convesso.

(ii) Affermiamo che basta porre $N(n) = N(n, n; 3)$. Sia S un insieme di $N(n)$ punti. Numeriamoli e coloriamo i triangoli di rosso o blu secondo che il percorso dal numero minore a quello maggiore, passando per quello intermedio, sia orario o antiorario. Esiste un sottoinsieme di n punti i cui triangoli hanno tutti lo stesso colore, diciamo rosso. Mostriamo che tale insieme non può contenere la configurazione della figura 3.2.

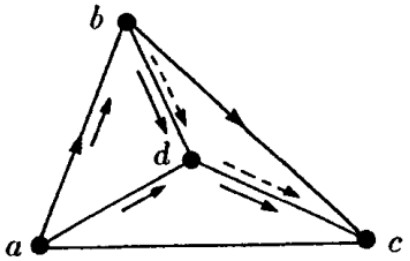


Figura 3.2

Senza perdita di generalità, $a < b < c$. Dal triangolo adc segue $a < d < c$. Dal triangolo abd segue allora $a < b < d$. Ma il triangolo bcd è quindi blu: contraddizione. Tutti i quadrilateri formati dai punti del sottoinsieme sono dunque convessi e, per (i), abbiamo finito. □

Problema 3E. Un *torneo* su n vertici è un orientamento di K_n. Un *torneo transitivo* è un torneo i cui vertici possono essere numerati in modo che (i, j) sia uno spigolo se e solo se $i < j$.

(a) Mostrate che, se $k \leq \log_2 n$, ogni torneo su n vertici contiene un sottotorneo transitivo su k vertici.

(b) Mostrate che, se $k > 1 + 2\log_2 n$, esiste un torneo su n vertici privo di sottotornei transitivi su k vertici.

Orig. 34

Problema 3F. Dimostrate che per ogni $r \in \mathbb{N}$ esiste un minimo numero $N(r)$ con la seguente proprietà: se $n \geq N(r)$ e gli interi di $\{1, 2, \ldots, n\}$ sono colorati con r colori, esistono tre elementi x, y, z, non necessariamente distinti, dello stesso colore e tali che $x+y = z$. (Risultato dovuto a I. Schur.) Determinate $N(2)$. Mostrate con un argomento elementare che $N(3) > 13$.

Problema 3G. Sia dato m. Mostrate che, se n è sufficientemente grande, ogni matrice $(0, 1)$ di ordine n ha una sottomatrice principale di ordine m nella quale gli elementi sotto la diagonale siano tutti uguali e quelli sopra la diagonale siano tutti uguali.

Problema 3H. Mostrate che, se gli spigoli di K_{17} sono colorati con tre colori, deve esistere un triangolo monocromatico.

Problema 3I. Sia $\{1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ il gruppo moltiplicativo di $\mathbb{F}_{16}$. Numeriamo i vertici di K_{16} con gli elementi di $\mathbb{F}_{16}$. Coloriamo gli spigoli con tre colori, assegnando a $\{i, j\}$ un colore che dipenda soltanto da ν, dove $i - j = \alpha^\nu$. Fatelo in modo che non vi siano triangoli monocromatici. (Nella notazione del teorema 3.3, questo problema e il precedente mostrano che $N(3, 3, 3; 2) = 17$.)

Problema 3J. Gli spigoli di K_n sono colorati di rosso e blu in modo che ogni spigolo rosso appartenga ad al più un triangolo rosso. Mostrate che esiste un sottografo K_k, con $k \geq \lfloor\sqrt{2n}\rfloor$, privo di triangoli rossi.

Problema 3K. Sia G un grafo che soddisfa le condizioni del teorema 3.1. Mostrate che eliminando al più n/d spigoli si può ottenere un sottografo G' di numero cromatico $\leq d - 1$.

Note

La congettura dei quattro colori era considerata uno dei più celebri problemi aperti della combinatoria fino al 1976. La soluzione di Appel e Haken ha suscitato molto dibattito perché la dimostrazione dipende da un'estesa analisi al calcolatore di numerosi casi. La validità dell'argomento dipende dalla fiducia nei calcolatori e nei programmi. (Si veda il capitolo 34 per due dimostrazioni del teorema dei cinque colori.)[7]

Il teorema di Brooks, teorema 3.1, scoperto quando egli era studente a Cambridge, è un esempio tipico degli argomenti ingegnosi spesso necessari in quella parte della teoria dei grafi in cui i metodi algebrici non si applicano. Orig. 35

F. P. Ramsey (1902–1928) morì troppo giovane per produrre i risultati che probabilmente avrebbe ottenuto.[8] Si interessava alle procedure di decisione per i sistemi logici e, curiosamente, questo lo condusse al teorema dal quale nacque la cosiddetta teoria di Ramsey.

Il teorema 3.5 è dovuto a P. Erdős (1947). Per altri metodi probabilistici si veda Erdős e Spencer (1974).

Valori e stime dei numeri $N(p, q; 2)$ si trovano in Radziszowski (1999). Il valore di $N(3, 9; 2)$ è dovuto a Grinstead e Roberts (1982).

La dimostrazione del teorema 3.6 non è quella originale di Erdős e Szekeres che di solito si trova nei libri.[9] Questa dimostrazione fu trovata durante un esame da uno studente di Haifa, M. Tarsy! Aveva perso la lezione nella quale era stata presentata la dimostrazione. Si veda Lewin (1976). Una dimostrazione di analogo spirito fu data da Johnson (1986).

Riferimenti bibliografici

K. Appel e W. Haken (1977)
Every planar map is four-colorable, *Illinois J. Math.* **21**, 429–567.

R. L. Brooks (1941)
On colouring the nodes of a network, *Cambridge Philos. Soc.* **37**, 194–197.

P. Erdős (1947)
Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53**, 292–294.

P. Erdős e J. L. Spencer (1974)
Probabilistic Methods in Combinatorics, Academic Press.

P. Erdős e G. Szekeres (1935)
A combinatorial problem in geometry, *Compositio Math.* **2**, 463–470.

R. L. Graham e B. L. Rothschild (1974)
A short proof of van der Waerden's theorem on arithmetic progressions, *Proc. Amer. Math. Soc.* **42**, 385–386.

R. L. Graham, B. L. Rothschild e J. L. Spencer (1980)
Ramsey Theory, Wiley.

C. M. Grinstead e S. M. Roberts (1982)
On the Ramsey numbers $R(3, 8)$ and $R(3, 9)$, *J. Combinatorial Theory (B)* **33**, 27–51.

S. Johnson (1986)
A new proof of the Erdős–Szekeres convex k-gon result, *J. Combinatorial Theory (A)* **42**, 318–319.

Orig. 36

M. Lewin (1976)
A new proof of a theorem of Erdős and Szekeres, *The Math. Gazette* **60**, 136–138, 298.

[7] Nota redazionale: il rinvio al capitolo 34 è rimasto dalla prima edizione; nella seconda edizione il teorema dei cinque colori è trattato nel capitolo 33.

[8] Nota redazionale: le date riportate nell'originale sono errate: Ramsey visse dal 1903 al 1930; si veda la voce Frank Ramsey, MacTutor, Università di St Andrews.

[9] Nota redazionale: il riferimento corretto è al teorema 3.8, sul poligono convesso, non al teorema 3.6.

S. P. Radziszowski (1999)
Small Ramsey Numbers, *The Electronic Journal of Combinatorics* **1**, DS 1.

F. P. Ramsey (1930)
On a problem of formal logic, *Proc. London Math. Soc.* (2) **30**, 264–286.

B. L. van der Waerden (1927)
Beweis einer Baudetschen Vermutung, *Nieuw Archief voor Wiskunde* **15**, 212–216.

Capitolo 4

Teorema di Turán e grafi estremali

Per introdurre l'argomento, chiediamoci quanti spigoli debba avere un grafo semplice perché sia garantita la presenza di un triangolo. Poiché $K_{m,m}$ e $K_{m,m+1}$ non contengono triangoli, vediamo che, se il grafo ha n vertici, $\lfloor n^2/4 \rfloor$ spigoli non bastano. Affermiamo che, se gli spigoli sono di più, il grafo contiene un triangolo (W. Mantel, 1907). La dimostrazione seguente è sorprendente. Sia G un grafo con n vertici, numerati da 1 a n, privo di triangoli. Attribuiamo al vertice i un peso $z_i \geq 0$, con $\sum z_i = 1$, e cerchiamo di massimizzare $S := \sum z_i z_j$, dove la somma è estesa a tutti gli spigoli $\{i, j\}$. Supponiamo che i vertici k e l non siano congiunti. Siano x e y i pesi totali dei vicini rispettivamente di k e di l, con $x \geq y$. Poiché Orig. 37

$$(z_k + \varepsilon)x + (z_l - \varepsilon)y \geq z_k x + z_l y,$$

il valore di S non diminuisce se trasferiamo parte del peso del vertice l al vertice k. Ne segue che S è massimo quando tutto il peso è concentrato su un sottografo completo di G, cioè su un solo spigolo! Pertanto $S \leq 1/4$. D'altra parte, prendendo tutti gli z_i uguali a n^{-1} si ottiene $S = n^{-2}|E|$. Quindi $|E| \leq n^2/4$.

Il teorema di Ramsey afferma che, se un grafo su n vertici soddisfa $n \geq N(p, q; 2)$, esso contiene un sottografo completo su p vertici oppure un insieme di q vertici senza spigoli fra loro, detto *insieme indipendente*. Ci chiediamo ora se una condizione sul numero degli spigoli garantisca un sottografo K_p. Abbiamo già visto la risposta per $p = 3$ e abbiamo anche un'idea di come evitare un K_p. Dividiamo i vertici in $p-1$ sottoinsiemi $S_1, \ldots, S_{p-1}$ di cardinalità quasi uguale: r sottoinsiemi di cardinalità $t+1$ e $p-1-r$ di cardinalità t, dove $n = t(p-1)+r$, con $1 \leq r \leq p-1$. All'interno di ciascun S_i non vi sono spigoli, ma ogni vertice di S_i è congiunto a ogni vertice di S_j quando $i \neq j$. Questo è un *grafo multipartito completo*. Il numero degli spigoli è Orig. 38

$$M(n,p) := \frac{p-2}{2(p-1)} n^2 - \frac{r(p-1-r)}{2(p-1)}.$$

Teorema 4.1 (Turán, 1941). Se un grafo semplice su n vertici ha più di $M(n,p)$ spigoli, allora contiene un K_p come sottografo.

Dimostrazione. Procediamo per induzione su t. Per $t = 0$ il teorema è ovvio. Consideriamo un grafo G con n vertici, senza K_p e con il massimo numero di spigoli compatibile con queste proprietà. Chiaramente G contiene un K_{p-1}, diciamo H: altrimenti l'aggiunta di uno spigolo non potrebbe produrre un K_p. Ciascuno dei vertici rimanenti è congiunto ad al più $p-2$ vertici di H. I restanti $n-p+1$ vertici non contengono un K_p come sottografo. Poiché $n-p+1 = (t-1)(p-1)+r$, possiamo applicare a questo insieme l'ipotesi induttiva. Il numero degli spigoli di G è quindi al più

$$M(n-p+1, p) + (n-p+1)(p-2) + \binom{p-1}{2},$$

che è uguale a $M(n,p)$. □

Osservazione. L'argomento usato per il teorema di Mantel mostrerebbe che, in assenza di K_p, si ha $|E| \leq \frac{p-2}{2(p-1)} n^2$.

Problema 4A. Sia G un grafo semplice con 10 vertici e 26 spigoli. Mostrate che G contiene almeno 5 triangoli. Può verificarsi l'uguaglianza?

L'articolo di Turán contenente il teorema 4.1 è considerato il punto di partenza di ciò che oggi si chiama *teoria estremale dei grafi*; si veda Bollobás (1978). Un semplice problema estremale chiede il massimo numero di spigoli che può avere un grafo dotato di una certa proprietà. I grafi nei quali questo numero è massimo sono detti *grafi estremali* rispetto alla proprietà.

Gli unici grafi estremali per il problema di Turán sono i grafi multipartiti completi descritti sopra. Ciò segue da un'analisi della dimostrazione del teorema 4.1; nel problema seguente chiediamo al lettore di svolgerla almeno nel caso $p = 3$.

Orig. 39

Problema 4B. Mostrate che un grafo semplice su n vertici con $\lfloor n^2/4 \rfloor$ spigoli e senza triangoli è un grafo bipartito completo $K_{k,k}$ se $n = 2k$, oppure $K_{k,k+1}$ se $n = 2k + 1$.

Problema 4C. Se un grafo semplice su n vertici ha e spigoli, allora contiene almeno $\frac{e}{3n}(4e - n^2)$ triangoli.

La *maglia* di un grafo G è la lunghezza del suo poligono P_n più corto. (Una foresta ha maglia infinita.) Per definizione, un grafo è semplice se e solo se ha maglia ≥ 3. Per il teorema di Mantel, un grafo con più di $n^2/4$ spigoli ha maglia ≤ 3.

Teorema 4.2. Se un grafo G su n vertici ha più di $\frac{1}{2}n\sqrt{n-1}$ spigoli, allora ha maglia ≤ 4. In altre parole, G non è semplice oppure contiene un P_3 o un P_4, cioè un triangolo o un quadrilatero.

Dimostrazione. Supponiamo che G abbia maglia ≥ 5. Siano $y_1, y_2, \ldots, y_d$ i vertici adiacenti a un vertice x, dove $d := \deg(x)$. Nessuna coppia di essi è adiacente, perché G non contiene triangoli. Inoltre nessun vertice diverso da x può essere adiacente a più di uno fra $y_1, \ldots, y_d$, poiché in G non vi sono quadrilateri. Pertanto $(\deg(y_1) - 1) + \cdots + (\deg(y_d) - 1) + (d + 1)$ non può superare il numero totale n dei vertici. Cioè

$$\sum_{y \text{ adiacente a } x} \deg(y) \leq n - 1.$$

Allora

$$\begin{aligned} n(n-1) &\geq \sum_x \sum_{y \text{ adiacente a } x} \deg(y) = \sum_y \deg(y)^2 \\ &\geq \frac{1}{n}\left(\sum_y \deg(y)\right)^2 = \frac{1}{n}(2|E(G)|)^2. \end{aligned}$$

□

Il numero $\frac{1}{2}n\sqrt{n-1}$ del teorema 4.2 è soltanto un limite, non la risposta esatta per ogni n. Determinare i grafi estremali per questo problema, ossia quelli con il massimo numero di spigoli sotto la condizione di maglia ≥ 5, per tutti i valori di n, è un compito di difficoltà proibitiva; è stato però quasi possibile determinare i grafi per i quali vale l'uguaglianza. Forse sorprendentemente, esistono al più quattro grafi con $n > 2$ vertici, maglia ≥ 5 e $\frac{1}{2}n\sqrt{n-1}$ spigoli: il pentagono ($n = 5$), il grafo di Petersen ($n = 10$), uno con $n = 50$ ed eventualmente uno con $n = 3250$. Si vedano le note e il capitolo 21.

Orig. 40

Problema 4D. Supponete che G sia regolare di grado r e abbia maglia almeno g. Trovate un limite inferiore per $|V(G)|$. (Distinguete i casi g pari e g dispari.)

Non è altrettanto interessante chiedersi quanti spigoli siano necessari per imporre un circuito hamiltoniano. Possiamo invece chiedere quale limite sul grado minimo garantisca il risultato.

Teorema 4.3. Se un grafo semplice G su n vertici ha tutti i gradi almeno uguali a $n/2$, allora contiene un P_n come sottografo, cioè ammette un circuito hamiltoniano.[1]

Dimostrazione. Supponiamo falso il teorema e sia G un grafo che soddisfa l'ipotesi per qualche n ma non ha circuiti hamiltoniani. Possiamo prendere G con il massimo numero di spigoli fra i controesempi; l'aggiunta di uno spigolo qualsiasi, cioè il collegamento di due vertici non adiacenti, crea allora un circuito hamiltoniano.

Siano y e z vertici non adiacenti. Poiché aggiungere $\{y, z\}$ crea un circuito hamiltoniano, esiste un cammino semplice da y a z con successione dei vertici $y = x_1, x_2, \ldots, x_n = z$. Gli insiemi

$$\{i : y \text{ è adiacente a } x_{i+1}\} \quad \text{e} \quad \{i : z \text{ è adiacente a } x_i\}$$

[1] Nota redazionale: si sottintende $n \geq 3$; per $n = 2$ il grafo semplice K_2 soddisfa la condizione sul grado ma non contiene un poligono.

hanno entrambi cardinalità $\geq n/2$ e sono contenuti in $\{1, 2, 3, \ldots, n-1\}$, quindi devono intersecarsi; sia i_0 un elemento comune. Allora

$$y = x_1, x_2, \ldots, x_{i_0}, z = x_n, x_{n-1}, \ldots, x_{i_0+1}, x_1 = y$$

è la successione dei vertici di un cammino semplice chiuso di lunghezza n in G, contraddicendo la scelta di G come controesempio. □

Il teorema 4.3 è dovuto a G. A. Dirac ed è ottimale almeno nel senso che non rimane vero sostituendo $n/2$ con $(n-1)/2$. Per esempio, i grafi bipartiti completi $K_{k,k+1}$ non hanno circuiti hamiltoniani. Il teorema ammette però miglioramenti e generalizzazioni: si veda, per esempio, Lovász (1979), problema 10.21. Orig. 41

Problema 4E. Un cubo di formaggio $3 \times 3 \times 3$ è diviso in 27 cubetti $1 \times 1 \times 1$. Un topo mangia un cubetto ogni giorno e il giorno successivo ne mangia uno adiacente, cioè con una faccia in comune. Può mangiare il cubetto centrale l'ultimo giorno?

Problema 4F. Sia G un grafo semplice con n vertici. Dimostrate che, se ogni vertice ha grado almeno $(n+1)/2$, per ogni spigolo e esiste un circuito hamiltoniano di G che passa per e.

Problema 4G. Dimostrate l'osservazione che segue il teorema 4.1.

Problema 4H. Mostrate che un grafo su n vertici che non contiene un circuito su quattro vertici ha al più $\frac{n}{4}(1 + \sqrt{4n-3})$ spigoli.[2]

Note

P. Turán (1910–1976), uno dei celebri matematici ungheresi del XX secolo, è noto soprattutto per i suoi lavori in teoria analitica dei numeri e in analisi reale e complessa.

Per ogni $r \geq 2$ e $g \geq 2$ esiste un grafo regolare di grado r e di maglia $\geq g$. Si veda Lovász (1979), problema 10.12.

L'analisi della dimostrazione del teorema 4.2 mostra che un grafo con $n > 2$ vertici, maglia ≥ 5 e $\frac{1}{2}n\sqrt{n-1}$ spigoli è regolare di grado $k := \sqrt{n-1}$ e che ogni coppia di vertici non adiacenti è congiunta da un unico cammino di lunghezza 2. Nella notazione del capitolo 21, un tale grafo è uno $\mathrm{srg}(n, k, 0, 1)$; i metodi di quel capitolo mostrano che $k = 2, 3, 7$ oppure 57. Questo fu dimostrato per la prima volta da Hoffman e Singleton (1960), che descrissero anche un esempio con $k = 7$ e $n = 50$, oggi noto come grafo di Hoffman–Singleton. Al momento non è noto se esista uno $\mathrm{srg}(3250, 57, 0, 1)$.

Riferimenti bibliografici

B. Bollobás (1978)
Extremal Graph Theory, Academic Press.

A. J. Hoffman e R. R. Singleton (1960)
On Moore graphs with diameters two and three, *IBM J. Res. Develop.* **4**, 497–504.

Orig. 42

L. Lovász (1979)
Combinatorial Problems and Exercises, North Holland.

W. Mantel (1907)
Problem 28, *Wiskundige Opgaven* **10**, 60–61.

P. Turán (1941)
An extremal problem in graph theory (in ungherese), *Mat. Fiz. Lapok* **48**, 435–452.

[2] Nota redazionale: qui il grafo si intende semplice; senza tale ipotesi la presenza di spigoli paralleli renderebbe falsa la limitazione.

Capitolo 5

Sistemi di rappresentanti distinti

Diamo dapprima due formulazioni di un risultato noto come *teorema dei matrimoni di P. Hall*. Ne forniremo una dimostrazione costruttiva e una enumerativa. Se A è un sottoinsieme dei vertici di un grafo, indichiamo con $\Gamma(A)$ l'insieme $\bigcup_{a\in A}\Gamma(a)$. Consideriamo un grafo bipartito G con insieme dei vertici $X \cup Y$, in cui ogni spigolo ha un estremo in X e uno in Y. Un *accoppiamento* in G è un sottoinsieme E_1 degli spigoli tale che nessun vertice sia incidente con più di uno spigolo di E_1. Un *accoppiamento completo da X a Y* è un accoppiamento nel quale ogni vertice di X è incidente con uno spigolo di E_1. Se pensiamo ai vertici di X e Y come a ragazzi e ragazze, rispettivamente, o viceversa, e poniamo uno spigolo quando le persone ai suoi estremi provano simpatia reciproca, un accoppiamento completo rappresenta una possibile assegnazione di partner matrimoniali alle persone di X. Orig. 43

Teorema 5.1. Condizione necessaria e sufficiente affinché esista in G un accoppiamento completo da X a Y è che $|\Gamma(A)| \geq |A|$ per ogni $A \subseteq X$.

Dimostrazione. (i) La necessità è evidente.

(ii) Supponiamo che $|\Gamma(A)| \geq |A|$ per ogni $A \subseteq X$. Siano $|X| = n$ e $m < n$, e supponiamo di avere un accoppiamento M con m spigoli. Mostreremo che ne esiste uno più grande, nel senso della cardinalità: potrebbe non esistere un accoppiamento completo contenente proprio questi m spigoli.

Chiamiamo rossi gli spigoli di M e blu tutti gli altri. Sia $x_0 \in X$ un vertice non incidente con uno spigolo dell'accoppiamento. Affermiamo che esiste un cammino semplice di lunghezza dispari che inizia in x_0 con uno spigolo blu, usa alternativamente spigoli rossi e blu e termina con uno spigolo blu in un vertice y non incidente con alcuno spigolo dell'accoppiamento. Trovato un tale cammino p, abbiamo finito: eliminando da M gli spigoli rossi di p e sostituendoli con quelli blu di p, otteniamo un accoppiamento con $m+1$ spigoli. In altre parole, scambiamo i colori lungo p. Orig. 44

Poiché $|\Gamma(\{x_0\})| \geq 1$, esiste un vertice y_1 adiacente a x_0, ovviamente tramite uno spigolo blu, dato che x_0 non è incidente con spigoli rossi. Se neppure y_1 è incidente con uno spigolo rosso, abbiamo il cammino richiesto, di lunghezza uno. Altrimenti sia x_1 l'altro estremo dello spigolo rosso incidente con y_1. Definiamo ricorsivamente $x_0, x_1, \ldots$ e $y_1, y_2, \ldots$ così: definiti $x_0, x_1, \ldots, x_k$ e $y_1, \ldots, y_k$, dalla disuguaglianza $|\Gamma(\{x_0, x_1, \ldots, x_k\})| \geq k+1$ segue l'esistenza di un vertice y_{k+1}, diverso da $y_1, \ldots, y_k$, adiacente ad almeno un vertice di $\{x_0, x_1, \ldots, x_k\}$. Se y_{k+1} non è incidente con uno spigolo rosso ci fermiamo; altrimenti chiamiamo x_{k+1} l'altro estremo di quello spigolo.

Quando il procedimento termina, costruiamo p partendo da y_{k+1} e dallo spigolo blu che lo congiunge, diciamo, a x_{i_1}, con $i_1 < k+1$. Aggiungiamo lo spigolo rosso $\{x_{i_1}, y_{i_1}\}$. Per costruzione, y_{i_1} è congiunto da uno spigolo necessariamente blu a un x_{i_2}, con $i_2 < i_1$. Aggiungiamo lo spigolo rosso $\{x_{i_2}, y_{i_2}\}$ e continuiamo così fino a raggiungere x_0. □

Problema 5A. Un *accoppiamento perfetto* in un grafo G, non necessariamente bipartito, è un accoppiamento tale che ogni vertice di G sia incidente con uno dei suoi spigoli. (i) Mostrate che un grafo bipartito finito regolare di grado $d > 0$ ha un accoppiamento perfetto. (ii) Trovate un grafo semplice trivalente, cioè regolare di grado 3, senza accoppiamenti perfetti. (iii) Sia G bipartito con vertici $X \cup Y$, con ogni spigolo avente un estremo in ciascuna parte. Supponete inoltre che ogni vertice di X abbia lo stesso grado $s > 0$ e ogni vertice di Y lo stesso grado t. Questa proprietà si chiama *semiregolarità*. Dimostrate che, se $|X| \leq |Y|$, equivalentemente $s \geq t$, esiste un accoppiamento completo di X in Y.

Esempio 5.1. Un gioco di prestigio con un normale mazzo di 52 carte si svolge così. Vi vengono distribuite cinque carte a caso. Ne trattenete una e mettete le altre quattro, in un ordine preciso, in una busta che viene portata al vostro compagno in un'altra stanza. Il compagno le guarda e annuncia quale sia la quinta carta, quella trattenuta. Usando semi e valori si possono ideare metodi ingegnosi o relativamente semplici per decidere quale carta trattenere e quali trasmettere, e perché il compagno individui quella trattenuta; si vedano le note. Ignorando la complessità della soluzione, il problema matematico generale, per un mazzo di N carte, è il seguente: esiste un'applicazione iniettiva f dall'insieme X dei $\binom{N}{5}$ sottoinsiemi di cinque carte all'insieme Y delle $N(N-1)(N-2)(N-3)$ quadruple ordinate di carte distinte, con la condizione che, se $f(S) = (c_1, c_2, c_3, c_4)$, allora $\{c_1, c_2, c_3, c_4\} \subseteq S$? Orig. 45

In termini di accoppiamenti, consideriamo il grafo bipartito G con vertici $X \cup Y$ definiti sopra, e poniamo uno spigolo fra $S \in X$ e $(c_1, c_2, c_3, c_4) \in Y$ esattamente quando $\{c_1, c_2, c_3, c_4\} \subseteq S$. Cerchiamo un accoppiamento completo di X in Y. Il lettore può verificare che G è semiregolare e che $|X| \leq |Y|$ se e solo se $N \leq 124$. Per il problema 5A(iii), tale accoppiamento esiste dunque per $N \leq 124$.

Riformuliamo ora il teorema 5.1 in termini di insiemi: oltre a dimostrarlo, forniremo un limite inferiore al numero degli accoppiamenti. Consideriamo sottoinsiemi $A_0, A_1, \ldots, A_{n-1}$ di un insieme finito S. Diremo che la famiglia ha la *proprietà H*, o *condizione di Hall*, se, per ogni k, l'unione di qualunque k-upla di sottoinsiemi A_i ha almeno k elementi. Se l'unione di una k-upla contiene esattamente k elementi, con $0 < k < n$, chiameremo quella k-upla un *blocco critico*.

Un *sistema di rappresentanti distinti*, abbreviato SDR, degli insiemi $A_0, \ldots, A_{n-1}$ è una successione di n elementi distinti $a_0, \ldots, a_{n-1}$, con $a_i \in A_i$ per $0 \leq i \leq n-1$.

Siano $m_0 \leq m_1 \leq \cdots \leq m_{n-1}$. Definiamo

$$F_n(m_0, m_1, \ldots, m_{n-1}) := \prod_{i=0}^{n-1} (m_i - i)_*,$$

dove $(a)_* := \max\{1, a\}$. D'ora in poi supponiamo non decrescente la successione $m_i := |A_i|$. Per dimostrare il risultato principale occorre un lemma.

Lemma 5.2. Per $n \geq 1$, definiamo $f_n : \mathbb{Z}^n \to \mathbb{N}$ ponendo

$$f_n(a_0, a_1, \ldots, a_{n-1}) := F_n(m_0, m_1, \ldots, m_{n-1}),$$

dove $(m_0, \ldots, m_{n-1})$ è un riordinamento non decrescente di $(a_0, \ldots, a_{n-1})$. Allora f_n è non decrescente rispetto a ciascuna variabile a_i. Orig. 46

Dimostrazione. Sia

$$m_0 \leq \cdots \leq m_{k-1} \leq a_i = m_k \leq m_{k+1} \leq \cdots \leq m_l \leq m_{l+1} \leq \cdots \leq m_{n-1}$$

un riordinamento non decrescente di $(a_0, \ldots, a_{n-1})$. Se $a'_i \geq a_i$ e

$$m_0 \leq \cdots \leq m_{k-1} \leq m_{k+1} \leq \cdots \leq m_l \leq a'_i \leq m_{l+1} \leq \cdots \leq m_{n-1}$$

è un riordinamento non decrescente di $(a_0, \ldots, a_{i-1}, a'_i, a_{i+1}, \ldots, a_{n-1})$, allora

$$\frac{f_n(a_0, \ldots, a_{i-1}, a'_i, a_{i+1}, \ldots, a_{n-1})}{f_n(a_0, \ldots, a_{n-1})} = \frac{(m_{k+1} - k)_*}{(a_i - k)_*} \cdot \frac{(a'_i - l)_*}{(m_l - l)_*} \prod_{j=k+1}^{l-1} \frac{(m_{j+1} - j)_*}{(m_j - j)_*},$$

e questo rapporto è almeno 1, perché $a_i \leq m_{k+1}$, $a'_i \geq m_l$ e $m_{j+1} \geq m_j$ per $j = k+1, \ldots, l-1$. □

Veniamo alla seconda forma del teorema di Hall. Indichiamo con $N(A_0, \ldots, A_{n-1})$ il numero di SDR di $(A_0, \ldots, A_{n-1})$.

Teorema 5.3. Sia $(A_0, \ldots, A_{n-1})$ una successione di sottoinsiemi di S. Poniamo $m_i := |A_i|$, per $i = 0, \ldots, n-1$, e supponiamo $m_0 \leq \cdots \leq m_{n-1}$. Se la successione ha la proprietà H, allora

$$N(A_0, \ldots, A_{n-1}) \geq F_n(m_0, \ldots, m_{n-1}).$$

Dimostrazione. Procediamo per induzione. Il teorema è chiaramente vero per $n = 1$. Distinguiamo due casi.

Caso 1. Non vi sono blocchi critici. Scegliamo come rappresentante di A_0 un suo elemento arbitrario a, poi eliminiamo a da tutti gli altri insiemi. Otteniamo così gli insiemi $A_1(a), \dots, A_{n-1}(a)$, che soddisfano ancora la proprietà H. Per l'ipotesi induttiva e il lemma, Orig. 47

$$\begin{aligned} N(A_0, \dots, A_{n-1}) &\geq \sum_{a \in A_0} f_{n-1}(|A_1(a)|, \dots, |A_{n-1}(a)|) \\ &\geq \sum_{a \in A_0} f_{n-1}(m_1 - 1, \dots, m_{n-1} - 1) \\ &= m_0 f_{n-1}(m_1 - 1, \dots, m_{n-1} - 1) \\ &= F_n(m_0, m_1, \dots, m_{n-1}). \end{aligned}$$

Caso 2. Esiste un blocco critico $(A_{\nu_0}, \dots, A_{\nu_{k-1}})$, con $\nu_0 < \cdots < \nu_{k-1}$ e $0 < k < n$. Eliminiamo tutti gli elementi di $A_{\nu_0} \cup \cdots \cup A_{\nu_{k-1}}$ da ciascuno degli altri A_i, ottenendo $A'_{\mu_0}, \dots, A'_{\mu_{l-1}}$, dove $\{\nu_0, \dots, \nu_{k-1}, \mu_0, \dots, \mu_{l-1}\} = \{0, 1, \dots, n-1\}$ e $k + l = n$.

Sia $(A_{\nu_0}, \dots, A_{\nu_{k-1}})$ sia $(A'_{\mu_0}, \dots, A'_{\mu_{l-1}})$ soddisfano la proprietà H, e gli SDR delle due successioni sono sempre disgiunti. Per l'ipotesi induttiva e il lemma,

$$\begin{aligned} N(A_0, \dots, A_{n-1}) &= N(A_{\nu_0}, \dots, A_{\nu_{k-1}}) N(A'_{\mu_0}, \dots, A'_{\mu_{l-1}}) \\ &\geq f_k(m_{\nu_0}, \dots, m_{\nu_{k-1}}) f_l(|A'_{\mu_0}|, \dots, |A'_{\mu_{l-1}}|) \\ &\geq f_k(m_{\nu_0}, \dots, m_{\nu_{k-1}}) f_l(m_{\mu_0} - k, \dots, m_{\mu_{l-1}} - k) \\ &\geq f_k(m_0, \dots, m_{k-1}) f_l(m_{\mu_0} - k, \dots, m_{\mu_{l-1}} - k). \end{aligned} \tag{5.1}$$

Osserviamo ora che

$$m_{\nu_{k-1}} \leq |A_{\nu_0} \cup \cdots \cup A_{\nu_{k-1}}| = k.$$

Pertanto $(m_r - r)_* = 1$ se $k \leq r \leq \nu_{k-1}$, e $(m_{\mu_i} - k - i)_* = 1$ se $\mu_i \leq \nu_{k-1}$. Ne segue

$$f_k(m_0, \dots, m_{k-1}) = \prod_{0 \leq i \leq \nu_{k-1}} (m_i - i)_*,$$

$$f_l(m_{\mu_0} - k, \dots, m_{\mu_{l-1}} - k) = \prod_{\nu_{k-1} < j < n} (m_j - j)_*,$$

cioè il prodotto finale della (5.1) è uguale a $F_n(m_0, \dots, m_{n-1})$, e il teorema è dimostrato. □ Orig. 48

Problema 5B. Mostrate che il teorema 5.3 fornisce il miglior limite inferiore al numero degli SDR degli insiemi A_i che dipenda soltanto dalle cardinalità $|A_i|$.

Veniamo ora a un risultato noto come *teorema di König*. Esso è equivalente, qualunque cosa questo significhi, al teorema di Hall. Nell'enunciato, A è una matrice $(0, 1)$ con elementi a_{ij}. Per *linea* intendiamo una riga oppure una colonna di A.

Teorema 5.4. Il minimo numero di linee di A che contengono tutti gli 1 di A è uguale al massimo numero di 1 in A dei quali nessuna coppia appartenga alla stessa linea.

Dimostrazione. Sia m il minimo numero di linee di A che contengono tutti gli 1, e sia M il massimo numero di 1 dei quali nessuna coppia sia sulla stessa linea. Chiaramente $m \geq M$. Un ricoprimento minimo mediante linee sia formato da r righe e s colonne, con $r + s = m$. Senza perdita di generalità sono le prime r righe e le prime s colonne. Definiamo $A_i := \{j > s : a_{ij} = 1\}$, per $1 \leq i \leq r$. Se l'unione di una k-upla di questi insiemi avesse meno di k elementi, potremmo sostituire le corrispondenti k righe con $k - 1$ colonne, continuando a coprire tutti gli 1. Poiché ciò è impossibile, gli A_i soddisfano la proprietà H e hanno dunque un SDR. Esistono perciò r elementi uguali a 1, a due a due su linee distinte, nelle prime r righe e fuori dalle prime s colonne. Analogamente ne esistono s nelle prime s colonne e fuori dalle prime r righe. Quindi $M \geq r + s = m$, come volevamo. □

Il teorema seguente di G. Birkhoff è un'applicazione del teorema di Hall.

Teorema 5.5. Sia $A = (a_{ij})$ una matrice $n \times n$ con elementi interi non negativi, tale che ogni riga e ogni colonna abbia somma l. Allora A è somma di l matrici di permutazione.

Dimostrazione. Definiamo $A_i := \{j : a_{ij} > 0\}$, per $1 \leq i \leq n$. Per ogni k-upla degli A_i, la somma delle righe corrispondenti di A è kl. Poiché ogni colonna di A ha somma l, gli elementi non nulli delle k Orig. 49

righe scelte devono trovarsi in almeno k colonne. Gli A_i soddisfano quindi la proprietà H. Un loro SDR corrisponde a una matrice di permutazione $P = (p_{ij})$ tale che $a_{ij} > 0$ quando $p_{ij} = 1$. Il teorema segue ora per induzione su l. □

Problema 5C. Nell'ipotesi del teorema 5.5 sostituite «interi» con «reali». Mostrate che A è allora una combinazione lineare non negativa di matrici di permutazione. Equivalentemente, ogni matrice doppiamente stocastica, si veda il capitolo 11, è una combinazione convessa di matrici di permutazione.

Problema 5D. Sia $S = \{1, 2, \ldots, mn\}$. Partizioniamo S in m insiemi $A_1, \ldots, A_m$ di cardinalità n, e sia $B_1, \ldots, B_m$ una seconda partizione in m insiemi di cardinalità n. Mostrate che gli A_i possono essere rinumerati in modo che $A_i \cap B_i \neq \varnothing$.

Problema 5E. Sia $A_i = \{i-1, i, i+1\} \cap \{1, 2, \ldots, n\}$, per $i = 1, 2, \ldots, n$. Indichiamo con S_n il numero di SDR della famiglia $\{A_1, \ldots, A_n\}$. Determinate S_n e $\lim_{n\to\infty} S_n^{1/n}$.

Sia G un grafo bipartito, finito o infinito, il cui insieme dei vertici sia partizionato in X e Y, con ogni spigolo avente un estremo in ciascuna parte. Un accoppiamento M in G *copre* un sottoinsieme S dei vertici se ogni vertice di S è incidente con uno spigolo di M.

Teorema 5.6. Se esiste un accoppiamento M_1 che copre un sottoinsieme X_0 di X e un accoppiamento M_2 che copre un sottoinsieme Y_0 di Y, allora esiste un accoppiamento M_3 che copre $X_0 \cup Y_0$.

Dimostrazione. Pensiamo agli spigoli di M_1 come rossi e a quelli di M_2 come blu. Uno spigolo appartenente a entrambi è «viola».

È facile vedere che un grafo connesso i cui vertici abbiano tutti grado al più due è uno dei seguenti: un grafo-cammino finito, compreso il caso banale di lunghezza zero con un solo vertice e nessuno spigolo; un poligono finito; un grafo-cammino infinito «unilaterale», con un solo vertice monovalente; oppure un grafo-cammino infinito «bilaterale». Nel grafo H avente gli stessi vertici di G e insieme degli spigoli $M_1 \cup M_2$, ogni vertice ha grado al più due; le sue componenti connesse sono quindi dei tipi elencati. Salvo le componenti formate da uno spigolo viola e dai suoi estremi, gli spigoli di ogni componente alternano rosso e blu; in particolare, tutti i poligoni hanno lunghezza pari. Ogni vertice di $X_0 \cup Y_0$ appartiene a una componente non banale. Orig. 50

Per costruire M_3 prendiamo tutti gli spigoli viola e, da ogni altra componente di H, tutti gli spigoli rossi oppure tutti quelli blu. Per i cicli e i cammini infiniti bilaterali la scelta è indifferente: entrambi i colori coprono tutti i vertici della componente. Per i cammini di lunghezza dispari e quelli infiniti unilaterali prendiamo gli spigoli del colore del primo spigolo. In un cammino di lunghezza dispari il primo e l'ultimo spigolo hanno lo stesso colore, quindi il lato da cui si parte è irrilevante. Anche qui gli spigoli scelti coprono tutti i vertici.

Serve appena un po' più di attenzione per una componente che sia un cammino finito P di lunghezza pari, con vertici $v_0, v_1, \ldots, v_k$. Il numero dei vertici è dispari ed essi appartengono alternativamente a X e a Y, quindi v_0 e v_k sono entrambi in X oppure entrambi in Y. Nel primo caso mettiamo in M_3 tutti gli spigoli rossi di P, cioè quelli di M_1; nel secondo, tutti quelli blu. Soltanto un estremo del cammino rimane scoperto.

Supponiamo $v_0, v_k \in X$; il caso in cui siano in Y è analogo. Se il primo spigolo di P è rosso, l'ultimo è blu e $v_k \notin X_0$, poiché nessuno spigolo di M_1 copre v_k. Gli spigoli rossi coprono dunque tutti i vertici di X_0 e Y_0 appartenenti a P. Se il primo spigolo è blu, analogamente $v_0 \notin X_0$ e gli spigoli rossi coprono ancora tutti i vertici richiesti. □

Nel caso $X_0 = X$, $Y_0 = Y$ e G bipartito completo, gli accoppiamenti che coprono X_0 o Y_0 corrispondono ad applicazioni iniettive rispettivamente $X \to Y$ e $Y \to X$. Il teorema 5.6 afferma quindi:

Corollario. Se fra due insiemi X e Y esistono applicazioni iniettive $f : X \to Y$ e $g : Y \to X$, allora esiste un'applicazione biiettiva da X a Y, o da Y a X: i due insiemi sono in corrispondenza biunivoca.

In termini di cardinalità, se $|X| \leq |Y|$ e $|Y| \leq |X|$, allora $|X| = |Y|$. È il *teorema di Schröder–Bernstein*; si veda la sezione 22 di P. R. Halmos (1974). Per insiemi finiti è naturalmente banale. Orig. 51

Problema 5F. Siano $A_1, A_2, \ldots, A_n$ insiemi finiti. Mostrate che, se

$$\sum_{1 \leq i < j \leq n} \frac{|A_i \cap A_j|}{|A_i|\,|A_j|} < 1,$$

allora gli insiemi $A_1, A_2, \ldots, A_n$ hanno un sistema di rappresentanti distinti.[1]

Problema 5G. (i) Dal problema 5A sappiamo che un grafo bipartito su $2n$ vertici regolare di grado 3 ha un accoppiamento perfetto. Quanti accoppiamenti perfetti distinti vi sono se $n = 4$? (ii) Stessa domanda per un grafo bipartito su 10 vertici regolare di grado 4.

Note

Philip Hall pubblicò il suo risultato nel 1935, con una dimostrazione piuttosto difficile. Quella che abbiamo presentato generalizza idee di Halmos e Vaughan, Rado e M. Hall; è dovuta a Ostrand (1970) e Hautus e Van Lint (1972). Si veda Van Lint (1974). Il problema degli accoppiamenti completi è spesso chiamato *problema dei matrimoni*.

D. König (1884–1944) fu professore a Budapest. Scrisse il primo trattato organico sulla teoria dei grafi, *Theorie der endlichen und unendlichen Graphen* (1936). König (1916) contiene la prima dimostrazione di uno dei risultati chiamati teorema di König.

Poco prima del teorema 5.4 abbiamo parlato di «equivalenza» fra questi teoremi. L'espressione si usa spesso quando ciascuno dei due è una conseguenza più o meno immediata dell'altro.

Il teorema di Birkhoff (1946), cioè il teorema 5.5, è estremamente utile e verrà applicato più volte nei capitoli successivi.

Ecco una soluzione al problema delle carte dell'esempio 5.1. In un insieme di cinque carte almeno un seme compare due volte. La prima carta trasmessa al compagno sarà la «maggiore» di due carte dello stesso seme; tratterrete la «minore». Pensiamo ai valori $2, 3, \ldots, 10, J, Q, K, A$ disposti in senso orario su un cerchio, modulo 13; per «minore» intendiamo la carta dalla quale si deve percorrere la distanza più breve in senso orario per raggiungere l'altra. Per esempio, se $S = \{3\spadesuit, Q\diamondsuit, 6\clubsuit, 3\diamondsuit, 7\spadesuit\}$, trasmetterete il $7\spadesuit$ oppure il $3\diamondsuit$. Questo comunica già al compagno il seme della carta trattenuta e la restringe a sei possibilità in quel seme. Per determinare di quanto retrocedere in senso antiorario dal valore della prima carta, userete l'ordine delle altre tre carte, ordinando lessicograficamente tutte le 52 carte, e concorderete una corrispondenza fra le sei permutazioni di tre oggetti e gli interi da 1 a 6. Orig. 52

Riferimenti bibliografici

G. Birkhoff (1946)
Tres observaciones sobre el algebra lineal, *Univ. Nac. Tucumán, Rev. Ser. A* **5**, 147–151.

P. Hall (1935)
On representatives of subsets, *J. London Math. Soc.* **10**, 26–30.

P. R. Halmos (1974)
Naive Set Theory, Springer-Verlag.

D. König (1916)
Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, *Math. Annalen* **77**, 453–465.

J. H. van Lint (1974)
Combinatorial Theory Seminar Eindhoven University of Technology, Lecture Notes in Mathematics **382**, Springer-Verlag.

P. Ostrand (1970)
Systems of distinct representatives, *J. of Math. Analysis and Applic.* **32**, 1–4.

[1] Nota redazionale: si sottintende che tutti gli A_i siano non vuoti, affinché le frazioni siano definite.

Capitolo 6

Teorema di Dilworth e teoria estremale degli insiemi

Un *insieme parzialmente ordinato*, o *poset*, è un insieme S dotato di una relazione binaria $\leq$, talvolta indicata con $\subseteq$, tale che: Orig. 53

(i) $a \leq a$ per ogni $a \in S$ (riflessività);

(ii) se $a \leq b$ e $b \leq c$, allora $a \leq c$ (transitività);

(iii) se $a \leq b$ e $b \leq a$, allora $a = b$ (antisimmetria).

Se per ogni $a, b \in S$ si ha $a \leq b$ oppure $b \leq a$, l'ordine parziale si chiama *ordine totale*, o *lineare*. Se $a \leq b$ e $a \neq b$, scriviamo anche $a < b$. Esempi di poset sono gli interi con l'ordine usuale e i sottoinsiemi di un insieme ordinati per inclusione. Un sottoinsieme totalmente ordinato di S si chiama *catena*. Un'*anticatena* è un insieme di elementi a due a due incomparabili.

Il teorema seguente è dovuto a R. Dilworth (1950); questa dimostrazione è di H. Tverberg (1967).

Teorema 6.1. Sia P un insieme finito parzialmente ordinato. Il minimo numero m di catene disgiunte che, insieme, contengono tutti gli elementi di P è uguale al massimo numero M di elementi di un'anticatena di P.

Dimostrazione. (i) È immediato che $m \geq M$.

(ii) Procediamo per induzione su $|P|$. Per $|P| = 0$ non vi è nulla da dimostrare. Sia C una catena massimale di P. Se ogni anticatena di $P \setminus C$ ha al più $M-1$ elementi, abbiamo finito. Supponiamo dunque che $\{a_1, \ldots, a_M\}$ sia un'anticatena di $P \setminus C$. Definiamo $S^- := \{x \in P : \exists i\, [x \leq a_i]\}$ e analogamente S^+. Poiché C è massimale, il suo elemento massimo non appartiene a S^-; per l'ipotesi induttiva il teorema vale quindi per S^-. Quest'ultimo è unione di M catene disgiunte $S_1^-, \ldots, S_M^-$, con $a_i \in S_i^-$. Se $x \in S_i^-$ e $x > a_i$, esisterebbe j con $x \leq a_j$, da cui $a_i < a_j$, assurdo. Quindi a_i è il massimo della catena S_i^-, per $i = 1, \ldots, M$. Facciamo lo stesso per S^+. Unendo le catene corrispondenti si ottiene il teorema. □ Orig. 54

Un risultato «duale» del teorema di Dilworth fu dato da Mirsky (1971).

Teorema 6.2. Sia P un insieme parzialmente ordinato. Se P non contiene catene di $m+1$ elementi, allora è unione di m anticatene.

Dimostrazione. Per $m = 1$ il risultato è banale. Sia $m \geq 2$ e supponiamo vero il teorema per $m-1$. Sia P un insieme parzialmente ordinato senza catene di $m+1$ elementi. L'insieme M degli elementi massimali di P è un'anticatena. Se $x_1 < x_2 < \cdots < x_m$ fosse una catena in $P \setminus M$, sarebbe anche massimale in P e dunque $x_m \in M$, assurdo. Pertanto $P \setminus M$ non contiene catene di m elementi e, per induzione, è unione di $m-1$ anticatene. Questo dimostra il teorema. □

Il celebre teorema seguente, dovuto a Sperner (1928), ha natura analoga. Questa dimostrazione è di Lubell (1966).

Teorema 6.3. Se $A_1, A_2, \ldots, A_m$ sono sottoinsiemi di $N := \{1, 2, \ldots, n\}$ tali che A_i non sia un sottoinsieme di A_j per $i \neq j$, allora

$$m \leq \binom{n}{\lfloor n/2 \rfloor}.$$

DIMOSTRAZIONE. Consideriamo il poset dei sottoinsiemi di N. La famiglia $\mathcal{A} := \{A_1, \dots, A_m\}$ è un'anticatena.

Una catena massimale C contiene un sottoinsieme di ciascuna cardinalità $0, 1, \dots, n$; la si ottiene partendo dall'insieme vuoto, scegliendo poi un singoletto (n possibilità), un sottoinsieme di due elementi che lo contenga ($n-1$ possibilità), uno di tre elementi che contenga il precedente ($n-2$ possibilità), e così via. Esistono dunque $n!$ catene massimali. Analogamente, esattamente $k!(n-k)!$ catene massimali contengono un dato sottoinsieme A di N di cardinalità k.

Contiamo le coppie ordinate (A, C) nelle quali $A \in \mathcal{A}$, C è massimale e $A \in C$. Ogni catena massimale contiene al più un elemento di un'anticatena, quindi il numero è al più $n!$. Se α_k è il numero di insiemi $A \in \mathcal{A}$ di cardinalità k, lo stesso numero è $\sum_{k=0}^{n} \alpha_k k!(n-k)!$. Pertanto

$$\sum_{k=0}^{n} \alpha_k k!(n-k)! \le n!, \qquad \text{equivalentemente} \qquad \sum_{k=0}^{n} \frac{\alpha_k}{\binom{n}{k}} \le 1.$$

Poiché $\binom{n}{k}$ è massimo per $k = \lfloor n/2 \rfloor$ e $\sum \alpha_k = m$, il risultato segue. □ Orig. 55

Nel teorema 6.3 vale l'uguaglianza se si prende come anticatena la famiglia di tutti i sottoinsiemi di N di cardinalità $\lfloor n/2 \rfloor$.

Consideriamo ora il poset B_n, con 2^n elementi, dei sottoinsiemi dell'insieme N di n elementi, ordinati per inclusione. Indichiamo con $\mathcal{A}_i$ la famiglia dei sottoinsiemi di cardinalità i. Una *catena simmetrica* in B_n è una successione $P_k, P_{k+1}, \dots, P_{n-k}$ tale che $P_i \in \mathcal{A}_i$ e $P_i \subseteq P_{i+1}$ per $i = k, k+1, \dots, n-k-1$. Descriviamo un algoritmo di De Bruijn, Van Ebbenhorst Tengbergen e Kruyswijk (1949) che suddivide B_n in catene simmetriche disgiunte.

Algoritmo. Partiamo da B_1 e procediamo per induzione. Se B_n è stato suddiviso in catene simmetriche, per ciascuna $P_k, \dots, P_{n-k}$ definiamo in B_{n+1} le due catene

$$P_{k+1}, \dots, P_{n-k}$$

e

$$P_k,\ P_k \cup \{n+1\},\ P_{k+1} \cup \{n+1\}, \dots, P_{n-k} \cup \{n+1\}.$$

È facile vedere che l'algoritmo ha la proprietà dichiarata. Inoltre fornisce un accoppiamento naturale fra i sottoinsiemi di k e di $n-k$ elementi di B_n; si confronti il teorema 5.1 e si veda il problema 6D.

Problema 6A. Sia $a_1, a_2, \dots, a_{n^2+1}$ una permutazione degli interi $1, 2, \dots, n^2+1$. Mostrate che dal teorema di Dilworth segue che la successione ha una sottosuccessione monotona di lunghezza $n+1$.

Eccone una bella dimostrazione diretta. Supponiamo che non vi siano sottosuccessioni crescenti di $n+1$ termini. Definiamo b_i come la lunghezza della più lunga sottosuccessione crescente che inizia con a_i. Per il principio dei cassetti, almeno $n+1$ termini della successione (b_i) hanno lo stesso valore. Poiché $i < j$ e $b_i = b_j$ implicano $a_i > a_j$, otteniamo una sottosuccessione decrescente di $n+1$ termini.

Per mostrare un legame fra i capitoli 5 e 6, dimostriamo che il teorema 5.1 segue immediatamente dal teorema 6.1. Consideriamo il grafo bipartito G del teorema 5.1. Siano $|X| = n$ e $|Y| = n' \ge n$. Introduciamo un ordine parziale ponendo $x_i < y_j$ se e solo se esiste uno spigolo fra x_i e y_j. La più grande anticatena abbia s elementi, diciamo $\{x_1, \dots, x_h, y_1, \dots, y_k\}$, con $h + k = s$. Poiché $\Gamma(\{x_1, \dots, x_h\}) \subseteq Y \setminus \{y_1, \dots, y_k\}$, si ha $h \le n' - k$, e quindi $s \le n'$. Il poset è unione di s catene disgiunte, costituite da un accoppiamento di cardinalità a, dai rimanenti $n-a$ elementi di X e dai rimanenti $n'-a$ elementi di Y. Pertanto $n + n' - a = s \le n'$, cioè $a \ge n$: abbiamo un accoppiamento completo. Orig. 56

Il teorema 6.3 è un esempio piuttosto facile di un'area detta *teoria estremale degli insiemi*, nella quale i problemi sono spesso assai difficili. Diamo un altro esempio come semplice esercizio.

Problema 6B. Siano A_i, per $1 \le i \le k$, sottoinsiemi distinti di $\{1, 2, \dots, n\}$. Supponete che $A_i \cap A_j \ne \varnothing$ per tutti gli i, j. Mostrate che $k \le 2^{n-1}$ e date un esempio di uguaglianza.

Diamo ora un altro esempio del metodo usato per il teorema di Sperner, dimostrando il cosiddetto *teorema di Erdős–Ko–Rado* (1961).

Teorema 6.4. Sia $\mathcal{A} = \{A_1, \dots, A_m\}$ una famiglia di m sottoinsiemi distinti di $\{1, 2, \dots, n\}$, tutti di cardinalità k, con $k \le n/2$, tale che ogni coppia abbia intersezione non vuota. Allora $m \le \binom{n-1}{k-1}$.

DIMOSTRAZIONE. Disponiamo gli interi da 1 a n su un cerchio e consideriamo la famiglia $\mathcal{F} := \{F_1, \dots, F_n\}$ di tutte le k-uple consecutive sul cerchio, cioè $F_i = \{i, i+1, \dots, i+k-1\}$,

con gli interi presi modulo n. Osserviamo che $|\mathcal{A} \cap \mathcal{F}| \le k$: se un F_i coincide con un A_j, al più uno dei due insiemi $\{l, l+1, \dots, l+k-1\}$ e $\{l-k, \dots, l-1\}$ può appartenere a $\mathcal{A}$, per $i < l < i+k$. La stessa affermazione vale per $\mathcal{F}^\pi$, ottenuta applicando a $\{1, \dots, n\}$ una permutazione π. Quindi

$$\Sigma := \sum_{\pi \in S_n} |\mathcal{A} \cap \mathcal{F}^\pi| \le k\, n!.$$

Contiamo ora la somma fissando $A_j \in \mathcal{A}$ e $F_i \in \mathcal{F}$: vi sono $k!(n-k)!$ permutazioni π con $F_i^\pi = A_j$. Dunque $\Sigma = mnk!(n-k)!$, e il teorema segue. □

Con una lieve modifica della dimostrazione si può mostrare che il risultato vale anche se gli insiemi di $\mathcal{A}$ hanno cardinalità al più k e formano un'anticatena. Daremo però una dimostrazione che usa il teorema 5.1.

Orig. 57

Teorema 6.5. Sia $\mathcal{A} = \{A_1, \dots, A_m\}$ una famiglia di sottoinsiemi di $N := \{1, 2, \dots, n\}$ tale che $A_i \not\subseteq A_j$ e $A_i \cap A_j \neq \varnothing$ per $i \neq j$, e $|A_i| \le k \le n/2$ per ogni i. Allora $m \le \binom{n-1}{k-1}$.

Dimostrazione. (i) Se tutti gli insiemi hanno cardinalità k, basta il teorema 6.4.

(ii) Siano $A_1, \dots, A_s$ gli insiemi di cardinalità minima, diciamo $l \le n/2 - 1$. Consideriamo tutti i sottoinsiemi B_j di N di cardinalità $l+1$ che contengono almeno uno degli A_i, $1 \le i \le s$. Nessuno di essi appartiene a $\mathcal{A}$. Ogni A_i è contenuto in esattamente $n-l$ dei B_j, e ogni B_j contiene al più $l+1 \le n-l$ degli A_i. Per il teorema 5.1 possiamo scegliere s insiemi distinti, diciamo $B_1, \dots, B_s$, con $A_i \subseteq B_i$. Sostituendo $A_1, \dots, A_s$ con $B_1, \dots, B_s$, la nuova famiglia $\mathcal{A}'$ soddisfa le ipotesi del teorema e la sua cardinalità minima è maggiore di l. Per induzione ci riconduciamo al caso (i). □

Sostituendo il conteggio della dimostrazione del teorema 6.4 con un conteggio pesato dei sottoinsiemi, possiamo dimostrare la generalizzazione seguente, dovuta a B. Bollobás (1973).

Teorema 6.6. Sia $\mathcal{A} = \{A_1, \dots, A_m\}$ una famiglia di m sottoinsiemi distinti di $\{1, 2, \dots, n\}$, con $|A_i| \le n/2$ per $i = 1, \dots, m$, tale che ogni coppia abbia intersezione non vuota. Allora

$$\sum_{i=1}^{m} \frac{1}{\binom{n-1}{|A_i|-1}} \le 1.$$

[1]

Dimostrazione. Sia π una permutazione di $1, 2, \dots, n$ disposta su un cerchio, e scriviamo $A_i \in \pi$ se gli elementi di A_i compaiono consecutivamente in qualche posizione sul cerchio. Con lo stesso argomento della dimostrazione del teorema 6.4, se $A_i \in \pi$, allora $A_j \in \pi$ per al più $|A_i|$ valori di j.

Definiamo

$$f(\pi, i) := \begin{cases} 1/|A_i|, & \text{se } A_i \in \pi, \\ 0, & \text{altrimenti.} \end{cases}$$

Per quanto appena osservato, $\sum_{\pi \in S_n} \sum_{i=1}^{m} f(\pi, i) \le n!$. Scambiando l'ordine delle somme dobbiamo contare, per un A_i fissato, le permutazioni disposte sul cerchio per le quali $A_i \in \pi$. Con lo stesso argomento del teorema 6.4, questo numero è $n|A_i|!(n-|A_i|)!$. Quindi

Orig. 58

$$\sum_{i=1}^{m} \frac{1}{|A_i|}\, n|A_i|!(n-|A_i|)! \le n!,$$

da cui segue il risultato. □

Problema 6C. Sia $\mathcal{A} = \{A_1, \dots, A_m\}$ una famiglia di sottoinsiemi distinti di $N := \{1, 2, \dots, n\}$ tale che, per $i \neq j$, si abbia $A_i \not\subseteq A_j$, $A_i \cap A_j \neq \varnothing$ e $A_i \cup A_j \neq N$. Dimostrate che

$$m \le \binom{n-1}{\lfloor n/2 \rfloor - 1}.$$

Problema 6D. Considerate la decomposizione di B_n in catene simmetriche descritta sopra. Mostrate che il teorema 6.3 ne segue immediatamente. Mostrate che, tramite questa decomposizione, il teorema 6.5 si riduce al teorema 6.4. Quante catene hanno l'elemento minimo in $\mathcal{A}_i$?

[1] Nota redazionale: nell'enunciato originale manca l'ipotesi che $\mathcal{A}$ sia un'anticatena di insiemi non vuoti. Senza di essa la disuguaglianza è falsa: per $n = 4$, la famiglia $\{\{1\}, \{1,2\}\}$ dà $1 + 1/3 > 1$. La dimostrazione è da leggere con questa ipotesi, coerentemente con il teorema precedente.

Problema 6E. Ecco un algoritmo per costruire una catena simmetrica di B_n contenente un dato elemento S, cioè un sottoinsieme di $\{1, 2, \ldots, n\}$. Considerate il vettore caratteristico x di S: per esempio, per $n = 7$ e $S = \{3, 4, 7\}$, si ha $x = 0011001$. Marcate tutte le coppie consecutive 10, eliminatele temporaneamente, marcate di nuovo tutte le coppie consecutive 10 e ripetete finché rimane soltanto una stringa della forma $00\cdots01\cdots11$. Nell'esempio otteniamo $00\dot{1}\dot{1}\dot{0}\dot{0}1$, con le coordinate $3, 4, 5, 6$ marcate; eliminandole rimane 001. I vettori caratteristici dei sottoinsiemi della catena si ottengono lasciando fisse le coordinate marcate e facendo variare le altre fra le stringhe $0\cdots000$, $0\cdots001$, $0\cdots011$, …, $1\cdots111$. Nell'esempio i vettori sono

$$00\dot{1}\dot{1}\dot{0}\dot{0}0,$$
$$00\dot{1}\dot{1}\dot{0}\dot{0}1,$$
$$01\dot{1}\dot{1}\dot{0}\dot{0}1,$$
$$11\dot{1}\dot{1}\dot{0}\dot{0}1,$$

che corrispondono ai sottoinsiemi

Orig. 59

$$\{3, 4\}, \quad \{3, 4, 7\}, \quad \{2, 3, 4, 7\}, \quad \{1, 2, 3, 4, 7\}.$$

Mostrate che l'algoritmo produce esattamente la stessa catena simmetrica contenente S dell'algoritmo induttivo di De Bruijn e collaboratori descritto sopra.

Note

Torneremo sugli insiemi parzialmente ordinati nei capitoli 23 e 25.

E. Sperner (1905–1980) è noto soprattutto per un lemma di topologia combinatoria, il «lemma di Sperner», contenuto nella sua tesi del 1928 e usato per dimostrare il teorema del punto fisso di Brouwer. Un altro legame con la combinatoria: la sua prima cattedra fu a Königsberg! Fu uno dei pionieri del celebre istituto di ricerca di Oberwolfach.

Per una rassegna della teoria estremale degli insiemi rimandiamo a Frankl (1988). La breve dimostrazione del teorema di Erdős–Ko–Rado è dovuta a Katona (1974). Il teorema 6.5 è dovuto a Kleitman e Spencer (1973) e a Schönheim (1971). La dimostrazione del teorema 6.6 è di Greene, Katona e Kleitman (1976).

Riferimenti bibliografici

B. Bollobás (1973)
Sperner systems consisting of pairs of complementary subsets, *J. Combinatorial Theory (A)* **15**, 363–366.

N. G. de Bruijn, C. van Ebbenhorst Tengbergen e D. Kruyswijk (1949)
On the set of divisors of a number, *Nieuw Archief v. Wisk.* (2) **23**, 191–193.

R. P. Dilworth (1950)
A decomposition theorem for partially ordered sets, *Annals of Math.* (2) **51**, 161–166.

P. Erdős, Chao Ko e R. Rado (1961)
Extremal problems among subsets of a set, *Quart. J. Math. Oxford Ser.* (2) **12**, 313–318.

P. Frankl (1988)
Old and new problems on finite sets, *Proc. Nineteenth S. E. Conf. on Combinatorics, Graph Th. and Computing*, Baton Rouge, 1988.

C. Greene, G. Katona e D. J. Kleitman (1976)
Extensions of the Erdős–Ko–Rado theorem, *Stud. Appl. Math.* **55**, 1–8.

Orig. 60

G. O. H. Katona (1974)
Extremal problems for hypergraphs, in *Combinatorics*, a cura di M. Hall, Jr. e J. H. van Lint, Reidel.

D. J. Kleitman e J. Spencer (1973)
Families of k-independent sets, *Discrete Math.* **6**, 255–262.

D. Lubell (1966)
A short proof of Sperner's lemma, *J. Combinatorial Theory* **1**, 299.

L. Mirsky (1971)
A dual of Dilworth's decomposition theorem, *Amer. Math. Monthly* **78**, 876–877.

J. Schönheim (1971)
A generalization of results of P. Erdős, G. Katona, and D. J. Kleitman concerning Sperner's theorem, *J. Combinatorial Theory (A)* **11**, 111–117.

E. Sperner (1928)
Ein Satz über Untermengen einer endlichen Menge, *Math. Zeitschrift* **27**, 544–548.

H. Tverberg (1967)
On Dilworth's decomposition theorem for partially ordered sets, *J. Combinatorial Theory* **3**, 305–306.

Capitolo 7

Flussi nelle reti

Orig. 61

Per *rete di trasporto* intendiamo un grafo orientato finito D con due vertici distinti s e t, chiamati rispettivamente *sorgente* e *pozzo*, dotato di una funzione c che associa a ogni spigolo e un numero reale non negativo $c(e)$, detto *capacità*. Possiamo inoltre supporre che non vi siano cappi né spigoli multipli, che nessuno spigolo entri nella sorgente s e che nessuno esca dal pozzo t. Ammettere tali spigoli non causerebbe difficoltà sostanziali, ma richiederebbe qualche attenzione in più in un paio di definizioni.

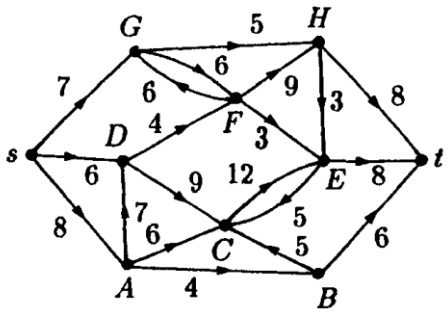


Figura 7.1

La figura 7.1 dà un esempio. Possiamo pensare a una rete di tubi nei quali un liquido scorra nel verso delle frecce: la capacità indica il massimo flusso possibile per unità di tempo in quel tratto di tubo.

Un *flusso* in una rete di trasporto è una funzione f che assegna a ogni spigolo e un numero reale $f(e)$ tale che:

(a) $0 \le f(e) \le c(e)$ per ogni spigolo e (*ammissibilità*);

(b) per ogni vertice x diverso da sorgente e pozzo, la somma dei valori di f sugli spigoli entranti sia uguale alla somma sui suoi spigoli uscenti (*conservazione del flusso*). Orig. 62

La somma dei valori di f sugli spigoli uscenti dalla sorgente si chiama *valore* del flusso e si indica con $|f|$. Sembra evidente che essa coincida con la somma dei valori di f sugli spigoli entranti nel pozzo; il lettore può provare a verificarlo formalmente prima di proseguire.

Uno dei nostri obiettivi è trovare un metodo per costruire un *flusso massimo*, cioè un flusso di valore massimo. Prima di iniziare è utile avere un traguardo, o un limite superiore per il valore di un flusso: per esempio, la somma delle capacità di tutti gli spigoli uscenti dalla sorgente è chiaramente un tale limite. Più in generale, un *taglio che separa s e t*, o semplicemente *taglio*, è una coppia (X, Y) di sottoinsiemi che partizionano $V := V(D)$, con $s \in X$ e $t \in Y$. La sua *capacità* $c(X, Y)$ è la somma delle capacità degli spigoli diretti da X a Y, cioè degli spigoli $e = (x, y)$ con $x \in X$ e $y \in Y$. Affermiamo che la capacità di qualsiasi taglio è un limite superiore al valore di qualsiasi flusso. Più precisamente, la legge di conservazione implica, come vedremo, che

$$|f| = f(X, Y) - f(Y, X), \tag{7.1}$$

dove $f(A, B)$ è la somma dei valori di f sugli spigoli diretti da A a B. Dall'ammissibilità segue subito $|f| \le c(X, Y)$. Quindi la capacità minima fra tutti i tagli di una rete, pari a 20 nell'esempio della figura 7.1, è un limite superiore al valore dei flussi nella rete.

Per dimostrare la (7.1), introduciamo la funzione ϕ ponendo, per ogni coppia (x, e) con x incidente con e, $\phi(x, e) := -1$ se lo spigolo è entrante e $\phi(x, e) := +1$ se è uscente; se x non è incidente con e, poniamo $\phi(x, e) = 0$. Osserviamo che ϕ è essenzialmente la matrice di incidenza del grafo orientato; si veda il capitolo 36. La conservazione equivale a $\sum_{e\in E} \phi(x, e)f(e) = 0$ per $x \neq s, t$. La somma $\sum_{x\in X} \phi(x, e)$ è $+1$ se e va da X a Y, -1 se va da Y a X, e 0 se ha entrambi gli estremi nella stessa parte. Pertanto Orig. 63

$$\begin{aligned} |f| &= \sum_{e\in E} \phi(s, e)f(e) = \sum_{x\in X} \sum_{e\in E} \phi(x, e)f(e) \\ &= \sum_{e\in E} f(e) \sum_{x\in X} \phi(x, e) = f(X, Y) - f(Y, X). \end{aligned}$$

Nella prima somma doppia la somma interna è nulla per ogni x diverso da s.

Un caso particolare della (7.1) è $|f| = f(V \setminus \{t\}, \{t\})$, l'affermazione sulla quale avevamo invitato il lettore a riflettere.

Costruiamo ora i flussi. Fissiamo un flusso f, eventualmente nullo. Una successione x_0, x_1, …, x_{k-1}, x_k di vertici distinti si chiama *cammino speciale* da x_0 a x_k se, per ogni i, $1 \leq i \leq k$, vale almeno una delle condizioni:

(i) $e = (x_{i-1}, x_i)$ è uno spigolo con $c(e) - f(e) > 0$;

(ii) $e = (x_i, x_{i-1})$ è uno spigolo con $f(e) > 0$.

Uno spigolo e con $f(e) = c(e)$ si dice *saturo*. Le due condizioni richiedono che gli spigoli percorsi «in avanti» non siano saturi e quelli percorsi «all'indietro» abbiano flusso positivo, sempre rispetto a f. Supponiamo che esista un tale cammino da s a t. Definiamo α_i come $c(e) - f(e)$ nel primo caso e come $f(e)$ nel secondo, scegliendo uno spigolo se entrambi i casi si verificano; sia α il minimo di questi numeri positivi. Aumentiamo di α il flusso su ogni spigolo di tipo (i) e lo diminuiamo di α su ogni spigolo di tipo (ii). Si verifica facilmente che ammissibilità e conservazione rimangono soddisfatte. Il nuovo flusso ha valore $|f| + \alpha$.

L'idea diventa un algoritmo se la iteriamo, partendo dal flusso nullo, e incorporiamo una procedura sistematica per cercare cammini speciali da s a t rispetto al flusso corrente. Nelle note discuteremo brevemente la terminazione. Ma che cosa accade quando non si può più proseguire?

Supponiamo che rispetto a un flusso f_0 non esista alcun cammino speciale dalla sorgente al pozzo. Sia X_0 l'insieme dei vertici raggiungibili da s mediante un cammino speciale e Y_0 quello dei vertici rimanenti. Otteniamo un taglio. Se $x \in X_0$, $y \in Y_0$ ed $e = (x, y)$ è uno spigolo, esso deve essere saturo: altrimenti aggiungendo y a un cammino speciale da s a x ne otterremmo uno da s a y, contro la definizione delle due parti. Se invece $e = (y, x)$ è uno spigolo, per una ragione analoga deve essere $f_0(e) = 0$. Dalla (7.1) segue Orig. 64

$$|f_0| = f_0(X_0, Y_0) - f_0(Y_0, X_0) = c(X_0, Y_0).$$

Non soltanto il metodo dei cammini speciali non può produrre un flusso di valore maggiore: nessun flusso di valore maggiore esiste, perché $|f| \leq c(X_0, Y_0)$ per ogni f.

Se scegliamo f_0 massimo, la cui esistenza segue dalla continuità se non siamo certi della terminazione dell'algoritmo, non esistono certamente cammini speciali da s a t. Il taglio costruito (X_0, Y_0) è minimo, cioè di capacità minima, poiché $c(X, Y) \geq |f_0|$ per ogni taglio. Abbiamo così dimostrato il celebre teorema di Ford e Fulkerson (1956).

Teorema 7.1. In una rete di trasporto, il massimo valore di $|f|$ fra tutti i flussi f è uguale al minimo valore di $c(X, Y)$ fra tutti i tagli (X, Y).

Questo è solitamente chiamato *teorema del flusso massimo e del taglio minimo*. La procedura di incremento del flusso usata sopra dimostra qualcosa di più.

Teorema 7.2. Se tutte le capacità di una rete di trasporto sono intere, esiste un flusso massimo f tale che tutti i valori $f(e)$ siano interi.

Dimostrazione. Partiamo dal flusso nullo. L'argomento precedente permette di aumentarne il valore fino a raggiungere un massimo. A ogni passo α è intero, quindi anche il nuovo flusso ha valori interi. □

Problema 7A. Costruite un flusso massimo per la rete di trasporto della figura 7.1.

Problema 7B. Un *flusso elementare* è un flusso ottenuto assegnando un valore positivo costante α agli spigoli di un cammino semplice orientato da s a t e zero a tutti gli altri. Mostrate che ogni flusso è somma Orig. 65

di flussi elementari e, eventualmente, di un flusso di valore zero. Questo significa che si può raggiungere un flusso massimo partendo da quello nullo e usando soltanto cammini speciali con spigoli «in avanti». Date un esempio di una rete e di un flusso non massimo rispetto al quale non esistano cammini speciali formati soltanto da spigoli «in avanti».

Problema 7C. Siano (X_1, Y_1) e (X_2, Y_2) tagli minimi in una rete. Mostrate che anche $(X_1 \cup X_2, Y_1 \cap Y_2)$ è un taglio minimo. Si può procedere direttamente dalle definizioni oppure usare un argomento basato sui flussi massimi.

Problema 7D. Dedurre il teorema dei matrimoni di P. Hall, teorema 5.1, dai teoremi 7.1 e 7.2.

L'argomento di questo capitolo ha evidentemente grande importanza pratica. Gli schemi di instradamento di prodotti di ogni genere dipendono da algoritmi che producono flussi ottimali nelle reti di trasporto. Non approfondiremo gli aspetti algoritmici; mostreremo invece una bella applicazione del teorema 7.2 a un problema legato al teorema di Birkhoff, teorema 5.5. Prima dell'enunciato e della dimostrazione, osserviamo che vari tentativi di ridurre il risultato al teorema 5.5 non ebbero successo. La dimostrazione seguente è dovuta ad A. Schrijver. Se $b = v$ nel teorema 7.3, siamo nella situazione del teorema 5.5.

Teorema 7.3. Sia A una matrice $(0,1)$ di dimensioni $b \times v$, con k elementi uguali a 1 per riga e r per colonna, cosicché $bk = vr$. Sia α razionale, con $0 < \alpha < 1$, tale che $k' = \alpha k$ e $r' = \alpha r$ siano interi. Esiste allora una matrice $(0,1)$ A' di dimensioni $b \times v$, con k' elementi uguali a 1 per riga e r' per colonna, tale che $a'_{ij} = 1$ soltanto quando $a_{ij} = 1$. In altre parole, A' si ottiene da A cambiando alcuni 1 in 0.

Dimostrazione. Costruiamo una rete con vertici s, la sorgente, $x_1, \ldots, x_b$, corrispondenti alle righe di A, $y_1, \ldots, y_v$, corrispondenti alle colonne, e t, il pozzo. Gli spigoli sono (s, x_i) di capacità k, per $1 \le i \le b$; (x_i, y_j) di capacità 1 se e solo se $a_{ij} = 1$; e (y_j, t) di capacità r, per $1 \le j \le v$. La definizione garantisce un flusso massimo che satura tutti gli spigoli. Modifichiamo le capacità degli spigoli uscenti dalla sorgente portandole a k', e quelle degli spigoli entranti nel pozzo portandole a r'. Tutte le capacità sono ancora intere, ed esiste chiaramente un flusso massimo con $f((x_i, y_j)) = \alpha$. Per il teorema 7.2 esiste anche un flusso massimo f^* a valori interi, dunque con $f^*((x_i, y_j))$ uguale a 0 oppure a 1. Da esso ricaviamo immediatamente la matrice A' richiesta. □ Orig. 66

Il risultato può essere generalizzato in vari modi con essenzialmente la stessa idea; più avanti vedremo un approccio leggermente diverso.

Per alcune applicazioni combinatorie è comodo il teorema seguente, che non richiede capacità né il concetto di valore del flusso. Si può dedurre dal teorema 7.2, si veda Ford e Fulkerson (1956), ma preferiamo darne una dimostrazione diretta.

Una *circolazione* su un digrafo D è un'applicazione $f : E(D) \to \mathbb{R}$ che soddisfa la conservazione del flusso in ogni vertice. Non richiediamo che sia non negativa. Le circolazioni si identificano con i vettori del nucleo della matrice di incidenza del digrafo.

Teorema 7.4. Sia f una circolazione su un digrafo finito D. Esiste una circolazione intera g tale che, per ogni spigolo e, $g(e)$ sia uguale a $\lfloor f(e) \rfloor$ oppure a $\lceil f(e) \rceil$.

Possiamo dire che i valori di g si ottengono da quelli di f «arrotondando per eccesso o per difetto». Se $f(e)$ è già intero, naturalmente $g(e) = f(e)$.

Dimostrazione. Data f, consideriamo una circolazione g che soddisfi

$$\lfloor f(e) \rfloor \le g(e) \le \lceil f(e) \rceil \tag{7.2}$$

e per la quale il numero degli spigoli e con $g(e)$ intero sia massimo fra le circolazioni che soddisfano la (7.2).

Sia H il sottografo ricoprente di D formato dagli spigoli per i quali $g(e)$ non è intero, cioè per i quali entrambe le disuguaglianze della (7.2) sono strette. La conservazione implica che nessun vertice di H abbia grado 1; se g non è intera, H contiene quindi un poligono.

Sia P un poligono di H e percorriamolo con un cammino semplice chiuso. Siano A gli spigoli di P percorsi in avanti rispetto all'orientamento di D e B quelli percorsi all'indietro. Per ogni costante c otteniamo una nuova circolazione ponendo Orig. 67

$$g'(e) := \begin{cases} g(e) + c, & e \in A, \\ g(e) - c, & e \in B, \\ g(e), & e \notin E(P). \end{cases}$$

Se c è piccolo, la (7.2) vale ancora con g' al posto di g. Scegliamo ora

$$c := \min\left\{\min_{e\in A}\big(\lceil f(e)\rceil - g(e)\big),\ \min_{e\in B}\big(g(e) - \lfloor f(e)\rfloor\big)\right\}.$$

Allora g' soddisfa ancora la (7.2), ma assume un valore intero su almeno uno spigolo in più, precisamente su ogni spigolo che realizza quel minimo. Se g non fosse intera, questo contraddirebbe la sua scelta. □

Corollario. Sia f una circolazione intera su un digrafo finito D e sia d un intero positivo. Si può scrivere $f = g_1 + g_2 + \cdots + g_d$, dove ogni g_j è una circolazione intera e, per ogni j e ogni spigolo e,

$$\lfloor f(e)/d\rfloor \le g_j(e) \le \lceil f(e)/d\rceil. \tag{7.3}$$

Dimostrazione. Per induzione su d. Se $d = 1$, non vi è nulla da provare. Dato $d \ge 2$, applichiamo il teorema 7.4 a f/d e troviamo una circolazione intera g_1 che soddisfa la (7.3) per $j = 1$. Per l'ipotesi induttiva possiamo scrivere

$$f - g_1 = g_2 + g_3 + \cdots + g_d,$$

dove per $j = 2, 3, \ldots, d$ la circolazione intera g_j soddisfa

$$\left\lfloor \frac{f(e) - g_1(e)}{d-1}\right\rfloor \le g_j(e) \le \left\lceil \frac{f(e) - g_1(e)}{d-1}\right\rceil.$$

È un semplice esercizio verificare che, se a è intero e b è $\lfloor a/d\rfloor$ oppure $\lceil a/d\rceil$, allora

$$\left\lfloor \frac{a}{d}\right\rfloor \le \left\lfloor \frac{a-b}{d-1}\right\rfloor, \qquad \left\lceil \frac{a-b}{d-1}\right\rceil \le \left\lceil \frac{a}{d}\right\rceil.$$

Le disuguaglianze precedenti implicano dunque la (7.3) per $j = 2, 3, \ldots, d$. □ Da una matrice Orig. 68
A di dimensioni $m \times n$ con elementi reali a_{ij}, non necessariamente non negativi o interi, otteniamo una circolazione su un digrafo con $m + n + 2$ vertici e $mn + m + n + 1$ spigoli. Il digrafo è simile a quello usato nella dimostrazione del teorema 7.3. Vi sono vertici $x_1, \ldots, x_m$ corrispondenti alle righe, vertici $y_1, \ldots, y_n$ corrispondenti alle colonne e altri due vertici s e t. Vi è uno spigolo da x_i a y_j con valore della circolazione a_{ij}, uno da s a x_i con valore pari alla somma r_i della riga i, uno da y_j a t con valore pari alla somma k_j della colonna j, per $i = 1, \ldots, m$ e $j = 1, \ldots, n$, e uno da t a s con valore pari alla somma di tutti gli elementi di A.[1] Moltiplicando la circolazione f per uno scalare α, applicando il teorema 7.4 ad αf e reinterpretando la circolazione intera come matrice, otteniamo la parte (i) del teorema seguente. La parte (ii) segue dal corollario.

Teorema 7.5. (i) Dati una matrice A e un numero reale α, esiste una matrice intera B tale che gli elementi, le somme delle righe, le somme delle colonne e la somma di tutti gli elementi di B siano i corrispondenti valori di αA arrotondati per eccesso o per difetto.

(ii) Se A è una matrice intera e d un intero positivo, allora

$$A = B_1 + B_2 + \cdots + B_d,$$

dove ogni B_i è intera e i suoi elementi, le somme delle righe, le somme delle colonne e la somma di tutti gli elementi sono i corrispondenti valori di $(1/d)A$ arrotondati per eccesso o per difetto.

Problema 7E. Mostrate che dal teorema 7.5 si deducono rapidamente: (i) il problema 5A(iii); (ii) il teorema 5.5; (iii) il teorema 7.3; (iv) un grafo finito con tutti i gradi pari ammette un orientamento *bilanciato*, nel quale grado entrante e uscente di ogni vertice coincidono; (v) se un grafo bipartito ha grado minimo $\underline{d}$ e grado massimo $\overline{d}$, se ne possono colorare gli spigoli con $\overline{d}$ colori in modo che i colori incidenti con ogni vertice siano distinti, e con $\underline{d}$ colori in modo che tutti i colori compaiano in ogni vertice.

Problema 7F. Mostrate che lo spazio vettoriale delle circolazioni su un digrafo connesso D ha dimensione $|E(D)| - |V(D)| + 1$. Orig. 69

[1] Nota redazionale: in quest'ultima occorrenza l'originale scrive M anziché A.

Note

Si usa spesso il termine *cammino aumentante* al posto di cammino speciale.

Se le capacità sono intere, il metodo dei cammini speciali termina dopo un numero finito di iterazioni, perché il valore aumenta ogni volta di almeno uno. Ma Ford e Fulkerson (1962) danno un esempio con capacità irrazionali nel quale scelte appositamente costruite dei cammini speciali producono una successione infinita di flussi i cui valori convergono soltanto a un quarto del massimo effettivo! Se invece si scelgono con cura cammini speciali di lunghezza minima, si può dimostrare che si raggiunge un flusso massimo dopo al più $O(n^3)$ iterazioni, dove n è il numero dei vertici. Si veda Edmonds e Karp (1972).

Trovare un flusso massimo è un problema di programmazione lineare e può essere risolto, per esempio, con l'algoritmo del simplesso. Il caso delle reti è particolare perché la sua matrice è totalmente unimodulare; questo è un modo di spiegare il teorema 7.2. Per approfondire la programmazione lineare e intera si vedano i riferimenti. I metodi grafici sono di solito più rapidi del simplesso e forniscono ulteriori intuizioni.

In topologia algebrica le circolazioni su un digrafo si chiamano *1-cicli*. Un analogo del teorema 7.4 vale per vettori f nel nucleo di una qualsiasi matrice totalmente unimodulare.

I teoremi 7.1, 7.2, 7.4 e l'algoritmo hanno molte altre applicazioni combinatorie, perché certi problemi possono essere formulati in termini di reti di trasporto. Per esempio, trovare un accoppiamento massimo in un grafo bipartito equivale a trovare un flusso massimo intero in una rete associata; si vedano i riferimenti. Esiste dunque un buon algoritmo per trovare un accoppiamento massimo. Daremo altre applicazioni nel capitolo 16, a un problema di esistenza di matrici $(0, 1)$, e nel capitolo 38, a un problema sulle partizioni di insiemi.

Riferimenti bibliografici

J. Edmonds e R. M. Karp (1972)
Theoretical improvements in algorithm efficiency for network flow problems, *J. Assn. for Computing Machinery* **19**, 248–264.

Orig. 70

L. R. Ford, Jr. e D. R. Fulkerson (1962)
Flows in Networks, Princeton University Press.

T. C. Hu (1969)
Integer Programming and Network Flows, Addison-Wesley.

V. Chvátal (1983)
Linear Programming, W. H. Freeman.

Capitolo 8

Successioni di De Bruijn

Il problema seguente ha un'origine pratica: il cosiddetto problema del tamburo rotante. Consideriamo un tamburo rotante come nella figura 8.1. Orig. 71

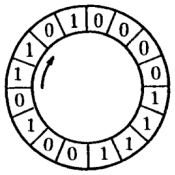


Figura 8.1

Ogni segmento è di uno di due tipi, indicati con 0 e 1. Vogliamo che quattro segmenti consecutivi qualsiasi determinino univocamente la posizione del tamburo. Ciò significa che le 16 possibili quadruple consecutive di 0 e 1 sul tamburo devono essere le rappresentazioni binarie degli interi da 0 a 15. È possibile? E, in caso affermativo, in quanti modi diversi? È facile rispondere alla prima domanda. Entrambe furono trattate da N. G. de Bruijn (1946); per questa ragione i grafi descritti qui sotto e le corrispondenti successioni circolari di 0 e 1 sono spesso chiamati, rispettivamente, *grafi di De Bruijn* e *successioni di De Bruijn*.

Consideriamo un grafo orientato (che chiameremo più avanti G_4) i cui vertici sono tutte le terne di 0 e 1, ossia le parole binarie di tre bit, e colleghiamo il vertice $x_1x_2x_3$ mediante un arco orientato a x_2x_30 e a x_2x_31. L'arco $(x_1x_2x_3, x_2x_3x_4)$ è numerato e_j, dove $x_1x_2x_3x_4$ è la rappresentazione binaria dell'intero j. Il grafo ha un cappio in 000 e uno in 111. Come abbiamo già visto, esso possiede un circuito euleriano, perché ogni vertice ha grado entrante 2 e grado uscente 2. Un tale cammino chiuso produce la successione di 16 bit richiesta per il tamburo. Una successione circolare di questo tipo si chiama *successione di De Bruijn*. Per esempio, il cammino Orig. 72

$$000 \to 000 \to 001 \to 011 \to 111 \to 111 \to 110 \to 100 \to 001$$
$$\to 010 \to 101 \to 011 \to 110 \to 101 \to 010 \to 100 \to 000$$

corrisponde a 0000111100101101, da leggere circolarmente. Chiameremo un tale cammino *ciclo completo*.

Definiamo, in modo analogo, G_n come il grafo orientato sulle $(n-1)$-uple di 0 e 1. Dunque G_n ha 2^n spigoli. Il grafo G_4 è rappresentato nella figura 8.2. In questo capitolo chiameremo *grafo 2-entrante 2-uscente* un grafo orientato nel quale ogni vertice ha grado entrante 2 e grado uscente 2. Per un tale grafo G definiamo il grafo «raddoppiato» G^* nel modo seguente:

(i) a ogni spigolo di G corrisponde un vertice di G^*;

(ii) se a e b sono vertici di G^*, vi è uno spigolo da a a b se e solo se l'estremo finale (testa) dello spigolo di G corrispondente ad a coincide con l'estremo iniziale (coda) dello spigolo corrispondente a b.

Chiaramente $G_n^* = G_{n+1}$.

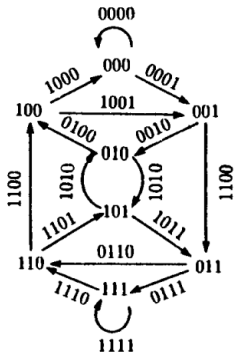


Figura 8.2

Teorema 8.1. Sia G un grafo 2-entrante 2-uscente con m vertici e M cicli completi. Allora G^* ha $2^{m-1}M$ cicli completi.

Dimostrazione. Procediamo per induzione su m.

(a) Se $m = 1$, G ha un unico vertice p e due cappi da p a p. Allora $G^* = G_2$, che ha un solo ciclo completo. (b) Possiamo supporre che G sia connesso. Se G ha m vertici e vi è un cappio in ogni vertice, allora, a parte questi cappi, G è un circuito $p_1 \to p_2 \to \cdots \to p_m \to p_1$. Siano A_i il cappio $p_i \to p_i$ e B_i l'arco $p_i \to p_{i+1}$. Indicheremo sempre i vertici corrispondenti di G^* con lettere minuscole. La situazione in G^* è illustrata nella figura 8.3. Orig. 73

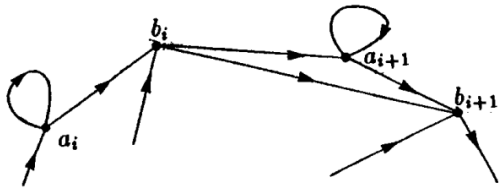


Figura 8.3

Chiaramente, in G^* un ciclo ha due modi di andare da b_i a b_{i+1}. Quindi G^* ha 2^{m-1} cicli completi, mentre G ne ha soltanto uno.

(c) Supponiamo ora che G abbia un vertice x privo di cappio. La situazione è quella della figura 8.4, dove P, Q, R, S sono spigoli distinti di G, benché alcuni dei vertici a, b, c, d possano coincidere.

Da G formiamo un nuovo grafo 2-entrante 2-uscente con un vertice in meno eliminando x. Possiamo farlo in due modi: G_1 si ottiene identificando $P = R$, $Q = S$, mentre G_2 si ottiene identificando $P = S$, $Q = R$. Per l'ipotesi induttiva, il teorema vale per G_1 e per G_2.

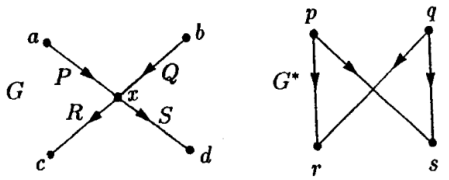


Figura 8.4

Vi sono tre tipi diversi di ciclo completo in G^*, a seconda che i due cammini che escono da r e ritornano a p oppure a q vadano entrambi a p, entrambi a q, oppure uno a p e uno a q. Trattiamo un caso; gli altri due sono analoghi e vengono lasciati al lettore. Nella figura 8.5 il cammino 1 va da r a p, il 2 da s a q, il 3 da s a p e il 4 da r a q. Orig. 74

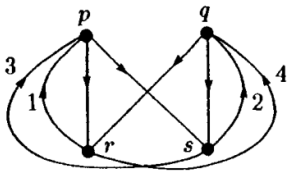


Figura 8.5

Essi danno i seguenti quattro cicli completi di G^*:

$$\begin{array}{cccccccc} 1, & pr, & 4, & qs, & 3, & ps, & 2, & qr \\ 1, & ps, & 2, & qr, & 4, & qs, & 3, & pr \\ 1, & ps, & 3, & pr, & 4, & qs, & 2, & qr \\ 1, & ps, & 2, & qs, & 3, & pr, & 4, & qr. \end{array}$$

In G_1^* e G_2^* la situazione si riduce alla figura 8.6.

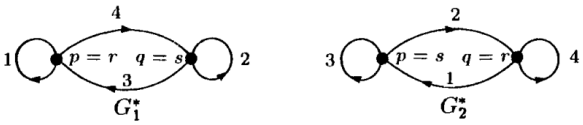


Figura 8.6

In ciascuno di G_1^* e G_2^* è possibile un solo ciclo completo che utilizzi i cammini 1, 2, 3, 4. Anche nei due casi rimanenti troviamo due cicli completi in G_1^* e G_2^* corrispondenti a quattro cicli completi in G^*. Pertanto il numero di cicli completi di G^* è il doppio della somma dei numeri corrispondenti per G_1^* e G_2^*. D'altra parte, il numero di cicli completi di G è chiaramente uguale alla somma dei numeri corrispondenti per G_1 e G_2. Il teorema segue quindi dall'ipotesi induttiva. □

Possiamo ora rispondere alla domanda sul numero di cicli completi di un grafo di De Bruijn.

Orig. 75

Teorema 8.2. G_n ha esattamente $2^{2^{n-1}-n}$ cicli completi.

DIMOSTRAZIONE. Il teorema è vero per $n = 1$. Poiché $G_n^* = G_{n+1}$, il risultato segue per induzione dal teorema 8.1. □

Per una seconda dimostrazione si veda il capitolo 36.

Problema 8A. Sia α un elemento primitivo di $\mathbb{F}_{2^n}$. Per $1 \le i \le m := 2^n - 1$, sia

$$\alpha^i = \sum_{j=0}^{n-1} c_{ij}\alpha^j.$$

Mostrare che la successione $0, c_{10}, c_{20}, \ldots, c_{m0}$ è una successione di De Bruijn.

Problema 8B. Trovare una successione ternaria circolare, con simboli 0, 1, 2, di lunghezza 27, in modo che ogni possibile terna ordinata ternaria compaia in tre posizioni consecutive in senso circolare. Disegnare dapprima un opportuno grafo orientato con 9 vertici, i cui circuiti euleriani corrispondano a tali successioni.

Problema 8C. Vogliamo costruire una successione circolare $a_0, \ldots, a_7$ (con indici modulo 8) in modo che una finestra scorrevole a_i, a_{i+1}, a_{i+3}, $i = 0, 1, \ldots, 7$, contenga una volta ciascuna delle possibili terne. Mostrare, senza limitarsi a procedere per tentativi, che ciò è impossibile.

Problema 8D. Sia $m := 2^n - 1$. Un algoritmo per costruire una successione di De Bruijn $a_0, a_1, \ldots, a_m$ funziona nel modo seguente. Si inizia ponendo $a_0 = a_1 = \cdots = a_{n-1} = 0$. Per $k \ge n$, si definisce a_k come il massimo valore in $\{0, 1\}$ per il quale la successione $(a_{k-n+1}, \ldots, a_{k-1}, a_k)$ non sia già comparsa in $(a_0, \ldots, a_{k-1})$ come sottosuccessione di termini consecutivi. La successione risultante è nota come *successione di Ford*. Dimostrare che questo algoritmo produce effettivamente una successione di De Bruijn. [1]

[1] Nota di traduzione: l'originale scrive $k > n$, lasciando così indefinito a_n. Si è esplicitato il limite corretto $k \ge n$.

Note

Benché i grafi di questo capitolo siano comunemente chiamati grafi di De Bruijn, il teorema 8.1 fu dimostrato nel 1894 da C. Flye Sainte-Marie. Il fatto rimase inosservato per molto tempo. Rimandiamo a De Bruijn (1975). N. G. de Bruijn (1918–), uno dei matematici olandesi più noti, lavorò in molti settori, fra cui analisi, teoria dei numeri, combinatoria, informatica e cristallografia. Orig. 76

Segnaliamo una particolarità relativa alla grafia di alcuni cognomi olandesi. Quando si omettono le iniziali di N. G. de Bruijn, si deve scrivere «De» con la maiuscola; inoltre il cognome va ordinato sotto la lettera B. Analogamente, «Van der Waerden» è corretto quando si omettono le iniziali, e il cognome va ordinato sotto la W.

Per una dimostrazione del teorema 8.1 con metodi algebrici rimandiamo al capitolo 36.

Bibliografia

N. G. de Bruijn (1946), A combinatorial problem, *Proc. Kon. Ned. Akad. v. Wetensch.* **49**, 758–764.

N. G. de Bruijn (1975), Acknowledgement of priority to C. Flye Sainte-Marie on the counting of circular arrangements of 2^n zeros and ones that show each n-letter word exactly once, T. H. report 75-WSK-06, Eindhoven University of Technology.

C. Flye Sainte-Marie (1894), Solution to question nr. 48, *Intermédiaire des Mathématiciens* **1**, 107–110.

Capitolo 9

Due problemi su $(0, 1, *)$: indirizzamento dei grafi e uno schema di codifica hash

Orig. 77

Il problema seguente trae origine dalla teoria delle comunicazioni. In una rete telefonica, prima che i messaggi possano fluire in una delle due direzioni si stabilisce un collegamento fra i terminali A e B. Per una rete di calcolatori è auspicabile poter inviare un messaggio da A a B senza che B sappia che un messaggio sta arrivando. L'idea è di far precedere il messaggio da un «indirizzo» di B tale che, in ciascun nodo della rete, si possa decidere in quale direzione inoltrarlo.

Un tentativo naturale consiste nell'assegnare a ogni vertice di un grafo G un indirizzo binario, per esempio in $\{0,1\}^k$, in modo che la distanza fra due vertici del grafo sia uguale alla cosiddetta *distanza di Hamming* fra i loro indirizzi, cioè al numero di posizioni nelle quali questi differiscono. Ciò equivale a considerare G come un sottografo indotto dell'ipercubo H_k, dove $V(H_k) := \{0,1\}^k$ e due k-uple sono adiacenti quando differiscono in una sola coordinata.[1] Già l'esempio $G = K_3$ mostra che questo non è sempre possibile. Introduciamo allora un nuovo alfabeto $\{0, 1, *\}$ e formiamo gli indirizzi con n-uple su tale alfabeto. Definiamo la distanza fra due indirizzi come il numero di posizioni nelle quali uno ha uno 0 e l'altro un 1: gli asterischi, quindi, non contribuiscono alla distanza. Per un *indirizzamento* di un grafo G richiediamo che la distanza fra due vertici qualsiasi di G coincida con la distanza fra i loro indirizzi. È immediato mostrare che ciò è possibile per n abbastanza grande. Indichiamo con $N(G)$ il minimo valore di n per il quale esiste un indirizzamento di G di lunghezza n. Per un albero possiamo fare a meno degli

Orig. 78

asterischi nel modo seguente. Procediamo per induzione. Per un albero con due vertici esiste un ovvio indirizzamento di lunghezza 1. Supponiamo di saper indirizzare gli alberi con k vertici. Se $x_0, x_1, \ldots, x_k$ sono i vertici dell'albero T e x_0 è un vertice di grado uno, consideriamo un indirizzamento dell'albero ottenuto eliminando x_0. Sia $\mathbf{x}_i$ l'indirizzo di x_i e supponiamo che x_0 sia adiacente a x_1. Sostituiamo tutti gli indirizzi con $(0, \mathbf{x}_i)$, $1 \le i \le k$, e assegniamo a x_0 l'indirizzo $(1, \mathbf{x}_1)$. Chiaramente questo è un indirizzamento di T. Per un albero abbiamo dunque $N(T) \le |V(T)| - 1$.

Come secondo esempio consideriamo K_m. Nella matrice identità di ordine $m - 1$ sostituiamo con asterischi gli zeri sopra la diagonale e aggiungiamo una riga di zeri. Due righe qualsiasi hanno ora distanza 1, perciò $N(K_m) \le m - 1$.

Come terzo esempio consideriamo il grafo della figura 9.1.

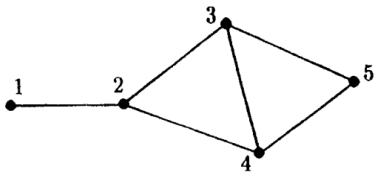


Figura 9.1

[1] Nota di traduzione: per l'equivalenza è necessario che l'immersione nell'ipercubo sia *isometrica*; essere soltanto un sottografo indotto non basta in generale.

Un possibile indirizzamento, benché non ottimale, è

$$\begin{array}{c|ccccc} 1 & 1 & 1 & 1 & * & * \\ 2 & 1 & 0 & * & 1 & * \\ 3 & * & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 1 & * & * \\ 5 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Mostriamo ora una corrispondenza fra gli indirizzamenti di un grafo e le forme quadratiche, dovuta a Graham e Pollak (1971). Consideriamo il grafo G della figura 9.1 e l'indirizzamento appena dato. Alla prima colonna associamo il prodotto $(x_1 + x_2)(x_4 + x_5)$. Qui x_i compare nel primo o nel secondo fattore a seconda che l'indirizzo di i abbia un 1 o uno 0 nella prima colonna. Procedendo nello stesso modo per ogni colonna e sommando i termini, otteniamo una forma quadratica $\sum_{i<j} d_{ij}x_ix_j$, dove d_{ij} è la distanza fra i vertici i e j di G. Un indirizzamento di G corrisponde quindi a scrivere la forma quadratica $\sum_{i<j} d_{ij}x_ix_j$ come somma di n prodotti Orig. 79

$$(x_{i_1} + \cdots + x_{i_k})(x_{j_1} + \cdots + x_{j_l})$$

in cui nessuna variabile x_i compaia in entrambi i fattori. Il numero di variabili è $|V(G)|$.

Teorema 9.1. Siano n_+ e n_- rispettivamente il numero degli autovalori positivi e negativi della matrice delle distanze (d_{ij}) di G. Allora $N(G) \geq \max\{n_+, n_-\}$.

Dimostrazione. Ciascuna delle forme quadratiche appena menzionate si può rappresentare come $\frac{1}{2}\mathbf{x}^\mathsf{T}A\mathbf{x}$, dove $\mathbf{x} := (x_1, x_2, \ldots, x_{|V(G)|})$ e la matrice simmetrica A ha entrata $a_{ij} = 1$ se il termine x_ix_j compare nella forma quadratica, e 0 altrimenti. Una tale matrice ha rango 2 e traccia 0. Ha quindi un autovalore positivo e uno negativo. Poiché (d_{ij}) è la somma delle matrici corrispondenti alle forme quadratiche, essa può avere al più n autovalori positivi e al più n autovalori negativi. □

Teorema 9.2. $N(K_m) = m - 1$.

Dimostrazione. Abbiamo già visto che $N(K_m) \leq m - 1$. La matrice delle distanze di K_m è $J - I$, di ordine m, i cui autovalori sono $m - 1$, con molteplicità 1, e -1, con molteplicità $m - 1$. Il risultato segue dunque dal teorema 9.1. □

Con un po' di lavoro in più mostreremo ora che il più corto indirizzamento di un albero T ha lunghezza $|V(T)| - 1$.

Teorema 9.3. Se T è un albero con n vertici, allora $N(T) = n - 1$.

Dimostrazione. Calcoliamo dapprima il determinante della matrice delle distanze (d_{ij}) di T. Numeriamo i vertici $p_1, \ldots, p_n$ in modo che p_n sia un estremo adiacente a p_{n-1}. Nella matrice delle distanze sottraiamo la riga $n - 1$ dalla riga n, e facciamo lo stesso con le colonne. Tutte le entrate della nuova ultima riga e dell'ultima colonna sono allora 1, salvo l'elemento diagonale, che è -2. Rinumeriamo ora i vertici $p_1, \ldots, p_{n-1}$ in modo che il nuovo vertice p_{n-1} sia un estremo di $T \setminus \{p_n\}$ adiacente a p_{n-2}. Ripetiamo il procedimento per le righe e le colonne di indice $n - 1$ e $n - 2$. Dopo $n - 1$ passi otteniamo il determinante Orig. 80

$$\begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & -2 & 0 & \cdots & 0 \\ 1 & 0 & -2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -2 \end{vmatrix}.$$

Ne ricaviamo il risultato notevole che il determinante D_n della matrice delle distanze di un albero con n vertici soddisfa

$$D_n = (-1)^{n-1}(n-1)2^{n-2},$$

cioè dipende soltanto da $|V(T)|$. Se numeriamo i vertici con il procedimento appena descritto, la sottomatrice principale $k \times k$ nell'angolo superiore sinistro della matrice delle distanze è la matrice delle distanze di un sottoalbero con k vertici. Pertanto la successione $1, D_1, D_2, \ldots, D_n$, dove D_k è il determinante di questa sottomatrice, è

$$1, 0, -1, 4, -12, \ldots, (-1)^{n-1}(n-1)2^{n-2}.$$

Se attribuiamo a 0 segno positivo, questa successione presenta una sola coppia di termini consecutivi dello stesso segno. Per un teorema elementare sulle forme quadratiche, ciò implica che la forma quadratica

corrispondente ha indice positivo 1; quindi (d_{ij}) ha un solo autovalore positivo. Si veda B. W. Jones (1950), teorema 4. Il risultato segue ora dal teorema 9.1. □

La congettura che $N(G) \leq |V(G)| - 1$ per ogni grafo connesso G fu dimostrata da P. Winkler nel 1983. La dimostrazione è costruttiva. Per descrivere l'indirizzamento occorrono alcuni preparativi. Consideriamo il grafo della figura 9.2. Orig. 81

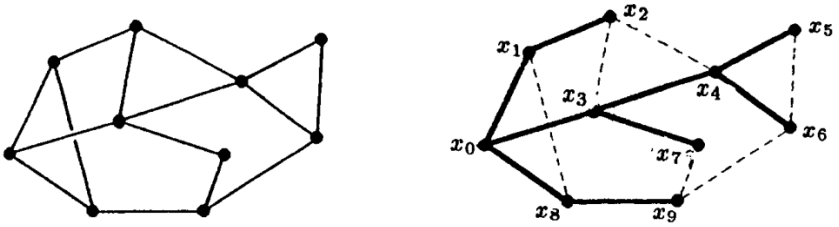


Figura 9.2

Scegliamo un vertice x_0, costruiamo un albero ricoprente T mediante una visita in ampiezza e poi numeriamo i vertici mediante una visita in profondità. Il risultato compare a destra nella figura 9.2, dove gli spigoli di $E(G) \setminus E(T)$ sono tratteggiati.

Sia $n := |V(G)| - 1$. Ci occorrono alcune definizioni. Per $i \leq n$ poniamo

$$P(i) := \{j : x_j \text{ appartiene al cammino da } x_0 \text{ a } x_i \text{ in } T\}.$$

Per esempio, $P(6) = \{0, 3, 4, 6\}$. Poniamo

$$i \wedge j := \max(P(i) \cap P(j)).$$

La situazione generale è descritta nella figura 9.3.

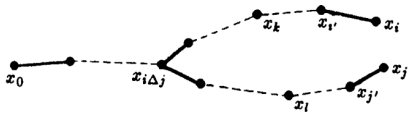


Figura 9.3

Si noti che, nella figura 9.3, $i < j$ se e solo se $k < l$. Per $1 \leq i \leq n$ definiamo

$$i' := \max(P(i) \setminus \{i\}).$$

Per esempio, nella figura 9.2, $7' = 3$. Definiamo

$$i \sim j \quad \Longleftrightarrow \quad P(i) \subseteq P(j) \text{ oppure } P(j) \subseteq P(i).$$

Indichiamo con d_G e d_T le distanze in G e in T, rispettivamente. Definiamo la *funzione di discrepanza* $c(i, j)$ mediante Orig. 82

$$c(i, j) := d_T(x_i, x_j) - d_G(x_i, x_j).$$

Per esempio, nella figura 9.2, $c(6, 9) = 4$.

Lemma 9.4. (i) $c(i, j) = c(j, i) \geq 0$;

(ii) se $i \sim j$, allora $c(i, j) = 0$;

(iii) se $i \not\sim j$, allora $c(i, j') \leq c(i, j) \leq c(i, j') + 2$.

Dimostrazione. (i) è immediato. (ii) segue dalla definizione di T, poiché

$$d_G(x_i, x_j) \geq |d_G(x_j, x_0) - d_G(x_i, x_0)| = d_T(x_i, x_j).$$

(iii) segue da $|d_G(x_i, x_j) - d_G(x_i, x_{j'})| \leq 1$ e da $d_T(x_i, x_j) = 1 + d_T(x_i, x_{j'})$. □

Possiamo ora definire l'indirizzamento. Per $0 \le i \le n$ assegniamo al vertice x_i l'indirizzo $\mathbf{a}_i \in \{0,1,*\}^n$, dove $\mathbf{a}_i = (a_i(1), a_i(2), \ldots, a_i(n))$ e

$$a_i(j) := \begin{cases} 1 & \text{se } j \in P(i), \\ * & \text{se } \begin{cases} c(i,j) - c(i,j') = 2, \text{ oppure} \\ c(i,j) - c(i,j') = 1,\ i < j,\ c(i,j) \text{ pari, oppure} \\ c(i,j) - c(i,j') = 1,\ i > j,\ c(i,j) \text{ dispari,} \end{cases} \\ 0 & \text{altrimenti.} \end{cases}$$

Teorema 9.5. $d(\mathbf{a}_i, \mathbf{a}_k) = d_G(x_i, x_k)$.

Dimostrazione. Possiamo supporre $i < k$.

(i) Supponiamo $i \sim k$. Allora $d_G(x_i, x_k) = |P(k) \setminus P(i)|$. I valori $j \in P(k) \setminus P(i)$ sono precisamente le posizioni in cui $a_k(j) = 1$, $a_i(j) \neq 1$. Per tali valori di j abbiamo $c(i,j) = 0$, dunque $a_i(j) = 0$, e la tesi è dimostrata.

(ii) Il caso difficile è $i \not\sim k$. L'osservazione chiave è la seguente. Sia $n_1 \le n_2 \le \cdots \le n_l$ una successione non decrescente di interi tale che $|n_{i+1} - n_i| \le 2$ per ogni i. Se un intero pari m, compreso fra n_1 e n_l, non compare nella successione, esiste un i per cui $n_i = m-1$, $n_{i+1} = m+1$. Consideriamo ora la successione Orig. 83

$$c(i,k) \ge c(i,k') \ge c(i,k'') \ge \cdots \ge c(i, i \wedge k) = 0.$$

Per la definizione di $a_i(j)$ e per l'osservazione precedente, le condizioni $a_i(j) = *$ e $a_k(j) = 1$ si verificano tante volte quanti sono gli interi pari fra $c(i, i \wedge k)$ e $c(i,k)$. Analogamente, $a_k(j) = *$ e $a_i(j) = 1$ si verificano tante volte quanti sono gli interi dispari fra $c(i, i \wedge k)$ e $c(i,k)$. Qui si contano gli interi strettamente maggiori di 0 e non maggiori di $c(i,k)$. Quindi

$$\begin{aligned} d(\mathbf{a}_i, \mathbf{a}_k) &= |P(k) \setminus P(i)| + |P(i) \setminus P(k)| - c(i,k) \\ &= d_T(x_i, x_k) - c(i,k) = d_G(x_i, x_k). \end{aligned}$$

□

Abbiamo dunque dimostrato il seguente teorema.

Teorema 9.6. $N(G) \le |V(G)| - 1$.

Problema 9A. Applicando lo schema appena definito, quali sono gli indirizzi di x_2 e x_6 nella figura 9.2?

Problema 9B. Sia G un ciclo, cioè un poligono, con $2n$ vertici. Determinare $N(G)$.

Problema 9C. Sia G un ciclo con $2n+1$ vertici. Dimostrare che $N(G) = 2n$. Suggerimento: se C_k è la matrice di permutazione con $c_{ij} = 1$ se e solo se $j - i \equiv 1 \pmod k$ e $\zeta^k = 1$, allora $(1, \zeta, \zeta^2, \ldots, \zeta^{k-1})$ è un autovettore di C_k.

* * *

Consideriamo ora un secondo problema riguardante k-uple sull'alfabeto $\{0,1,*\}$. Gli oggetti che studieremo furono introdotti da Rivest (1974), che diede loro il nome, poco felice, di *disegni a blocchi associativi*; per i disegni a blocchi si veda il capitolo 19. Un ABD(k,w) è un insieme di $b := 2^w$ elementi di $\{0,1,*\}^k$ con le proprietà seguenti: disponendo gli elementi come righe di una matrice C di dimensione $b \times k$, si ha (i) ogni riga di C contiene $k-w$ asterischi; Orig. 84

(ii) ogni colonna di C contiene $b(k-w)/k$ asterischi;

(iii) due righe distinte qualsiasi hanno distanza almeno 1.

Si noti che la definizione implica che ogni vettore di $\mathbb{F}_2^k$ ha distanza 0 da una e una sola riga di C.

Il problema nasce nel modo seguente. Consideriamo un archivio di parole binarie di k bit. Ogni successione di $\{0,1,*\}^k$ si chiama *interrogazione a corrispondenza parziale*. Il problema del recupero per corrispondenza parziale consiste nell'estrarre dall'archivio tutte le parole che concordano con l'interrogazione nelle posizioni in cui essa specifica un bit. I cosiddetti schemi di *codifica hash* dividono un archivio in b liste disgiunte $L_1, L_2, \ldots, L_b$. Un record $\mathbf{x}$ viene memorizzato nella lista di indice $h(\mathbf{x})$, dove h è la

funzione hash da $\{0,1\}^k$ su $\{1,2,\dots,b\}$. Per una data interrogazione a corrispondenza parziale occorre esaminare alcune delle liste. L'analisi del numero di liste da esaminare nel caso peggiore condusse al concetto di ABD. In questo caso $h(\mathbf{x})$ è l'indice dell'unica riga di C che ha distanza 0 da $\mathbf{x}$.

Esempio 9.1. La matrice seguente è un ABD(4, 3):

$$\begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 1 & 0 \\ 0 & 0 & * & 1 \\ 0 & 1 & 0 & * \\ & 1 & 1 & 1 \\ 1 & * & 0 & 1 \\ 1 & 1 & * & 0 \\ 1 & 0 & 1 & * \end{pmatrix}.$$

Dimostriamo dapprima alcune proprietà elementari di un ABD.

Teorema 9.7. Se esiste un ABD(k, w), allora:

(1) ogni sua colonna contiene esattamente $bw/(2k)$ zeri e $bw/(2k)$ uni;

(2) per ogni $\mathbf{x} \in \mathbb{F}_2^k$, esistono esattamente $\binom{w}{u}$ righe che concordano con $\mathbf{x}$ in u posizioni;

(3) i parametri soddisfano $w^2 \geq 2k(1 - 1/b)$; (4) per ogni riga, il numero di righe che hanno gli asterischi nelle medesime posizioni è pari. Orig. 85

Dimostrazione. Sia C l'ABD(k, w).

(1) Una riga di C che ha un asterisco, oppure uno zero, nella colonna j rappresenta, cioè ha distanza 0 da, rispettivamente 2^{k-w-1} oppure 2^{k-w} vettori binari con coordinata j nulla.[2] Dalle proprietà (i) e (ii) della definizione segue che la colonna j deve contenere $bw/(2k)$ zeri.

(2) Sia $\mathbf{x} \in \mathbb{F}_2^k$. Indichiamo con n_i il numero di righe di C che concordano con $\mathbf{x}$ in i posizioni. Vi sono $\binom{k}{l}$ vettori di $\mathbb{F}_2^k$ che concordano con $\mathbf{x}$ in esattamente l posizioni. Pertanto

$$\binom{k}{l} = \sum_i n_i \binom{k-w}{l-i}, \qquad \text{ossia} \qquad (1+z)^k = (1+z)^{k-w} \sum_i n_i z^i.$$

Questo dimostra che $n_i = \binom{w}{i}$.

(3) Per (1), la somma delle distanze fra le coppie di righe di C è $k\big(bw/(2k)\big)^2$. Poiché due righe qualsiasi hanno distanza almeno 1, tale somma è almeno $\binom{b}{2}$.

(4) Consideriamo una riga di C e contiamo i vettori di $\mathbb{F}_2^k$ che hanno zeri nelle posizioni in cui la riga ha asterischi. Ogni riga con una diversa disposizione degli asterischi rappresenta un numero pari di tali vettori, mentre ogni riga con la stessa disposizione ne rappresenta esattamente uno. □

Si noti che la proprietà (1) del teorema 9.7 implica che una condizione necessaria per l'esistenza di un ABD(k, w) è che k divida $w\,2^{w-1}$.[3]

Il seguente rafforzamento del teorema 9.7(3) è dovuto ad A. E. Brouwer (1999).

Teorema 9.8. Sia C un ABD(k, w) con $w > 3$.

(1) Se due righe di C concordano in tutte le posizioni tranne una, allora $\binom{w}{2} \geq k$;

(2) altrimenti $w^2 > 2k$. Orig. 86

Dimostrazione. Supponiamo che $\mathbf{c}_1$ e $\mathbf{c}_2$ siano due righe di C che differiscono soltanto nella prima posizione. Allora ogni altra riga di C deve differire da $\mathbf{c}_1$ in qualche altra posizione. Per (i) della definizione e per il teorema 9.7(1), otteniamo

$$b - 2 \leq (w-1)\frac{bw}{2k}.$$

[2] Nota di traduzione: nell'originale manca la precisazione sulla coordinata j nulla; senza di essa il primo conteggio non sarebbe corretto.

[3] Nota di traduzione: il rinvio originale «Theorem 9.7(3)» è incongruo; si tratta della proprietà (1). La proprietà (4) presuppone $w > 0$, come nel caso non banale trattato qui.

Per dimostrare l'asserto dobbiamo mostrare che il membro destro non può essere uguale a $b-2$ né a $b-1$. In entrambi i casi l'uguaglianza implicherebbe $2^{w-1} \mid k$, in contraddizione con il teorema 9.7, salvo quando $w = 4$, caso che si esclude per sostituzione.

(ii) Consideriamo due righe di C con la stessa disposizione degli asterischi. Per ipotesi esse differiscono in più di una posizione. Calcoliamo di nuovo la somma delle distanze di tutte le righe da una delle due. Essa è almeno $2+(b-2) = b$ e, per il teorema 9.7(1), è uguale a $w \cdot bw/(2k)$. Quindi $w^2 \geq 2k$. Dobbiamo escludere l'uguaglianza. Per il ragionamento precedente, l'uguaglianza implicherebbe che le righe con la stessa disposizione degli asterischi compaiano in coppie a distanza 2 e che tutte le altre righe abbiano distanza 1 da ciascuna riga della coppia. Senza perdita di generalità, una tale coppia sarebbe

$$(* * \cdots * \, 00 \cdots 000) \quad \text{e} \quad (* * \cdots * \, 00 \cdots 011).$$

Le altre $bw/(2k)-1$ righe che terminano con 1 dovrebbero terminare con 01, altrimenti avrebbero distanza 0 dalla seconda riga o distanza maggiore di 1 dalla prima. Analogamente vi sarebbero $bw/(2k)-1$ righe che terminano con 10. Poiché abbiamo ora righe a distanza 2, necessariamente $bw/(2k)-1 = 1$. Pertanto $2^w = 2w$, impossibile per $w \geq 3$. □

Corollario. Non esiste un ABD$(8, 4)$.

Con questi risultati è facile trovare tutti gli ABD(k, w) con $w \leq 4$. Naturalmente $w = 0$ è banale. Per $w = 1, 2$ oppure 4 deve essere $k = w$, senza asterischi. Se $w = 3$, si ha $k = 3$, senza asterischi, oppure $k = 4$. In quest'ultimo caso esistono due tipi di ABD, uno dei quali è dato nell'esempio 9.1.

Problema 9D. Costruire un ABD$(4, 3)$ con le stesse prime quattro righe dell'esempio 9.1, ma diverso nelle altre.

Nel 1987 La Poutré e Van Lint dimostrarono che non esiste un ABD$(10, 5)$, ma la possibilità più piccola ABD$(8, 5)$ si rivelò piuttosto difficile da trattare. Nel 1999 D. E. Knuth chiese a Brouwer se vi fossero stati progressi dopo i primi risultati, e questo convinse Brouwer che era tempo di risolvere la questione. Un esempio si trova in Brouwer (1999). Non sembra possedere alcuna struttura. Il più piccolo caso ancora aperto è ora l'esistenza di un ABD$(12, 6)$. Orig. 87

Descriveremo alcuni metodi di costruzione. Alcune delle idee verranno riprese in altri capitoli.

Teorema 9.9. Se esiste un ABD(k_i, w_i) per $i = 1, 2$, allora esiste un ABD(k_1k_2, w_1w_2).

Dimostrazione. Possiamo supporre $w_2 > 0$. Dividiamo le righe dell'ABD(k_2, w_2) in due classi R_0 e R_1 della stessa cardinalità. Nell'ABD(k_1, w_1) sostituiamo ogni asterisco con una riga di k_2 asterischi, ogni 0 con una riga di R_0 e ogni 1 con una riga di R_1, in tutti i modi possibili. Un calcolo immediato mostra che la matrice risultante è un ABD(k_1k_2, w_1w_2). □

Corollario. Esiste un ABD$(4^t, 3^t)$.

Per dimostrare il prossimo teorema introduciamo un nuovo simbolo, $-$. Una k-upla sui simboli 0, 1, $*$ e $-$ rappresenta tutte le parole sui soli simboli 0, 1, $*$ ottenibili sostituendo ciascun $-$ con 0 oppure 1, in tutti i modi possibili.

Teorema 9.10. Sia $w > 0$. Supponiamo che esista un ABD(k, w), dove $k = k_0\, 2^l$ e k_0 è dispari. Allora esiste un ABD$(k, w + ik_0)$ per $0 \leq i \leq (k-w)/k_0$.

Dimostrazione. Basta considerare $i = 1$. Sia C l'ABD(k, w). Definiamo una matrice A delle stesse dimensioni ponendo $a_{ij} = 1$ se $C_{ij} = *$ e $a_{ij} = 0$ altrimenti. Per il teorema 7.3, A è somma di due matrici A_1 e A_2, dove A_1 ha k_0 uni in ogni riga e 2^{w-l} uni in ogni colonna. In ogni riga di C sostituiamo con $-$ gli asterischi che si trovano nelle posizioni in cui A_1 ha un 1. Otteniamo l'ABD$(k, w + k_0)$ richiesto. □

Teorema 9.11. Se esiste un ABD(k, w) e $\alpha \geq 1$ è un numero tale che αk e αw siano interi, allora esiste un ABD$(\alpha k, \alpha w)$.

Dimostrazione. Basta mostrare che esiste un ABD$(k+l, w+m)$ per $(k+l)/(w+m) = k/w$ e $(l, m) = 1$. Sia $k = k_0\, 2^e$, con k_0 dispari. Dalla proprietà (ii) della definizione sappiamo che $k_0 \mid w$. Quindi $wl = mk$ e $(l, m) = 1$ implicano che l è una potenza di 2. Consideriamo la matrice circolante $l \times l$ la cui prima riga consiste di $l - m$ asterischi e m segni meno. Poiché l divide b, possiamo affiancare alla matrice C dell'ABD(k, w) una colonna di b/l copie di questa matrice circolante. Si verifica facilmente che la matrice più grande così ottenuta rappresenta un ABD$(k + l, w + m)$. □ Orig. 88

Esempio 9.2. Dal corollario al teorema 9.9 abbiamo un ABD$(64, 27)$. Il teorema 9.10 mostra allora che esiste un ABD$(64, w)$ per $27 \leq w \leq 64$. In particolare esiste un ABD$(64, 32)$. Il teorema 9.11 implica quindi che esiste un ABD$(2w, w)$ per ogni $w \geq 32$. Come già osservato, la non esistenza è stata dimostrata per $w = 4$ e $w = 5$, mentre il caso $w = 6$ è ancora aperto.

Note

Il primo problema di questo capitolo fu introdotto da J. R. Pierce ai Bell Laboratories come *loop switching problem*. Diverse persone, fra cui uno degli autori di questo libro, tentarono invano di risolverlo. Poco dopo che R. L. Graham ebbe portato a 200 dollari il premio per la soluzione, P. Winkler lo risolse. È interessante che Winkler dichiarasse di avere l'abitudine di numerare i vertici nel modo usato nella dimostrazione grazie alla propria formazione informatica. Riesaminando la dimostrazione si vede che quella numerazione svolge davvero un ruolo cruciale.

Bibliografia

A. E. Brouwer (1999), An Associative Block Design ABD(8,5), *SIAM J. Comput.* **28**, 1970–1971.

R. L. Graham e H. O. Pollak (1971), On the addressing problem for loop switching, *Bell System Tech. J.* **50**, 2495–2519.

B. W. Jones (1950), *The Theory of Quadratic Forms*, Carus Math. Monogr. **10**, Math. Assoc. of America.

J. A. La Poutré e J. H. van Lint (1985), An associative block design ABD(10,5) does not exist, *Utilitas Math.* **31**, 219–225.

P. Winkler (1983), Proof of the squashed cube conjecture, *Combinatorica* **3**, 135–139.

Capitolo 10

Il principio di inclusione ed esclusione; formule di inversione

Orig. 89

Come abbiamo visto in diversi capitoli precedenti, molti problemi di analisi combinatoria richiedono di contare determinati oggetti. Trattiamo ora uno dei metodi di conteggio più utili, noto come *principio di inclusione ed esclusione*. L'idea è la seguente. Se A e B sono sottoinsiemi di S e vogliamo contare gli elementi di $S \setminus (A \cup B)$, la risposta non è $|S| - |A| - |B|$, perché gli elementi di $A \cap B$ sono stati sottratti due volte. La risposta corretta è invece $|S| - |A| - |B| + |A \cap B|$. Il teorema seguente generalizza questa idea.

Teorema 10.1. Sia S un insieme di N elementi e siano $E_1, \ldots, E_r$ sottoinsiemi di S, non necessariamente distinti. Per ogni sottoinsieme M di $\{1, \ldots, r\}$, indichiamo con $N(M)$ il numero di elementi di S appartenenti a $\bigcap_{i \in M} E_i$; per $0 \leq j \leq r$ poniamo $N_j := \sum_{|M|=j} N(M)$. Allora il numero di elementi di S che non appartengono ad alcuno degli E_i, $1 \leq i \leq r$, è

$$N - N_1 + N_2 - N_3 + \cdots + (-1)^r N_r. \tag{10.1}$$

Dimostrazione. (i) Se $x \in S$ non appartiene ad alcuno degli E_i, il suo contributo all'espressione (10.1) è 1.

(ii) Se $x \in S$ appartiene esattamente a k degli insiemi E_i, il suo contributo alla (10.1) è

$$1 - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k} = (1-1)^k = 0.$$

□

Orig. 90

Osservazione. Se tronchiamo la somma (10.1) dopo un termine positivo, oppure negativo, otteniamo rispettivamente un limite superiore, oppure inferiore, per il numero di elementi di S che non appartengono ad alcuno degli E_i.

Data l'importanza di questo metodo, ne illustreremo l'uso con diversi esempi.

Esempio 10.1. Indichiamo con d_n il numero delle permutazioni π di $1, 2, \ldots, n$ tali che $\pi(i) \neq i$ per ogni i; queste permutazioni si chiamano *scompigli*. Sia $S := S_n$ e sia E_i il sottoinsieme delle permutazioni π per cui $\pi(i) = i$. Dalla (10.1) ricaviamo

$$d_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \tag{10.2}$$

Questa formula mostra che, per n grande, la probabilità che una permutazione sia uno scompiglio è circa e^{-1}. Applicando la (10.2) a n e a $n-1$ otteniamo una relazione di ricorrenza per d_n:

$$d_n = n d_{n-1} + (-1)^n. \tag{10.3}$$

La (10.2) si può ottenere anche per inversione, nel modo seguente. Consideriamo la serie di potenze $D(x) := \sum_{n=0}^{\infty} d_n x^n/n!$, con $d_0 = 1$. Se $F(x) := e^x D(x)$, allora

$$F(x) = \sum_{m=0}^{\infty} \left\{ \sum_{r=0}^{m} \binom{m}{r} d_{m-r} \right\} \frac{x^m}{m!}.$$

Poiché $\sum_{r=0}^{m} \binom{m}{r} d_{m-r} = m!$, abbiamo $F(x) = (1-x)^{-1}$. Ne segue che $D(x) = e^{-x}(1-x)^{-1}$ e, moltiplicando le serie di potenze dei due fattori, ritroviamo la (10.2).

Esempio 10.2. Siano X un insieme di n elementi e $Y = \{y_1, \ldots, y_k\}$ un insieme di k elementi. Contiamo le applicazioni suriettive da X a Y. Sia S l'insieme di tutte le applicazioni da X a Y ed E_i il sottoinsieme delle applicazioni per cui y_i non appartiene all'immagine di X. Per la (10.1), il numero delle suriezioni è $\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$. Esso è evidentemente 0 per $k > n$ e $n!$ per $k = n$. Abbiamo dunque dimostrato

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n = \begin{cases} n! & \text{se } k = n, \\ 0 & \text{se } k > n. \end{cases} \tag{10.4}$$

Vi sono molte formule simili alla (10.4) che sono spesso piuttosto difficili da dimostrare direttamente. La presenza di $(-1)^i$ è di solito un indizio che si può ottenere la formula contando opportuni oggetti mediante il principio di inclusione ed esclusione, come in questo esempio. È tuttavia utile, in questo caso, vedere un'altra dimostrazione. Orig. 91

Sia $P(x)$ un polinomio di grado n con coefficiente direttivo a_n. Indichiamo con $\mathbf{P}$ la successione $P(0), P(1), \ldots$. Consideriamo la successione delle differenze $P(1) - P(0), P(2) - P(1), \ldots$. Essa è $\mathbf{Q}_1$, dove $Q_1(x) := P(x+1) - P(x)$ è un polinomio di grado $n-1$ con coefficiente direttivo na_n. Ripetendo il procedimento otteniamo una successione $\mathbf{Q}_k$ i cui termini sono $\sum_{i=0}^{k} (-1)^i \binom{k}{i} P(x+k-i)$, corrispondente al polinomio $Q_k(x)$ di grado $n-k$ con coefficiente direttivo $n(n-1)\cdots(n-k+1)a_n$. Se $k = n$, tutti i termini di $\mathbf{Q}_k$ sono $n!a_n$; se $k > n$, sono tutti 0. Ponendo $P(x) = x^n$ ritroviamo la (10.4).

Esempio 10.3. La seguente identità è una nota relazione fra coefficienti binomiali:

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{m+n-i}{k-i} = \begin{cases} \binom{m}{k} & \text{se } m \geq k, \\ 0 & \text{se } m < k. \end{cases} \tag{10.5}$$

Se vogliamo dimostrarla mediante inclusione ed esclusione, vediamo che gli insiemi E_i da escludere devono corrispondere a scelte in un insieme di n elementi; dopo averne scelti i, dobbiamo scegliere $k-i$ elementi in un insieme di cardinalità $m+n-i$. Questo suggerisce il problema combinatorio che conduce alla (10.5). Consideriamo un insieme $Z = X \cup Y$, dove $X = \{x_1, \ldots, x_n\}$ è un insieme di n punti blu e Y un insieme di m punti rossi. Quanti sottoinsiemi di k elementi sono formati soltanto da punti rossi? La risposta è evidentemente il membro destro della (10.5). Se prendiamo come S l'insieme di tutti i sottoinsiemi di k elementi di Z e come E_i quelli che contengono x_i, la (10.1) fornisce il membro sinistro della (10.5).

Possiamo di nuovo chiederci se il risultato ammetta una dimostrazione diretta. La risposta è sì. Usiamo lo sviluppo

$$\sum_{j=0}^{\infty} \binom{a+j}{j} x^j = (1-x)^{-a-1}. \tag{10.6}$$

Si noti che $(-1)^i \binom{n}{i}$ è il coefficiente di x^i nello sviluppo di $(1-x)^n$. Dalla (10.6), $\binom{m+n-i}{k-i}$ è il coefficiente di x^{k-i} nello sviluppo di $(1-x)^{k-m-n-1}$. Quindi il membro sinistro della (10.5) è il coefficiente di x^k nello sviluppo di $(1-x)^{k-m-1}$. Se $m \leq k-1$, esso è evidentemente 0; se $m \geq k$, è $\binom{m}{k}$, ancora per la (10.6). Orig. 92

Esempio 10.4 (La funzione di Eulero). Sia $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ un intero positivo. Indichiamo con $\phi(n)$ il numero degli interi k, $1 \leq k \leq n$, tali che il massimo comune divisore (n, k) sia 1. Applichiamo il teorema 10.1 con $S := \{1, 2, \ldots, n\}$ ed E_i uguale all'insieme degli interi divisibili per p_i, $1 \leq i \leq r$. La (10.1) dà

$$\phi(n) = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - \cdots = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \tag{10.7}$$

Il prossimo teorema viene usato molto spesso.

Teorema 10.2. $\displaystyle\sum_{d|n}\phi(d)=n.$

DIMOSTRAZIONE. Consideriamo $N=\{1,2,\dots,n\}$. Per ogni $m\in N$ abbiamo $(m,n)\mid n$. Il numero degli interi m con $(m,n)=d$, ossia $m=m_1d$, $n=n_1d$ e $(m_1,n_1)=1$, è chiaramente $\phi(n_1)=\phi(n/d)$. Quindi $n=\sum_{d|n}\phi(n/d)$, che equivale alla tesi. □

A questo punto è utile introdurre la cosiddetta *funzione di Möbius*:

$$\mu(d):=\begin{cases}1 & \text{se } d \text{ è prodotto di un numero pari di primi distinti,}\\ -1 & \text{se } d \text{ è prodotto di un numero dispari di primi distinti,}\\ 0 & \text{altrimenti, cioè se } d \text{ non è privo di fattori quadrati.}\end{cases}\tag{10.8}$$

Il prodotto di zero primi vale 1, dunque $\mu(1)=1$.

Teorema 10.3. $\displaystyle\sum_{d|n}\mu(d)=\begin{cases}1 & \text{se } n=1,\\ 0 & \text{altrimenti.}\end{cases}$

DIMOSTRAZIONE. Se $n=1$, non vi è nulla da dimostrare. Se $n=p_1^{a_1}\cdots p_r^{a_r}$, allora per la (10.8) abbiamo Orig. 93

$$\sum_{d|n}\mu(d)=\sum_{i=0}^{r}(-1)^i\binom{r}{i}=(1-1)^r=0.$$

□

Si osservi la somiglianza fra le dimostrazioni dei teoremi 10.1 e 10.3. Usando la funzione di Möbius possiamo riscrivere la (10.7) come

$$\frac{\phi(n)}{n}=\sum_{d|n}\frac{\mu(d)}{d}.\tag{10.9}$$

Problema 10A. Quanti interi positivi minori di 1000 non hanno alcun divisore compreso fra 1 e 10?[1]

Problema 10B. Quanti polinomi monici di grado n in $\mathbb{F}_p[x]$ non assumono il valore 0 per alcun $x\in\mathbb{F}_p$?

Problema 10C. Determinare $\displaystyle\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor$.

Problema 10D. Una delle funzioni più famose dell'analisi complessa è la cosiddetta funzione ζ di Riemann, $\zeta(s):=\sum_{n=1}^{\infty}n^{-s}$, definita nel piano complesso per $\mathrm{Re}(s)>1$. Dimostrare che $1/\zeta(s)=\sum_{n=1}^{\infty}\mu(n)n^{-s}$.

Problema 10E. Sia $f_n(z)$ la funzione che ha come zeri tutti i numeri η tali che $\eta^n=1$ ma $\eta^k\neq1$ per $1\le k<n$. Dimostrare che

$$f_n(z)=\prod_{k|n}(z^k-1)^{\mu(n/k)}.$$

[2]

Il teorema 10.3 consente di ricavare una formula di inversione molto utile, nota come *formula di inversione di Möbius*.

Teorema 10.4. Siano $f(n)$ e $g(n)$ funzioni definite per ogni intero positivo n e tali che

$$f(n)=\sum_{d|n}g(d).\tag{10.10}$$

Allora g soddisfa

$$g(n)=\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right).\tag{10.11}$$ Orig. 94

[1] Nota di traduzione: si intende un divisore maggiore di 1 e non maggiore di 10; il divisore 1 va escluso dalla condizione.

[2] Nota di traduzione: la formula identifica f_n come il polinomio monico i cui zeri sono, ciascuno con molteplicità uno, le radici primitive n-esime dell'unità; la sola indicazione degli zeri non determina una funzione univocamente.

DIMOSTRAZIONE. Per la (10.10) abbiamo

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$
$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} g(d') = \sum_{d'|n} g(d') \sum_{m|(n/d')} \mu(m).$$

Per il teorema 10.3, la somma interna al membro destro è 0 salvo quando $d' = n$. □

Osservazione. Anche la (10.11) implica la (10.10).

Esempio 10.5. Contiamo il numero N_n delle successioni circolari di 0 e 1, di lunghezza n, considerando uguali due successioni ottenibili l'una dall'altra per rotazione. Sia $M(d)$ il numero delle successioni circolari di lunghezza d che non sono periodiche. Allora $N_n = \sum_{d|n} M(d)$. Osserviamo che $\sum_{d|n} dM(d) = 2^n$, poiché così contiamo tutte le possibili successioni circolari con una posizione iniziale fissata. Per il teorema 10.4 ricaviamo $nM(n) = \sum_{d|n} \mu(d) 2^{n/d}$, e quindi

$$\begin{aligned} N_n &= \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \sum_{l|d} \mu\left(\frac{d}{l}\right) 2^l \\ &= \sum_{l|n} \frac{2^l}{l} \sum_{k|(n/l)} \frac{\mu(k)}{k} = \frac{1}{n} \sum_{l|n} \phi\left(\frac{n}{l}\right) 2^l. \end{aligned} \tag{10.12}$$

L'ultima espressione ha il vantaggio di avere tutti i termini positivi. Sorge quindi la domanda se avremmo potuto ottenerla con un'altra tecnica di conteggio. Vedremo che il teorema seguente, noto come lemma di Burnside, benché sia in realtà dovuto a Cauchy e Frobenius (si vedano le note), fornisce la risposta. Orig. 95

Teorema 10.5. Sia G un gruppo di permutazioni che agisce su un insieme X. Per $g \in G$, sia $\psi(g)$ il numero dei punti di X fissati da g. Allora il numero delle orbite di G è $\dfrac{1}{|G|} \displaystyle\sum_{g \in G} \psi(g)$.

DIMOSTRAZIONE. Contiamo le coppie (g, x) con $g \in G$, $x \in X$ e $x^g = x$. Partendo da g troviamo $\sum_{g \in G} \psi(g)$. Per ogni $x \in X$ vi sono $|G|/|O_x|$ coppie di questo tipo, dove O_x è l'orbita di x. Il numero totale è quindi $|G| \sum_{x \in X} 1/|O_x|$. Le orbite di G partizionano X e, sommando $1/|O_x|$ su tutti gli x di una particolare orbita, otteniamo 1. Dunque $\sum_{x \in X} 1/|O_x|$ è il numero delle orbite. □

Esempio 10.5 (continuazione). Sia G il gruppo ciclico di ordine n, cioè il gruppo delle rotazioni di una successione circolare di 0 e 1. Se $d \mid n$, vi sono $\phi(n/d)$ interi g fra 1 e n con $(n, g) = d$; per ciascuno di essi vi sono 2^d successioni fissate dalla rotazione di g posizioni. Il teorema 10.5 dà quindi immediatamente la (10.12).

Esempio 10.6. Il problema seguente, introdotto da Lucas nel 1891, è noto come *problème des ménages*. Vogliamo disporre n coppie sposate attorno a un tavolo circolare, con uomini e donne alternati, in modo che nessun marito sieda accanto alla propria moglie. In quanti modi è possibile? Supponiamo che le donne siano già sedute in posti alternati. Numeriamo le donne da 1 a n e i rispettivi mariti nello stesso modo. Il problema equivale a disporre gli interi da 1 a n su un cerchio con posizioni numerate da 1 a n, in modo che per ogni i l'intero i non occupi né la posizione i né la posizione $i + 1$ (modulo n). Sia E_i l'insieme delle disposizioni in cui il marito i siede accanto alla moglie. Per applicare inclusione ed esclusione dobbiamo calcolare in quanti modi sia possibile sistemare r mariti in posizioni vietate. Chiamiamo A_r questo numero.

Consideriamo una successione circolare di $2n$ posizioni. Mettiamo un 1 nella posizione $2i - 1$ se il marito i siede alla destra della moglie, e nella posizione $2i$ se siede alla sua sinistra; nelle posizioni rimanenti mettiamo 0. Le configurazioni da contare sono quindi successioni circolari di $2n$ zeri e uni, con esattamente r uni, nessuno dei quali adiacente a un altro. Sia A'_r il numero delle successioni che iniziano con 1, seguito da 0. Considerando 10 come un unico simbolo, vediamo che dobbiamo scegliere $r - 1$ posizioni fra $2n - r - 1$. Per contare il numero A''_r delle successioni che iniziano con 0, spostiamo tale 0 alla fine: dobbiamo allora scegliere r posizioni fra $2n - r$. Dunque Orig. 96

$$A_r = A'_r + A''_r = \binom{2n - r - 1}{r - 1} + \binom{2n - r}{r} = \frac{2n}{2n - r} \binom{2n - r}{r}.$$

Dalla (10.1) ricaviamo che il numero dei modi di far sedere gli uomini è

$$\sum_{r=0}^{n}(-1)^r(n-r)!\binom{2n-r}{r}\frac{2n}{2n-r}. \tag{10.13}$$

Problema 10F. Coloriamo di rosso o di blu gli interi da 1 a $2n$ in modo che, se i è rosso, $i-1$ non sia blu. Dimostrare che

$$\sum_{k=0}^{n}(-1)^k\binom{2n-k}{k}2^{2n-2k}=2n+1.$$

Si può dimostrare direttamente questa identità?

Problema 10G. Contare le permutazioni $x_1, x_2, \ldots, x_{2n}$ degli interi da 1 a $2n$ tali che $x_i+x_{i+1}\neq 2n+1$ per $i=1,2,\ldots,2n-1$.

Problema 10H. Dimostrare che, per $0\le k\le n$,

$$\sum_{i=0}^{k}\binom{k}{i}d_{n-i}=\sum_{j=0}^{n-k}(-1)^j\binom{n-k}{j}(n-j)!.$$

3

Note

Il principio di inclusione ed esclusione compare già in un lavoro di Da Silva del 1854 e, successivamente, in uno di Sylvester del 1883. Per questo motivo la (10.1) e formule analoghe vengono talvolta chiamate formule di Da Silva o di Sylvester. Un nome migliore, anch'esso frequente, è «formula del crivello». Essa è infatti un esempio di un principio largamente impiegato nella teoria dei numeri con il nome di «metodi di crivello». Un esempio probabilmente noto alla maggior parte dei lettori è il crivello di Eratostene: per trovare i primi $\le n^2$, si prendono gli interi $\le n^2$ e si eliminano i multipli dei primi $\le n$. Gli scompigli dell'esempio 10.1 ricompaiono negli esempi 14.1 e 14.10. La prima comparsa di questo problema si trova in uno dei primi libri sui giochi d'azzardo: *Essai d'analyse sur les jeux de hazard* di P. R. de Montmort (1678–1719). Lo si indica ancora spesso con il nome che gli diede l'autore, *problème des rencontres*. La (10.2) viene talvolta enunciata così. Se n persone depositano i loro ombrelli — un esempio tipicamente olandese: in Olanda piove sempre — e poi, dopo un'interruzione della corrente, ne riprendono uno a caso al buio, la probabilità che nessuno riprenda il proprio ombrello è approssimativamente e^{-1}, per n grande. Orig. 97

La seconda dimostrazione dell'esempio 10.2 illustra l'uso del *calcolo delle differenze finite*, ampiamente impiegato nell'analisi numerica.

A. F. Möbius (1790–1868) fu un astronomo e, prima ancora, assistente di Gauss; diede importanti contributi alla geometria e alla topologia, fra cui il nastro di Möbius.

G. F. B. Riemann (1826–1866) fu professore a Göttingen, dove aveva anche conseguito il dottorato sotto la guida di Gauss. È famoso per molte idee, fra cui l'integrale di Riemann, le superfici e le varietà riemanniane e, naturalmente, la cosiddetta ipotesi di Riemann sulla posizione degli zeri della funzione ζ. Ci si chiede che cosa ci avrebbe lasciato se non fosse morto tanto giovane.

Nella maggior parte dei libri in cui compare, il teorema 10.5 è chiamato lemma di Burnside. È soltanto uno dei tanti esempi di risultati attribuiti alla persona sbagliata. Per la storia di questa denominazione impropria rimandiamo a Neumann (1979).

F. E. A. Lucas (1842–1891) fu un teorico dei numeri francese. È noto per i suoi libri di teoria dei numeri e di ricreazioni matematiche. Il primo conteneva il problema dell'esempio 10.6. Fu Lucas a dare ai numeri di Fibonacci questo nome; si vedano le note al capitolo 14.

Bibliografia

F. E. A. Lucas (1891), *Théorie des nombres*, Gauthier-Villars, Paris.

[3] Nota di traduzione: l'originale usa qui D_{n-i}, mentre nell'esempio 10.1 il numero degli scompigli è indicato con d_{n-i}. Si è uniformata la notazione.

P. M. Neumann (1979), A lemma that is not Burnside's, *Math. Scientist* **4**, 133–141.

Capitolo 11

Permanenti

Orig. 98

Prima di introdurre l'argomento principale di questo capitolo, presentiamo una generalizzazione del Teorema 10.1. Come in quel teorema, sia S un insieme di n elementi e siano $E_1, \dots, E_r$ sottoinsiemi di S, non necessariamente distinti. Sia F un campo qualsiasi. A ogni elemento $a \in S$ assegniamo un *peso* $w(a)$ in F. Per ogni sottoinsieme M di $\{1, 2, \dots, r\}$, definiamo $W(M)$ come la somma dei pesi degli elementi di S appartenenti a $\bigcap_{i\in M} E_i$. Per $0 \le j \le r$ poniamo $W_j := \sum_{|M|=j} W(M)$; dunque $W_0 = \sum_{a\in S} w(a)$.

Teorema 11.1. Se $E(m)$ denota la somma dei pesi degli elementi di S contenuti in esattamente m dei sottoinsiemi E_i, $1 \le i \le r$, allora

$$E(m) = \sum_{i=0}^{r-m} (-1)^i \binom{m+i}{i} W_{m+i}. \tag{11.1}$$

Dimostrazione. La dimostrazione è quasi identica a quella del Teorema 10.1. Se $x \in S$ appartiene a esattamente m dei sottoinsiemi E_i, il contributo di x alla somma in (11.1) è $w(x)$. Se invece $x \in S$ appartiene a esattamente $m + k$ di tali sottoinsiemi, il suo contributo è

$$w(x) \sum_{i=0}^{k} (-1)^i \binom{m+i}{i}\binom{m+k}{m+i} = w(x)\binom{m+k}{k} \sum_{i=0}^{k} (-1)^i \binom{k}{i} = 0.$$

□

Orig. 99

Diamo ora la definizione di permanente. Sia $A = (\mathbf{a}_1, \dots, \mathbf{a}_n)$ una matrice $n \times n$ con colonne $\mathbf{a}_j = (a_{1j}, \dots, a_{nj})^{\mathsf{T}}$. Il *permanente* di A, indicato con $\operatorname{per} A$, è definito da

$$\operatorname{per} A := \sum_{\pi\in S_n} a_{1\pi(1)} \cdots a_{n\pi(n)}. \tag{11.2}$$

Il permanente è dunque definito come il determinante, ma senza i segni che dipendono dalla parità della permutazione π.

Dalla definizione risultano evidenti le seguenti proprietà:

$$\operatorname{per} A = \operatorname{per} A^{\mathsf{T}}; \tag{11.3}$$

$$\operatorname{per} A = \operatorname{per} PAQ \quad \text{se } P \text{ e } Q \text{ sono matrici di permutazione;} \tag{11.4}$$

$$\operatorname{per} A \text{ è una funzione lineare di } \mathbf{a}_j,\ 1 \le j \le n. \tag{11.5}$$

Naturalmente il permanente è anche una funzione lineare di ciascuna riga di A. Calcolarlo è molto più difficile che calcolare il determinante. Tuttavia (11.2) mostra chiaramente che è possibile svilupparlo per righe o per colonne. Indichiamo quindi con A_{ij} la matrice ottenuta da A sopprimendo la riga i e la colonna j. Allora

$$\operatorname{per} A = \begin{cases} \displaystyle\sum_{i=1}^{n} a_{ij} \operatorname{per} A_{ij}, & 1 \le j \le n, \\ \displaystyle\sum_{j=1}^{n} a_{ij} \operatorname{per} A_{ij}, & 1 \le i \le n. \end{cases} \tag{11.6}$$

Il seguente metodo di calcolo del permanente, dovuto a Ryser, è un'applicazione del Teorema 11.1.

Teorema 11.2. Sia A una matrice $n \times n$. Se A_r si ottiene da A eliminando r colonne, indichiamo con $S(A_r)$ il prodotto delle somme delle righe di A_r. Sia Σ_r la somma dei valori $S(A_r)$ per tutte le possibili scelte di A_r. Allora

$$\operatorname{per} A = \sum_{r=0}^{n-1} (-1)^r \Sigma_r. \tag{11.7}$$

Orig. 100

DIMOSTRAZIONE. Sia S l'insieme di tutti i prodotti $p = a_{1i_1} \cdots a_{ni_n}$ e poniamo $w(p) := p$. Definiamo E_j come l'insieme dei prodotti p per i quali $j \notin \{i_1, \ldots, i_n\}$. Il permanente di A è la somma dei pesi degli elementi di S che non appartengono ad alcuno dei sottoinsiemi E_j. Pertanto (11.7) segue immediatamente da (11.1). □

Problema 11A. Dimostrare (10.4) usando il Teorema 11.2.

Osservazione. Se $A_1, \ldots, A_n$ sono sottoinsiemi di $\{1, \ldots, n\}$ e $a_{ij} = 1$ quando $j \in A_i$, e 0 altrimenti, allora per A conta i sistemi di rappresentanti distinti (SDR) degli insiemi $A_1, \ldots, A_n$.

Esempio 11.1. Troviamo un'altra formula per il numero degli scompigli di $1, 2, \ldots, n$. Il permanente della matrice $J - I$ di ordine n è chiaramente d_n. Da (11.7) ricaviamo

$$d_n = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^r (n-r-1)^{n-r}. \tag{11.8}$$

Sviluppando il termine $(n-1-r)^{n-r}$ e applicando (10.4) dopo aver scambiato l'ordine delle somme, si ottiene una dimostrazione piuttosto complicata di (10.2).

Negli anni Settanta furono dimostrate varie note congetture sui permanenti di matrici a elementi 0 e 1, spesso mediante argomenti ingegnosi. In effetti, gran parte della ricerca sui permanenti era motivata da queste congetture. Dedicheremo quindi attenzione ad alcuni di questi risultati in questo capitolo e nel successivo. Come introduzione, consideriamo matrici $(0,1)$ con due elementi uguali a 1 in ogni riga e in ogni colonna.

Teorema 11.3. Se A è una matrice $(0,1)$ nella quale tutte le somme delle righe e delle colonne sono 2, allora

$$\operatorname{per} A \leq 2^{\lfloor n/2 \rfloor}.$$

DIMOSTRAZIONE. Consideriamo il grafo G i cui vertici corrispondono alle righe di A, i cui spigoli corrispondono alle colonne di A, e in cui il vertice i e lo spigolo j sono incidenti esattamente quando $A(i,j) = 1$. Questo grafo è regolare di grado 2 e quindi è unione disgiunta di poligoni. La sottomatrice corrispondente ai vertici e agli spigoli di un poligono, dopo aver eventualmente riordinato righe e colonne, è una matrice circolante

Orig. 101

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

(Può ridursi a una matrice 2×2 di soli 1.) La matrice A è somma diretta di matrici di questo tipo, ciascuna delle quali ha permanente 2. Il numero dei fattori è al più $\lfloor n/2 \rfloor$; l'uguaglianza nel teorema vale se A è somma diretta di $\lfloor n/2 \rfloor$ matrici J di ordine 2. □

Questo teorema elementare riguarda la relazione tra le somme delle righe di una matrice e il suo permanente; lo stesso vale per molti dei teoremi successivi. Arriviamo così alla prima questione difficile. Nel 1967 H. Minc congetturò che, se A è una matrice $(0,1)$ con somme delle righe $r_1, \ldots, r_n$, allora

$$\operatorname{per} A \leq \prod_{j=1}^{n} (r_j!)^{1/r_j}. \tag{11.9}$$

La dimostrazione del Teorema 11.3 mostra che in (11.9) può valere l'uguaglianza; questa vale infatti quando A è somma diretta di matrici J_m. Furono dimostrati diversi risultati più deboli di (11.9), spesso mediante argomenti lunghi e intricati. La congettura fu infine dimostrata da L. M. Brégman nel 1973. È tanto più sorprendente che nel 1977 A. Schrijver abbia trovato una dimostrazione estremamente elegante e brevissima della congettura di Minc. La dimostrazione si basa sul lemma seguente.

Lemma 11.4. Se $t_1, t_2, \dots, t_r$ sono numeri reali non negativi, allora

$$\left(\frac{t_1+\cdots+t_r}{r}\right)^{t_1+\cdots+t_r} \le t_1^{t_1}\cdots t_r^{t_r}.$$

DIMOSTRAZIONE. Poiché $x\log x$ è una funzione convessa, si ha

$$\frac{t_1+\cdots+t_r}{r}\log\left(\frac{t_1+\cdots+t_r}{r}\right) \le \frac{t_1\log t_1+\cdots+t_r\log t_r}{r},$$

da cui segue l'asserto. □ Orig. 102

Nel seguito utilizziamo (11.6) nella forma

$$\operatorname{per} A = \sum_{k:\, a_{ik}=1} \operatorname{per} A_{ik}.$$

Teorema 11.5. Sia A una matrice $(0,1)$ di ordine n, con r_i elementi uguali a 1 nella riga i, $1 \le i \le n$. Allora

$$\operatorname{per} A \le \prod_{i=1}^{n} (r_i!)^{1/r_i}.$$

DIMOSTRAZIONE. Procediamo per induzione su n. Per $n = 1$ il teorema è banale. Supponiamo che sia vero per le matrici di ordine $n-1$. L'idea è stimare $(\operatorname{per} A)^{n\operatorname{per} A}$ e scomporre questa espressione in vari prodotti. Osserviamo che r_i è il numero dei valori di k per i quali $a_{ik} = 1$ e applichiamo il lemma. Otteniamo

$$(\operatorname{per} A)^{n\operatorname{per} A} = \prod_{i=1}^{n} (\operatorname{per} A)^{\operatorname{per} A} \le \prod_{i=1}^{n}\left(r_i^{\operatorname{per} A}\prod_{k:\, a_{ik}=1}(\operatorname{per} A_{ik})^{\operatorname{per} A_{ik}}\right). \tag{11.10}$$

Sia ora S l'insieme di tutte le permutazioni ν di $\{1,\dots,n\}$ tali che $a_{i\nu_i} = 1$ per $i = 1,\dots,n$. Dunque $|S| = \operatorname{per} A$. Inoltre il numero di $\nu \in S$ con $\nu_i = k$ è $\operatorname{per} A_{ik}$ se $a_{ik} = 1$, e 0 altrimenti. Il secondo membro di (11.10) è perciò uguale a

$$\prod_{\nu\in S}\left\{\left(\prod_{i=1}^{n} r_i\right)\left(\prod_{i=1}^{n}\operatorname{per} A_{i\nu_i}\right)\right\}. \tag{11.11}$$

Applichiamo ora l'ipotesi induttiva a ciascuna matrice $A_{i\nu_i}$. Ne segue

$$(\operatorname{per} A)^{n\operatorname{per} A} \le \prod_{\nu\in S}\left\{\left(\prod_{i=1}^{n} r_i\right)\prod_{i=1}^{n}\left[\prod_{\substack{j\ne i\\ a_{j\nu_i}=0}}(r_j!)^{1/r_j}\prod_{\substack{j\ne i\\ a_{j\nu_i}=1}}((r_j-1)!)^{1/(r_j-1)}\right]\right\}. \tag{11.12}$$

Poiché il numero degli indici i tali che $i \ne j$ e $a_{j\nu_i} = 0$ è $n - r_j$, mentre quello degli indici i tali che $i \ne j$ e $a_{j\nu_i} = 1$ è $r_j - 1$, il secondo membro di (11.12) può essere sostituito da Orig. 103

$$\prod_{\nu\in S}\left\{\left(\prod_{i=1}^{n} r_i\right)\prod_{j=1}^{n}\left[(r_j!)^{(n-r_j)/r_j}(r_j-1)!\right]\right\}$$
$$= \prod_{\nu\in S}\left(\prod_{i=1}^{n}(r_i!)^{n/r_i}\right) = \left(\prod_{i=1}^{n}(r_i!)^{1/r_i}\right)^{n\operatorname{per} A},$$

e l'asserto è dimostrato. □

Consideriamo ora una classe particolare di matrici $(0,1)$: quelle che hanno esattamente k elementi uguali a 1 in ogni riga e in ogni colonna. Indichiamo tale classe con $\mathcal{A}(n,k)$ e definiamo

$$M(n,k) := \max\{\operatorname{per} A : A \in \mathcal{A}(n,k)\}, \tag{11.13}$$
$$m(n,k) := \min\{\operatorname{per} A : A \in \mathcal{A}(n,k)\}. \tag{11.14}$$

Prendendo somme dirette otteniamo le disuguaglianze

$$M(n_1+n_2,k) \geq M(n_1,k)M(n_2,k), \tag{11.15}$$
$$m(n_1+n_2,k) \leq m(n_1,k)m(n_2,k). \tag{11.16}$$

Queste due disuguaglianze permettono di introdurre altre due funzioni usando il risultato seguente, noto come *lemma di Fekete*.

Lemma 11.6. Sia $f : \mathbb{N} \to \mathbb{N}$ una funzione tale che $f(m+n) \geq f(m)f(n)$ per tutti $m, n \in \mathbb{N}$. Allora esiste $\lim_{n\to\infty} f(n)^{1/n}$, eventualmente uguale a ∞.

Dimostrazione. Fissiamo m e l, con $l \leq m$. Per induzione, dalla disuguaglianza per f ricaviamo $f(l+km) \geq f(l)[f(m)]^k$. Pertanto

$$\liminf f(l+km)^{1/(l+km)} \geq f(m)^{1/m},$$

e, poiché vi sono m possibili valori di l, in realtà si ha

Orig. 104

$$\liminf f(n)^{1/n} \geq f(m)^{1/m}.$$

Facendo tendere m a ∞ troviamo

$$\liminf f(n)^{1/n} \geq \limsup f(m)^{1/m},$$

e dunque i due valori coincidono. □

L'asserto del lemma resta vero sostituendo $\geq$ con $\leq$ nella disuguaglianza per f. Applicandolo a (11.15) e (11.16), possiamo definire

$$M(k) := \lim_{n\to\infty} \{M(n,k)\}^{1/n}, \tag{11.17}$$
$$m(k) := \lim_{n\to\infty} \{m(n,k)\}^{1/n}. \tag{11.18}$$

Problema 11B. Dimostrare che $M(n,k) \geq k!$. Dimostrare che $M(k) \leq (k!)^{1/k}$. Mostrare con un esempio che $M(k) \geq (k!)^{1/k}$. Ne segue che $M(k) = (k!)^{1/k}$.

La funzione $m(n,k)$ è molto più difficile da trattare. Ciò che ci si può aspettare si basa su un famoso problema ancora chiamato *congettura di Van der Waerden*, benché nel 1981 ne siano apparse due dimostrazioni differenti, dopo quasi cinquant'anni di ricerche! Formuliamo qui la congettura; la dimostrazione sarà data nel prossimo capitolo.

Congettura. Se A è una matrice $n \times n$ a elementi non negativi nella quale tutte le somme delle righe e delle colonne sono 1, allora

$$\operatorname{per} A \geq n!\, n^{-n}. \tag{11.19}$$

Le matrici considerate nella congettura si chiamano solitamente *doppiamente stocastiche*. Se $A \in \mathcal{A}(n,k)$, dividendo tutti gli elementi di A per k si ottiene una matrice doppiamente stocastica. La congettura, ora teorema, mostra quindi che $m(k) \geq k/e$. Questo è notevole, perché il valore di $M(k)$ dato nel Problema 11B tende a k/e per $k \to \infty$ (si vedano le note). Ciò significa che, per n grande e per A arbitraria in $\mathcal{A}(n,k)$, il valore di $(\operatorname{per} A)^{1/n}$ è vicino a k/e. Per molto tempo la migliore limitazione inferiore di $m(n,3)$ fu $n+3$, e già questa non era facile da dimostrare. Ancora una volta, il miglioramento successivo fu insieme considerevole ed elementare. Diamo ora la dimostrazione di tale risultato, dovuto a Voorhoeve (1979).

Orig. 105

Teorema 11.7. $m(n,3) \geq 6\,(4/3)^{n-3}$.

Dimostrazione. Indichiamo con U_n l'insieme delle matrici $n \times n$ a elementi interi non negativi nelle quali tutte le somme delle righe e delle colonne sono 3; poniamo $u(n) := \min\{\operatorname{per} A : A \in U_n\}$. Sia V_n

l'insieme di tutte le matrici ottenute da elementi di U_n diminuendo di 1 un elemento positivo; poniamo $v(n) := \min\{\operatorname{per} A : A \in V_n\}$. Mostriamo anzitutto che

$$u(n) \geq \left\lceil \frac{3}{2} v(n) \right\rceil . \tag{11.20}$$

Sia $A \in U_n$ con prima riga $\mathbf{a} = (\alpha_1, \alpha_2, \alpha_3, 0, \ldots, 0)$, dove $\alpha_i \geq 0$ per $i = 1, 2, 3$. Poiché

$$\begin{aligned} 2\mathbf{a} = {} & \alpha_1(\alpha_1 - 1, \alpha_2, \alpha_3, 0, \ldots, 0) + \alpha_2(\alpha_1, \alpha_2 - 1, \alpha_3, 0, \ldots, 0) \\ & + \alpha_3(\alpha_1, \alpha_2, \alpha_3 - 1, 0, \ldots, 0), \end{aligned}$$

da (11.5) si ricava $2u(n) \geq (\alpha_1 + \alpha_2 + \alpha_3)v(n) = 3v(n)$, che dimostra l'asserto.

Mostriamo poi che

$$v(n) \geq \left\lceil \frac{4}{3} v(n-1) \right\rceil . \tag{11.21}$$

Dobbiamo distinguere due casi. Nel primo, $A \in V_n$ ha prima riga $(1, 1, 0, \ldots, 0)$ e la matrice ottenuta sopprimendo tale riga ha la forma $(\mathbf{c}_1, \mathbf{c}_2, B)$. La somma degli elementi di $\mathbf{c}_3 := \mathbf{c}_1 + \mathbf{c}_2$ è 3 oppure 4. Per (11.6),

$$\operatorname{per} A = \operatorname{per}(\mathbf{c}_1, B) + \operatorname{per}(\mathbf{c}_2, B) = \operatorname{per}(\mathbf{c}_3, B).$$

Se la somma della colonna $\mathbf{c}_3$ è 3, la matrice $(\mathbf{c}_3, B)$ appartiene a U_{n-1} e la conclusione segue da (11.20). Se la somma è 4, usiamo lo stesso espediente: scriviamo $3\mathbf{c}_3$ come combinazione lineare di quattro vettori $\mathbf{d}_i$ tali che ciascuna matrice $(\mathbf{d}_i, B)$ appartenga a V_{n-1}; otteniamo così $3 \operatorname{per} A \geq 4v(n-1)$. Orig. 106

Nel secondo caso A ha prima riga $(2, 0, \ldots, 0)$. Eliminando la prima riga e la prima colonna si presentano ancora due possibilità: si ottiene una matrice B che appartiene a U_{n-1} oppure a V_{n-1}. Pertanto $\operatorname{per} A \geq 2 \min\{u(n-1), v(n-1)\}$ e la conclusione segue da (11.20). Combinando (11.20) e (11.21) con l'ovvio valore $v(1) = 2$, si ottiene l'asserto del teorema. □

Consideriamo ora una classe più ampia di matrici $n \times n$: quelle a elementi interi non negativi nelle quali tutte le somme delle righe e delle colonne sono uguali a k. Indichiamo questa classe con $\Lambda(n, k)$ e con $\lambda(n, k)$ il minimo permanente nella classe. Ancora una volta si ha $\lambda(m + n, k) \leq \lambda(m, k)\lambda(n, k)$ e, per il lemma di Fekete, possiamo definire

$$\theta(k) := \lim_{n \to \infty} (\lambda(n, k))^{1/n}. \tag{11.22}$$

Dai Teoremi 11.3 e 11.7 sappiamo che $\lambda(n, 2) = 2$ e $\lambda(n, 3) \geq 6(4/3)^{n-3}$. Da (11.19) abbiamo visto sopra che $\lambda(n, k) \geq n!(k/n)^n$. Abbiamo anche osservato un legame fra permanenti e SDR. Mostriamo ora una dimostrazione che sfrutta tale legame.

Teorema 11.8. $\lambda(n, k) \leq k^{2n} / \binom{nk}{n}$.

Dimostrazione. Indichiamo con $\mathcal{P}_{n,k}$ la collezione di tutte le partizioni ordinate dell'insieme $\{1, 2, \ldots, nk\}$ in classi di k elementi. Si ha

$$p_{n,k} := |\mathcal{P}_{n,k}| = \frac{(nk)!}{(k!)^n}. \tag{11.23}$$

Sia $\mathcal{A} := (A_1, \ldots, A_n)$ una di queste partizioni. Il numero degli SDR dei sottoinsiemi $A_1, \ldots, A_n$ è k^n. Consideriamo una seconda partizione $\mathcal{B} := (B_1, \ldots, B_n)$ e indichiamo con $s(\mathcal{A}, \mathcal{B})$ il numero degli SDR comuni ad $\mathcal{A}$ e $\mathcal{B}$. Definiamo una matrice $n \times n$, $A = (\alpha_{ij})$, ponendo $\alpha_{ij} := |A_i \cap B_j|$. Il punto essenziale è che per A conta gli SDR comuni ad $\mathcal{A}$ e $\mathcal{B}$. Inoltre, per definizione delle partizioni, $A \in \Lambda(n, k)$. Dunque $s(\mathcal{A}, \mathcal{B}) = \operatorname{per} A \geq \lambda(n, k)$. Fissati $\mathcal{A} \in \mathcal{P}_{n,k}$ e uno dei suoi SDR, vi sono $n! p_{n,k-1}$ partizioni ordinate $\mathcal{B}$ aventi quello stesso SDR. Pertanto Orig. 107

$$\sum_{\mathcal{B} \in \mathcal{P}_{n,k}} s(\mathcal{A}, \mathcal{B}) = k^n \, n! \, p_{n,k-1}.$$

Combinando questa identità con (11.23) e con la disuguaglianza per $\lambda(n, k)$, troviamo

$$\lambda(n, k) \leq \frac{k^n \, n! \, p_{n,k-1}}{p_{n,k}} = \frac{k^{2n}}{\binom{nk}{n}}.$$

□

Questa dimostrazione è dovuta a Schrijver e Valiant (1980), che diedero anche il seguente corollario.

Corollario. $\theta(k) \le \dfrac{(k-1)^{k-1}}{k^{k-2}}$.

DIMOSTRAZIONE. Segue nel modo consueto dal teorema precedente usando la formula di Stirling: $n! \sim n^n e^{-n}(2\pi n)^{1/2}$. □

Il corollario, insieme con il Teorema 11.7, fornisce un altro valore di $\theta(k)$: $\theta(3) = 4/3$.

Problema 11C. Consideriamo l'insieme degli interi $1, 2, \dots, 64$. Eliminiamo dapprima quelli congrui a 1 modulo 9, cioè $x_1 = 1, \dots, x_8 = 64$. Eliminiamo poi gli interi x_i+8, interpretando 72 come 8. Rimane un insieme S di 48 elementi. Partizioniamo S nei sottoinsiemi $A_1, \dots, A_8$ e anche nei sottoinsiemi $B_1, \dots, B_8$, dove A_i contiene gli interi nell'intervallo $(8(i-1), 8i]$ e B_i quelli congrui a i modulo 8. Quanti SDR comuni hanno i sistemi $A_1, \dots, A_8$ e $B_1, \dots, B_8$?

Problema 11D. Torniamo al Problema 5G. Consideriamo ancora un grafo bipartito regolare di grado 3 su $2n$ vertici. Dare una limitazione inferiore del numero dei suoi accoppiamenti perfetti.

Problema 11E. Su una disposizione circolare degli interi $1, 2, \dots, n$, consideriamo i sottoinsiemi $\{i, i+1, i+2\}$, per $i = 1, 2, \dots, n$, interpretando gli interi modulo n. Quanti SDR possiede questa collezione di insiemi?

Orig. 108

Note

Nel libro *Permanents*, H. Minc (1978) ricorda che il nome *permanente* risale sostanzialmente a Cauchy (1812), sebbene la parola sia stata usata per la prima volta da Muir nel 1882. Eppure un revisore di uno dei primi articoli di Minc lo rimproverò di aver inventato questo nome ridicolo! Per una trattazione estesa dei permanenti rimandiamo al libro di Minc. Vi si trova gran parte della teoria sviluppata soprattutto per risolvere la congettura di Van der Waerden, ancora senza successo all'epoca della stesura.

Il Teorema 11.2 è tratto da Ryser (1963).

Per diversi risultati legati alla congettura di Minc rinviamo a Van Lint (1974).

Il lemma noto come lemma di Fekete compare in Fekete (1923). Per un'altra applicazione rimandiamo a J. W. Moon (1968).

Il termine *matrice doppiamente stocastica* si può motivare interpretando gli elementi come probabilità condizionate. I permanenti, tuttavia, non sembrano svolgere un ruolo importante nella teoria della probabilità.

Le osservazioni su $m(k)$ e $M(k)$ che precedono il Teorema 11.7 si basano sulla formula di Stirling e sulla disuguaglianza collegata $n! \ge n^n e^{-n}$. Quest'ultima si dimostra facilmente per induzione usando il fatto che $(1+n^{-1})^n$ è crescente e tende a e. In realtà la formula di Stirling fu data per la prima volta da de Moivre. Stirling ricavò una serie asintotica per la funzione gamma, da cui segue la stima

$$\Gamma(x) = x^{x-1/2}e^{-x}(2\pi)^{1/2}e^{\theta/(12x)},$$

dove $0 < \theta < 1$; inoltre $n! = \Gamma(n+1)$.

A. Schrijver (1998) ha stabilito l'uguaglianza nel corollario al Teorema 11.8 dimostrando che

$$\lambda(n,k) \ge \left(\frac{(k-1)^{k-1}}{k^{k-2}}\right)^n.$$

Riferimenti bibliografici

L. M. Brégman (1973)
Certain properties of nonnegative matrices and their permanents, *Dokl. Akad. Nauk SSSR* **211**, 27–30 (*Soviet Math. Dokl.* **14**, 945–949).

Orig. 109

M. Fekete (1923)
Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Zeitschr.* **17**, 228–249.

J. H. van Lint (1974)
Combinatorial Theory Seminar Eindhoven University of Technology, Lecture Notes in Mathematics **382**, Springer-Verlag.

H. Minc (1967)
An inequality for permanents of (0,1) matrices, *J. Combinatorial Theory* **2**, 321–326.

H. Minc (1978)
Permanents, Encyclopedia of Mathematics and its Applications, vol. 6, Addison-Wesley; ristampato da Cambridge University Press.

J. W. Moon (1968)
Topics on Tournaments, Holt, Rinehart and Winston.

H. J. Ryser (1963)
Combinatorial Mathematics, Carus Math. Monograph **14**.

A. Schrijver (1978)
A short proof of Minc's conjecture, *J. Combinatorial Theory (A)* **25**, 80–83.

A. Schrijver e W. G. Valiant (1980)
On lower bounds for permanents, *Proc. Kon. Ned. Akad. v. Wetensch. A* **83**, 425–427.

A. Schrijver (1998)
Counting 1-factors in regular bipartite graphs, *J. Combinatorial Theory (B)* **72**, 122–135.

M. Voorhoeve (1979)
A lower bound for the permanents of certain (0,1)-matrices, *Proc. Kon. Ned. Akad. v. Wetensch. A* **82**, 83–86.

Capitolo 12

La congettura di Van der Waerden

In questo capitolo indichiamo con Ω_n l'insieme di tutte le matrici doppiamente stocastiche di ordine n. Orig. 110
Il sottoinsieme delle matrici i cui elementi sono tutti positivi è indicato con Ω_n^*. Definiamo $J_n := n^{-1}J$, dove J denota la matrice $n \times n$ di soli 1. Il vettore $(1, 1, \ldots, 1)^\mathsf{T}$ è indicato con $\mathbf{j}$.

Nel 1926 B. L. van der Waerden propose il problema di determinare il minimo permanente fra tutte le matrici doppiamente stocastiche. Era naturale supporre che tale minimo fosse $\operatorname{per} J_n = n!\, n^{-n}$, come affermato in (11.19). L'asserzione

$$(A \in \Omega_n \text{ e } A \neq J_n) \quad \Longrightarrow \quad \operatorname{per} A > \operatorname{per} J_n \tag{12.1}$$

divenne nota come "congettura di Van der Waerden", sebbene nel 1969 egli abbia detto a uno degli autori di non aver mai sentito prima quel nome e di non aver formulato una simile congettura. Nel 1981 apparvero due diverse dimostrazioni: una di D. I. Falikman, presentata nel 1979, e una di G. P. Egoritsjev, presentata nel 1980. Daremo la nostra versione della dimostrazione di Egoritsjev, il cui risultato era leggermente più forte di quello di Falikman; si veda Van Lint (1981).

Nel seguito chiameremo *matrice minimizzante* una matrice $A \in \Omega_n$ tale che $\operatorname{per} A = \min\{\operatorname{per} S : S \in \Omega_n\}$. Come al solito, A_{ij} denota la matrice ottenuta da A sopprimendo la riga i e la colonna j. Considereremo spesso A come una successione di n colonne, scrivendo $A = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$. Più avanti considereremo permanenti di matrici di ordine $n-1$, ma vorremo usare la notazione per matrici di ordine n. L'espediente consiste nello scrivere $\operatorname{per}(\mathbf{a}_1, \ldots, \mathbf{a}_{n-1}, \mathbf{e}_j)$, dove $\mathbf{e}_j$ è il j-esimo vettore della base canonica. Questo permanente non cambia valore sopprimendo la riga j e l'ultima colonna. Ricordiamo che, per il Orig. 111
Problema 5C (Birkhoff), Ω_n è un insieme convesso avente come vertici le matrici di permutazione.

Ci occorrono alcuni risultati elementari sulle matrici di Ω_n. Il primo enunciato coincide con il Teorema 5.4.

Teorema 12.1. Se A è una matrice $n \times n$ a elementi non negativi, allora $\operatorname{per} A = 0$ se e solo se A contiene una sottomatrice nulla $s \times t$ con $s + t = n + 1$.

Diremo che una matrice $n \times n$ è *parzialmente decomponibile* se contiene una sottomatrice nulla $k \times (n - k)$. Dunque A è parzialmente decomponibile se esistono matrici di permutazione P e Q tali che

$$PAQ = \begin{pmatrix} B & C \\ O & D \end{pmatrix},$$

dove B e D sono quadrate. Una matrice che non sia parzialmente decomponibile sarà detta *totalmente indecomponibile*. Se $A \in \Omega_n$ è parzialmente decomponibile, nella rappresentazione precedente deve essere $C = O$: infatti la somma degli elementi di B è uguale al numero delle sue colonne, mentre la somma degli elementi di B e C è uguale al numero delle righe di B. In questo caso A è quindi la somma diretta $B \oplus D$ di un elemento di Ω_k e di un elemento di Ω_{n-k}.

Problema 12A. Sia A una matrice $n \times n$ a elementi non negativi, con $n \geq 2$. Dimostrare che A è totalmente indecomponibile se e solo se $\operatorname{per} A_{ij} > 0$ per ogni i, j.

Problema 12B. Sia A una matrice $n \times n$ a elementi non negativi. Dimostrare che, se A è totalmente indecomponibile, lo sono anche AA^T e $A^\mathsf{T}A$.

Teorema 12.2. Una matrice minimizzante è totalmente indecomponibile.

DIMOSTRAZIONE. Sia $A \in \Omega_n$ minimizzante e supponiamo che sia parzialmente decomponibile. Come abbiamo visto, $A = B \oplus C$, con $B \in \Omega_k$ e $C \in \Omega_{n-k}$. Per il Teorema 12.1, per $A_{k,k+1} = 0$ e per $A_{k+1,k} = 0$. Per il teorema di Birkhoff possiamo supporre che B e C abbiano elementi diagonali positivi. In A sostituiamo b_{kk} con $b_{kk} - \varepsilon$, c_{11} con $c_{11} - \varepsilon$, e poniamo ε nelle posizioni $(k, k+1)$ e $(k+1, k)$. Per ε abbastanza piccolo la nuova matrice appartiene ancora a Ω_n e il suo permanente è Orig. 112

$$\operatorname{per} A - \varepsilon \operatorname{per} A_{kk} - \varepsilon \operatorname{per} A_{k+1,k+1} + O(\varepsilon^2).$$

Poiché $\operatorname{per} A_{kk}$ e $\operatorname{per} A_{k+1,k+1}$ sono entrambi positivi, per ε sufficientemente piccolo questo permanente è minore di $\operatorname{per} A$. La contraddizione dimostra l'asserto. □

Corollario. (i) Ogni riga di una matrice minimizzante contiene almeno due elementi positivi.

(ii) Per ogni elemento a_{ij} di una matrice minimizzante, esiste una permutazione σ tale che $\sigma(i) = j$ e $a_{s,\sigma(s)} > 0$ per $1 \le s \le n$, $s \ne i$.

DIMOSTRAZIONE. La parte (i) è evidente; la parte (ii) segue dal Problema 12A. □

Vediamo ora fin dove si può arrivare con l'analisi. Un passo molto importante verso la dimostrazione di (12.1) è il seguente sorprendente risultato di Marcus e Newman (1959).

Teorema 12.3. Se $A \in \Omega_n$ è una matrice minimizzante e $a_{hk} > 0$, allora $\operatorname{per} A_{hk} = \operatorname{per} A$.

DIMOSTRAZIONE. Sia S il sottoinsieme di Ω_n formato dalle matrici doppiamente stocastiche X per le quali $x_{ij} = 0$ quando $a_{ij} = 0$. La matrice A è un punto interno di S, considerato come sottoinsieme di un opportuno $\mathbb{R}^m$. Denotando con Z l'insieme delle coppie (i, j) per cui $a_{ij} = 0$, possiamo descrivere S mediante le relazioni

$$\begin{aligned}
\sum_{i=1}^{n} x_{ij} &= 1, && j = 1, \dots, n;\\
\sum_{j=1}^{n} x_{ij} &= 1, && i = 1, \dots, n;\\
x_{ij} &\ge 0, && i, j = 1, \dots, n;\\
x_{ij} &= 0, && (i, j) \in Z.
\end{aligned}$$

Poiché A è minimizzante, la funzione permanente ha un minimo relativo nel punto interno A di S. Possiamo quindi usare i moltiplicatori di Lagrange e definire Orig. 113

$$F(X) := \operatorname{per} X - \sum_{i=1}^{n} \lambda_i \left(\sum_{k=1}^{n} x_{ik} - 1 \right) - \sum_{j=1}^{n} \mu_j \left(\sum_{k=1}^{n} x_{kj} - 1 \right).$$

Per $(i, j) \notin Z$ si ha

$$\frac{\partial F(X)}{\partial x_{ij}} = \operatorname{per} X_{ij} - \lambda_i - \mu_j.$$

Ne segue $\operatorname{per} A_{ij} = \lambda_i + \mu_j$. Per $1 \le i \le n$ ricaviamo quindi

$$\operatorname{per} A = \sum_{j=1}^{n} a_{ij} \operatorname{per} A_{ij} = \sum_{j=1}^{n} a_{ij}(\lambda_i + \mu_j) = \lambda_i + \sum_{j=1}^{n} a_{ij}\mu_j, \tag{12.2}$$

e analogamente, per $1 \le j \le n$,

$$\operatorname{per} A = \mu_j + \sum_{i=1}^{n} a_{ij}\lambda_i. \tag{12.3}$$

Introduciamo i vettori $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n)^{\mathsf{T}}$ e $\boldsymbol{\mu} = (\mu_1, \dots, \mu_n)^{\mathsf{T}}$. Da (12.2) e (12.3) otteniamo

$$(\operatorname{per} A)\mathbf{j} = \boldsymbol{\lambda} + A\boldsymbol{\mu} = \boldsymbol{\mu} + A^{\mathsf{T}}\boldsymbol{\lambda}. \tag{12.4}$$

Moltiplicando per A^{T} troviamo

$$(\operatorname{per} A)\mathbf{j} = A^{\mathsf{T}}\boldsymbol{\lambda} + A^{\mathsf{T}}A\boldsymbol{\mu},$$

e quindi $\boldsymbol{\mu} = A^{\mathsf{T}}A\boldsymbol{\mu}$; analogamente $\boldsymbol{\lambda} = AA^{\mathsf{T}}\boldsymbol{\lambda}$. Le matrici AA^{T} e $A^{\mathsf{T}}A$ appartengono entrambe a Ω_n e, per il Problema 12B e il Teorema 12.2, hanno autovalore 1 di molteplicità uno, corrispondente all'autovettore $\mathbf{j}$. Dunque $\boldsymbol{\lambda}$ e $\boldsymbol{\mu}$ sono entrambi multipli di $\mathbf{j}$. Per (12.4), $\lambda_i + \mu_j = \operatorname{per} A$; poiché $\operatorname{per} A_{ij} = \lambda_i + \mu_j$, la dimostrazione è conclusa. □ Orig. 114

Osservazione. Marcus e Newman mostrarono che dal Teorema 12.3 segue che una matrice minimizzante in Ω_n^* deve essere J_n. La dimostrazione si basa sull'idea seguente. Sia $A \in \Omega_n$ tale che $\operatorname{per} A_{hk} = \operatorname{per} A$ per ogni h, k. Se sostituiamo una qualsiasi colonna di A con un vettore $\mathbf{x}$ la cui somma delle coordinate è 1, il valore del permanente non cambia, per (11.6). Chiameremo questa osservazione *principio di sostituzione*. Se A è una matrice minimizzante in Ω_n^*, il principio permette di sostituire due colonne qualsiasi con la loro media e di ottenere così una nuova matrice minimizzante. Si costruisce in questo modo una successione di matrici minimizzanti che tende a J_n. L'unicità del minimo richiede ancora un po' di lavoro.

Un ultimo risultato che utilizza idee dell'analisi è la seguente generalizzazione del Teorema 12.3, dovuta a London (1971).

Teorema 12.4. Se $A \in \Omega_n$ è una matrice minimizzante, allora $\operatorname{per} A_{ij} \geq \operatorname{per} A$ per ogni i, j.

DIMOSTRAZIONE. Fissiamo i, j. Per il Corollario (ii) del Teorema 12.2 esiste una permutazione σ tale che $\sigma(i) = j$ e $a_{s,\sigma(s)} > 0$ per $1 \leq s \leq n$, $s \neq i$. Sia P la corrispondente matrice di permutazione. Per $0 \leq \theta \leq 1$ definiamo $f(\theta) := \operatorname{per}((1-\theta)A + \theta P)$. Poiché A è minimizzante, $f'(0) \geq 0$, cioè

$$0 \leq \sum_{i=1}^{n}\sum_{j=1}^{n}(-a_{ij} + p_{ij}) \operatorname{per} A_{ij} = -n \operatorname{per} A + \sum_{s=1}^{n} \operatorname{per} A_{s,\sigma(s)}.$$

Per il Teorema 12.3 si ha $\operatorname{per} A_{s,\sigma(s)} = \operatorname{per} A$ per $s \neq i$; dunque $\operatorname{per} A_{ij} \geq \operatorname{per} A$. □

Problema 12C. Mostrare che dal Teorema 12.3 segue che, se $A \in \Omega_5^*$ è minimizzante, esiste una matrice minimizzante $B \in \Omega_5^*$ avente come sottomatrice principale una matrice aJ di ordine 4. Mostrare poi che necessariamente $a = 1/5$.

Arriviamo allo strumento principale della dimostrazione della congettura di Van der Waerden. Questa volta occorre l'algebra lineare. Daremo una dimostrazione diretta di un teorema sulle forme bilineari simmetriche che conduce alla disuguaglianza ricavata da Egoritsjev dalle cosiddette disuguaglianze di Alexandroff–Fenchel, che qui non tratteremo. Orig. 115

Consideriamo $\mathbb{R}^n$ con un prodotto interno simmetrico $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\mathsf{T} Q \mathbf{y}$. Se Q ha un autovalore positivo e $n-1$ autovalori negativi, parleremo di *spazio di Lorentz*. Usiamo la terminologia abituale: un vettore non nullo $\mathbf{x}$ è *isotropo* se $\langle \mathbf{x}, \mathbf{x} \rangle = 0$; è *positivo*, rispettivamente *negativo*, se $\langle \mathbf{x}, \mathbf{x} \rangle$ è positivo, rispettivamente negativo.

Ogni vettore non nullo nel sottospazio di dimensione $n-1$ generato dagli autovettori negativi è negativo. Pertanto, se $\mathbf{a}$ è positivo e $\mathbf{b}$ non è un suo multiplo scalare, il piano generato da $\mathbf{a}$ e $\mathbf{b}$ deve contenere un vettore negativo. Il polinomio quadratico in λ dato da $\langle \mathbf{a} + \lambda\mathbf{b}, \mathbf{a} + \lambda\mathbf{b} \rangle$ deve quindi avere discriminante positivo. Otteniamo così la seguente disuguaglianza, analoga a quella di Cauchy ma con il verso opposto.

Teorema 12.5. Se $\mathbf{a}$ è un vettore positivo in uno spazio di Lorentz e $\mathbf{b}$ è arbitrario, allora

$$\langle \mathbf{a}, \mathbf{b} \rangle^2 \geq \langle \mathbf{a}, \mathbf{a} \rangle \langle \mathbf{b}, \mathbf{b} \rangle,$$

con uguaglianza se e solo se $\mathbf{b} = \lambda\mathbf{a}$ per una costante λ.

Il legame con i permanenti è fornito dalla definizione seguente. Consideriamo vettori $\mathbf{a}_1, \ldots, \mathbf{a}_{n-2}$ in $\mathbb{R}^n$ con coordinate positive e, come al solito, la base canonica $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Definiamo un prodotto interno su $\mathbb{R}^n$ mediante

$$\langle \mathbf{x}, \mathbf{y} \rangle := \operatorname{per}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-2}, \mathbf{x}, \mathbf{y}), \tag{12.5}$$

ossia $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\mathsf{T} Q \mathbf{y}$, dove

$$q_{ij} := \operatorname{per}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-2}, \mathbf{e}_i, \mathbf{e}_j). \tag{12.6}$$

Si osservi che, se da una matrice A con colonne $\mathbf{a}_1, \ldots, \mathbf{a}_n$ si eliminano le ultime due colonne e le righe di indici i, j, il permanente della matrice ridotta è q_{ij}. Orig. 116

Teorema 12.6. Lo spazio $\mathbb{R}^n$ con il prodotto interno definito da (12.5) è uno spazio di Lorentz.

DIMOSTRAZIONE. Procediamo per induzione. Per $n = 2$ si ha $Q = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ e l'asserto è vero. Supponiamo che il teorema valga per $\mathbb{R}^{n-1}$. Nel primo passo mostriamo che Q non ha autovalore 0. Supponiamo $Q\mathbf{c} = 0$, cioè

$$\operatorname{per}(\mathbf{a}_1, \ldots, \mathbf{a}_{n-2}, \mathbf{c}, \mathbf{e}_j) = 0 \qquad (1 \leq j \leq n). \tag{12.7}$$

Eliminando l'ultima colonna e la riga j, possiamo considerare (12.7) come una relazione fra vettori di $\mathbb{R}^{n-1}$. Consideriamo il prodotto interno dato da

$$\operatorname{per}(\mathbf{a}_1, \dots, \mathbf{a}_{n-3}, \mathbf{x}, \mathbf{y}, \mathbf{e}_j), \tag{12.8}$$

e applichiamo l'ipotesi induttiva, (12.7) e il Teorema 12.5. Ponendo $\mathbf{x} = \mathbf{a}_{n-2}$ e $\mathbf{y} = \mathbf{a}_{n-2}$ in (12.8) si ottiene un valore positivo; ponendo $\mathbf{x} = \mathbf{a}_{n-2}$ e $\mathbf{y} = \mathbf{c}$ si ottiene 0. Pertanto

$$\operatorname{per}(\mathbf{a}_1, \dots, \mathbf{a}_{n-3}, \mathbf{c}, \mathbf{c}, \mathbf{e}_j) \le 0 \qquad (1 \le j \le n), \tag{12.9}$$

e per ogni j l'uguaglianza vale se e solo se tutte le coordinate di $\mathbf{c}$, eccetto c_j, sono nulle. Moltiplicando il primo membro di (12.9) per la coordinata j-esima di $\mathbf{a}_{n-2}$ e sommando su j, si ottiene $\mathbf{c}^{\mathsf{T}} Q \mathbf{c}$. L'ipotesi $Q\mathbf{c} = 0$ implica quindi $\mathbf{c} = 0$.

Per $0 \le \theta \le 1$ definiamo Q_θ mediante (12.5), sostituendo ciascun $\mathbf{a}_i$ con $\theta \mathbf{a}_i + (1-\theta)\mathbf{j}$. Quanto appena dimostrato implica che Q_θ non ha autovalore 0 per nessun $\theta \in [0,1]$. Il numero degli autovalori positivi è dunque costante. Poiché per $\theta = 0$ tale numero è uno, lo è anche per $\theta = 1$, e l'asserto è dimostrato. □

Formuliamo la combinazione dei Teoremi 12.5 e 12.6 come corollario. L'ultima affermazione segue per continuità.

Corollario. Se $\mathbf{a}_1, \dots, \mathbf{a}_{n-1}$ sono vettori di $\mathbb{R}^n$ con coordinate positive e $\mathbf{b} \in \mathbb{R}^n$, allora

$$\big(\operatorname{per}(\mathbf{a}_1, \dots, \mathbf{a}_{n-1}, \mathbf{b})\big)^2 \ge \operatorname{per}(\mathbf{a}_1, \dots, \mathbf{a}_{n-1}, \mathbf{a}_{n-1}) \cdot \operatorname{per}(\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}, \mathbf{b}),$$

e l'uguaglianza vale se e solo se $\mathbf{b} = \lambda \mathbf{a}_{n-1}$ per una costante λ. La disuguaglianza resta valida se alcune coordinate dei vettori $\mathbf{a}_i$ sono nulle, ma in tal caso non si può più affermare la conclusione relativa al caso di uguaglianza. Orig. 117

Possiamo ora generalizzare il Teorema 12.3.

Teorema 12.7. Se $A \in \Omega_n$ è minimizzante, allora $\operatorname{per} A_{ij} = \operatorname{per} A$ per ogni i, j.

Dimostrazione. Supponiamo che l'asserto sia falso. Per il Teorema 12.4 esiste allora una coppia r, s tale che $\operatorname{per} A_{rs} > \operatorname{per} A$. Scegliamo t con $a_{rt} > 0$. Consideriamo il prodotto di due fattori per A. Nel primo sostituiamo $\mathbf{a}_s$ con $\mathbf{a}_t$, nel secondo sostituiamo $\mathbf{a}_t$ con $\mathbf{a}_s$. Sviluppiamo poi il primo permanente secondo la colonna s e il secondo secondo la colonna t. Per il Teorema 12.5 e il corollario al Teorema 12.6 si ha

$$(\operatorname{per} A)^2 \ge \left(\sum_{k=1}^{n} a_{kt} \operatorname{per} A_{ks} \right) \left(\sum_{k=1}^{n} a_{ks} \operatorname{per} A_{kt} \right).$$

Per il Teorema 12.4, ciascun sottopermanente a destra è almeno per A, e per $A_{rs} > \operatorname{per} A$. Poiché per A_{rs} è moltiplicato per $a_{rt} > 0$, il secondo membro è maggiore di $(\operatorname{per} A)^2$: una contraddizione. □

Usiamo ora il principio di sostituzione nel modo seguente. Presa una matrice minimizzante A, siano $\mathbf{u}, \mathbf{v}$ due sue colonne. Sostituendole entrambe con $\frac{1}{2}(\mathbf{u} + \mathbf{v})$ si ottiene ancora una matrice minimizzante, per il Teorema 12.7.

Sia A una matrice minimizzante qualsiasi e sia $\mathbf{b}$ una sua colonna, per esempio l'ultima. Per il Corollario (i) al Teorema 12.2 ogni riga di A contiene almeno due elementi positivi. Applichiamo ripetutamente il principio di sostituzione, come appena descritto, senza mai modificare l'ultima colonna. Possiamo così trovare una matrice minimizzante $A' = (\mathbf{a}'_1, \dots, \mathbf{a}'_{n-1}, \mathbf{b})$ in cui $\mathbf{a}'_1, \dots, \mathbf{a}'_{n-1}$ hanno tutte coordinate positive. Applichiamo il corollario al Teorema 12.6. Per il principio di sostituzione deve valere l'uguaglianza. Dunque $\mathbf{b}$ è multiplo di $\mathbf{a}'_i$ per ogni $1 \le i \le n-1$. Ne segue $\mathbf{b} = n^{-1}\mathbf{j}$ e pertanto $A = J_n = n^{-1}J$, il che conclude la dimostrazione della congettura di Van der Waerden.[1] Orig. 118

Teorema 12.8. L'implicazione (12.1) è vera.

Note

Per una panoramica delle due dimostrazioni della congettura di Van der Waerden rimandiamo a Van Lint (1982), dove si trovano anche osservazioni storiche e un simpatico aneddoto sulla congettura.

[1] Nota redazionale: nell'ultima uguaglianza del testo originale compare $A = n^{-1}J_n$, incompatibile con la definizione $J_n = n^{-1}J$ data all'inizio del capitolo. Qui è esplicitata la normalizzazione coerente con quella definizione.

B. L. van der Waerden (1903–1996), matematico olandese, fu noto soprattutto per il lavoro in algebra, sebbene abbia pubblicato in vari campi. La sua opera *Moderne Algebra* (1931) segnò l'orientamento della disciplina per molti decenni.

Il libro di Minc sui permanenti è il miglior riferimento per tutto il lavoro svolto sulla congettura di Van der Waerden fino al 1978.

Il nome *spazio di Lorentz* è legato alla teoria della relatività e al gruppo delle trasformazioni che lasciano invariata la forma quadratica $x^2 + y^2 + z^2 - t^2$. H. A. Lorentz fu un fisico olandese insignito del premio Nobel per le sue ricerche.

Riferimenti bibliografici

J. H. van Lint (1981)
Notes on Egoritsjev's proof of the Van der Waerden conjecture, *Linear Algebra and its Applications* **39**, 1–8.

J. H. van Lint (1982)
The van der Waerden Conjecture: Two proofs in one year, *The Math. Intelligencer* **39**, 72–77.

D. London (1971)
Some notes on the van der Waerden conjecture, *Linear Algebra and its Applications* **4**, 155–160.

M. Marcus e M. Newman (1959)
On the minimum of the permanent of a doubly stochastic matrix, *Duke Math. J.* **26**, 61–72.

H. Minc (1978)
Permanents, Encyclopedia of Mathematics and its Applications, vol. 6, Addison-Wesley; ristampato da Cambridge University Press (1984).

B. L. van der Waerden (1926)
Jber. D. M. V. **35**.

Capitolo 13

Conteggio elementare; numeri di Stirling

I prossimi capitoli saranno dedicati alle tecniche di conteggio e ad alcuni particolari problemi enumerativi combinatori. Cominciamo con vari metodi elementari di uso frequente. Consideriamo le applicazioni da $\{1, 2, \dots, n\}$ a $\{1, 2, \dots, k\}$: sono in totale k^n. Nell'Esempio 10.2 abbiamo studiato il caso in cui si richiede che siano suriettive; torneremo sulla questione nel Teorema 13.5. Se le applicazioni sono iniettive, il loro numero è il *fattoriale decrescente* Orig. 119

$$(k)_n := k(k-1)\cdots(k-n+1) = \frac{k!}{(k-n)!}. \tag{13.1}$$

Consideriamo ora un problema analogo. Gli n oggetti da associare non sono più distinguibili, mentre lo sono le loro immagini. Possiamo formulare il problema così: dobbiamo distribuire n palline indistinguibili in k scatole numerate $1, 2, \dots, k$. In quanti modi diversi è possibile farlo? La soluzione si trova mediante l'espediente seguente. Immaginiamo che le palline siano blu e disponiamole in fila davanti alle scatole cui sono destinate. Inseriamo poi una pallina rossa fra ogni coppia di scatole consecutive. Otteniamo una fila di $n + k - 1$ palline, di cui $k - 1$ rosse, che descrive la distribuzione. La risposta è quindi $\binom{n+k-1}{k-1}$. Formuliamola come teorema.

Teorema 13.1. Il numero delle soluzioni in interi non negativi dell'equazione

$$x_1 + x_2 + \cdots + x_k = n \tag{13.2}$$

è $\binom{n+k-1}{k-1}$.

DIMOSTRAZIONE. Basta interpretare x_i come il numero delle palline nella scatola i. □ Orig. 120

Corollario. Il numero delle soluzioni in interi positivi dell'equazione (13.2) è $\binom{n-1}{k-1}$.

DIMOSTRAZIONE. Sostituiamo x_i con $y_i := x_i - 1$. Allora $\sum y_i = n - k$. Applichiamo il Teorema 13.1.□

Esempio 13.1. Per analogia con la questione incontrata nell'Esempio 10.6, consideriamo il problema di scegliere r interi fra $1, 2, \dots, n$ in modo che non ve ne siano due consecutivi. Sia $x_1 < x_2 < \cdots < x_r$ una successione di questo tipo. Allora $x_1 \geq 1$, $x_2 - x_1 \geq 2$, …, $x_r - x_{r-1} \geq 2$. Definiamo

$$y_1 := x_1, \qquad y_i := x_i - x_{i-1} - 1 \quad (2 \leq i \leq r), \qquad y_{r+1} := n - x_r + 1.$$

Gli y_i sono interi positivi e $\sum_{i=1}^{r+1} y_i = n - r + 2$. Per il corollario al Teorema 13.1 vi sono $\binom{n-r+1}{r}$ soluzioni.

Problema 13A. Su una disposizione circolare con n posizioni vogliamo collocare gli interi $1, 2, \dots, r$ in ordine orario, in modo che interi consecutivi, compresa la coppia $(r, 1)$, non occupino posizioni adiacenti. Disposizioni ottenute l'una dall'altra per rotazione sono considerate uguali. In quanti modi si può procedere?

Esempio 13.2. In quanti modi possiamo disporre r_1 palline del colore 1, r_2 del colore 2, …, r_k del colore k in una successione di lunghezza $n := r_1 + r_2 + \cdots + r_k$? Numerando le palline da 1 a n si hanno

$n!$ disposizioni. Poiché ignoriamo la numerazione, ogni permutazione delle r_i palline del colore i, per $1 \le i \le k$, produce la stessa disposizione. La risposta è quindi il coefficiente multinomiale $\binom{n}{r_1,\dots,r_k}$; si veda (2.1).

Esempio 13.3. Vogliamo suddividere $\{1, 2, \dots, n\}$ in b_1 sottoinsiemi di cardinalità 1, b_2 di cardinalità 2, ..., b_k di cardinalità k, dove $\sum_{i=1}^{k} ib_i = n$. Si applica lo stesso argomento dell'Esempio 13.2. Inoltre i sottoinsiemi della stessa cardinalità possono essere permutati fra loro senza modificare la configurazione. La soluzione è dunque

$$\frac{n!}{b_1! \cdots b_k! (1!)^{b_1} (2!)^{b_2} \cdots (k!)^{b_k}}. \tag{13.3}$$

Diversi problemi di conteggio, spesso con coefficienti binomiali, possono essere affrontati in un modo più o meno ovvio, che conduce a un calcolo talvolta difficile. Spesso esiste però un modo "combinatorio", meno ovvio, che dà immediatamente la risposta. Ecco alcuni esempi. Orig. 121

Esempio 13.4. Sia A variabile fra tutti i sottoinsiemi di $\{1, 2, \dots, n\}$. Calcolare $S = \sum |A|$. Poiché vi sono $\binom{n}{i}$ sottoinsiemi di cardinalità i, sembra necessario calcolare $\sum_{i=0}^{n} i\binom{n}{i}$. Derivando $(1+x)^n$ troviamo

$$\sum_{i=1}^{n} i\binom{n}{i} x^{i-1} = n(1+x)^{n-1};$$

ponendo $x = 1$ si ottiene $S = n2^{n-1}$. Se avessimo riflettuto un po' di più, la risposta sarebbe stata evidente! Un insieme A e il suo complementare contengono insieme n elementi, e tali coppie sono esattamente 2^{n-1}.

Esempio 13.5. Nel Capitolo 10 abbiamo incontrato formule con coefficienti binomiali la cui dimostrazione combinatoria era più semplice di quella diretta. La nota relazione

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} \tag{13.4}$$

ne è un altro esempio. Naturalmente la somma si può calcolare determinando il coefficiente di x^n in $(1+x)^n(1+x)^n$ e usando la formula binomiale. Tuttavia ciascun membro di (13.4) conta, in due modi diversi, le scelte di n palline da un insieme formato da n palline rosse e n blu.

Problema 13B. Mostrare che la seguente formula per i coefficienti binomiali è una conseguenza diretta di (10.6):

$$\binom{n+1}{a+b+1} = \sum_{k=0}^{n} \binom{k}{a}\binom{n-k}{b}.$$

Dare una dimostrazione combinatoria considerando i sottoinsiemi di cardinalità $a+b+1$ di $\{0, 1, \dots, n\}$, ordinandone gli elementi in modo crescente e osservando poi il valore dell'intero che occupa la posizione $a+1$.

Esempio 13.6. Consideriamo un esempio un po' più complicato, nel quale le conoscenze precedenti potrebbero portarci a una soluzione laboriosa. Quante successioni $A_1, \dots, A_k$ soddisfano $A_i \subseteq \{1, 2, \dots, n\}$, $1 \le i \le k$, e $\bigcup_{i=1}^{k} A_i = \{1, 2, \dots, n\}$? Poiché vogliamo evitare che un intero j, $1 \le j \le n$, non appartenga all'unione degli A_i, siamo tentati di usare l'inclusione-esclusione. Scegliendo i elementi di $\{1, 2, \dots, n\}$ e considerando tutte le successioni $A_1, \dots, A_k$ che non contengono nessuno di tali elementi, troviamo $(2^{n-i})^k$ successioni. Per il Teorema 10.1 la soluzione è quindi Orig. 122

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} 2^{(n-i)k} = (2^k - 1)^n.$$

La risposta mostra che sarebbe stato preferibile un altro approccio. Descriviamo una successione $A_1, \dots, A_k$ mediante una matrice $(0,1)$ di dimensioni $k \times n$, le cui righe sono le funzioni caratteristiche dei sottoinsiemi. La condizione equivale a richiedere che la matrice non abbia colonne nulle. Vi sono dunque $(2^k - 1)^n$ matrici di questo tipo!

Problema 13C. Dare una soluzione che utilizzi coefficienti binomiali e una soluzione combinatoria della seguente questione: quante coppie (A_1, A_2) di sottoinsiemi di $\{1, 2, \dots, n\}$ soddisfano $A_1 \cap A_2 = \varnothing$?

Problema 13D. Sia S l'insieme di tutte le k-uple ordinate $\mathcal{A} = (A_1, \dots, A_k)$ di sottoinsiemi di $\{1, 2, \dots, n\}$. Determinare

$$\sum_{\mathcal{A}\in S} |A_1 \cup A_2 \cup \cdots \cup A_k|.$$

Problema 13E. La nota relazione

$$\sum_{m=k}^{l} \binom{m}{k} = \binom{l+1}{k+1}$$

si dimostra facilmente per induzione. Il lettore che lo desideri può trovarne una dimostrazione più complicata usando (10.6). Trovarne una dimostrazione combinatoria contando i cammini da $(0,0)$ a $(l+1, k+1)$ nel piano X-Y, in cui ciascun passo sia del tipo $(x, y) \mapsto (x+1, y)$ oppure $(x, y) \mapsto (x+1, y+1)$. Usare poi la formula per mostrare che il numero delle soluzioni in interi non negativi di

$$x_1 + x_2 + \cdots + x_k \le n$$

è $\binom{n+k}{k}$. Sapete dimostrare quest'ultimo risultato combinatoriamente?

Orig. 123

È spesso possibile dimostrare relazioni fra coefficienti binomiali considerando formalmente $\binom{a}{k}$ come il polinomio in a definito da

$$\binom{a}{k} := \frac{a(a-1)\cdots(a-k+1)}{k!}.$$

Se due polinomi di grado al più k coincidono per $k+1$ valori della variabile, sono identici. Diamo un esempio. Poniamo

$$F(a) := \sum_{k=0}^{n} \binom{a}{k} x^k y^{n-k}, \qquad G(a) := \sum_{k=0}^{n} \binom{n-a}{k} (-x)^k (x+y)^{n-k}.$$

Per il teorema binomiale, se a è un intero nell'intervallo $[0, n]$, si ha $F(a) = (x+y)^a y^{n-a}$; ancora per il teorema binomiale, lo stesso vale per $G(a)$. I polinomi sono quindi identici e possiamo sostituire numeri qualsiasi ad a, x, y per ottenere relazioni fra coefficienti binomiali. Per esempio, $y = 2x$ e $a = 2n+1$ danno

$$\sum_{k=0}^{n} \binom{2n+1}{k} 2^{n-k} = \sum_{k=0}^{n} \binom{n+k}{k} 3^{n-k},$$

una relazione che sarebbe estremamente difficile dimostrare mediante conteggio.

Due famiglie di numeri che compaiono in molti problemi combinatori sono i cosiddetti *numeri di Stirling della prima e della seconda specie*. Spesso sono definiti dalle formule (13.8) e (13.12) che daremo più avanti; preferiamo una definizione combinatoria.

Sia $c(n, k)$ il numero delle permutazioni $\pi \in S_n$ aventi esattamente k cicli. Questo numero si chiama *numero di Stirling senza segno della prima specie*. Poniamo inoltre $c(0,0) = 1$ e $c(n, k) = 0$ se $n \le 0$ oppure $k \le 0$, con $(n, k) \ne (0, 0)$. I numeri di Stirling della prima specie $s(n, k)$ sono definiti da

$$s(n, k) := (-1)^{n-k} c(n, k). \tag{13.5}$$

Orig. 124

Teorema 13.2. I numeri $c(n, k)$ soddisfano la relazione di ricorrenza

$$c(n, k) = (n-1)c(n-1, k) + c(n-1, k-1). \tag{13.6}$$

DIMOSTRAZIONE. Se $\pi \in S_{n-1}$ ha k cicli, vi sono $n-1$ posizioni in cui inserire l'intero n per ottenere una permutazione $\pi' \in S_n$ con k cicli. Possiamo anche aggiungere il ciclo (n) a una qualsiasi permutazione di S_{n-1} con $k-1$ cicli. Queste due possibilità spiegano i due termini del secondo membro di (13.6). □

Teorema 13.3. Per $n \ge 0$ si ha

$$\sum_{k=0}^{n} c(n, k) x^k = x(x+1)\cdots(x+n-1) \tag{13.7}$$

e

$$\sum_{k=0}^{n} s(n,k)x^k = (x)_n, \tag{13.8}$$

dove $(x)_n$ è definito come in (13.1).

DIMOSTRAZIONE. Scriviamo il secondo membro di (13.7) come $F_n(x) = \sum_{k=0}^{n} b(n,k)x^k$. Chiaramente $b(0,0) = 1$. Poniamo $b(n,k) := 0$ se $n \leq 0$ oppure $k \leq 0$, con $(n,k) \neq (0,0)$. Poiché

$$\begin{aligned} F_n(x) &= (x+n-1)F_{n-1}(x) \\ &= \sum_{k=1}^{n} b(n-1,k-1)x^k + (n-1)\sum_{k=0}^{n-1} b(n-1,k)x^k, \end{aligned}$$

i numeri $b(n,k)$ soddisfano la stessa ricorrenza (13.6) dei numeri $c(n,k)$. Essendo uguali per $n \leq 0$ oppure $k \leq 0$, coincidono per ogni n,k. Per dimostrare (13.8), sostituiamo x con $-x$ e usiamo (13.5). □ Orig. 125

Osserviamo che si può dare una dimostrazione combinatoria di (13.7), mostrando che i due membri contano gli stessi oggetti.

Definiamo ora i *numeri di Stirling della seconda specie*. Indichiamo con $P(n,k)$ l'insieme di tutte le partizioni di un insieme di n elementi in k sottoinsiemi non vuoti, detti *blocchi*. Poniamo

$$S(n,k) := |P(n,k)|. \tag{13.9}$$

Anche qui $S(0,0) = 1$; poniamo uguali a 0 i numeri per tutti i valori dei parametri non coperti dalla definizione precedente. Si ha ancora una semplice ricorrenza.

Teorema 13.4. I numeri di Stirling della seconda specie soddisfano

$$S(n,k) = kS(n-1,k) + S(n-1,k-1). \tag{13.10}$$

DIMOSTRAZIONE. La dimostrazione è quasi la stessa di quella del Teorema 13.3. Da una partizione di $\{1,2,\ldots,n-1\}$ si ottiene una partizione di $\{1,2,\ldots,n\}$ aggiungendo n a uno dei blocchi, oppure aumentando di uno il numero dei blocchi mediante il nuovo blocco $\{n\}$. □

Definiamo il *numero di Bell* $B(n)$ come il numero totale delle partizioni di un insieme di n elementi, cioè

$$B(n) := \sum_{k=1}^{n} S(n,k) \qquad (n \geq 1). \tag{13.11}$$

Per i numeri di Stirling della seconda specie vale una formula analoga a (13.8).

Teorema 13.5. Per $n \geq 0$ si ha

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k. \tag{13.12}$$

DIMOSTRAZIONE. Osserviamo anzitutto che, per (13.9), il numero delle applicazioni suriettive da un insieme di n elementi a uno di k elementi è $k!S(n,k)$: ogni blocco della partizione è la controimmagine di un elemento del secondo insieme. Per l'Esempio 10.2, Orig. 126

$$S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n. \tag{13.13}$$

Sia ora x intero. Vi sono x^n applicazioni dall'insieme $N := \{1,2,\ldots,n\}$ all'insieme $\{1,2,\ldots,x\}$. Per ogni suo sottoinsieme Y di cardinalità k, vi sono $k!S(n,k)$ suriezioni da N a Y. Pertanto

$$x^n = \sum_{k=0}^{n}\binom{x}{k}k!S(n,k) = \sum_{k=0}^{n} S(n,k)(x)_k.$$

□

Nell'Esempio 10.1 abbiamo visto che può essere utile associare a una successione $a_1, a_2, \ldots$ una cosiddetta *funzione generatrice*. Nel Capitolo 14 ne vedremo molte applicazioni. Qui trattiamo le funzioni generatrici dei numeri di Stirling.

Teorema 13.6. $\displaystyle\sum_{n\geq k} S(n,k)\frac{x^n}{n!} = \frac{1}{k!}(e^x-1)^k$ per $k \geq 0$.

DIMOSTRAZIONE. Indichiamo con $F_k(x)$ la somma a sinistra. Per (13.10),

$$F_k'(x) = kF_k(x) + F_{k-1}(x).$$

Il risultato segue per induzione. Poiché $S(n,1) = 1$, l'asserto è vero per $k = 1$. L'ipotesi induttiva dà un'equazione differenziale per F_k che, insieme con la condizione $S(k,k) = 1$, ha come unica soluzione il secondo membro dell'identità enunciata. □

Per i numeri di Stirling della prima specie trovare la funzione generatrice è un po' più difficile.

Teorema 13.7. $\displaystyle\sum_{n=k}^{\infty} s(n,k)\frac{z^n}{n!} = \frac{1}{k!}\big(\log(1+z)\big)^k$.

DIMOSTRAZIONE. Poiché

$$(1+z)^x = e^{x\log(1+z)} = \sum_{k=0}^{\infty}\frac{1}{k!}\big(\log(1+z)\big)^k x^k,$$

il secondo membro dell'asserto è il coefficiente di x^k nello sviluppo di $(1+z)^x$. D'altra parte, per $|z| < 1$, Orig. 127

$$\begin{aligned}(1+z)^x &= \sum_{n=0}^{\infty}\binom{x}{n}z^n = \sum_{n=0}^{\infty}\frac{1}{n!}(x)_n z^n \\ &= \sum_{n=0}^{\infty}\frac{z^n}{n!}\sum_{r=0}^{n} s(n,r)x^r = \sum_{r=0}^{\infty}x^r\sum_{n=r}^{\infty}s(n,r)\frac{z^n}{n!}.\end{aligned}$$

La dimostrazione è così conclusa. □

Problema 13F. Mostrare direttamente che il numero delle permutazioni degli interi da 1 a n aventi un numero pari di cicli coincide con quello delle permutazioni aventi un numero dispari di cicli, per $n > 1$. Mostrare anche che il risultato segue dal Teorema 13.7.

Infine, i numeri di Stirling della prima e della seconda specie sono legati da

$$\sum_{k=m}^{n} S(n,k)s(k,m) = \delta_{mn}. \tag{13.14}$$

La formula segue immediatamente sostituendo (13.8) in (13.12). Poiché tanto le funzioni x^n quanto le funzioni $(x)_n$, con $n \geq 0$, formano una base dello spazio vettoriale $\mathbb{C}[x]$, (13.14) non è altro che l'usuale relazione fra le matrici di cambiamento di base.

Problema 13G. Mostrare che (13.12) conduce a $B(n) = \dfrac{1}{e}\displaystyle\sum_{k=0}^{\infty}\frac{k^n}{k!}$.

Problema 13H. Sia A la matrice $n \times n$ con $a_{ij} := \binom{i}{j}$, per $i, j = 0, \ldots, n-1$. Determinare A^{-1}.

Problema 13I. Ponendo $x = 1/2$ in (10.6), si trova $\sum_{j=0}^{\infty}\binom{a+j}{j}2^{-j} = 2^{a+1}$. Usando un metodo di questo capitolo, dimostrare che

$$\sum_{j=0}^{a}\binom{a+j}{j}2^{-j} = 2^a.$$

Dimostrare lo stesso risultato direttamente, definendo

$$a_n = \sum_{j=0}^{a}\binom{a+j}{j}2^{-a-j},$$

e sostituendo la ricorrenza fondamentale per i coefficienti binomiali, così da ottenere $a_n = \frac{1}{2}a_n + \frac{1}{2}a_{n-1}$.[1] Orig. 128

[1] Nota redazionale: l'originale usa qui a_n per una somma parametrizzata da a. Per rendere coerenti gli indici nel calcolo diretto si può porre $a = n$ nella definizione.

Problema 13J. Chiamiamo *bello* un insieme la cui cardinalità è divisibile per 3. Quanti sottoinsiemi belli possiede un insieme di n elementi?

Problema 13K. Dimostrare che $\sum_{n=1}^{\infty} S(n, n-2)x^n = \frac{x(1+2x)}{(1-x)^5}$.[2]

Note

I numeri di Stirling della prima e della seconda specie compaiono in molti campi della matematica: per esempio intervengono in varie formule di interpolazione e nel calcolo delle differenze finite. Tavole di questi numeri si trovano in diversi volumi di tavole di funzioni matematiche.

Questi numeri ricompariranno nel Capitolo 37.

James Stirling (1692–1770), matematico scozzese, studiò a Oxford. Insegnò matematica a Venezia e a Londra, ma a quarantatré anni passò a una carriera negli affari.

[2] Nota redazionale: l'identità è riportata come nell'originale. Con la definizione (13.9), il primo membro inizia dal grado 3; la forma coerente è $x^3(1+2x)/(1-x)^5$.

Capitolo 14

Ricorrenze e funzioni generatrici

Molti problemi combinatori di conteggio, la cui soluzione a_n dipende da un parametro n, si possono risolvere trovando una relazione di ricorrenza per a_n e risolvendola. Talvolta si introduce una *funzione generatrice ordinaria* Orig. 129

$$f(x) := \sum_{n\geq 0} a_n x^n,$$

oppure una *funzione generatrice esponenziale*

$$f(x) := \sum_{n\geq 0} a_n \frac{x^n}{n!},$$

e si usa la ricorrenza per trovare un'equazione, eventualmente differenziale, soddisfatta da $f(x)$, che viene poi risolta. Illustreremo varie tecniche di questo tipo.

Esempio 14.1. Come introduzione, riprendiamo l'Esempio 10.1. Sia π uno scompiglio di $\{1, 2, \ldots, n+1\}$. Vi sono n scelte per $\pi(n+1)$. Se $\pi(n+1) = i$ e $\pi(i) = n+1$, allora π induce anche uno scompiglio sull'insieme $\{1, 2, \ldots, n\} \setminus \{i\}$. Se invece $\pi(n+1) = i$ e $\pi(i) \neq n+1 = \pi(j)$, sostituendo $\pi(j)$ con i si ottiene uno scompiglio di $\{1, 2, \ldots, n\}$. Pertanto

$$d_{n+1} = n(d_n + d_{n-1}), \tag{14.1}$$

che è anche una conseguenza immediata di (10.3). Sia $D(x)$ la funzione generatrice esponenziale della successione $d_0 = 1, d_1 = 0, d_2, \ldots$. Da (14.1) segue subito

$$(1-x)D'(x) = xD(x),$$

da cui $D(x) = e^{-x}/(1-x)$ e quindi (10.2).

In molti casi usiamo le funzioni generatrici soltanto per tenere traccia dei conteggi; le operazioni di addizione, moltiplicazione e, come vedremo, anche di sostituzione e derivazione, vanno interpretate formalmente. È possibile costruire una teoria del tutto rigorosa delle serie formali di potenze come oggetti algebrici; ne daremo un'introduzione nell'Appendice 2. Nella maggior parte dei casi la legittimità delle operazioni è intuitivamente chiara e facile da verificare. Se le serie utilizzate convergono effettivamente, possiamo applicare tutti i risultati pertinenti dell'analisi, come nell'Esempio 14.1. Diamo un altro esempio elementare. Orig. 130

Esempio 14.2. Supponiamo di avere k scatole numerate da 1 a k, e che la scatola i contenga r_i palline, $1 \leq i \leq k$. Un espediente formale per elencare tutte le configurazioni consiste nell'associare a questa il termine $x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}$ nel prodotto

$$(1 + x_1 + x_1^2 + \cdots)(1 + x_2 + x_2^2 + \cdots) \cdots (1 + x_k + x_k^2 + \cdots).$$

Raccogliamo tutti i termini relativi a esattamente n palline ponendo $x_i = x$ per ogni i e considerando i termini uguali a x^n. Il numero dei modi di distribuire n palline in k scatole distinguibili è quindi il coefficiente di x^n nello sviluppo di $(1-x)^{-k}$; per (10.6) esso è $\binom{k-1+n}{n}$. Otteniamo così una seconda dimostrazione del Teorema 13.1.

In molti casi il problema combinatorio conduce a una ricorrenza lineare a coefficienti costanti, facilmente risolvibile con metodi standard.

Esempio 14.3. Consideriamo cammini di lunghezza n nel piano X-Y che partono da $(0,0)$ e hanno passi

$$R : (x,y) \mapsto (x+1,y), \quad L : (x,y) \mapsto (x-1,y), \quad U : (x,y) \mapsto (x,y+1),$$

cioè verso destra, verso sinistra o verso l'alto. Richiediamo che un passo R non sia seguito da un passo L, e viceversa. Sia a_n il numero di questi cammini. Se b_n indica il numero dei cammini di lunghezza n che iniziano con U, si ha $b_n = a_{n-1}$; inoltre è evidente che $b_{n+m} \geq b_n b_m$ e $b_n \leq 3^{n-1}$. Per il lemma di Fekete, Lemma 11.6, esiste $\lim_{n\to\infty} b_n^{1/n}$ ed è al più 3. Osserviamo poi che $a_0 = 1$ e $a_1 = 3$. Suddividiamo l'insieme dei cammini di lunghezza n secondo l'ultimo passo o gli ultimi due. Chiaramente a_{n-1} cammini terminano con U. Prendiamo un cammino di lunghezza $n-1$ e ripetiamone l'ultimo passo, se è L oppure R; se è U, aggiungiamo un passo L. Otteniamo tutti i cammini di lunghezza n terminanti in LL, RR oppure UL: sono dunque a_{n-1}. Restano quelli terminanti in UR, che sono evidentemente a_{n-2}. Abbiamo dimostrato

Orig. 131

$$a_n = 2a_{n-1} + a_{n-2} \qquad (n \geq 2).$$

Poniamo $f(x) = \sum_{n=0}^{\infty} a_n x^n$. La ricorrenza implica

$$f(x) = 1 + 3x + 2x(f(x) - 1) + x^2 f(x),$$

ossia

$$f(x) = \frac{1+x}{1-2x-x^2} = \frac{\alpha/2}{1-\alpha x} + \frac{\beta/2}{1-\beta x},$$

dove $\alpha = 1+\sqrt{2}$ e $\beta = 1-\sqrt{2}$. Pertanto

$$a_n = \frac{1}{2}(\alpha^{n+1} + \beta^{n+1}), \qquad \lim_{n\to\infty} a_n^{1/n} = 1+\sqrt{2}.$$

Problema 14A. (i) Sia a_n il numero delle successioni di 0 e 1 di lunghezza n che non contengono due 0 consecutivi. Determinare a_n.

(ii) Sia b_n il numero delle successioni di 0 e 1 di lunghezza n senza due 1 consecutivi, nelle quali ogni blocco di 0 consecutivi abbia lunghezza 2 oppure 3, anche quando si trova all'inizio o alla fine. Mostrare che $b_n^{1/n} \to c$ per una certa costante c e approssimarla.

Esempio 14.4. Sia $a(r,n)$, con $0 \leq r \leq n$, il numero delle soluzioni del problema dell'Esempio 13.1, con $a(0,0) = 1$. Suddividiamo le successioni ammissibili in quelle con $x_1 = 1$ e quelle con $x_1 > 1$. Il primo sottoinsieme contiene chiaramente $a(r-1,n-2)$ elementi, il secondo $a(r,n-1)$. Quindi

$$a(r,n) = a(r,n-1) + a(r-1,n-2) \qquad (n > 1). \tag{14.2}$$

Da questa ricorrenza si può dimostrare per induzione che $a(r,n) = \binom{n-r+1}{r}$. Usare la funzione generatrice è più difficile. Proviamo a porre

Orig. 132

$$f(x,y) := \sum_{n=0}^{\infty} \sum_{r=0}^{\infty} a(r,n) x^n y^r.$$

Da (14.2) segue

$$f(x,y) = 1 + x + xy + x(-1 + f(x,y)) + x^2 y f(x,y),$$

ossia

$$f(x,y) = \frac{1+xy}{1-x-x^2y} = \frac{1}{1-x} + \sum_{a=1}^{\infty} \frac{x^{2a-1}y^a}{(1-x)^{a+1}}.$$

Sostituendo lo sviluppo (10.6) di $(1-x)^{-a-1}$ si ottiene il coefficiente binomiale richiesto per $a(r,n)$.

Come nell'Esempio 14.3 e nel Problema 14A, una ricorrenza lineare a coefficienti costanti conduce a una funzione generatrice razionale, e viceversa. Infatti, se $a_n = \sum_{k=1}^{l} \alpha_k a_{n-k}$ per $n > l$ e $f(x) = \sum_{n=0}^{\infty} a_n x^n$, allora $(1 - \sum_{k=1}^{l} \alpha_k x^k) f(x)$ è una serie di potenze nella quale il coefficiente di x^n è nullo per $n > l$.

L'esempio seguente, dovuto a Klarner (1967), presenta un caso interessante di ricorrenza lineare trovata mediante la funzione generatrice e per nulla evidente dal punto di vista combinatorio.

Esempio 14.5. Consideriamo configurazioni del piano, chiamate *polimini*, come in Fig. 14.1. La configurazione è formata da strati, ciascuno costituito da quadrati consecutivi. Due strati consecutivi si incontrano lungo i lati di un numero di quadrati almeno uguale a uno. Più precisamente, consideriamo polimini *orizzontalmente convessi*.

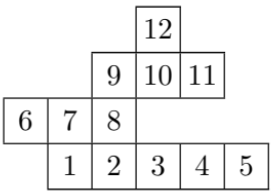


Figura 14.1

Orig. 133

Sia a_n il numero dei polimini di n quadrati e poniamo $f(x) := \sum_{n=1}^{\infty} a_n x^n$. Per trovare f, introduciamo $a(m,n)$, numero dei polimini con m quadrati nello strato inferiore e n quadrati in totale. Poniamo $a(m,n) := 0$ se $m > n$. Chiaramente

$$a(m,n) = \sum_{l=1}^{\infty} (m+l-1)a(l,n-m). \tag{14.3}$$

Definiamo

$$F(x,y) := \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} a(m,n)x^n y^m. \tag{14.4}$$

Allora $f(x) = F(x,1)$. Poiché servirà in seguito, definiamo anche

$$g(x) := \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} ma(m,n)x^n.$$

Vorremmo scrivere

$$g(x) = \left(\frac{\partial F}{\partial y}\right)_{y=1}. \tag{14.5}$$

Pur disponendo di una teoria delle serie formali, può essere istruttivo mostrare che il secondo membro di (14.4) converge in una regione sufficientemente ampia. Ciò offre anche un modo rapido di ottenere una stima grossolana di a_n. Numeriamo i quadrati del polimino nel modo evidente illustrato in Fig. 14.1. A ciascun quadrato associamo una quadrupla (x_0, x_1, x_2, x_3) di 0 e 1: $x_0 = 1$ significa che sotto quel quadrato ve n'è un altro del polimino; $x_1 = 1$ significa che ve n'è uno a sinistra; $x_2 = 1$ che ve n'è uno sopra; $x_3 = 1$ che ve n'è uno a destra. In Fig. 14.1 la prima quadrupla è $(0,0,1,1)$. La successione delle quadruple determina univocamente il polimino: per esempio, la quinta è la prima che termina in 0, e ciò mostra che $m = 5$, e così via. Ne segue $a_n \le 15^n$. Da questa stima e da (14.3) otteniamo $a(m,n) \le n15^{n-m}$, sufficiente a giustificare (14.5). Sostituendo (14.3) in (14.4) e svolgendo un calcolo diretto, si trova

Orig. 134

$$F(x,y) = \frac{xy}{1-xy} + \frac{(xy)^2}{(1-xy)^2}f(x) + \frac{xy}{1-xy}g(x). \tag{14.6}$$

Derivando rispetto a y entrambi i membri e ponendo $y = 1$, usando (14.5), otteniamo

$$g(x) = \frac{x}{(1-x)^2} + \frac{2x^2}{(1-x)^3}f(x) + \frac{x}{(1-x)^2}g(x). \tag{14.7}$$

Ricaviamo $g(x)$ da (14.7), sostituiamolo in (14.6) e poniamo $y = 1$:

$$f(x) = \frac{x(1-x)^3}{1-5x+7x^2-4x^3}. \tag{14.8}$$

Da (14.8) vediamo che a_n soddisfa

$$a_n = 5a_{n-1} - 7a_{n-2} + 4a_{n-3} \qquad (n \ge 5). \tag{14.9}$$

Come già osservato, non è affatto evidente come dimostrarlo direttamente; eppure una dimostrazione diretta esiste.

Osservazione. Da (14.9) troviamo $\lim_{n\to\infty} a_n^{1/n} = \theta$, dove θ è lo zero di massimo valore assoluto del polinomio $x^3 - 5x^2 + 7x - 4$, con $\theta \approx 3{,}2$.

L'esempio seguente fornisce un risultato importante nella teoria dei campi finiti. Combina una generalizzazione dell'idea dell'Esempio 14.2 con le operazioni formali sulle serie di potenze. La lettrice dovrebbe convincersi della correttezza delle operazioni con i logaritmi senza ricorrere alla convergenza.

Esempio 14.6. Contiamo i polinomi irriducibili di grado n su un campo di q elementi. Enumeriamo tutti i polinomi monici irriducibili di grado almeno uno su tale campo:

$$f_1(x), f_2(x), f_3(x), \ldots,$$

con gradi rispettivi $d_1, d_2, d_3, \ldots$. Sia N_d il numero di quelli di grado d, per $d = 1, 2, 3, \ldots$. Orig. 135

Per ogni successione di interi non negativi $i_1, i_2, i_3, \ldots$, tutti nulli salvo un numero finito, otteniamo un polinomio monico

$$f(x) = f_1(x)^{i_1} f_2(x)^{i_2} f_3(x)^{i_3} \cdots$$

di grado $n = i_1 d_1 + i_2 d_2 + i_3 d_3 + \cdots$. Per l'unicità della fattorizzazione ogni polinomio monico di grado n si presenta esattamente una volta in questo modo. In altri termini, i polinomi monici di grado n sono in corrispondenza biunivoca con le successioni di interi non negativi $i_1, i_2, \ldots$ tali che $n = i_1 d_1 + i_2 d_2 + \cdots$.

Naturalmente i polinomi monici di grado n sono q^n, cioè il coefficiente di x^n in

$$\frac{1}{1-qx} = 1 + qx + (qx)^2 + (qx)^3 + \cdots .$$

Come nell'Esempio 14.2, il numero delle successioni con $n = i_1 d_1 + i_2 d_2 + \cdots$ è il coefficiente di x^n nella serie formale

$$(1 + x^{d_1} + x^{2d_1} + x^{3d_1} + \cdots)(1 + x^{d_2} + x^{2d_2} + x^{3d_2} + \cdots)\cdots .$$

Concludiamo quindi che

$$\frac{1}{1-qx} = \prod_{i=1}^{\infty} \frac{1}{1-x^{d_i}} = \prod_{d=1}^{\infty} \left(\frac{1}{1-x^d}\right)^{N_d}.$$

Ricordando che $\log \frac{1}{1-z} = z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \cdots$, prendiamo i logaritmi formali dei due membri estremi:

$$\sum_{n=1}^{\infty} \frac{(qx)^n}{n} = \sum_{d=1}^{\infty} N_d \sum_{j=1}^{\infty} \frac{x^{jd}}{j}.$$

Confrontando i coefficienti di x^n otteniamo

$$\frac{q^n}{n} = \sum_{d|n} \frac{N_d}{n/d},$$

ossia $q^n = \sum_{d|n} dN_d$. Era questa l'identità cercata. L'abbiamo ricavata combinatoriamente dall'unicità della fattorizzazione; essa ammette però un'elegante interpretazione attraverso la fattorizzazione di $x^{q^n} - x$ sul campo di q elementi. Applicando l'inversione di Möbius, Teorema 10.4, otteniamo il risultato seguente. Orig. 136

Teorema 14.1. Se q è una potenza di un primo, il numero dei polinomi monici irriducibili di grado n sul campo di q elementi è

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Una conseguenza diretta è $N_d > 0$: esistono dunque polinomi irriducibili di ogni grado d. Ne segue immediatamente una dimostrazione dell'esistenza di campi con p^d elementi per ogni primo p, senza ricorrere al consueto espediente delle chiusure algebriche dei campi primi.

* * *

Arriviamo a un'ampia classe di problemi di conteggio aventi tutti la stessa soluzione. È nota come *famiglia di Catalan*, perché Catalan (1838) trattò l'Esempio 14.7. In realtà il problema equivalente denominato Quesito 3 nell'Esempio 14.9 era già stato studiato da von Segner ed Euler nel Settecento. Indichiamo le soluzioni con u_n; mostreremo che $u_n = \frac{1}{n}\binom{2n-2}{n-1}$. Questi sono i *numeri di Catalan*.

Esempio 14.7. Supponiamo che su un insieme S sia definita un'operazione di prodotto non associativa. Un'espressione $x_1x_2\cdots x_n$, con $x_i \in S$, non ha senso senza parentesi che indichino l'ordine delle operazioni. Sia u_n il numero dei modi di inserirle per n fattori. Per esempio, $u_4 = \frac{1}{4}\binom{6}{3} = 5$, corrispondenti ai prodotti $(a(b(cd)))$, $(a((bc)d))$, $((ab)(cd))$, $((a(bc))d)$ e $(((ab)c)d)$. Dentro le parentesi più esterne ogni prodotto contiene due espressioni: la prima è un prodotto di m fattori e la seconda di $n-m$ fattori, con $1 \le m \le n-1$. I numeri u_n soddisfano quindi Orig. 137

$$u_n = \sum_{m=1}^{n-1} u_m u_{n-m} \qquad (n \ge 2). \tag{14.10}$$

Da (14.10) e $u_1 = 1$, la funzione generatrice $f(x) := \sum_{n=1}^{\infty} u_n x^n$ soddisfa

$$f(x) = x + \sum_{n=2}^{\infty} \left(\sum_{m=1}^{n-1} u_m u_{n-m} \right) x^n = x + f(x)^2. \tag{14.11}$$

Risolvendo l'equazione quadratica e tenendo conto di $f(0) = 0$, troviamo $f(x) = (1 - \sqrt{1-4x})/2$. Dalla serie binomiale ricaviamo

$$u_n = \frac{1}{n}\binom{2n-2}{n-1}. \tag{14.12}$$

Tutte queste operazioni sono giustificabili formalmente sulle serie di potenze; anche la serie binomiale si può trattare formalmente senza preoccuparsi della convergenza. Chi non si sente a proprio agio con questo approccio ha due rimedi. Il primo è trovare la soluzione come sopra e dimostrarne poi la correttezza mediante (14.10) e l'induzione. Chi desideri davvero assicurarsi che la funzione generatrice sia definita da una serie convergente può usare il risultato del calcolo per trovare una stima grossolana di u_n, dimostrarla con (14.11) e stabilire così la convergenza. Per esempio, proviamo $u_n \le c^{n-1}/n^2$. È vera per $n = 1$ e ogni $c > 0$, e per $n = 2$ se $c \ge 4$. Il passo induttivo con (14.11) dà

$$u_n \le c^{n-2} \sum_{m=1}^{n-1} \frac{1}{m^2(n-m)^2} \le c^{n-2} \frac{2}{(n/2)^2} \sum_{m=1}^{\infty} \frac{1}{m^2} < \frac{c^{n-1}}{n^2},$$

se $c > \frac{4}{3}\pi^2$. Dunque la serie $\sum_{n=1}^{\infty} u_n x^n$ ha raggio di convergenza positivo. Orig. 138

Osservazione. La formula (14.10) mostra che $u_n \ge u_m u_{n-m}$; il lemma di Fekete implica allora l'esistenza di $\lim_{n\to\infty} u_n^{1/n}$. La formula (14.12) mostra che tale limite è 4.

Come già osservato, i numeri di Catalan ricompaiono regolarmente nei problemi combinatori di conteggio. Si pone quindi il problema di dimostrare gli altri risultati combinatoriamente, stabilendo una corrispondenza biunivoca fra gli oggetti da contare e quelli dell'Esempio 14.7. Alcuni casi saranno trattati nell'Esempio 14.9. Consideriamo prima un altro famoso problema avente per soluzione i numeri di Catalan.

Esempio 14.8. Consideriamo passeggiate nel piano X-Y in cui ogni passo è $U : (x, y) \mapsto (x+1, y+1)$ oppure $D : (x, y) \mapsto (x+1, y-1)$. Partendo da $(0, 0)$, in quanti modi si può raggiungere $(2n, 0)$ senza attraversare l'asse X? La soluzione usa un elegante espediente noto come *principio di riflessione di André* (1887). Nella Fig. 14.2 consideriamo due punti A, B nel semipiano superiore e un possibile cammino che li congiunge incontrando o attraversando l'asse X.

Riflettiamo rispetto all'asse X il tratto fra A e il primo incontro con l'asse, il punto C in Fig. 14.2. Otteniamo un cammino dal punto riflesso A' a B. Si stabilisce così una corrispondenza biunivoca fra i cammini da A' a B e quelli da A a B che incontrano o attraversano l'asse X.

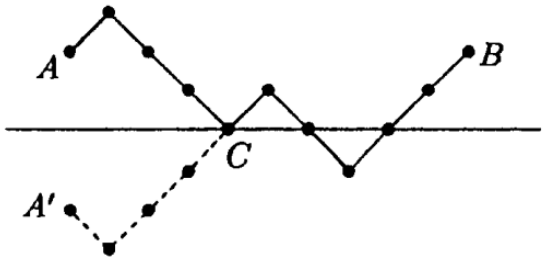


Figura 14.2

Se $A = (0, k)$ e $B = (n, m)$, vi sono quindi $\binom{n}{l_1}$ cammini da A a B che incontrano o attraversano l'asse X, dove $2l_1 := n - k - m$. Poiché in totale i cammini da A a B sono $\binom{n}{l_2}$, dove $2l_2 := n - m + k$, quelli che non incontrano l'asse sono $\binom{n}{l_2} - \binom{n}{l_1}$. Un cammino da $(0, 0)$ a $(2n, 0)$ nel semipiano superiore, che non incontri l'asse fra gli estremi, va da $(0, 0)$ ad $A := (1, 1)$, da A a $B := (2n - 1, 1)$ senza incontrare l'asse, e infine da B a $(2n, 0)$. Per l'argomento precedente questi cammini sono u_n. Se permettiamo che tocchino l'asse senza attraversarlo, sono u_{n+1}. Orig. 139

Il numero dei cammini da $(0, 0)$ a $(2n, 0)$ nel semipiano superiore che non incontrano l'asse fra gli estremi coincide con il numero delle successioni di 0 e 1, $(x_1, x_2, \ldots, x_{2n})$, tali che

$$x_1 + \cdots + x_j \begin{cases} < j/2, & 1 \le j \le 2n - 1, \\ = n, & j = 2n. \end{cases} \tag{14.13}$$

La corrispondenza associa 1 a un passo D.

Mostriamo ora combinatoriamente che vari problemi conducono ai numeri di Catalan.

Esempio 14.9. Consideriamo i tre quesiti seguenti.

Quesito 1. Un albero disegnato nel piano è detto *albero piano*. Quanti alberi piani radicati con n vertici hanno la radice di grado 1? Questi sono detti *alberi piani piantati*.

Quesito 2. Un albero piano piantato è detto *trivalente*, o *albero binario*, se ogni vertice ha grado 1 oppure 3. Quanti alberi piani piantati trivalenti hanno n vertici di grado 1?

Quesito 3. In quanti modi si può decomporre un poligono convesso di n lati in triangoli mediante $n-3$ diagonali non intersecantisi?

La prima corrispondenza è quella fra il Quesito 2 e l'Esempio 14.7. La Fig. 14.3 è sufficiente a illustrarla. Orig. 140

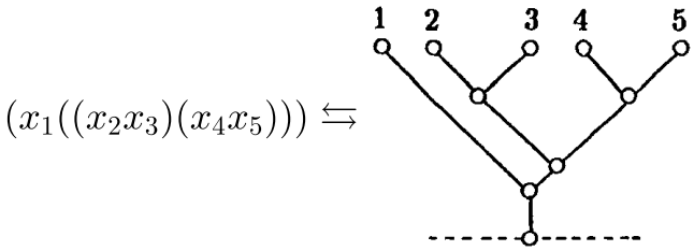


Figura 14.3

Ne segue che la soluzione del Quesito 2 è u_{n-1}. Anche la corrispondenza fra il Quesito 1 e l'Esempio 14.8 è illustrata da una figura, la Fig. 14.4.

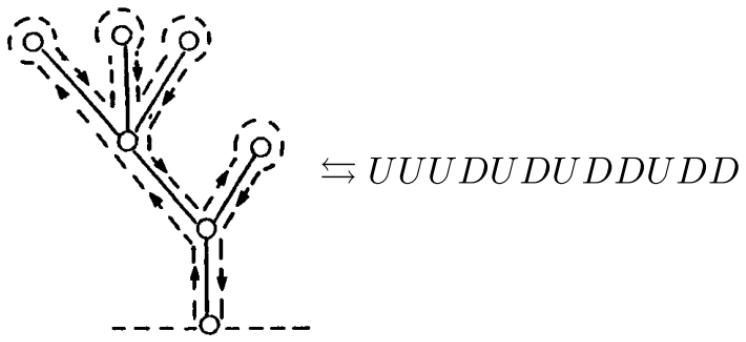


Figura 14.4

L'albero della figura si descrive mediante una passeggiata attorno ad esso, indicata dalla linea tratteggiata. Chiamiamo U un passo verso l'alto e D un passo verso il basso: si ottiene una successione di dodici passi.

Sostituendo U con 0 e D con 1 si ottiene una successione che evidentemente soddisfa (14.13). La soluzione del Quesito 1 è quindi anch'essa u_{n-1}.

Infine colleghiamo il Quesito 3 al Quesito 2. Consideriamo un n-gono suddiviso in triangoli e distinguiamo un suo lato. Costruiamo un albero come in Fig. 14.5.

Orig. 141

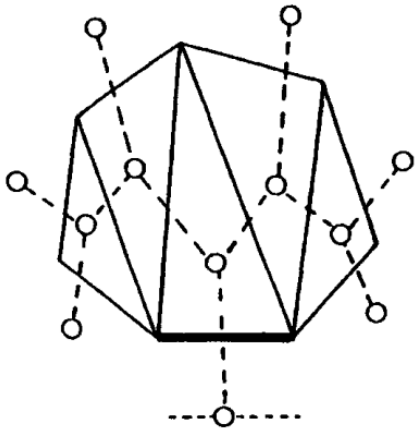


Figura 14.5

L'albero è binario: i vertici di grado 1 corrispondono ai lati dell'n-gono, quelli di grado 3 ai triangoli. È piantato nel vertice corrispondente al lato distinto. Troviamo quindi ancora u_{n-1} soluzioni.

Problema 14B. Descrivere con una figura una corrispondenza fra i grafi del Quesito 1 e quelli del Quesito 2.

Problema 14C. Trovare una corrispondenza biunivoca diretta fra gli n-goni del Quesito 3 e i prodotti dell'Esempio 14.7.

Passiamo a problemi per i quali è utile la funzione generatrice esponenziale. Daremo una trattazione un po' più sistematica di questo caso. Per un'esposizione completa dei metodi rimandiamo ad A. Joyal (1981).

Sia M un "tipo" di struttura combinatoria, per esempio alberi, poligoni, insiemi (strutture "uniformi"), permutazioni, e così via. Sia m_k il numero dei modi di dotare un insieme etichettato di k elementi di una tale struttura. In ogni caso specificheremo se assumiamo $m_0 = 0$ oppure $m_0 = 1$. Usiamo lettere maiuscole per le strutture e minuscole per le successioni enumerative. Definiamo

$$M(x) := \sum_{k=0}^{\infty} m_k \frac{x^k}{k!}. \tag{14.14}$$

Se T indica la struttura di albero etichettato, dal Teorema 2.1 sappiamo che

Orig. 142

$$T(x) = \sum_{k=0}^{\infty} k^{k-2} \frac{x^k}{k!}.$$

Se S indica la struttura uniforme, cioè un insieme, si ha $s_k = 1$ per ogni k e quindi $S(x) = e^x$. Se C indica un "circuito orientato", possiamo partire dal vertice 1 e vi sono evidentemente $(k-1)!$ modi di proseguire. Pertanto $C(x) = -\log(1-x)$.

Supponiamo di voler contare i modi di partizionare un insieme etichettato di n elementi in due parti, una dotata di una struttura di tipo A e l'altra di tipo B. Il numero è chiaramente $\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$. Chiamando $A \cdot B$ questo tipo di struttura, segue

$$(A \cdot B)(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \right) \frac{x^n}{n!} = A(x)B(x). \tag{14.15}$$

Il lettore deve usare con cautela (14.15). L'asserto è vero soltanto se dalla struttura composta si può ricostruire in modo unico la partizione nelle due parti che l'ha prodotta. Per esempio, se A e B coincidono, il risultato è chiaramente falso.

Esempio 14.10. Consideriamo ancora gli scompigli, struttura di tipo D, e indichiamo con Π la struttura "permutazione". Chiaramente $\Pi(x) = (1-x)^{-1}$. Ogni permutazione consiste in un insieme di punti fissi, interpretato semplicemente come insieme, e in uno scompiglio dei punti rimanenti. Per (14.15),

$$(1-x)^{-1} = D(x)S(x), \qquad D(x) = e^{-x}(1-x)^{-1},$$

come già mostrato nell'Esempio 10.1.

Esempio 14.11. In quanti modi si può suddividere un insieme etichettato di n elementi in un certo numero di coppie (P) e di singoletti (S)? Per suddividere $2k$ punti in coppie scegliamo prima un punto x_1 da abbinare al punto 1, poi suddividiamo in coppie i rimanenti $2k-2$ punti. Dunque $p_{2k} = (2k-1)!!$ e

$$P(x) = \sum_{k=0}^{\infty} (2k-1)!! \frac{x^{2k}}{(2k)!} = \exp(x^2/2).$$

Ne segue

$$(P \cdot S)(x) = \exp(x + x^2/2). \tag{14.16}$$

Orig. 143

Proviamo a ottenere lo stesso risultato mediante una ricorrenza. Indichiamo con B la struttura $P \cdot S$. Nell'insieme $\{1, 2, \ldots, n\}$ possiamo lasciare n come singoletto oppure formare una coppia $\{x, n\}$ con $1 \le x \le n-1$. Quindi

$$b_n = b_{n-1} + (n-1)b_{n-2} \qquad (n \ge 1).$$

Ne segue $B'(x) = (1+x)B(x)$; poiché $B(0) = 1$, ritroviamo (14.16). Torneremo su questa ricorrenza nell'Esempio 14.15.

Problema 14D. Considerare le strutture M_0, applicazione di un insieme in sé senza punti fissi; M_1, applicazione di un insieme in sé con esattamente un punto fisso; e A, arborescenza. Trovare una relazione fra $M_0(x)$, $M_1(x)$ e $A(x)$ e controllare i primi termini per verificarne la correttezza.

Rendiamo il problema leggermente più difficile. Vogliamo partizionare un insieme di n elementi in parti e assegnare a ciascuna una struttura N, con $n_0 = 0$. Affermiamo che la funzione generatrice esponenziale della struttura composta è $\exp(N(x))$. Un esempio semplice è quello in cui N è la struttura uniforme, con la convenzione $n_0 = 0$, e quindi $N(x) = e^x - 1$. La struttura composta è la "partizione"; dal Teorema 13.6 la sua funzione generatrice esponenziale è

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} S(n,k) \right) \frac{x^n}{n!} = \sum_{k=0}^{\infty} \frac{(e^x-1)^k}{k!} = \exp(e^x - 1) = \exp(N(x)).$$

Formuliamo il metodo come teorema.

Teorema 14.2. Se la struttura composta $S(N)$ si ottiene suddividendo un insieme in parti, ciascuna dotata di una struttura di tipo N, allora

$$S(N)(x) = \exp(N(x)).$$

Orig. 144

Dimostrazione. Generalizzando leggermente (13.3), se la partizione dell'insieme di n elementi consiste in b_1 parti di cardinalità 1, b_2 di cardinalità 2, …, b_k di cardinalità k, dove $b_1 + 2b_2 + \cdots + kb_k = n$, il numero delle strutture composte è

$$\left(\frac{n_1}{1!}\right)^{b_1} \cdots \left(\frac{n_k}{k!}\right)^{b_k} \frac{n!}{b_1! \cdots b_k!}.$$

Per ottenere il contributo al coefficiente di x^n nella funzione generatrice esponenziale dobbiamo dividere per $n!$. Se $b_1 + \cdots + b_k = m$, lo stesso contributo compare in $\exp(N(x))$ nel termine $N(x)^m/m!$, precisamente come

$$\frac{1}{m!} \binom{m}{b_1, \ldots, b_k} \left(n_1 \frac{x}{1!}\right)^{b_1} \cdots \left(n_k \frac{x^k}{k!}\right)^{b_k}.$$

Questo dimostra l'asserto. □

Non è difficile vedere che il teorema è un caso particolare di un metodo più generale. Interpretiamo la situazione precedente così: su un insieme di k punti abbiamo una struttura uniforme, e sostituiamo ciascun

punto con una struttura di tipo N. La configurazione risultante appartiene alla struttura composta appena discussa. Se la prima struttura non è uniforme ma, per esempio, di tipo R, la funzione generatrice esponenziale della struttura composta è $R(N(x))$, per lo stesso argomento. Talvolta chiamiamo questa procedura *sostituzione di N in R*; è piacevole che si debba compiere la stessa operazione sulle funzioni generatrici!

Esempio 14.12. Sostituendo la struttura "ciclo orientato" nella struttura uniforme, si ottiene una partizione di un insieme di n elementi in cicli orientati: cioè la struttura Π, con la solita convenzione $\pi_0 = 1$. Deve quindi essere $\Pi(x) = \exp(C(x))$; infatti $\Pi(x) = (1-x)^{-1}$ e $C(x) = -\log(1-x)$.

Esempio 14.13. Riprendiamo la Fig. 2.2 e aggiungiamo cappi nei vertici 1 e 21. Otteniamo la descrizione di un'applicazione di un insieme di n elementi in sé, con $n = 21$ in questo caso. Possiamo però interpretarla anche come un elemento della struttura Π, precisamente $(1)(4,5,3)(7)(20,12)(21)$, nel quale ciascun punto è stato sostituito da un'arborescenza avente quel punto come radice. Indicando con A le arborescenze, dal teorema di Cayley, Teorema 2.1, troviamo Orig. 145

$$A(x) = \sum_{n=1}^{\infty} n^{n-1} \frac{x^n}{n!}. \tag{14.17}$$

Il fattore aggiuntivo n deriva dalla scelta della radice. Poiché vi sono n^n applicazioni di un insieme di n elementi in sé, il metodo del Teorema 14.2 mostra che deve valere

$$\Pi(A(x)) = \frac{1}{1-A(x)} = \sum_{n=0}^{\infty} n^n \frac{x^n}{n!}. \tag{14.18}$$

Verificheremo questa identità dopo il prossimo esempio.

Il seguente noto risultato di analisi complessa interviene spesso nei problemi combinatori con funzioni generatrici. È la *formula di inversione di Lagrange*. Si trova nei testi di analisi con dimostrazioni analitiche; si vedano le note. Il teorema si può dimostrare anche nella teoria delle serie formali, usando la derivazione formale e così via; daremo questa dimostrazione nell'Appendice 2.

Teorema 14.3. Sia f analitica in un intorno di $z = 0$, con $f(0) \neq 0$. Se $w = z/f(z)$, allora z si può esprimere come una serie $z = \sum_{k=1}^{\infty} c_k w^k$ con raggio di convergenza positivo, dove

$$c_k = \frac{1}{k!} \left\{ \left(\frac{d}{dz} \right)^{k-1} f(z)^k \right\}_{z=0}. \tag{14.19}$$

Esempio 14.14. Troviamo una quarta dimostrazione del Teorema 2.1. Sia T la struttura "albero etichettato". Vogliamo mostrare che $t_n = n^{n-2}$ per $n \geq 1$. Se A indica ancora le arborescenze, si ha evidentemente $a_n = nt_n$, cioè $A(x) = xT'(x)$. Inoltre, per il Teorema 14.2, $\exp(A(x))$ è la funzione generatrice esponenziale della struttura "foresta radicata", indicata con F. Consideriamo un albero etichettato su $n+1$ vertici come un'arborescenza con radice $n+1$, e sopprimiamo la radice e tutti gli spigoli incidenti. Otteniamo una foresta radicata su n vertici. Il procedimento è reversibile, dunque stabilisce una corrispondenza biunivoca. Pertanto Orig. 146

$$e^{A(x)} = 1 + \sum_{n=1}^{\infty} f_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} t_{n+1} \frac{x^n}{n!} = T'(x) = x^{-1} A(x), \tag{14.20}$$

ossia

$$\frac{A(x)}{e^{A(x)}} = x. \tag{14.21}$$

Applichiamo il Teorema 14.3 con $z = A(x)$, $f(z) = e^z = e^{A(x)}$, $w = x$. Troviamo $A(x) = \sum_{k=1}^{\infty} c_k x^k$ con

$$c_k = \frac{1}{k!} \left\{ \left(\frac{d}{dz} \right)^{k-1} e^{kz} \right\}_{z=0} = \frac{k^{k-1}}{k!},$$

da cui $t_n = n^{n-2}$. Vediamo inoltre che le foreste radicate etichettate su n vertici sono $(n+1)^{n-1}$.

Osservazione. Abbiamo ora una verifica di (14.18), perché (14.20) implica $A'(x) = e^{A(x)} + xe^{A(x)}A'(x)$, cioè

$$\sum_{n=1}^{\infty} n^n \frac{x^n}{n!} = xA'(x) = \frac{xe^{A(x)}}{1 - xe^{A(x)}} = \frac{A(x)}{1 - A(x)}.$$

Osservazione. Il procedimento dell'Esempio 14.14, che elimina un punto da una struttura combinatoria su $n+1$ punti, si chiama *derivazione* e corrisponde effettivamente alla derivazione delle funzioni generatrici. Un altro esempio è l'eliminazione di un vertice da un ciclo orientato su $n+1$ vertici: rimane un cammino orientato su n vertici, e questi sono $n!$. La loro funzione generatrice esponenziale è $(1-x)^{-1}$, che è proprio $C'(x)$.

Problema 14E. Sia a_n il numero dei modi di decomporre un poligono convesso di $n+1$ lati in quadrilateri inserendo corde non intersecantisi. Per convenzione $a_0 = 0$, $a_1 = 1$. Mostrare che $\sum_{k+l+m=n} a_k a_l a_m = a_n$ per $n \geq 3$. Se $f(x)$ è la funzione generatrice ordinaria della successione a_n, trovare un'equazione funzionale per $f(x)$ e risolverla usando il Teorema 14.3. Il risultato si può dimostrare anche combinatoriamente. Orig. 147

Abbiamo insistito sul fatto che nella maggior parte dei casi le serie possono essere considerate formali; diversi esempi hanno però mostrato che l'analisi è uno strumento importante in molti problemi combinatori. Diamo un altro esempio, che illustra un metodo applicabile a numerose ricorrenze.

Esempio 14.15. Nell'Esempio 14.11 abbiamo incontrato la ricorrenza

$$a_n = a_{n-1} + (n-1)a_{n-2} \tag{14.22}$$

e la corrispondente funzione generatrice esponenziale. Negli esempi precedenti la funzione enumerativa cresceva più o meno come c^n per una costante c. Qui a_n cresce chiaramente più rapidamente: qual è una buona approssimazione del suo comportamento asintotico? Il primo passo per rispondere usa un metodo applicabile a molte ricorrenze. In (14.22) poniamo

$$a_n = \int_C \psi(z) z^n \, dz, \tag{14.23}$$

dove C è un cammino in $\mathbb{C}$ ancora da scegliere e ψ una funzione ancora da determinare. Sostituendo (14.23) in (14.22), il termine $(n-1)a_{n-2}$ dà $\int_C \psi(z)(n-1)z^{n-2}\,dz$. Richiediamo che l'integrazione per parti lasci soltanto l'integrale contenente $\psi'(z)$, annullando il termine al bordo mediante un'opportuna scelta di C. La ricorrenza diventa

$$\int_C \left\{ \psi(z)[z^n - z^{n-1}] + \psi'(z) z^{n-1} \right\} dz = 0, \tag{14.24}$$

vera per ogni $n \in \mathbb{N}$ se $\psi(z)(1-z) = \psi'(z)$, ossia $\psi(z) = \alpha e^{z - z^2/2}$. Determinata ψ, la condizione su C mostra che l'asse reale da $-\infty$ a ∞ è una buona scelta. Da $a_0 = 1$ ricaviamo $\alpha = (2\pi e)^{-1/2}$.

Per trovare il comportamento asintotico di a_n dobbiamo ora analizzare

$$I := \int_{-\infty}^{\infty} e^{x - x^2/2} x^n \, dx. \tag{14.25}$$

Poiché l'integranda è massima vicino a $x = \sqrt{n}$, poniamo $x = y + \sqrt{n}$ e troviamo Orig. 148

$$I = e^{-n/2 + \sqrt{n}} n^{n/2} \int_{-\infty}^{\infty} e^{y - y^2/2} \exp\left(-y\sqrt{n} + n \log\left(1 + \frac{y}{\sqrt{n}}\right)\right) dy. \tag{14.26}$$

Osserviamo che, per $u, v < 0$, $|e^u - e^v| < |u - v|$. Usiamo inoltre la rappresentazione

$$\log(1+t) = \int_0^t \frac{ds}{1+s} = t - \frac{t^2}{2} + \int_0^t \frac{s^2}{1+s}\, ds$$

per ottenere

$$\left| -y\sqrt{n} + n \log\left(1 + \frac{y}{\sqrt{n}}\right) + \frac{y^2}{2} \right| \leq \frac{|y|^3}{\sqrt{n}}.$$

Sostituendo in (14.26) si vede che l'integrale tende a

$$\int_{-\infty}^{\infty} e^{y-y^2}\,dy = \sqrt{\pi}e^{1/4}.$$

Abbiamo dimostrato

$$a_n \sim \frac{e^{-1/4}}{\sqrt{2}}\, n^{n/2} e^{-n/2+\sqrt{n}}. \tag{14.27}$$

È chiaro che questo risultato non si trova facilmente![1]

Problema 14F. Sia $F_n(x)$ lo sviluppo in serie di potenze di $(1-x^n)^{-\mu(n)/n}$. Considerare anche lo sviluppo di e^x come serie formale. Dimostrare che

$$e^x = \prod_{n=1}^{\infty} F_n(x)$$

è un'identità fra serie formali.

Problema 14G. Trovare la funzione generatrice esponenziale del numero delle matrici di permutazione simmetriche di ordine n.

Problema 14H. Disponiamo su una circonferenza n simboli 0 e n simboli 1 in ordine arbitrario. Mostrare che si possono numerare consecutivamente le posizioni da 1 a $2n$ in modo che la successione soddisfi (14.13) sostituendo la disuguaglianza stretta $<$ con $\leq$. Orig. 149

Problema 14I. Siano i punti $1,\dots,2n$ disposti consecutivamente su una circonferenza. Vogliamo congiungerli a coppie mediante n corde non intersecantisi. In quanti modi è possibile farlo?

Problema 14J. Trovare la funzione generatrice esponenziale del numero dei grafi etichettati regolari di grado 2 con n vertici.

Problema 14K. Considerare passeggiate nel piano X-Y con passi $R : (x,y) \mapsto (x+1,y)$ oppure $U : (x,y) \mapsto (x,y+1)$. Partendo da $(0,0)$, in quanti modi si può arrivare a $(2n,2n)$ senza passare per uno dei punti $(2i-1,2i-1)$, $i = 1,\dots,n$? Dimostrare che il numero è il numero di Catalan u_{2n+1}.

Problema 14L. Considerare passeggiate nel piano X-Y con passi $R : (x,y) \mapsto (x+1,y)$ oppure $U_a : (x,y) \mapsto (x,y+a)$, dove a è un intero positivo. Vi sono cinque passeggiate contenenti un punto della retta $x+y=2$: RR, RU_1, U_1R, U_1U_1 e U_2. Sia a_n il numero delle passeggiate contenenti un punto della retta $x+y=n$, dunque $a_2 = 5$. Mostrare che $a_n = F_{2n}$, dove F_n sono i numeri di Fibonacci con $F_0 = F_1 = 1$.

Problema 14M. Contare le coppie di funzioni (f,g), dove f manda $\{1,2,\dots,r\}$ in $\{1,2,\dots,n\}$ e g è una permutazione di $\{1,2,\dots,n\}$ che fissa puntualmente l'immagine di f. Contandole in due modi, dimostrare che, per $n \geq r$,

$$\sum_{k=1}^{n} \binom{n}{k} k^r d_{n-k} = B(r)\, n!,$$

dove d_m è il numero degli scompigli di $1,2,\dots,m$ e $B(r)$ è un numero di Bell.

Problema 14N. Considerare passeggiate nel piano X-Y con passi $R : (x,y) \mapsto (x+1,y)$, $U : (x,y) \mapsto (x,y+1)$ oppure $D : (x,y) \mapsto (x+1,y+1)$. Vogliamo contare quelle da $(0,0)$ a (n,n) che rimangono sotto la retta $x=y$ o su di essa. Trovare una ricorrenza per il loro numero analoga a (14.10). Orig. 150

Note

Per una trattazione estesa del materiale di questo capitolo rimandiamo a Goulden e Jackson (1983) e a Stanley (1986). Un'ottima panoramica, di lettura agevole, è Stanley (1978).

[1] Nota redazionale: la discussione asintotica dell'originale è sintetica. L'espressione con il logaritmo reale in (14.26) va usata nella regione $y > -\sqrt{n}$; per una giustificazione completa occorre separare e stimare la coda restante e localizzare la stima del resto logaritmico. La formula asintotica finale è mantenuta.

Il primo riferimento tratta diffusamente la teoria delle serie formali di potenze. Si vedano anche Niven (1969) e l'Appendice 2. In generale le operazioni con serie di potenze sono "formali" e non richiedono discussioni di convergenza quando il coefficiente di ogni monomio, per esempio x^n, in una somma o in un prodotto è determinato da un numero finito di operazioni, senza limiti. Per esempio $\sum_{n=0}^{\infty}(\frac{1}{2}+x)^n$ non è ammessa nelle operazioni formali, perché già il termine costante non è una somma finita; invece $\sum_{n=0}^{\infty}(n!x+x^2)^n$ è ammessa, benché non converga per $x \neq 0$, perché il coefficiente di ogni potenza richiede un calcolo finito; si veda il Problema 14F.

La prima ricorrenza lineare che solitamente si impara a risolvere è $a_{n+1} = a_n + a_{n-1}$. Conduce alla famosa successione di Fibonacci; si veda il Problema 14A. Come osservato nel Capitolo 10, questo nome è dovuto a Lucas. La successione è legata a un problema del *Liber abaci* (1203) di Leonardo da Pisa, noto come Fibonacci.

Nell'Esempio 14.5 abbiamo mostrato che il numero a_n dei polimini di n quadrati è minore di c^n, usando $c = 15$. Si osservi che l'asserto segue anche dal lemma di Fekete. Abbiamo ottenuto la disuguaglianza mediante un'opportuna codifica delle celle. Il lettore può provare a dimostrare $a(m,n) < mc^n$ per una costante opportuna, usando (14.3) e l'induzione. L'osservazione dopo (14.9) si basa su un'affermazione di Stanley (1986), che attribuisce a D. Hickerson una dimostrazione combinatoria non pubblicata.

Il risultato dell'Esempio 14.6 è legato al fatto che $\mathbb{F}_{p^n}$ contiene come sottocampi i campi $\mathbb{F}_{p^d}$ per $d \mid n$. Ne segue che $x^{p^n} - x$ è il prodotto di tutti i polinomi irriducibili su $\mathbb{F}_p$ di grado divisore di n, da cui la formula dimostrata nell'esempio.

Nonostante l'ampia letteratura sui problemi aventi per soluzione i numeri di Catalan, essi ricompaiono regolarmente, per esempio nelle rubriche di problemi delle riviste. Come già detto, il matematico belga E. Catalan (1814–1894) studiò le parentesizzazioni ben formate dell'Esempio 14.7.

Orig. 151

Il principio di riflessione della Fig. 14.2 fu usato dal combinatorista francese D. André (1840–1917) nella soluzione del famoso problema dello scrutinio di Bertrand: se al termine di un'elezione il candidato P ha p voti e Q ne ha q, con $p < q$, la probabilità che Q sia rimasto sempre in vantaggio durante lo scrutinio è $(q-p)/(q+p)$.

La formula di inversione di Lagrange è uno dei numerosi contributi all'analisi di J. L. Lagrange; si vedano le note al Capitolo 19. Una dimostrazione è nel §7.32 di Whittaker e Watson (1927). Il teorema fu pubblicato nel 1770. Rimandiamo anche a G. N. Raney (1960).

Riferimenti bibliografici

E. Catalan (1838)
Note sur une équation aux différences finies, *J. M. Pures Appl.* **3**, 508–516.

I. P. Goulden e D. M. Jackson (1983)
Combinatorial Enumeration, Wiley-Interscience.

A. Joyal (1981)
Une théorie combinatoire des séries formelles, *Advances in Mathematics* **42**, 1–82.

D. A. Klarner (1967)
Cell growth problem, *Canad. J. Math.* **19**, 851–863.

I. Niven (1969)
Formal power series, *Amer. Math. Monthly* **76**, 871–889.

G. N. Raney (1960)
Functional composition patterns and power series reversion, *Trans. Amer. Math. Soc.* **94**, 441–451.

R. P. Stanley (1978)
Generating functions, pp. 100–141 in *Studies in Combinatorics* (G.-C. Rota, a cura di), Studies in Math. 17, Math. Assoc. of America.

R. P. Stanley (1986)
Enumerative Combinatorics, vol. I, Wadsworth and Brooks/Cole.

E. T. Whittaker e G. N. Watson (1927)
A Course in Modern Analysis, Cambridge University Press.

Capitolo 15

Partizioni

Orig. 152

Nei capitoli precedenti abbiamo considerato vari problemi di partizione. Arriviamo ora al più difficile: le partizioni non ordinate di n in k parti oppure in un numero arbitrario di parti. Definiamo $p_k(n)$ come il numero delle soluzioni di

$$n = x_1 + x_2 + \cdots + x_k, \qquad x_1 \geq x_2 \geq \cdots \geq x_k \geq 1. \tag{15.1}$$

Per esempio $7 = 5+1+1 = 4+2+1 = 3+3+1 = 3+2+2$, dunque $p_3(7) = 4$.

Usando la stessa idea del corollario al Teorema 13.1, $p_k(n)$ coincide con il numero delle soluzioni di $n-k = y_1 + \cdots + y_k$ con $y_1 \geq \cdots \geq y_k \geq 0$. Se esattamente s degli interi y_i sono positivi, per (15.1) vi sono $p_s(n-k)$ soluzioni $(y_1, \ldots, y_k)$. Pertanto

$$p_k(n) = \sum_{s=1}^{k} p_s(n-k). \tag{15.2}$$

Problema 15A. Mostrare che $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$ e usare questa relazione per dimostrare (15.2).

Le condizioni iniziali evidenti $p_k(n) = 0$ per $n < k$ e $p_k(k) = 1$ permettono di calcolare ricorsivamente questi numeri. Chiaramente $p_1(n) = 1$ e $p_2(n) = \lfloor n/2 \rfloor$.

Esempio 15.1. Mostriamo che $p_3(n) = \{n^2/12\}$, cioè l'intero più vicino a $n^2/12$, con un metodo utilizzabile anche per altri valori di k. Sia $a_3(n)$ il numero delle soluzioni di $n = x_1 + x_2 + x_3$, $x_1 \geq x_2 \geq x_3 \geq 0$. Allora $a_3(n) = p_3(n+3)$. Ponendo $y_3 = x_3$, $y_2 = x_2 - x_3$, $y_1 = x_1 - x_2$, vediamo che $a_3(n)$ è il numero delle soluzioni di $n = y_1 + 2y_2 + 3y_3$, con $y_i \geq 0$. Come nell'Esempio 14.2,

Orig. 153

$$\sum_{n=0}^{\infty} a_3(n)x^n = (1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}. \tag{15.3}$$

Sia $\omega = e^{2\pi i/3}$. La scomposizione in fratti semplici dà

$$\begin{aligned}\sum_{n=0}^{\infty} a_3(n)x^n = {} & \tfrac{1}{6}(1-x)^{-3} + \tfrac{1}{4}(1-x)^{-2} + \tfrac{17}{72}(1-x)^{-1} \\ & + \tfrac{1}{8}(1+x)^{-1} + \tfrac{1}{9}(1-\omega x)^{-1} + \tfrac{1}{9}(1-\omega^2 x)^{-1}.\end{aligned} \tag{15.4}$$

Usando (10.6), ricaviamo

$$a_3(n) = \frac{1}{12}(n+3)^2 - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{1}{9}(\omega^n + \omega^{2n}),$$

da cui

$$\left| a_3(n) - \frac{1}{12}(n+3)^2 \right| \leq \frac{7}{72} + \frac{1}{8} + \frac{2}{9} < \frac{1}{2}.$$

Pertanto

$$p_3(n) = \left\{ \frac{1}{12} n^2 \right\}. \tag{15.5}$$

Problema 15B. Scegliamo tre vertici di un n-gono regolare e consideriamo il triangolo che formano. Dimostrare direttamente che si possono formare $\{n^2/12\}$ triangoli a due a due non congruenti, ottenendo una seconda dimostrazione di (15.5).

Mostriamo ora che (15.5) è un esempio di un risultato più generale.

Teorema 15.1. Per k fissato,

$$p_k(n) \sim \frac{n^{k-1}}{k!(k-1)!} \qquad (n \to \infty).$$

Orig. 154

DIMOSTRAZIONE. (i) Se $n = x_1 + \cdots + x_k$, con $x_1 \geq \cdots \geq x_k \geq 1$, le $k!$ permutazioni di $(x_1, \ldots, x_k)$ danno soluzioni di (13.2) in interi positivi, non necessariamente tutte distinte. Quindi

$$k!p_k(n) \geq \binom{n-1}{k-1}. \tag{15.6}$$

Se poniamo $y_i := x_i + (k-i)$, $1 \leq i \leq k$, gli interi y_i sono distinti e la loro somma è $n + k(k-1)/2$. Pertanto

$$k!p_k(n) \leq \binom{n + k(k-1)/2 - 1}{k-1}. \tag{15.7}$$

Il risultato segue da (15.6) e (15.7). □

Problema 15C. Siano $a_1, \ldots, a_t$ interi positivi, non necessariamente distinti, con massimo comune divisore 1. Sia $f(n)$ il numero delle soluzioni di $n = a_1x_1 + \cdots + a_tx_t$ in interi non negativi $x_1, \ldots, x_t$. Qual è la funzione generatrice $F(x) := \sum f(n)x^n$? Mostrare che $f(n) \sim cn^{t-1}$ per una costante c ed esprimere esplicitamente c in funzione degli a_i.

Il problema del corollario al Teorema 13.1 riguarda il numero delle cosiddette *composizioni* di n in k parti. Il numero totale delle composizioni di n è quindi $\sum_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1}$. Il metodo del Teorema 13.1 lo mostra direttamente: consideriamo n palline blu e, in ciascuno spazio fra palline consecutive, collochiamo oppure no una pallina rossa. Le configurazioni sono evidentemente 2^{n-1} e rappresentano tutte le composizioni di n. Possiamo ottenere lo stesso risultato senza usare il Capitolo 13. Sia c_{nk} il numero delle composizioni di n in k parti e definiamo

$$c_k(x) := \sum_{n=k}^{\infty} c_{nk}x^n.$$

Con un metodo già usato più volte,

Orig. 155

$$c_k(x) = (x + x^2 + x^3 + \cdots)^k = x^k(1-x)^{-k} = \sum_{n=k}^{\infty} \binom{n-1}{k-1} x^n,$$

e

$$\sum_{k=1}^{\infty} c_k(x) = \sum_{k=1}^{\infty} x^k(1-x)^{-k} = \frac{x}{1-2x},$$

cioè n ha 2^{n-1} composizioni.

Problema 15D. Mostrare che, elencando tutte le 2^{n-1} composizioni di n, con $n \geq 4$, l'intero 3 compare esattamente $n2^{n-5}$ volte.

La funzione più difficile, e matematicamente più interessante e importante, di questa parte della combinatoria è definita da

$$p(n) := \text{numero delle partizioni non ordinate di } n. \tag{15.8}$$

Per esempio $p(5) = 7$, poiché le partizioni sono

$$1+1+1+1+1 = 2+1+1+1 = 3+1+1 = 2+2+1 = 4+1 = 3+2 = 5.$$

Chiaramente $p(n)$ è il numero delle soluzioni di

$$n = x_1 + x_2 + \cdots + x_n, \qquad x_1 \geq x_2 \geq \cdots \geq x_n \geq 0. \tag{15.9}$$

Come visto sopra, è anche il numero delle soluzioni di $n = y_1 + 2y_2 + \cdots + ny_n$, con $y_i \geq 0$, dove y_i conta le parti uguali a i nella prima definizione. Lo studio della cosiddetta *funzione delle partizioni* $p(n)$ ha condotto ad alcuni fra gli ambiti più affascinanti della teoria analitica dei numeri, dell'analisi, della geometria algebrica e così via. Potremo naturalmente considerare soltanto proprietà dimostrabili combinatoriamente.

Teorema 15.2. La funzione generatrice della funzione delle partizioni è

$$P(x) := \sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}(1-x^k)^{-1}.$$

Orig. 156

DIMOSTRAZIONE. Usiamo ancora l'idea dell'Esempio 14.2. La partizione $n = \sum_{i=1}^{m} ir_i$, con r_i parti uguali a i, corrisponde al termine $x_1^{r_1} \cdots x_m^{r_m}$ nel prodotto infinito formale $\prod_k (1 + x_k + x_k^2 + \cdots)$. Sostituendo x_k con x^k si ottiene il risultato. □

Molti teoremi sulle partizioni si dimostrano facilmente rappresentandole mediante *diagrammi di Ferrers*: ogni parte è rappresentata da una riga di punti, con le parti in ordine decrescente e la più grande in alto. Talvolta è più comodo usare quadrati invece di punti. In tal caso alcuni autori parlano di *diagramma di Young*, ma noi continueremo a chiamarlo diagramma di Ferrers. La partizione $(5, 4, 2, 1)$ di 12, per esempio, è rappresentata da entrambi i diagrammi della Fig. 15.1.

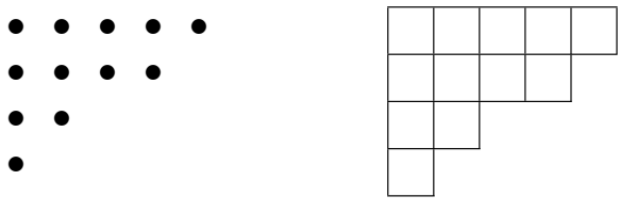


Figura 15.1

La partizione ottenuta leggendo il diagramma per colonne anziché per righe si chiama *coniugata*. La coniugata di $12 = 5+4+2+1$ è dunque $12 = 4+3+2+2+1$. La relazione è simmetrica. Diamo alcuni semplici esempi d'uso dei diagrammi.

Teorema 15.3. Il numero delle partizioni di n la cui parte più grande è k è $p_k(n)$.

DIMOSTRAZIONE. La coniugata di una partizione la cui parte più grande è k ha esattamente k parti, e viceversa. □

Problema 15E. Mostrare mediante un diagramma di Ferrers che il numero delle partizioni di $n + k$ in k parti coincide con quello delle partizioni di n in al più k parti. È la relazione (15.2).

In alcuni casi una dimostrazione con funzioni generatrici richiede meno ingegnosità di una con diagrammi di Ferrers. Il prossimo teorema si può dimostrare con un diagramma analogo, ma useremo le funzioni generatrici.

Orig. 157

Teorema 15.4. Il numero delle partizioni di n in parti dispari coincide con quello delle partizioni di n in parti distinte.

DIMOSTRAZIONE. La prima funzione generatrice è, per un'ovvia generalizzazione del Teorema 15.2, $\prod_{m=1}^{\infty}(1 - x^{2m-1})^{-1}$; la seconda è $\prod_{k=1}^{\infty}(1 + x^k)$, per lo stesso argomento usato nella dimostrazione di quel teorema. Poiché

$$\begin{aligned}\prod_{k=1}^{\infty}(1+x^k) &= \prod_{k=1}^{\infty}\frac{1-x^{2k}}{1-x^k} \\ &= \prod_{k=1}^{\infty}(1-x^{2k})\prod_{l=1}^{\infty}(1-x^l)^{-1} = \prod_{m=1}^{\infty}(1-x^{2m-1})^{-1},\end{aligned}$$

la dimostrazione è conclusa. □

Consideriamo ora $P(x)^{-1} = \prod_{k=1}^{\infty}(1 - x^k)$. Nello sviluppo una partizione di n in parti distinte contribuisce $+1$ al coefficiente di x^n se il numero delle parti è pari, e -1 se è dispari. Il coefficiente è

quindi $p_e(n) - p_o(n)$, dove $p_e(n)$ e $p_o(n)$ contano rispettivamente le partizioni di n in un numero pari e dispari di parti distinte. Euler mostrò che $p_e(n) = p_o(n)$, salvo quando $n = \omega(m) := (3m^2 - m)/2$ oppure $n = \omega(-m) = (3m^2 + m)/2$, nel qual caso la differenza è $(-1)^m$. I numeri $\omega(m)$ e $\omega(-m)$ sono detti *numeri pentagonali*. Il nome è spiegato dalla relazione $\omega(m) = \sum_{k=0}^{m-1}(3k + 1)$ e dalla Fig. 15.2.

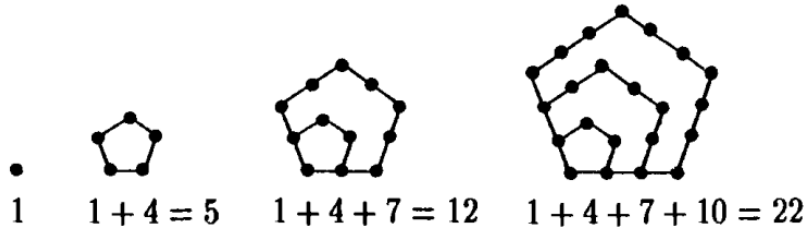


Figura 15.2

La seguente elegantissima dimostrazione figurativa dell'identità di Euler è dovuta a Franklin (1881). Orig. 158

Teorema 15.5. Si ha

$$\prod_{k=1}^{\infty}(1 - x^k) = 1 + \sum_{m=1}^{\infty}(-1)^m \left(x^{\omega(m)} + x^{\omega(-m)}\right).$$

Dimostrazione. Consideriamo il diagramma di Ferrers di una partizione di n in parti distinte, come $23 = 7 + 6 + 5 + 3 + 2$ nella Fig. 15.3.

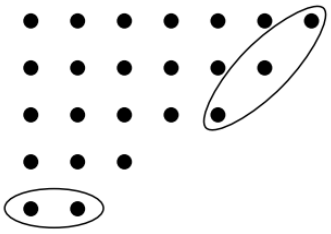


Figura 15.3

L'ultima riga si chiama *base*; il numero dei suoi punti è b. Nella figura è indicata da un segmento con $b = 2$ punti. Il più lungo segmento inclinato di 45° che congiunge l'ultimo punto della prima riga ad altri punti del diagramma si chiama *pendio*; il numero dei suoi punti è s. Nella figura il pendio ha $s = 3$ punti. Definiamo due operazioni, A e B.

A: se $b \leq s$, togliamo la base e la aggiungiamo a destra del diagramma, formando un nuovo pendio parallelo al precedente, salvo quando $b = s$ e base e pendio hanno un punto comune. Esamineremo questa eccezione più avanti.

B: se $b > s$, togliamo il pendio e lo aggiungiamo in fondo come nuova base, salvo quando $b = s + 1$ e base e pendio hanno un punto comune.

Nella Fig. 15.3 si può eseguire A, ottenendo $23 = 8+7+5+3$. La Fig. 15.4 mostra un caso eccezionale per B.

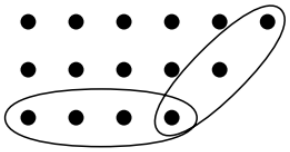


Figura 15.4

L'eccezione per A può presentarsi soltanto quando $n = b+(b+1)+\cdots+(2b-1)$, cioè $n = \omega(b)$. Quella per B si presenta quando $n = (s+1)+\cdots+2s$, cioè $n = \omega(-s)$. In tutti gli altri casi è eseguibile esattamente una delle operazioni: abbiamo così una corrispondenza biunivoca fra le partizioni in un numero pari e Orig. 159

quelle in un numero dispari di parti distinte. Per questi valori di n, dunque, $p_e(n) - p_o(n) = 0$. Nei casi eccezionali la differenza è $+1$ oppure -1. □

Euler usò il Teorema 15.5 per trovare la seguente ricorrenza per $p(n)$.

Teorema 15.6. Poniamo $p(n) = 0$ per $n < 0$. Per $n \geq 1$,

$$p(n) = \sum_{m=1}^{\infty} (-1)^{m+1} \{p(n - \omega(m)) + p(n - \omega(-m))\}. \tag{15.10}$$

Dimostrazione. È una conseguenza immediata dei Teoremi 15.2 e 15.5. □

La somma in (15.10) è finita. La ricorrenza permette di costruire rapidamente una tavola di $p(n)$ per piccoli valori di n.

I primi due termini coincidono con quelli della famosa ricorrenza di Fibonacci, si veda il Problema 5E. Sebbene seguano due termini negativi, si potrebbe immaginare che $p(n)$ cresca come i numeri di Fibonacci, cioè come c^n per una costante c. Non è così: mostreremo che cresce molto più lentamente. Il suo esatto comportamento asintotico richiede metodi complessi della teoria analitica dei numeri. Citiamo soltanto il termine principale:

$$\lim_{n\to\infty} n^{-1/2} \log p(n) = \pi \sqrt{\frac{2}{3}}.$$

Si può mostrare che $p(n)$ è in realtà molto minore di $\exp(\pi\sqrt{2n/3})$. Orig. 160

Teorema 15.7. Per $n > 2$,

$$p(n) < \frac{\pi}{\sqrt{6(n-1)}} e^{\pi\sqrt{2n/3}}.$$

Dimostrazione. Poniamo $f(t) := \log P(t)$. Dal Teorema 15.2,

$$f(t) = -\sum_{k=1}^{\infty} \log(1 - t^k) = \sum_{k=1}^{\infty} \sum_{j=1}^{\infty} \frac{t^{kj}}{j} = \sum_{j=1}^{\infty} \frac{j^{-1} t^j}{1 - t^j}.$$

Assumiamo ora $0 < t < 1$. Dalla relazione

$$(1-t)^{-1}(1-t^j) = 1 + t + \cdots + t^{j-1} > j t^{j-1}$$

ricaviamo

$$f(t) < \frac{t}{1-t} \sum_{j=1}^{\infty} j^{-2} = \frac{\pi^2}{6} \frac{t}{1-t}.$$

Poiché $p(n)$ è crescente, $P(t) > p(n) t^n (1-t)^{-1}$. Combinando le disuguaglianze e ponendo $t = (1+u)^{-1}$,

$$\begin{aligned} \log p(n) &< f(t) - n \log t + \log(1-t) \\ &< \frac{\pi^2}{6} \frac{t}{1-t} - n \log t + \log(1-t) \\ &= \frac{\pi^2}{6} u^{-1} + n \log(1+u) + \log \frac{u}{1+u}. \end{aligned}$$

Quindi $\log p(n) < \frac{1}{6}\pi^2 u^{-1} + (n-1)u + \log u$. La disuguaglianza richiesta si ottiene sostituendo $u = \pi\{6(n-1)\}^{-1/2}$. □

L'identità di Euler è un caso particolare di una famosa identità di Jacobi, importante nella teoria delle funzioni theta. Non menzioneremmo questa *identità del triplo prodotto di Jacobi* se non ne conoscessimo la bella dimostrazione combinatoria mediante un diagramma di Ferrers, dovuta a Wright (1965). Orig. 161

Teorema 15.8. Si ha

$$\prod_{n=1}^{\infty} (1 - q^{2n})(1 + q^{2n-1} t)(1 + q^{2n-1} t^{-1}) = \sum_{r=-\infty}^{\infty} q^{r^2} t^r.$$

Dimostrazione. Riscriviamo l'asserto come

$$\prod_{n=1}^{\infty}(1+q^{2n-1}t)(1+q^{2n-1}t^{-1}) = \sum_{r=-\infty}^{\infty} q^{r^2}t^r \prod_{n=1}^{\infty}(1-q^{2n})^{-1},$$

e poniamo $x = qt$, $y = qt^{-1}$. Ne segue

$$\prod_{n=1}^{\infty}\{(1+x^n y^{n-1})(1+x^{n-1}y^n)\} = \sum_{r=-\infty}^{\infty} x^{r(r+1)/2}y^{r(r-1)/2} \prod_{n=1}^{\infty}(1-x^n y^n)^{-1}. \tag{15.11}$$

Dimostreremo questa relazione interpretando i due membri come funzioni generatrici di opportuni oggetti combinatori e costruendo una corrispondenza biunivoca. Il primo membro conta le partizioni dell'intero gaussiano $n+mi$ in parti distinte dei tipi $a+(a-1)i$ e $(b-1)+bi$, con $a, b \geq 1$. Chiamiamo $\alpha(n,m)$ tale numero: il primo membro è quindi $\sum_{n,m\geq 0}\alpha(n,m)x^n y^m$.[1] Nel secondo membro usiamo il Teorema 15.2 e sostituiamo il prodotto con $\sum_{k=0}^{\infty} p(k)x^k y^k$. Dobbiamo quindi mostrare $\alpha(n,m) = p(k)$, dove $n = k + r(r+1)/2$ e $m = k + r(r-1)/2$. Senza perdita di generalità assumiamo $n \geq m$, cioè $r \geq 0$. Una partizione di $n+mi$ deve avere $v \geq 0$ parti del tipo $(b-1)+bi$ e $v+r$ del tipo $a+(a-1)i$. Quindi $n \geq r(r+1)/2$ e $k \geq 0$. Nella Fig. 15.5 consideriamo $(n,m) = (47,44)$, dunque $r = 3$ e $k = 41$. Prendiamo il diagramma di Ferrers di $41 = 12+10+8+5+2+2+2$ e aggiungiamo in alto righe di lunghezza $r, r-1, \ldots, 1$.

Orig. 162

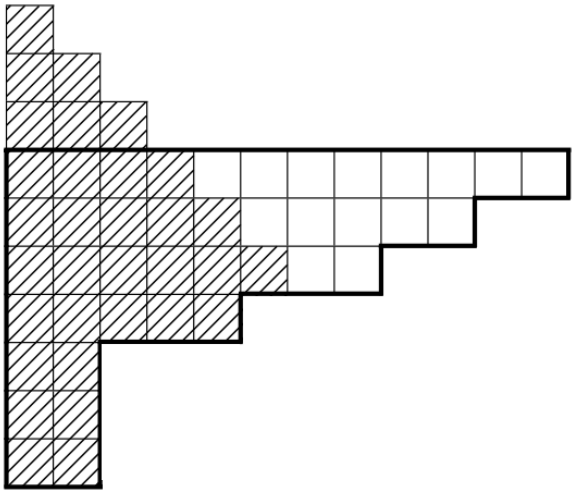


Figura 15.5

Il diagramma risultante si divide in due parti. La parte ombreggiata a sinistra è determinata dalla "scalinata" che inizia dalla porzione aggiunta in alto. La leggiamo per colonne: per costruzione le lunghezze formano una successione strettamente decrescente. Sono gli a delle parti $a+(a-1)i$. Leggiamo la parte non ombreggiata per righe: di nuovo otteniamo numeri strettamente decrescenti, i $b-1$ delle parti $(b-1)+bi$; l'ultimo b può essere 1, corrispondente a una riga non ombreggiata vuota. Il numero degli a supera quello dei $b-1$ di r, e la loro somma è chiaramente $k + r(r+1)/2$. Abbiamo dunque costruito una partizione di $n+mi$ del tipo richiesto. Il procedimento è facilmente reversibile: è la corrispondenza biunivoca cercata. □

Problema 15F. Dimostrare che il numero delle partizioni autoconiugate di n coincide con quello delle partizioni di n in parti dispari distinte.

Come ultimo problema relativo alle partizioni, consideriamo i *tableaux di Young*, detti anche *tableaux standard*. Un tableau di Young di forma $(n_1, n_2, \ldots, n_m)$ è un diagramma di Ferrers, o di Young, formato da quadrati nei quali sono inseriti gli interi da 1 a n, uno per quadrato, in modo che ogni riga e ogni colonna siano crescenti. La Fig. 15.6 mostra un tableau di forma $(5,4,2,1)$.

Orig. 163

[1] Nota redazionale: nell'originale i due indici di questa somma, e l'indice della successiva somma delle partizioni, partono da 1. Il prodotto ha però termine costante 1 e comprende anche termini su entrambi gli assi; occorre includere gli indici nulli.

1	3	4	7	11
2	5	10	12	
6	9			
8				

Figura 15.6

Vogliamo determinare il numero dei tableaux di una forma assegnata. Il problema può sembrare inizialmente artificioso. I tableaux di Young hanno però un ruolo importante nella teoria delle rappresentazioni dei gruppi e in altri campi. Un fatto interessante è la corrispondenza biunivoca fra i tableaux con n quadrati, che chiameremo *celle*, e le involuzioni di $\{1, \dots, n\}$, includendo fra esse l'identità. Possiamo quindi contarli complessivamente usando il Problema 14G. Per questa corrispondenza e diversi problemi collegati rinviamo a D. Knuth (1973).

Per contare i tableaux di una forma assegnata introduciamo la funzione

$$\Delta(x_1, \dots, x_m) := \prod_{1 \le i < j \le m} (x_i - x_j). \tag{15.12}$$

Si osservi che Δ è il valore del determinante di Vandermonde.

Lemma 15.9. Sia

$$\begin{aligned} g(x_1, \dots, x_m; y) := {} & x_1 \Delta(x_1 + y, x_2, \dots, x_m) \\ & + x_2 \Delta(x_1, x_2 + y, \dots, x_m) + \cdots + x_m \Delta(x_1, x_2, \dots, x_m + y). \end{aligned}$$

Allora

$$g(x_1, \dots, x_m; y) = \left(x_1 + \cdots + x_m + \binom{m}{2} y \right) \Delta(x_1, \dots, x_m).$$

DIMOSTRAZIONE. g è chiaramente un polinomio omogeneo di grado $1 + \deg \Delta$ nelle variabili $x_1, \dots, x_m, y$. Scambiando x_i e x_j, cambia segno. Quindi, per $x_i = x_j$, g è nullo: è divisibile per $x_i - x_j$, e dunque per $\Delta(x_1, \dots, x_m)$. Per $y = 0$ l'asserto è evidente. Resta da verificare il coefficiente $\binom{m}{2}$ di y. Sviluppando g, i termini di primo grado in y sono $x_i y \Delta/(x_i - x_j)$ e $-x_j y \Delta/(x_i - x_j)$ per ogni coppia $i < j$. Il loro coefficiente complessivo è evidentemente $\binom{m}{2}\Delta$. □ Orig. 164

Introduciamo una funzione f definita sulle m-uple $(n_1, \dots, n_m)$, $m \ge 1$, con le proprietà

$$f(n_1, \dots, n_m) = 0 \quad \text{se non vale } n_1 \ge n_2 \ge \cdots \ge n_m \ge 0; \tag{15.13}$$

$$f(n_1, \dots, n_m, 0) = f(n_1, \dots, n_m); \tag{15.14}$$

$$\begin{aligned} f(n_1, \dots, n_m) = {} & f(n_1 - 1, n_2, \dots, n_m) + f(n_1, n_2 - 1, \dots, n_m) \\ & + \cdots + f(n_1, n_2, \dots, n_m - 1), \\ & \qquad \text{se } n_1 \ge \cdots \ge n_m \ge 0; \end{aligned} \tag{15.15}$$

$$f(n) = 1 \quad \text{se } n \ge 0. \tag{15.16}$$

La funzione è chiaramente ben definita. Affermiamo che $f(n_1, \dots, n_m)$ conta i tableaux di Young di quella forma. Le condizioni (15.13), (15.14) e (15.16) sono evidenti. Per verificare (15.15), consideriamo la cella contenente n: deve essere l'ultima di una riga. Eliminandola otteniamo un tableau per $n-1$. Se più righe hanno la stessa lunghezza, n può comparire soltanto alla fine dell'ultima di esse; includere tutti i termini in (15.15) non crea però problemi, perché, per esempio, se $n_1 = n_2$, si ha $f(n_1 - 1, n_2, \dots, n_m) = 0$.

Teorema 15.10. Il numero dei tableaux di Young di forma $(n_1, \dots, n_m)$ è

$$f(n_1, \dots, n_m) = \frac{\Delta(n_1 + m - 1, n_2 + m - 2, \dots, n_m)\, n!}{(n_1 + m - 1)!(n_2 + m - 2)! \cdots n_m!}, \tag{15.17}$$

e la formula è corretta più generalmente se $n_1 + m - 1 \ge n_2 + m - 2 \ge \cdots \ge n_m$.

DIMOSTRAZIONE. Se per qualche i si ha $n_i + m - i = n_{i+1} + m - i - 1$, il fattore Δ a destra è nullo, in accordo con il fatto che la forma non è ammessa. Dobbiamo mostrare che il secondo membro soddisfa Orig. 165

(15.13)–(15.16). Tutte le verifiche sono immediate salvo (15.15), che si ottiene ponendo $x_i = n_i + m - i$ e $y = -1$ nel Lemma 15.9. □

Esiste una formulazione più interessante del teorema. Introduciamo l'*uncino* di una cella di un tableau: è l'unione della cella con tutte quelle alla sua destra nella stessa riga e tutte quelle sotto di essa nella stessa colonna. La *lunghezza dell'uncino* è il numero delle sue celle. La Fig. 15.7 mostra un diagramma di Young in cui ogni cella contiene la lunghezza dell'uncino corrispondente. La regione ombreggiata è l'uncino della cella nella seconda riga e terza colonna.

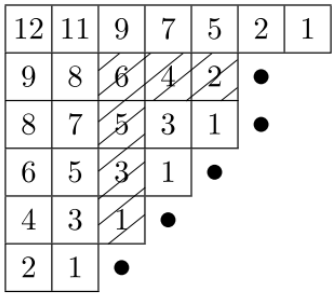


Figura 15.7

Otteniamo il seguente notevole teorema di J. S. Frame, G. de Beauregard Robinson e R. M. Thrall (1954).

Teorema 15.11. Il numero dei tableaux di Young di una forma assegnata con n celle è $n!$ diviso per il prodotto di tutte le lunghezze degli uncini.

Dimostrazione. In un tableau di forma $(n_1, \dots, n_m)$, la lunghezza dell'uncino della cella $(1,1)$ è $n_1 + m - 1$. Consideriamo gli uncini della prima riga. Nella Fig. 15.7 la seconda colonna ha la stessa lunghezza della prima; quindi la lunghezza dell'uncino successivo è $n_1 + m - 2$. Per la cella seguente diminuisce di 2, a causa della "cella mancante" indicata da un punto nell'ultima riga. Analogamente, nella colonna con due punti si ha un salto di 3. Nella prima riga troviamo quindi tutte le lunghezze da 1 a $n_1 + m - 1$, tranne i numeri $(n_1 + m - 1) - (n_j + m - j)$, $2 \le j \le m$. La riga i contiene analogamente gli interi da 1 a $n_i + m - i$, salvo $(n_i + m - i) - (n_j + m - j)$, $i + 1 \le j \le m$. Il prodotto delle lunghezze degli uncini è perciò Orig. 166

$$\frac{\prod_{i=1}^{m}(n_i + m - i)!}{\Delta(n_1 + m - 1, \dots, n_m)}.$$

Il risultato segue dal Lemma 15.9. □

Problema 15G. Considerare un tableau di forma (n, n). Definire $a_k := i$ se k si trova nella riga i, per $1 \le k \le 2n$, $i = 1, 2$. Usare questa successione per mostrare che il numero dei tableaux di tale forma è il numero di Catalan u_{n+1}, in accordo con il Teorema 15.11.

Problema 15H. Quanti diagrammi di Ferrers si possono contenere in un rettangolo $k \times (n - k)$?

Problema 15I. Dimostrare che il numero delle partizioni di n in parti non divisibili per d coincide con quello delle partizioni in cui nessuna parte compare più di $d - 1$ volte.

Problema 15J. Definire $P_n := \prod_{k=1}^{n} k!$. Dimostrare che $P_{n-1}^2 (n^2)!$ è divisibile per P_{2n-1}.

Note

L'uso dei diagrammi di Ferrers per dimostrare risultati come il Teorema 15.3 fu introdotto da Sylvester nel 1853. Scrisse che la dimostrazione gli era stata comunicata da N. M. Ferrers.

Per altre dimostrazioni con questi diagrammi e loro analoghi, per esempio una del Teorema 15.4, rimandiamo a Hardy e Wright (1954), MacMahon (1916) e Van Lint (1974).

Euler dimostrò il Teorema 15.5 per induzione. I numeri poligonali compaiono già nella matematica antica: i numeri triangolari furono considerati da Pitagora prima del 500 a.C.

Il Teorema 15.7 è dovuto a Van Lint (1974).

Il comportamento asintotico di $p(n)$ fu determinato da G. H. Hardy e S. Ramanujan (1918) nell'articolo in cui svilupparono il famoso "metodo del cerchio", poi ampiamente applicato in teoria dei numeri. Un ulteriore risultato asintotico è dovuto a H. Rademacher (1937). Le dimostrazioni dipendono dalla notevole equazione funzionale della funzione η di Dedekind,

Orig. 167

$$\eta(z) := e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}).$$

Per un'esposizione di tali dimostrazioni si veda Chandrasekharan (1970).

C. G. J. Jacobi (1804–1851) è noto soprattutto per lo sviluppo della teoria delle funzioni ellittiche. Divenne professore a Königsberg a ventitré anni. Due anni dopo pubblicò *Fundamenta Nova Theoriae Functionum Ellipticarum*; al §64 compare quella che oggi chiamiamo identità del triplo prodotto.

Il primo a usare tableaux come quello della Fig. 15.6 fu Frobenius! Un anno dopo, nel 1901, A. Young li introdusse indipendentemente nel suo lavoro sulle rappresentazioni matriciali dei gruppi di permutazioni. Il nome *tableaux di Young* è diventato la terminologia standard.

Riferimenti bibliografici

K. Chandrasekharan (1970)
Arithmetical Functions, Springer-Verlag.

J. S. Frame, G. de Beauregard Robinson e R. M. Thrall (1954)
The hook graphs of S_n, *Canad. J. Math.* **6**, 316–324.

F. Franklin (1881)
Sur le développement du produit infini $(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots$, *Comptes Rendus Acad. Sci. (Paris)* **92**, 448–450.

G. H. Hardy e S. Ramanujan (1918)
Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc. (2)* **17**, 75–115.

G. H. Hardy e E. M. Wright (1954)
An Introduction to the Theory of Numbers, 3a ed., Clarendon Press.

D. Knuth (1973)
The Art of Computer Programming, vol. 3, Addison-Wesley.

J. H. van Lint (1974)
Combinatorial Theory Seminar Eindhoven University of Technology, Lecture Notes in Math. 382, Springer-Verlag.

P. A. MacMahon (1916)
Combinatory Analysis, vol. II, Cambridge University Press.

H. Rademacher (1937)
On the partition function $p(n)$, *Proc. London Math. Soc.* **43**, 241–254.

Orig. 168

E. M. Wright (1965)
An enumerative proof of an identity of Jacobi, *J. London Math. Soc.* **40**, 55–57.

A. Young (1901)
On quantitative substitutional analysis, *Proc. London Math. Soc.* **33**, 97–146.

Capitolo 16

Matrici a elementi 0 e 1

Orig. 169

Le matrici $(0,1)$ sono comparse più volte nei capitoli precedenti; soprattutto quelle con somme costanti sulle righe e sulle colonne hanno condotto a problemi interessanti. Considereremo ora il problema dell'esistenza di matrici $(0,1)$ con somme assegnate e cercheremo di contarle, o stimarne il numero, nel caso di somme costanti. Nel primo problema le matrici non sono necessariamente quadrate. Se le somme delle righe di A sono $r_1, \dots, r_k$, chiameremo $\mathbf{r} := (r_1, \dots, r_k)$ il *vettore delle somme delle righe*; analogamente per le colonne.

Studiamo l'esistenza di una matrice $(0,1)$ con vettori delle somme delle righe e delle colonne assegnati, $\mathbf{r}$ e $\mathbf{s}$. Per comodità assumiamo le coordinate in ordine non crescente: $\mathbf{r}$ e $\mathbf{s}$ sono quindi partizioni, nelle quali in questo capitolo ammettiamo coordinate finali nulle.

Date due partizioni $\mathbf{r} = (r_1, \dots, r_n)$ e $\mathbf{s} = (s_1, \dots, s_m)$ dello stesso intero N, diciamo che $\mathbf{r}$ *maggiorizza* $\mathbf{s}$ se

$$r_1 + \cdots + r_k \geq s_1 + \cdots + s_k$$

per ogni k, interpretando r_k o s_k come 0 quando k supera rispettivamente n oppure m. Ricordiamo che la partizione coniugata $\mathbf{r}^*$ ha per r_i^* il numero degli indici j tali che $r_j \geq i$.

Problema 16A. Dimostrare che $\mathbf{r}$ maggiorizza $\mathbf{s}$ se e solo se quest'ultima si ottiene dalla prima mediante una successione di operazioni del tipo: "scegliere due parti a, b con $a \geq b+2$ e sostituirle con $a-1, b+1$". In altre parole, $\mathbf{s}$ è più "equilibrata" di $\mathbf{r}$. Per esempio $(5,4,1)$ maggiorizza $(3,3,3,1)$ e la seconda si ottiene dalla prima in vari modi, fra cui

Orig. 170

$$(5,4,1,0) \to (5,3,2,0) \to (5,3,1,1) \to (4,3,2,1) \to (3,3,3,1),$$

e

$$(5,4,1,0) \to (4,4,1,1) \to (4,3,2,1) \to (3,3,3,1).$$

Teorema 16.1. Siano $r_1, \dots, r_n$ e $s_1, \dots, s_m$ due successioni non crescenti di interi non negativi, entrambe di somma N. Esiste una matrice $(0,1)$ di dimensioni $n \times m$ con somme delle righe $\mathbf{r}$ e somme delle colonne $\mathbf{s}$ se e solo se $\mathbf{r}^*$ maggiorizza $\mathbf{s}$.

Dimostrazione. Per la necessità, fissiamo k e consideriamo le prime k colonne di una matrice ipotetica. Il numero degli 1 in tali colonne è

$$s_1 + \cdots + s_k \leq \sum_{i=1}^{n} \min(k, r_i) = \sum_{j=1}^{k} r_j^*.$$

L'ultima uguaglianza è evidente nel diagramma di Ferrers di $\mathbf{r}$, Fig. 16.1: entrambi i membri contano le celle nelle prime k colonne.

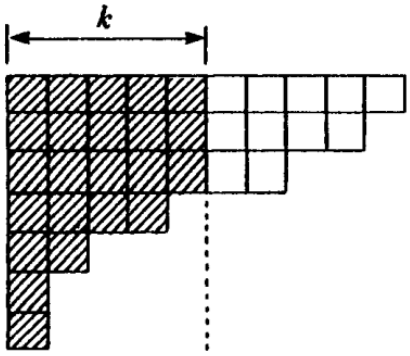


Figura 16.1

Introduciamo una rete di trasporto con sorgente S, pozzo T, un vertice x_i per ogni riga e un vertice y_j per ogni colonna. Vi è un arco di capacità r_i da S a x_i, uno di capacità s_j da y_j a T e uno di capacità 1 da x_i a y_j per ogni i, j. Affermiamo che la matrice cercata esiste se e solo se la rete ammette un flusso di valore N. Vi sono almeno due tagli di capacità N, quindi sarebbe un flusso massimo. Data la matrice (a_{ij}), il flusso si ottiene saturando gli archi incidenti a S, T e assegnando a_{ij} all'arco da x_i a y_j. Viceversa, se esiste un flusso di valore N, ne esiste uno intero dello stesso valore, per il Teorema 7.2. Gli archi incidenti a S o T devono essere saturi; sugli altri il flusso è 0 oppure 1. Orig. 171

Consideriamo un taglio A, B che separi S da T. Supponiamo che A contenga S, n_0 vertici di $X := \{x_1, \ldots, x_n\}$ e m_0 vertici di $Y := \{y_1, \ldots, y_m\}$. Gli archi da A a B comprendono $n - n_0$ archi uscenti da S, m_0 archi entranti in T e $n_0(m - m_0)$ archi da X a Y. La capacità del taglio è almeno

$$r_{n_0+1} + \cdots + r_n + s_{m-m_0+1} + \cdots + s_m + n_0(m - m_0).$$

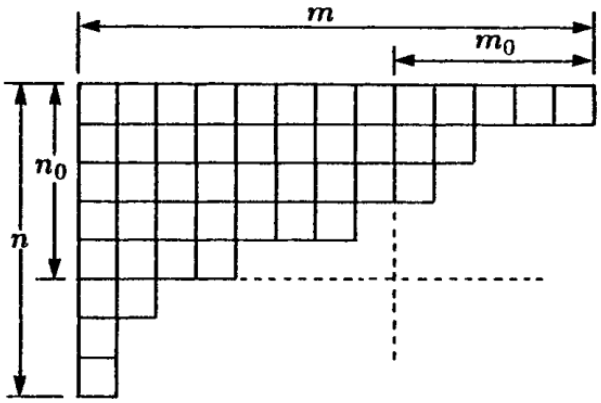


Figura 16.2

Ricorriamo ancora al diagramma di Ferrers di $\mathbf{r}$, Fig. 16.2, che contiene N celle. Chiaramente N è al più $n_0(m - m_0)$ più il numero delle celle nelle ultime $n - n_0$ righe più quello delle celle nelle ultime m_0 colonne. Quest'ultimo numero è la somma delle ultime m_0 parti della coniugata. Poiché $\mathbf{r}^*$ maggiorizza $\mathbf{s}$,

$$r^*_{m-m_0+1} + \cdots + r^*_m \le s_{m-m_0+1} + \cdots + s_m.$$

Ogni taglio ha dunque capacità almeno N. Per il teorema del flusso massimo e taglio minimo, Teorema 7.1, esiste il flusso richiesto. □ Orig. 172

Abbiamo dato questa dimostrazione per stabilire il legame fra flussi e matrici $(0, 1)$, ma la sufficienza della condizione ammette una dimostrazione più diretta. L'esposizione segue quella di Krause (1996).

Supponiamo di avere una matrice A_1 con somme delle righe $\mathbf{r}$ e somme delle colonne $\mathbf{s}_1$, e che $\mathbf{s}_2$ si ottenga da $\mathbf{s}_1$ con l'operazione del Problema 16A. È facile costruire una matrice A_2 con somme $\mathbf{r}, \mathbf{s}_2$. Se le parti a, b, con $a \ge b + 2$, sono le somme delle colonne j, k, esiste una riga i tale che l'elemento (i, j) sia 1 e l'elemento (i, k) sia 0. Scambiandoli si ottiene la matrice desiderata.

Supponiamo ora che $\mathbf{r}^*$ maggiorizzi $\mathbf{s}$. Partiamo dalla matrice A_0 corrispondente al diagramma di Ferrers di $\mathbf{r}$, aggiungendo se necessario colonne nulle per ottenere dimensioni $n \times m$. Il suo vettore delle

somme delle colonne è $\mathbf{r}^*$. Possiamo trovare una successione di partizioni

$$\mathbf{r}^* = \mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_l = \mathbf{s}$$

in cui ciascuna deriva dalla precedente mediante l'operazione del Problema 16A. L'osservazione precedente consente allora di ottenere da A_0, con l scambi, una matrice con somme $\mathbf{r}, \mathbf{s}$.

Esempio 16.1. Prendiamo $\mathbf{r} = (3,2,2,2,1)$ e $\mathbf{s} = (3,3,3,1)$. La coniugata $\mathbf{r}^* = (5,4,1)$ maggiorizza $\mathbf{s}$. L'algoritmo può dare la successione

$$\begin{pmatrix} 1&1&1&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&0&0&0 \end{pmatrix} \to \begin{pmatrix} 1&1&1&0\\ 0&1&1&0\\ 1&1&0&0\\ 1&1&0&0\\ 1&0&0&0 \end{pmatrix} \to \begin{pmatrix} 1&1&1&0\\ 0&1&1&0\\ 0&1&1&0\\ 1&1&0&0\\ 1&0&0&0 \end{pmatrix} \to \begin{pmatrix} 1&0&1&1\\ 0&1&1&0\\ 0&1&1&0\\ 1&1&0&0\\ 1&0&0&0 \end{pmatrix}.$$

I vettori delle somme delle colonne sono

Orig. 173

$$(5,4,1,0) \to (4,4,2,0) \to (3,4,3,0) \to (3,3,3,1).$$

Non importa che non siano sempre in ordine non crescente.

Estendiamo l'idea dell'algoritmo nel teorema seguente, ottenendo come conseguenza una stima grossolana del numero delle matrici con somme assegnate.

Teorema 16.2. Date partizioni $\mathbf{r}, \mathbf{s}$ di N, sia $M(\mathbf{r}, \mathbf{s})$ il numero delle matrici $(0,1)$ con tali somme delle righe e delle colonne. Se $\mathbf{r}$ maggiorizza $\mathbf{r}_0$ e $\mathbf{s}$ maggiorizza $\mathbf{s}_0$, allora $M(\mathbf{r}_0, \mathbf{s}_0) \geq M(\mathbf{r}, \mathbf{s})$.

Dimostrazione. Dimostriamo una semplice osservazione. Fissiamo $\mathbf{r} = (r_1, \ldots, r_n)$ e $\mathbf{s} = (s_1, \ldots, s_m)$ con la stessa somma, senza richiedere che siano non crescenti. Se $s_1 > s_2$, allora

$$M(\mathbf{r}, (s_1 - 1, s_2 + 1, s_3, \ldots, s_m)) \geq M(\mathbf{r}, (s_1, s_2, s_3, \ldots, s_m)).$$

Lo stesso vale naturalmente per qualsiasi coppia di colonne: scegliamo le prime due solo per comodità. Applicando l'idea alla trasposta, mantenere $\mathbf{s}$ e sostituire r_i, r_j, con $r_i > r_j$, mediante $r_i - 1, r_j + 1$ non diminuisce il numero delle matrici. Il teorema segue quindi dall'osservazione e dal Problema 16A.

Per dimostrarla, consideriamo matrici A di dimensioni $n \times (m-2)$ con somme delle colonne $(s_3, \ldots, s_m)$. Per una matrice fissata può essere possibile o impossibile anteporre due colonne ottenendo somme delle righe $\mathbf{r}$. Se è possibile, dobbiamo aggiungere due 1 in a righe, uno in b righe e nessuno in c righe, con $a + b + c = n$ e $2a + b = s_1 + s_2$. Il numero dei modi di ottenere somme delle nuove colonne s_1, s_2 è

$$\binom{b}{s_1 - a} = \binom{b}{s_2 - a},$$

ed è al più

Orig. 174

$$\binom{b}{s_1 - 1 - a} = \binom{b}{s_2 + 1 - a},$$

numero dei modi di ottenere le somme $s_1 - 1, s_2 + 1$, perché questi ultimi indici sono più vicini a $b/2$. □

La sufficienza nel Teorema 16.1 è un corollario immediato: se $\mathbf{r}^*$ maggiorizza $\mathbf{s}$, allora $M(\mathbf{r}, \mathbf{s}) \geq M(\mathbf{r}, \mathbf{r}^*) \geq 1$.

Problema 16B. Dimostrare che $M(\mathbf{r}, \mathbf{r}^*) = 1$.

Indichiamo con $A(n,k)$ il numero delle matrici $(0,1)$ di ordine n con tutte le somme delle righe e delle colonne uguali a k.

Corollario. $A(n,k) \geq \left\{ \binom{n}{k} / 2^{k+1} \right\}^n$.

Dimostrazione. Le matrici con somme delle righe $(k, k, \ldots, k)$ sono $\binom{n}{k}^n$. Ognuna ha somme delle colonne $(s_1, \ldots, s_n)$ con $0 \leq s_i \leq n$ e $\sum s_i = nk$. Ignorando i vincoli $s_i \leq n$, il Teorema 13.1 dà al più $\binom{nk+n-1}{n-1} \leq 2^{n(k+1)}$ possibili vettori. Il numero massimo di matrici associate si ottiene per il vettore $(k, \ldots, k)$ e quindi è almeno il numero medio. □

Problema 16C. Dimostrare il teorema seguente.

Teorema 16.3. Siano $\mathbf{d}, \mathbf{d}'$ due partizioni di un intero pari N. Se $\mathbf{d}$ maggiorizza $\mathbf{d}'$, vi sono almeno tanti grafi semplici etichettati con successione dei gradi $\mathbf{d}'$ quanti ve ne sono con successione $\mathbf{d}$.

Problema 16D. Per n pari si ha $A(n, n/2) \geq 2^{n^2}/n^{2n}$. Dimostrarlo modificando la dimostrazione del corollario al Teorema 16.2. La sostituzione diretta $k = n/2$ nel corollario darebbe un risultato debole.

Problema 16E. Sia $\mathbf{d} = (d_1, \ldots, d_n)$ una partizione di $\binom{n}{2}$, eventualmente con zeri. Dimostrare che esiste un torneo sull'insieme dei vertici $1, 2, \ldots, n$, cioè un orientamento di K_n, nel quale il vertice i abbia grado uscente d_i, se e solo se $\mathbf{d}$ è maggiorizzata da $(n-1, n-2, \ldots, 2, 1, 0)$. Orig. 175

Problema 16F. (i) Dato $m \leq \binom{n}{2}$, considerare il grafo sui vertici $1, \ldots, n$ i cui spigoli sono i primi m sottoinsiemi di due elementi in ordine lessicografico:

$$\{1,2\}, \{1,3\}, \ldots, \{1,n\}, \{2,3\}, \{2,4\}, \ldots, \{2,n\}, \{3,4\}, \ldots.$$

La sua successione dei gradi $\mathbf{r}$ è una partizione di $2m$. Per esempio, per $n = 8, m = 20$, è $(7,7,7,5,4,4,3,3)$. Dati n, m e una partizione $\mathbf{d}$ di $2m$, eventualmente con zeri, dimostrare che esiste un grafo semplice su n vertici con successione dei gradi $\mathbf{d}$ se e solo se $\mathbf{d}$ è maggiorizzata da $\mathbf{r}$.

(ii) Generalizzare agli ipergrafi semplici k-uniformi, ossia a un insieme di punti con una famiglia di sottoinsiemi di k elementi.[1]

* * *

Come nel Capitolo 11, sia $\mathcal{A}(n,2)$ l'insieme delle matrici $(0,1)$ di ordine n con tutte le somme uguali a 2. Un metodo del Capitolo 14 permette di contarne gli $A(n,2)$ elementi.

Sia $\mathcal{A}(n,2)^*$ il sottoinsieme delle matrici indecomponibili e poniamo $a_n := |\mathcal{A}(n,2)^*|$. È facile vedere che $a_n = \frac{1}{2}n!(n-1)!$: vi sono $\binom{n}{2}$ scelte per la prima riga. Se scegliamo $(1,1,0,\ldots,0)$, esiste un'altra riga, fra le $n-1$ rimanenti, con un 1 nella prima colonna e un secondo 1 non nella seconda colonna, per il quale vi sono $n-2$ scelte. Sono $(n-1)(n-2)$ possibilità, e così via. Definiamo

$$m_n := \frac{A(n,2)}{(n!)^2}, \qquad b_k := \frac{a_k}{(k!)^2}.$$

Con lo stesso argomento del Teorema 14.2, Orig. 176

$$1 + \sum_{n=2}^{\infty} m_n x^n = \exp\left(\sum_{k=2}^{\infty} b_k x^k\right). \tag{16.1}$$

Pertanto

$$1 + \sum_{n=2}^{\infty} m_n x^n = \exp\left(\frac{-x - \log(1-x)}{2}\right) = e^{-x/2}(1-x)^{-1/2}. \tag{16.2}$$

È un facile esercizio dedurre dallo sviluppo

$$(1-x)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} \left(\frac{x}{4}\right)^n$$

che $m_n \sim e^{-1/2}\binom{2n}{n}4^{-n}$ per $n \to \infty$. Abbiamo così dimostrato:

Teorema 16.4. $A(n,2) \sim e^{-1/2}\dfrac{(2n)!}{(2!)^{2n}}$.

È un caso particolare del teorema seguente, che dimostreremo soltanto per $k = 3$, con un metodo applicabile anche ad altri valori di k.

[1] Nota redazionale: l'affermazione (i), così formulata nell'originale, non è vera. Per $n = 4, m = 3$ il grafo lessicografico è una stella con gradi $(3,1,1,1)$; il triangolo con un vertice isolato ha gradi $(2,2,2,0)$, non maggiorizzati dalla stella perché $6 > 5$ alla terza somma parziale. L'enunciato è conservato per riconoscibilità, ma non va trattato come un risultato da dimostrare.

Teorema 16.5.

$$A(n,k) = \frac{(nk)!}{(k!)^{2n}} \exp\left(-\frac{(k-1)^2}{2}\right)\left\{1 + O\left(n^{-3/4}\right)\right\} \qquad (n \to \infty),$$

uniformemente in k per $1 \le k < \log n$.

Per ulteriori informazioni e per generalizzazioni a somme non costanti rimandiamo a B. D. McKay (1984).

Orig. 177

Per $k = 3$ dimostriamo un risultato leggermente più forte di quello ottenuto con la sostituzione diretta nel teorema. Usiamo la forma troncata dell'inclusione-esclusione, si veda l'osservazione al Teorema 10.1. Consideriamo $N := 3n$ elementi numerati

$$1_a, 1_b, 1_c, 2_a, 2_b, 2_c, \ldots, n_a, n_b, n_c.$$

Formiamo una permutazione dei N elementi e poi la corrispondente partizione ordinata in terne: $(x,y,z)(u,v,w)\cdots$. Diremo che si verifica una *ripetizione* quando in almeno una terna un numero compare più volte, come in $(5_a, 3_b, 5_c)$. Se non vi sono ripetizioni, associamo alla permutazione una matrice $(0,1)$ di ordine n: se la terna i è $(x_\alpha, y_\beta, z_\gamma)$, con indici in $\{a,b,c\}$, la riga i contiene 1 nelle colonne x, y, z e 0 altrove. Gli indici non influiscono sulla matrice, né conta l'ordine degli elementi nelle terne; quindi ogni matrice corrisponde a $(3!)^{2n}$ permutazioni. La matrice appartiene chiaramente a $\mathcal{A}(n,3)$. Dobbiamo stimare il numero P delle permutazioni senza ripetizioni fra tutte le $N_0 := N!$ permutazioni.

Fissiamo r terne, con $1 \le r \le n$, contiamo le permutazioni con una ripetizione in ciascuna e sommiamo su tutte le scelte delle r terne. Come nel Teorema 10.1, chiamiamo N_r il numero ottenuto. Per R pari,

$$\sum_{r=0}^{R+1} (-1)^r N_r \le P \le \sum_{r=0}^{R} (-1)^r N_r. \tag{16.3}$$

La parte difficile consiste nel trovare buone stime superiore e inferiore di N_r.

Cominciamo da quella superiore. Le terne si scelgono in $\binom{n}{r}$ modi. In ognuna fissiamo due posizioni che devono ripetere un numero, in 3^r modi. Scegliamo poi r numeri destinati a ripetersi e gli indici a, b, c: ancora $\binom{n}{r}3^r$ possibilità. Distribuiamo i numeri scelti nelle posizioni assegnate, in $2^r r!$ modi, e i rimanenti $N - 2r$ elementi arbitrariamente. Una permutazione con una terna del tipo $(5_a, 5_b, 5_c)$ è stata contata più volte. Pertanto

Orig. 178

$$\begin{aligned} N_r &\le \binom{n}{r}^2 3^{2r} 2^r r! (N-2r)! \\ &\le \frac{2^r}{r!}(3^2 n^2)^r (N-2r)! \le \frac{2^r}{r!} N! \left(\frac{N-2r}{N}\right)^{-2r} \\ &\le \frac{2^r}{r!} N! \left(1 + \frac{8r^2}{N}\right), \end{aligned} \tag{16.4}$$

se $r < \frac{1}{2}\sqrt{n}$. L'ultimo passaggio usa lo sviluppo di $(1-2r/N)^{-2r}$ e la scelta di r in modo che ogni termine sia al più metà del precedente.

Per la stima inferiore cominciamo allo stesso modo. Scelte e collocate le r coppie, completiamo prima le r terne con elementi aventi un numero diverso da quello ripetuto. È possibile in più di $(N-3r)^r$ modi. Distribuiamo poi gli elementi rimanenti. Alcune permutazioni da contare vengono escluse, quindi

$$\begin{aligned} N_r &\ge \binom{n}{r}^2 3^{2r} 2^r r! (N-3r)^r (N-3r)! \\ &\ge \frac{2^r}{r!} N! \left[\frac{n(n-1)\cdots(n-r+1)}{n^r}\right]^2 (3^2 n^2)^r \frac{(N-3r)^r}{N^{3r}} \\ &\ge \frac{2^r}{r!} N! \left(1 - \frac{r}{n}\right)^{2r} \left(1 - \frac{3r}{N}\right)^r \\ &\ge \frac{2^r}{r!} N! \left(1 - \frac{3r^2}{n}\right), \end{aligned} \tag{16.5}$$

se $r < \sqrt{n}$. Nell'ultimo passaggio abbiamo usato la nota disuguaglianza $(1 - r/n)^r \geq 1 - r^2/n$, per $1 \leq r \leq \sqrt{n}$.

Orig. 179

Combiniamo (16.3)–(16.5), scegliendo $R = \lfloor \frac{1}{2}\sqrt{n} \rfloor$. Troviamo

$$\frac{P}{N!} = e^{-2} + \Delta, \qquad |\Delta| < \frac{2^{R+1}}{(R+1)!} + \frac{3}{n}\sum_{r=0}^{\infty} \frac{2^r r^2}{r!},$$

e quindi $|\Delta| < 48/n + 18e^2/n < 200/n$. Abbiamo ottenuto la stima seguente, coerente con il Teorema 16.5.

Teorema 16.6. $A(n,3) = e^{-2}\dfrac{(3n)!}{(3!)^{2n}}\,(1 + O(1/n))$ per $n \to \infty$.

Osservazione. Per $k = 3$ il corollario al Teorema 16.2 mostra che $A(n,3)$ cresce almeno come $(cn^3)^n$ per una costante opportuna c; rispetto al Teorema 16.6 cambia soltanto la costante.

Problema 16G. Determinare $A(5,3)$.

Descriviamo un altro collegamento fra (16.2) e il Capitolo 14. Elevando al quadrato il secondo membro di (16.2), otteniamo la funzione generatrice esponenziale degli scompigli dell'Esempio 14.10. Dovremmo quindi poter mostrare combinatoriamente che

$$n!d_n = \sum_{k=0}^{n} \binom{n}{k}^2 A_k A_{n-k}, \tag{16.6}$$

dove A_n indica $A(n,2)$.

Come preparazione, consideriamo una componente indecomponibile di una matrice in $\mathcal{A}(n,2)$, per esempio questa sottomatrice 5×5 per $n = 9$:

	1	3	4	5	9
1	1	1	0	0	0
2	1	0	1	0	0
3	0	1	0	0	1
7	0	0	1	1	0
9	0	0	0	1	1

Partendo dai due 1 nella prima riga, si può descrivere la struttura ciclica in due modi:

Orig. 180

$$(1,3),(3,9),(9,5),(5,4),(4,1),$$

corrispondente alla permutazione (1 3 9 7 2) delle righe, e

$$(3,1),(1,4),(4,5),(5,9),(9,3),$$

corrispondente alla permutazione inversa (1 2 7 9 3). Chiamiamo il primo caso, con $1 < 3$, la variante *rossa*, e il secondo la variante *blu*.

Consideriamo l'insieme S delle matrici di $\mathcal{A}(n,2)$ i cui 1 sono colorati in rosso o blu, con colore uniforme in ogni componente indecomponibile. Chiaramente

$$|S| = \sum_{k=0}^{n} \binom{n}{k}^2 A_k A_{n-k}.$$

Definiamo una corrispondenza biunivoca fra S e le coppie di permutazioni $(a_1,\ldots,a_n)$, $(b_1,\ldots,b_n)$ nelle quali la prima è uno scompiglio. Vi sono $n!d_n$ coppie. Procediamo con un esempio:

$$\mathbf{a} = (2,7,1,8,4,5,9,6,3), \qquad \mathbf{b} = (3,1,4,5,9,2,6,8,7).$$

La decomposizione canonica in cicli di $\mathbf{a}$ è (1 2 7 9 3)(4 8 6 5). Suddividiamo $\mathbf{b}$ di conseguenza in (3 1 4 5 9) e (2 6 8 7). La prima coppia descrive la sottomatrice blu 5×5 considerata sopra; la seconda descrive una sottomatrice rossa 4×4. Questo stabilisce (16.6).

Il problema seguente dà un ulteriore collegamento con il Capitolo 14.

Problema 16H. Sia ancora $A_n := A(n,2)$. In una matrice di $\mathcal{A}(n,2)$ vi sono $\binom{n}{2}$ modi di scegliere i due 1 della prima riga. Supponiamo che siano nelle prime due colonne. È possibile che anche un'altra riga abbia due 1 nelle prime due colonne. Considerare l'altra possibilità e mostrare che

Orig. 181

$$A_n = \frac{n(n-1)}{2}\big(2A_{n-1} + (n-1)A_{n-2}\big). \tag{16.7}$$

Problema 16I. Sia $f(x)$ la funzione al primo membro di (16.1). Da (16.7) ricavare l'equazione differenziale $2(1-x)f' - xf = 0$ e dare una seconda dimostrazione di (16.2).

Note

Il Teorema 16.1 è dovuto a D. Gale (1957) e H. J. Ryser (1957). Per una trattazione più ampia delle classi di matrici considerate rimandiamo a Ryser (1963).

Il collegamento fra (16.2) e la funzione generatrice degli scompigli ci è stato segnalato da D. G. E. D. Rogers. La dimostrazione di (16.6) è dovuta a P. Diaconis e D. E. Knuth, comunicazione privata.

La relazione (16.7) fu annunciata senza dimostrazione da R. Bricard (1901).

Riferimenti bibliografici

R. Bricard (1901)
Problème de combinaisons, *L'Intermédiaire des Mathématiciens* **8**, 312–313.

D. Gale (1957)
A theorem on flows in networks, *Pacific J. Math.* **7**, 1073–1082.

M. Krause (1996)
A simple proof of the Gale-Ryser theorem, *Amer. Math. Monthly* **103**, 335–337.

B. D. McKay (1984)
Asymptotics for (0,1)-matrices with prescribed line sums, in *Enumeration and Design* (D. M. Jackson e S. A. Vanstone, a cura di), Academic Press.

H. J. Ryser (1957)
Combinatorial properties of matrices of zeros and ones, *Canad. J. Math.* **9**, 371–377.

H. J. Ryser (1963)
Combinatorial Mathematics, Carus Math. Monograph 14.

Capitolo 17

Quadrati latini

Un *quadrato latino* di ordine n è una quadrupla $(R, C, S; L)$, dove R, C, S sono insiemi di cardinalità n e L è un'applicazione $L : R \times C \to S$ tale che, per ogni $i \in R$ e $x \in S$, l'equazione Orig. 182

$$L(i, j) = x$$

ha un'unica soluzione $j \in C$ e, per ogni $j \in C$, $x \in S$, la stessa equazione ha un'unica soluzione $i \in R$. In altre parole, due qualunque fra $i \in R$, $j \in C$, $x \in S$ determinano univocamente il terzo in modo che $L(i, j) = x$. Gli elementi di R si chiamano *righe*, quelli di C *colonne* e quelli di S *simboli* o *elementi* del quadrato latino. Un quadrato latino si scrive solitamente come uno schieramento $n \times n$, la cui casella nella riga i e nella colonna j contiene il simbolo $L(i, j)$. La Figura 17.1 mostra un quadrato latino di ordine 5.

a	b	c	d	e
b	a	e	c	d
c	d	b	e	a
d	e	a	b	c
e	c	d	a	b

Figura 17.1

La denominazione «quadrato latino» risale a Eulero, che utilizzava per S un insieme di lettere latine.

Un *quasigruppo* è un quadrato latino $(X, X, X; \circ)$ in cui l'insieme delle righe, quello delle colonne e quello dei simboli coincidono con X. In questo caso abbreviamo la quadrupla e indichiamo il quasigruppo semplicemente con $(X, \circ)$. L'applicazione $\circ$ è ora un'operazione binaria su X e l'immagine di (x, y) si indica con $x \circ y$. Come caso particolare otteniamo quindi i quadrati latini costituiti dalle tavole di moltiplicazione dei gruppi. Orig. 183

Problema 17A. Fissate le prime due righe della Figura 17.1, vi sono molti modi di riempire le tre righe rimanenti per ottenere un quadrato latino (precisamente 24). Dimostrare che nessuno di questi quadrati latini è la tavola di moltiplicazione di un gruppo.

Si osservi che, se $(R, C, S; L)$ è un quadrato latino, le applicazioni $\sigma : R \to R'$, $\tau : C \to C'$, $\pi : S \to S'$ sono biiezioni e si definisce $L'(\sigma(i), \tau(j)) := \pi(L(i, j))$, allora $(R', C', S'; L')$ è un quadrato latino. I due quadrati latini si dicono *equivalenti*. Con questa nozione di equivalenza possiamo dunque supporre che un quadrato latino di ordine n sull'insieme $S := \{1, 2, \ldots, n\}$ abbia, nella prima riga e nella prima colonna, gli interi da 1 a n in questo ordine. Due quadrati latini diversi, normalizzati in questo modo, possono tuttavia essere equivalenti. Talvolta indicheremo un quadrato latino semplicemente con «$L : R \times C \to S$».

Uno *schieramento ortogonale* $\mathrm{OA}(n, 3)$ di ordine n e profondità 3 è uno schieramento $3 \times n^2$ con elementi interi da 1 a n, tale che, per due righe qualsiasi dello schieramento, le n^2 coppie verticali che compaiono in queste righe siano diverse. Supponiamo di avere un tale schieramento. Chiamiamo le righe r, c, s, in un ordine qualsiasi. Per ogni coppia (i, j) esiste un k tale che $r_k = i$, $c_k = j$. Costruiamo un quadrato ponendo s_k nella riga i e nella colonna j, per tutti gli i, j. La definizione di schieramento ortogonale garantisce che questo sia un quadrato latino; inoltre il procedimento si può invertire. Pertanto i concetti di quadrato latino e di schieramento ortogonale sono equivalenti. La Figura 17.2 mostra un $\mathrm{OA}(4, 3)$ e due quadrati latini corrispondenti.

Due quadrati latini i cui schieramenti ortogonali corrispondenti hanno le stesse tre righe, eventualmente in ordine diverso, si dicono *coniugati*. Per esempio, uno dei coniugati di un quadrato latino con $R = C$ è il suo trasposto. Come esercizio, il lettore scriva i sei coniugati del quadrato latino nella Figura 17.2. Due schieramenti ortogonali si dicono *isomorfi* se l'uno si ottiene dall'altro mediante permutazioni dei simboli in ciascuna riga e permutazioni delle righe e delle colonne dello schieramento. Si dicono isomorfi anche due quadrati latini i cui schieramenti ortogonali corrispondenti sono isomorfi. Ciò significa che uno è equivalente a un coniugato dell'altro.

Orig. 184

righe	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
colonne	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
simboli	3	2	4	1	1	4	2	3	4	3	1	2	2	1	3	4

3	2	4	1
1	4	2	3
4	3	1	2
2	1	3	4

simboli	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
colonne	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
righe	3	2	4	1	1	4	2	3	4	3	1	2	2	1	3	4

2	4	3	1
4	1	2	3
1	3	4	2
3	2	1	4

Figura 17.2

Problema 17B. Considerare i due quadrati latini ottenuti dalla Figura 17.3 ponendo, rispettivamente, $a = 1, b = 2$ e $a = 2, b = 1$.

1	2	3	4	5
2	1	4	5	3
3	5	a	b	4
4	3	5	a	b
5	4	b	3	a

Figura 17.3

Dimostrare che questi due quadrati sono equivalenti. Dimostrare che un quadrato non equivalente a essi corrisponde al gruppo ciclico di ordine 5.

Un quadrato latino si può anche interpretare come uno schieramento tridimensionale di 0 e 1, con esattamente un 1 su ogni linea dello schieramento parallela a uno dei lati. Per esempio, nella Figura 17.3 l'elemento 4 nella riga 2 e nella colonna 3 va allora interpretato come un 1 nella posizione $(2, 3, 4)$ dello schieramento.

In un capitolo successivo considereremo schieramenti ortogonali di profondità maggiore di 3. Spesso essi sono molto più difficili da costruire degli schieramenti $\mathrm{OA}(n, 3)$.

Problema 17C. Costruire un $\mathrm{OA}(4, 4)$, cioè una matrice A di dimensioni 4×16 con elementi 1,2,3,4 tale che, per due righe qualsiasi di A, diciamo la riga i e la riga j, le 16 coppie (a_{ik}, a_{jk}), $1 \le k \le 16$, siano tutte diverse. Un *sottoquadrato latino*, o semplicemente *sottoquadrato*, di un quadrato latino $(R, C, S; L)$ è un quadrato latino $(R_1, C_1, S_1; L_1)$ con $R_1 \subseteq R$, $C_1 \subseteq C$, $S_1 \subseteq S$ e $L_1(i, j) = L(i, j)$ per $(i, j) \in R_1 \times C_1$.

Orig. 185

Problema 17D. Siano m, n interi positivi, $m < n$. Dimostrare che $m \le \frac{1}{2}n$ è condizione necessaria e sufficiente per l'esistenza di un quadrato latino di ordine n contenente un sottoquadrato di ordine m.

I problemi che seguono hanno tutti natura simile. Riguardano una questione analoga a quella dei Problemi 17B e 17D: il completamento di un quadrato riempito solo in parte. Uno schieramento A di dimensioni $n \times n$, le cui caselle sono vuote oppure contengono esattamente un simbolo, si chiama *quadrato latino parziale* se nessun simbolo compare più di una volta in una stessa riga o colonna. (Sarebbe forse meglio dire che lo schieramento «ha la proprietà latina», ma useremo la prima terminologia.) Ci interessano condizioni che garantiscano che un quadrato latino parziale si possa completare a un quadrato latino di ordine n, cioè che le caselle vuote si possano riempire con simboli in modo da ottenere un quadrato latino. Per esempio, se A è un quadrato latino parziale con tutte le caselle piene, ossia non vuote, eccetto quelle dell'ultima riga, esiste chiaramente un unico modo di completarlo. Viceversa, i due quadrati latini parziali della Figura 17.4 non sono evidentemente completabili.

1	2	3	4	
				5

1				
	1			
		1		
			1	
				2

Figura 17.4

A un quadrato latino parziale possiamo associare uno schieramento come abbiamo fatto per i quadrati latini, considerando soltanto le caselle piene. Possiamo così definire il coniugato di un quadrato latino parziale. I due quadrati latini parziali della Figura 17.4 non sono sostanzialmente diversi: sono coniugati, come risulta dai loro «OA$(5,3)$ parziali» riportati qui sotto:

Orig. 186

$$\begin{array}{c}\text{righe}\\ \text{colonne}\\ \text{simboli}\end{array}\quad\begin{pmatrix}1&1&1&1&2\\1&2&3&4&5\\1&2&3&4&5\end{pmatrix}\qquad\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\\1&1&1&1&2\end{pmatrix}.$$

Se le prime k righe di un quadrato latino parziale, $k \le n$, sono piene e tutte le altre caselle sono vuote, A si chiama *rettangolo latino* $k \times n$.

Teorema 17.1. Un rettangolo latino $k\times n$, con $k < n$, si può estendere a un rettangolo latino $(k+1)\times n$ e quindi si può completare.

Dimostrazione. Sia B_j l'insieme degli interi positivi fra 1 e n che non compaiono nella colonna j di A. Ciascuno dei numeri da 1 a n compare k volte in A e quindi $n-k$ volte negli insiemi B_j. Presi l qualsiasi degli insiemi B_j, essi contengono complessivamente $l(n-k)$ elementi, contando le ripetizioni, e quindi almeno l elementi distinti. Gli insiemi B_j, $1 \le j \le n$, hanno dunque la proprietà H del Capitolo 5; per il Teorema 5.1 possiedono perciò un SDR. Questo SDR si può aggiungere come $(k+1)$-esima riga del rettangolo latino. □

Indichiamo con $L(n)$ il numero totale di quadrati latini distinti di ordine n. Il valore esatto di $L(n)$ è noto soltanto per $n \le 9$. Questi numeri crescono molto rapidamente: per esempio, benché esistano soltanto due quadrati latini di ordine 5 non equivalenti, ve ne sono $5!\cdot 4!\cdot 56$ distinti.

Teorema 17.2. $L(n) \ge (n!)^{2n}/n^{n^2}$.

Dimostrazione. Per costruire un quadrato latino di ordine n possiamo scegliere come prima riga una qualsiasi permutazione di $1,\dots,n$. Se abbiamo costruito un rettangolo latino con k righe, dalla dimostrazione del Teorema 17.1 segue che il numero di scelte per la riga successiva è per B, dove $b_{ij}=1$ se $i \in B_j$. Per il Teorema 12.8, ossia la congettura di Van der Waerden, questo permanente è almeno $(n-k)^n n!/n^n$. Troviamo dunque

$$L(n) \ge n! \prod_{k=1}^{n-1} \{(n-k)^n n!/n^n\} = (n!)^{2n}/n^{n^2}. \tag{17.1}$$

□ **Osservazione.** Applicando il Teorema 5.3 avremmo ottenuto la stima $L(n) \ge n!(n-1)!\cdots 1!$ (H. J. Ryser, 1969), migliore per piccoli n, ma asintoticamente molto più piccola di (17.1).

Orig. 187

Per $n = 8$, la stima (17.1) è minore di 10^{-4} volte il valore vero; asintoticamente, però, (17.1) è ottimale, come mostra il prossimo teorema.

Teorema 17.3. Posto $\mathcal{L}(n) := \{L(n)\}^{1/n^2}$, si ha

$$\mathcal{L}(n) \sim e^{-2}n \qquad (n \to \infty).$$

Dimostrazione. Da (17.1) e dalla formula di Stirling troviamo $n^{-1}\mathcal{L}(n) \ge e^{-2}$. Con lo stesso ragionamento usato nella dimostrazione del Teorema 17.2, stimando per B mediante il Teorema 11.5, otteniamo

$$L(n) \le \prod_{k=1}^{n} M(n,k) \le \prod_{k=1}^{n} (k!)^{n/k}.$$

Di conseguenza, usando ancora la formula di Stirling, con C una costante maggiore di $\sqrt{2\pi}$, abbiamo

$$\begin{aligned}\log \mathcal{L}(n) &\le \frac{1}{n}\sum_{k=1}^{n}\frac{1}{k}\log k! \\ &\le \frac{1}{n}\sum_{k=1}^{n}\left\{\log k - 1 + \frac{1}{2k}\log k + \frac{1}{k}\log C\right\} \\ &= \frac{1}{n}\sum_{k=1}^{n}\log k - 1 + o(1) \\ &= -2 + \log n + o(1) \qquad (n\to\infty).\end{aligned}$$

Combinando questa stima con quella inferiore si ottiene il risultato. □

Il teorema seguente, dovuto a H. J. Ryser (1951), generalizza il Problema 17D.

Teorema 17.4. Sia A un quadrato latino parziale di ordine n in cui la casella (i,j) è piena se e solo se $i \le r$ e $j \le s$. Allora A si può completare se e solo se $N(i) \ge r+s-n$ per $i = 1,\dots,n$, dove $N(i)$ indica il numero di elementi di A uguali a i. Orig. 188

Dimostrazione. Osserviamo anzitutto che, in un quadrato latino di ordine n, le prime r righe contengono esattamente r elementi uguali a i, dei quali al più $n-s$ si trovano nelle ultime $n-s$ colonne. La condizione su $N(i)$ è dunque banalmente necessaria. Dimostriamo che è anche sufficiente. Sia B la matrice $(0,1)$ di dimensioni $r\times n$ con $b_{ij}=1$ se e solo se l'elemento j non compare nella riga i di A. Chiaramente ogni riga di B ha somma $n-s$. La colonna j di B ha somma $r-N(j)\le n-s$. Per il Teorema 7.5, con $d := n-s$, abbiamo

$$B = L^{(s+1)} + \cdots + L^{(n)},$$

dove ogni $L^{(t)}$ è una matrice $(0,1)$ di dimensioni $r\times n$, con un 1 in ogni riga e al più un 1 in ogni colonna.

Come esempio, supponiamo che $r=s=4$, $n=7$ e che le prime quattro righe di A siano

$$\begin{array}{cccc}1&2&3&4\\5&3&1&6\\3&1&5&2\\7&4&2&5\end{array}.$$

Allora, per esempio,

$$B := \begin{pmatrix}0&0&0&0&1&1&1\\0&1&0&1&0&0&1\\0&0&0&1&0&1&1\\1&0&1&0&0&1&0\end{pmatrix} = L^{(5)}+L^{(6)}+L^{(7)},$$

$$L^{(5)} = \begin{pmatrix}0&0&0&0&0&0&1\\0&0&0&1&0&0&0\\0&0&0&0&0&1&0\\1&0&0&0&0&0&0\end{pmatrix},\quad L^{(6)} = \begin{pmatrix}0&0&0&0&0&1&0\\0&0&0&0&0&0&1\\0&0&0&1&0&0&0\\0&0&1&0&0&0&0\end{pmatrix},$$

$$L^{(7)} = \begin{pmatrix}0&0&0&0&1&0&0\\0&1&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&0&0&0&1&0\end{pmatrix}.$$

Scriviamo $L^{(t)} = [l_{ij}^{(t)}]$. Riempiamo la casella di A in posizione (i,j), con $i=1,\dots,r$ e $j=s+1,\dots,n$, mediante k se $l_{ik}^{(j)}=1$. Nel nostro esempio le ultime tre colonne vengono riempite con

$$\begin{array}{ccc}7&6&5\\4&7&2\\6&4&7\\1&3&6\end{array}\ ,\ \begin{array}{ccc}&&\\&&\\,&,&.\\&&\end{array}$$

Così A si trasforma in un quadrato latino parziale di ordine n con r righe complete, cioè in un rettangolo Orig. 189

latino. Per il Teorema 17.1, esso si può completare a un quadrato latino di ordine n. □

Gli esempi di quadrati latini parziali non completabili della Figura 17.4 hanno entrambi n caselle piene. La congettura secondo cui un quadrato latino parziale con meno di n caselle piene si può completare a un quadrato latino era nota come *congettura di Evans*, finché fu dimostrata da B. Smetaniuk (1981). La parte forse più importante della dimostrazione di Smetaniuk è la costruzione del Teorema 17.5.

Teorema 17.5. Sia A un quadrato latino di ordine n. Sia B uno schieramento $(n+1) \times (n+1)$ il cui elemento (i, j) coincide con l'elemento (i, j) di A per $i, j \geq 1$, $i + j \leq n + 1$, che ha un nuovo simbolo α sull'antidiagonale e le cui caselle al di sotto dell'antidiagonale sono vuote. Allora B si può completare a un quadrato latino di ordine $n + 1$.

Qui sotto sono riportati un quadrato latino A di ordine 5 e lo schieramento corrispondente B.

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \\ 2 & 5 & 1 & 3 & 4 \\ 5 & 1 & 4 & 2 & 3 \\ 3 & 4 & 2 & 5 & 1 \end{array} \qquad \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \alpha \\ 4 & 3 & 5 & 1 & \alpha & \\ 2 & 5 & 1 & \alpha & & \\ 5 & 1 & \alpha & & & \\ 3 & \alpha & & & & \\ \alpha & & & & & \end{array} .$$

Dimostrazione. Sia C lo schieramento $n \times n$ ottenuto da B eliminando l'ultima riga e l'ultima colonna. Nel nostro esempio, C è lo schieramento seguente.

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & \alpha \\ 2 & 5 & 1 & \alpha & \\ 5 & 1 & \alpha & & \\ 3 & \alpha & & & \end{array}$$

Descriviamo un algoritmo che riempie le caselle vuote di C riga per riga, imponendo che, dopo aver riempito le prime r righe, si ottenga un rettangolo latino $r \times n$ sui $n+1$ simboli $1, 2, \ldots, n, \alpha$, nel quale la colonna j contiene, in qualche ordine, gli stessi simboli presenti nelle prime r righe di A, salvo un simbolo, detto «mancante», per ciascuna colonna contenente α, e tale che gli $r - 1$ simboli mancanti siano tutti distinti.[1] Per $r = 1$ e $r = 2$ ciò è banale. Supponiamo di aver effettuato la costruzione per un certo r, $2 \leq r < n$, e che i simboli mancanti siano a questo punto

Orig. 190

$$x_{n-r+2}, x_{n-r+3}, \ldots, x_n.$$

Per riempire la riga $(r + 1)$ procediamo come segue.

Siano

$$y_{n-r+1}, y_{n-r+2}, y_{n-r+3}, \ldots, y_n$$

gli ultimi r simboli della riga $r+1$ di A, eliminati nella costruzione di C. Qui y_{n-r+1} è il simbolo sostituito da α e deve essere il nuovo elemento mancante in quella colonna. Possiamo provare a riempire la riga $r + 1$ con

$$y_{n-r+2}, y_{n-r+3}, \ldots, y_n;$$

questo va bene se

$$y_{n-r+1}, x_{n-r+2}, x_{n-r+3}, \ldots, x_n,$$

che sarebbero i nuovi simboli mancanti, sono distinti. Altrimenti consideriamo la successione

$$\begin{aligned} y_{n-r+1} &= x_{k_1}, \\ y_{k_1} &= x_{k_2}, \\ &\vdots \\ y_{k_{m-1}} &= x_{k_m}, \end{aligned}$$

prolungata finché è possibile, cioè finché y_{k_m} non coincide con nessuno degli x_j. Riempiamo allora la riga $r+1$ con $y_{n-r+2}, y_{n-r+3}, \ldots, y_n$, sostituendo però $y_{k_1}, y_{k_2}, \ldots, y_{k_m}$ rispettivamente con $x_{k_1}, x_{k_2}, \ldots, x_{k_m}$. Occorre verificare che l'intera riga $r + 1$ contenga simboli distinti. I nuovi simboli mancanti sono y_{n-r+1}

e $x_{n-r+2}, x_{n-r+3}, \ldots, x_n$, con $x_{k_1}, x_{k_2}, \ldots, x_{k_m}$ sostituiti rispettivamente da $y_{k_1}, y_{k_2}, \ldots, y_{k_m}$. Occorre verificare che siano distinti. Orig. 191

Una volta riempite le caselle vuote di C, le prime n caselle dell'ultima riga di B vanno riempite con α e con i simboli mancanti, per $r = n$. Abbiamo ora un rettangolo latino $(n+1) \times n$, che si completa in modo unico a un quadrato latino di ordine $n+1$. □

Problema 17E. Sia A il quadrato latino di ordine 10 riportato a sinistra qui sotto e sia C il rettangolo latino parziale 10×10 sugli 11 simboli $0, 1, 2, \ldots, 9, \alpha$ riportato a destra, escludendo l'ultima riga e l'ultima colonna. Usare l'algoritmo della dimostrazione del Teorema 17.5 per completare C a un rettangolo latino 10×10 sui simboli $0, 1, 2, \ldots, 9, \alpha$. Completare poi questo rettangolo latino a un quadrato latino di ordine 11.

4	1	3	5	9	6	0	2	8	7	
5	8	9	2	6	7	3	4	1	0	
9	4	5	6	0	3	7	8	2	1	
1	3	4	7	5	2	8	9	0	6	
2	6	1	3	7	4	5	0	9	8	
7	9	0	1	4	8	2	3	6	5	
6	7	8	9	1	0	4	5	3	2	
8	5	6	0	2	9	1	7	4	3	
3	0	2	4	8	5	6	1	7	9	
0	2	7	8	3	1	9	6	5	4	

4	1	3	5	9	6	0	2	8	7	α
5	8	9	2	6	7	3	4	1	α	
9	4	5	6	0	3	7	8	α		
1	3	4	7	5	2	8	α			
2	6	1	3	7	4	α				
7	9	0	1	4	α					
6	7	8	9	α						
8	5	6	α							
3	0	α								
0	α									
α										

(Per esempio, l'algoritmo riempie le prime cinque righe di C come indicato a destra qui sotto. Gli elementi «mancanti» dalla settima, ottava, nona e decima colonna sono a questo punto, rispettivamente, $5, 9, 2, 0$. Consideriamo ora la sesta riga. Il simbolo α nella sesta colonna impone che 8 sia l'elemento mancante da quella colonna. Ma 8 è diverso dagli elementi attualmente mancanti dalle altre colonne. Non occorre quindi fare altro: riempiamo semplicemente la sesta riga con gli elementi $2, 3, 6, 5$ della sesta riga di A.) Orig. 192

4	1	3	5	9	6	0	2	8	7	
5	8	9	2	6	7	3	4	1	0	
9	4	5	6	0	3	7	8	2	1	
1	3	4	7	5	2	8	9	0	6	
2	6	1	3	7	4	5	0	9	8	
7	9	0	1	4	8	2	3	6	5	

4	1	3	5	9	6	0	2	8	7	
5	8	9	2	6	7	3	4	1	α	
9	4	5	6	0	3	7	8	α	1	
1	3	4	7	5	2	8	α	0	6	
2	6	1	3	7	4	α	0	9	8	
7	9	0	1	4	α					

Problema 17F. (i) Siano A, B quadrati latini di ordine n sui simboli $1, 2, \ldots, n$. Siano A', B' i quadrati latini sui simboli $1, 2, \ldots, n+1$, con $n+1$ sull'antidiagonale, che coincidono rispettivamente con A, B al di sopra delle loro antidiagonali, costruiti come nella dimostrazione del Teorema 17.5. Dimostrare che, se A e B sono distinti, anche A' e B' sono distinti. Ciò dimostra che il numero di quadrati latini di ordine $n+1$ con $n+1$ sull'antidiagonale è maggiore o uguale al numero $N(n)$ dei quadrati latini di ordine n.

(ii) Spiegare come dalla parte (i) segue il risultato

$$L(n) \geq n!(n-1)! \cdots 2!1!$$

menzionato nell'osservazione successiva al Teorema 17.2.

Teorema 17.6. Un quadrato latino parziale di ordine n con al più $n-1$ caselle piene si può completare a un quadrato latino di ordine n.

Dimostrazione. Procediamo per induzione. Supponiamo il teorema vero per n e sia L un quadrato latino parziale di ordine $n+1$ con al più n caselle piene.

Supponiamo anzitutto che un simbolo x di L compaia una sola volta. Intendiamo permutare righe e colonne per portare tutte le caselle piene al di sopra dell'antidiagonale, tranne il singolo simbolo x, che verrà collocato sull'antidiagonale. Supponiamo che le righe non vuote abbiano $f_1, f_2, \ldots, f_k$ caselle piene, con $f_1 + \cdots + f_k \leq n$, e che x si trovi nella riga con f_1 caselle piene. Mettiamo questa riga in posizione $n+1-f_1$ e permutiamo le colonne per spostare a sinistra le caselle piene. Mettiamo la riga con f_2 caselle

[1]Nota di traduzione: nell'originale compare qui x al posto di α, e lo stesso scambio ricorre nell'ultimo passo della dimostrazione. Si uniforma il simbolo a quello dell'enunciato.

piene in posizione $n+1-f_1-f_2$ e permutiamo le colonne, eccettuate le prime f_1, per spostare a sinistra le caselle piene: queste si troveranno tutte nelle prime f_1+f_2 caselle della riga. Mettiamo la riga con f_3 caselle piene in posizione $n+1-f_1-f_2-f_3$, e così via, finché tutte le caselle piene si trovano al di sopra dell'antidiagonale. Se la casella contenente x nella riga $n+1-f_1$ si trova nella colonna j, scambiamo poi la colonna j con la colonna f_1+1. Orig. 193

Per l'ipotesi induttiva, la parte al di sopra dell'antidiagonale, che ha al più $n-1$ caselle piene, si può completare a un quadrato latino A di ordine n su simboli diversi da x. Lo schieramento B descritto nell'enunciato del Teorema 17.5 contiene le caselle originariamente piene di un quadrato latino parziale che differisce da L soltanto per permutazioni di righe e colonne. Quel teorema afferma che B si può completare, e quindi si può completare anche L.

A questo punto possiamo affermare che L è completabile anche se una riga contiene esattamente una casella piena o se una colonna contiene esattamente una casella piena: infatti un coniugato di L avrà un simbolo che compare una sola volta. Per esempio, ogni riga del quadrato parziale a destra nella Figura 17.4 contiene esattamente una casella piena e nel suo coniugato a sinistra ogni simbolo compare esattamente una volta. Un coniugato di L è completabile se e solo se lo è L.

Possiamo dunque supporre che nessuna riga o colonna contenga esattamente una casella piena. Le caselle piene sono perciò contenute in al più m righe e m colonne, dove $m := \lfloor n/2 \rfloor$. Permutando righe e colonne, possiamo fare in modo che tutte le caselle piene si trovino nel sottoschieramento di ordine m in alto a sinistra. Il Teorema 17.4 implica che ogni rettangolo latino $m \times m$ si può completare a un quadrato latino di ordine $n+1$. Basta quindi riempire le caselle vuote del sottoschieramento di ordine m in alto a sinistra, ottenendo un rettangolo latino. Questo è facile: abbiamo a disposizione $n+1$ simboli e possiamo procedere in un ordine qualsiasi, riempiendo ogni casella del sottoquadrato con un simbolo non ancora usato nella riga o nella colonna che la contiene. □

Passiamo ora a una generalizzazione dell'idea di quadrato latino. Supponiamo data una famiglia $\mathcal{C}$ di n-insiemi $C(i,j)$, $i,j = 1,2,\ldots,n$. Possiamo chiederci se esista una matrice A di dimensioni $n \times n$ nella quale gli elementi a_{ij} di ogni riga, e rispettivamente di ogni colonna, siano tutti diversi e tale che $a_{ij} \in C(i,j)$ per tutti gli i,j. Se tutti gli n-insiemi sono $\{1,2,\ldots,n\}$, la risposta è affermativa, perché ogni quadrato latino fornisce una soluzione. Se gli elementi di $\mathcal{C}$ sono a due a due disgiunti, la questione è banale. È forse sorprendente che la maggiore libertà derivante dal non richiedere che gli n-insiemi coincidano renda la questione più difficile. Infatti, in questo caso non vale un analogo del Teorema 17.1. La congettura secondo cui una tale matrice A esiste effettivamente era nota come *congettura di Dinitz*, finché F. Galvin (1995) la dimostrò. Orig. 194

Useremo la terminologia delle colorazioni dei grafi, argomento ampiamente trattato nel Capitolo 33. Sia G un grafo semplice. Un'*assegnazione di liste* a G è una funzione C che associa un insieme $C(v)$ a ogni vertice v di G. Una *C-colorazione* di G è una funzione A definita sull'insieme dei vertici, tale che $A(v) \in C(v)$ e tale che $A(v)$ e $A(w)$ siano diversi quando v e w sono adiacenti in G.

Sia f una funzione dall'insieme dei vertici di G negli interi. Diciamo che G è *f-colorabile* se esiste una C-colorazione di G per ogni C tale che $|C(v)| \geq f(v)$ per tutti i vertici v di G. Se k è un intero, un grafo si dice *k-colorabile per liste* se è f-colorabile per la funzione costante $f(v) = k$. Chiaramente, se G è k-colorabile per liste, allora k è almeno il numero cromatico $\chi(G)$, definito nel Capitolo 3.

Il *grafo degli spigoli* $L = L(G)$ di un grafo semplice G è il grafo semplice con insieme dei vertici $V(L) := E(G)$, nel quale $a,b \in E(G)$ sono adiacenti come vertici di L se e solo se, come spigoli di G, hanno un estremo in comune. Consideriamo ora il grafo degli spigoli $L_2(n)$ di $K_{n,n}$ (si veda il Capitolo 21). Esso ha n^2 vertici $\{i,j\}$, $i,j = 1,2,\ldots,n$, dove le coppie sono unite se e solo se hanno un elemento in comune.[2] La congettura di Dinitz si può formulare così: $L_2(n)$ è n-colorabile per liste. Il teorema dimostrato da Galvin afferma che, per un grafo bipartito G, il grafo degli spigoli $L = L(G)$ è $\chi(L)$-colorabile per liste. Poiché i quadrati latini esistono, $L_2(n)$ ha numero cromatico n e la congettura di Dinitz è dunque vera.

Dimostreremo due proposizioni dalle quali seguirà il teorema.

Un sottoinsieme K dell'insieme dei vertici di un digrafo D si chiama *nucleo* di D se nessuna coppia di vertici di K è unita da un arco e, per ogni $v \notin K$, esiste $w \in K$ tale che in D vi sia un arco da v a w.

Proposizione 17.7. Sia D un digrafo ogni cui sottografo indotto possiede un nucleo. Si ponga $f(v) := 1 + \text{grado uscente}(v)$ per ogni vertice v di D. Allora D è f-colorabile. Orig. 195

[2] Nota di traduzione: gli indici i e j appartengono alle due diverse parti del grafo bipartito; la loro etichettatura con gli stessi interi non identifica i vertici delle due parti.

DIMOSTRAZIONE. Usiamo l'induzione sul numero di vertici. I casi piccoli si verificano facilmente. (Si osservi che l'unico digrafo su tre vertici per il quale non valgono né la condizione né l'affermazione del problema è il circuito diretto.)

Sia C un'assegnazione di liste a D con $|C(v)| \geq f(v)$ per ogni v. Scegliamo un elemento x di uno degli insiemi di C e consideriamo tutti i vertici v tali che $x \in C(v)$. Chiamiamo D_1 il sottografo indotto su questi vertici. Per ipotesi, D_1 possiede un nucleo K. Sia D_2 il sottografo indotto sui vertici di $D \setminus K$. Per un vertice $v \notin K$ definiamo $C'(v) := C(v) \setminus \{x\}$. Per l'ipotesi induttiva, D_2 possiede una C'-colorazione A'. Definendo A su D mediante

$$A(v) := \begin{cases} A'(v) & \text{se } v \notin K, \\ x & \text{se } v \in K, \end{cases}$$

si ottiene chiaramente una C-colorazione di D. □

Per la prossima proposizione, diciamo che un orientamento di un grafo G è *normale* se ogni cricca di G è orientata come un torneo transitivo.

Proposizione 17.8. Ogni orientamento normale del grafo degli spigoli $L = L(G)$ di un grafo bipartito G possiede un nucleo.

DIMOSTRAZIONE. Usiamo l'induzione sul numero di spigoli di G. Per valori piccoli l'affermazione si verifica facilmente. Supponiamo $V(G) = X \cup Y$, con tutti gli spigoli fra X e Y. Possiamo supporre che ogni vertice di G abbia grado positivo. Sia D un orientamento normale di $L(G)$. Le cricche di $L(G)$ corrispondono a vertici di X o di Y.

Per ogni vertice $x \in X$ consideriamo la cricca corrispondente in $L(G)$ e definiamo $e(x) := \{x, y(x)\}$ come il pozzo di questa cricca rispetto a D. Supponiamo anzitutto che, per ogni $x \in X$, il vertice $e(x)$ di $L(G)$ sia la sorgente della cricca definita da $y(x) \in Y$. È allora evidente che gli $y(x)$, per $x \in X$, sono tutti distinti. Pertanto $K := \{\{x, y(x)\} : x \in X\}$ è un nucleo di $L(G)$.

Supponiamo ora che, per un certo $x \in X$, $e(x) := \{x, y(x)\}$ sia il pozzo della cricca corrispondente a x, ma che $e' := \{x', y(x)\}$, con $x' \neq x$, sia la sorgente della cricca corrispondente a $y(x)$. Eliminiamo da G lo spigolo $\{x', y(x)\}$. Per l'ipotesi induttiva, il grafo degli spigoli risultante possiede un nucleo K. Affermiamo che K è un nucleo anche per D. Dobbiamo mostrare che esiste un arco da e' a K. Se Orig. 196
$e(x) \in K$, abbiamo finito, perché e' è una sorgente. Se invece $e(x) \notin K$, esiste un arco da $e(x)$ a qualche elemento di K che, per la definizione di $e(x)$, deve essere della forma $\{x'', y(x)\}$. Poiché il torneo definito da $y(x)$ è transitivo, abbiamo concluso anche in questo caso. □

Possiamo ora dimostrare il risultato principale.

Teorema 17.9. Se G è un grafo bipartito, allora $L = L(G)$ è $\chi(L)$-colorabile per liste.[3]

DIMOSTRAZIONE. Sia G un grafo bipartito sull'insieme di vertici $X \cup Y$. Sia g una colorazione dei vertici di $L = L(G)$ con i colori $1, 2, \ldots, \chi(L)$. Orientiamo L formando un digrafo D nel modo seguente: se $e_1 = \{x_1, y_1\}$ ed $e_2 = \{x_2, y_2\}$ sono vertici adiacenti di L e $g(e_1) < g(e_2)$, allora

$$\begin{cases} \text{l'arco va da } e_1 \text{ a } e_2 & \text{se } x_1 = x_2, \\ \text{l'arco va da } e_2 \text{ a } e_1 & \text{se } y_1 = y_2. \end{cases}$$

Poiché ogni cricca di L corrisponde a un vertice $x \in X$ oppure $y \in Y$, questo orientamento è normale. Per la Proposizione 17.8, ogni sottografo indotto di D possiede un nucleo. Chiaramente 1+grado uscente$(e) \leq \chi(L)$ per ogni vertice e di D. La Proposizione 17.7 completa dunque la dimostrazione. □

Problema 17G. (a) Sia n pari. Trovare una permutazione $x_1, x_2, \ldots, x_n$ degli elementi di $\mathbb{Z}_n$ tale che le differenze $x_{i+1} - x_i$, $1 \leq i < n$, siano tutte diverse.

(b) Dimostrare che ciò non è possibile se n è dispari.

(c) Considerare la permutazione della parte (a). Definire $a_{ij} := x_i + x_j$. Dimostrare che il quadrato con elementi a_{ij}, $1 \leq i, j \leq n$, è un quadrato latino con la proprietà seguente: le $n(n-1)$ coppie adiacenti $(a_{ij}, a_{i,j+1})$ sono diverse. Un tale quadrato si dice *completo per righe*. Questo quadrato è anche *completo per colonne*.

[3]Nota di traduzione: nell'enunciato originale manca «per liste»; il contesto, la dimostrazione e l'affermazione del teorema a p. 194 mostrano che si tratta di un'omissione tipografica.

Problema 17H. Descrivere una corrispondenza biunivoca fra i quadrati latini simmetrici di ordine n nei quali tutti i simboli compaiono sulla diagonale principale e i quadrati latini simmetrici di ordine $n+1$ con tutti gli elementi diagonali uguali a $n+1$.

Orig. 197

Problema 17I. La prima riga di un quadrato latino sia $1, 2, \ldots, n$ e la seconda sia $2, 3, \ldots, n, 1$. Quante scelte sono possibili per la terza riga?

Problema 17J. La prima riga di un quadrato latino di ordine $2n$ sia $1, 2, \ldots, 2n-1, 2n$ e la seconda sia $2, 1, 4, 3, \ldots, 2n, 2n-1$.

(i) Trovare una formula per il numero di scelte possibili per la terza riga.

(ii) Dare un permanente il cui valore sia questo numero.

Note

Sebbene i quadrati latini siano studiati da più di 200 anni, gran parte del materiale di questo capitolo è recente. Il Teorema 17.1 è il più antico ed è dovuto a M. Hall, Jr. (1945).

Il Teorema 17.2 e l'osservazione che lo segue si trovano in H. J. Ryser (1969). Quando quell'articolo fu scritto, la congettura di Van der Waerden era ancora aperta.

Il Teorema 17.3 è nuovo.

Anche il Teorema 17.4 è dovuto a H. J. Ryser (1951).

La cosiddetta congettura di Evans compare come domanda, e non come congettura, in un articolo di T. Evans (1960). Prima che apparisse la dimostrazione di B. Smetaniuk furono pubblicati diversi risultati parziali.

La nostra esposizione della dimostrazione di Galvin della congettura di Dinitz si basa su alcune note inedite di D. Hoffman.

La trattazione più ampia dei quadrati latini si trova nel libro *Latin Squares* di J. Dénes e A. D. Keedwell (1991).

Riferimenti bibliografici

J. Dénes e A. D. Keedwell (1991) *Latin squares. New developments in the theory and applications.*, Annals of Discrete Mathematics **46**, North-Holland.

T. Evans (1960) Embedding incomplete Latin squares, *Amer. Math. Monthly* **67**, 958–961.

F. Galvin (1995) The list chromatic index of a bipartite multigraph, *J. Combin. Theory Ser. B* **63**, 153–158.

M. Hall, Jr. (1945) An existence theorem for Latin squares, *Bull. Amer. Math. Soc.* **51**, 387–388.

H. J. Ryser (1951) A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.* **2**, 550–552.

Orig. 198

H. J. Ryser (1969) Permanents and systems of distinct representatives, in: *Combinatorial Mathematics and its Applications*, University of North Carolina Press.

B. Smetaniuk (1981) A new construction on Latin squares I: A proof of the Evans conjecture, *Ars Combinatoria* **11**, 155–172.

Capitolo 18

Matrici di Hadamard, codici di Reed–Muller

Orig. 199

Hadamard considerò la questione seguente. Sia A una matrice $n \times n$ con elementi reali di valore assoluto al più 1. Quanto può essere grande, in valore assoluto, il determinante di A? Poiché ogni riga di A è un vettore di lunghezza al più $\sqrt{n}$, il determinante non può superare $n^{n/2}$. Il valore assoluto del determinante è infatti il volume n-dimensionale del parallelepipedo generato dai vettori riga nello spazio euclideo a n dimensioni. Può valere l'uguaglianza? In tal caso tutti gli elementi devono essere $+1$ o -1 e inoltre due righe qualsiasi devono essere ortogonali, cioè avere prodotto scalare nullo. Questo conduce alla definizione seguente.

Una *matrice di Hadamard* di ordine n è una matrice H di dimensioni $n \times n$, con elementi $+1$ e -1, tale che

$$HH^{\mathsf{T}} = nI. \tag{18.1}$$

Naturalmente anche due colonne qualsiasi di H sono ortogonali. Questa proprietà non cambia permutando righe o colonne, oppure moltiplicando alcune righe o colonne per -1. Due matrici di Hadamard così ottenute si dicono *equivalenti*. Data una matrice di Hadamard, possiamo trovarne una equivalente la cui prima riga e prima colonna consistano interamente di $+1$. Una tale matrice di Hadamard si dice *normalizzata*. Chiaramente le righe rimanenti, se esistono, hanno tanti $+1$ quanti -1; pertanto, se $n \neq 1$, n deve essere pari. Alcuni piccoli esempi sono

$$(1), \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix},$$

dove nell'ultimo esempio abbiamo indicato soltanto il segno degli elementi.

Orig. 200

Problema 18A. Dimostrare che due matrici di Hadamard qualsiasi di ordine 12 sono equivalenti.

Teorema 18.1. Se H è una matrice di Hadamard di ordine n, allora $n = 1$, $n = 2$ oppure $n \equiv 0 \pmod 4$.

Dimostrazione. Sia $n > 2$. Normalizziamo H. Possiamo permutare le colonne in modo che le prime tre righe diventino

$$\underbrace{\begin{matrix} + & + & \cdots & + & + \\ + & + & \cdots & + & + \\ + & + & \cdots & + & + \end{matrix}}_{a \text{ colonne}} \quad \underbrace{\begin{matrix} + & + & \cdots & + & + \\ + & + & \cdots & + & + \\ - & - & \cdots & - & - \end{matrix}}_{b \text{ colonne}} \quad \underbrace{\begin{matrix} + & + & \cdots & + & + \\ - & - & \cdots & - & - \\ + & + & \cdots & + & + \end{matrix}}_{c \text{ colonne}} \quad \underbrace{\begin{matrix} + & + & \cdots & + & + \\ - & - & \cdots & - & - \\ - & - & \cdots & - & - \end{matrix}}_{d \text{ colonne}}$$

Abbiamo $a+b+c+d = n$ e i tre prodotti scalari fra queste righe danno $a+b-c-d = 0$, $a-b+c-d = 0$ e $a-b-c+d = 0$. Sommando le equazioni troviamo $n = 4a$, il che dimostra il teorema. Analogamente si vede che $4b = 4c = 4d = n$. □

Una delle celebri congetture della teoria dei disegni combinatori afferma che esiste una matrice di Hadamard di ordine n per ogni $n \equiv 0 \pmod 4$. Siamo ancora molto lontani da una dimostrazione. Il più

piccolo n per il quale potrebbe esistere una matrice di Hadamard, ma non se ne conosce alcun esempio, è attualmente 428. Esistono moltissimi metodi di costruzione delle matrici di Hadamard; ne tratteremo alcuni. Definiamo anzitutto una seconda classe di matrici, molto simili a quelle di Hadamard.

Una *matrice di conferenza* C di ordine n è una matrice $n \times n$ con 0 sulla diagonale, $+1$ oppure -1 in tutte le altre posizioni e con la proprietà

$$CC^{\mathsf{T}} = (n-1)I. \tag{18.2}$$

Il nome deriva da un'applicazione ai circuiti per conferenze telefoniche. V. Belevitch (1950) studiò le cosiddette reti ideali non dissipative, costituite da trasformatori ideali, da utilizzare per realizzare una rete per conferenze telefoniche. La teoria condusse a una condizione necessaria per l'esistenza di una tale rete: l'esistenza di una matrice di conferenza di ordine n, dove n è il numero di terminali della rete. Questo spiega il nome di queste matrici.

Orig. 201

Problema 18B. Sia C una matrice di conferenza di ordine $n \neq 1$. Dimostrare che n è pari. Dimostrare che, permutando righe e colonne e moltiplicando alcune righe e colonne per -1, si può trovare una matrice di conferenza equivalente che sia simmetrica se $n \equiv 2 \pmod 4$ e antisimmetrica se $n \equiv 0 \pmod 4$.

Teorema 18.2. Se C è una matrice di conferenza antisimmetrica, allora $I + C$ è una matrice di Hadamard.

Dimostrazione. $(I+C)(I+C)^{\mathsf{T}} = I + C + C^{\mathsf{T}} + CC^{\mathsf{T}} = I + (n-1)I = nI$. □

Teorema 18.3. Se C è una matrice di conferenza simmetrica di ordine n, allora

$$H = \begin{pmatrix} I+C & -I+C \\ -I+C & -I-C \end{pmatrix}$$

è una matrice di Hadamard di ordine $2n$.

Dimostrazione. Basta ancora calcolare HH^{T} per ottenere il risultato. □

Uno dei metodi più comuni per costruire varie strutture combinatorie è il cosiddetto *metodo ricorsivo*: un oggetto grande del tipo desiderato si ottiene applicando un procedimento a due o più oggetti più piccoli dello stesso tipo. Nel prossimo teorema illustriamo un metodo di questo genere per costruire matrici di Hadamard.

Sia A una matrice $m \times n$ con elementi a_{ij} e sia B un'altra matrice. La matrice

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix},$$

costituita da mn blocchi delle stesse dimensioni di B, si chiama *prodotto di Kronecker* $A \otimes B$ delle matrici A e B.

Teorema 18.4. Se H_m e H_n sono matrici di Hadamard di ordine rispettivamente m e n, allora $H_m \otimes H_n$ è una matrice di Hadamard di ordine mn.

Dimostrazione. Un calcolo diretto mostra che

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

e che

$$(A \otimes B)^{\mathsf{T}} = A^{\mathsf{T}} \otimes B^{\mathsf{T}}.$$

Orig. 202

Prendiamo $A = C = H_m$ e $B = D = H_n$. Il risultato segue dalla definizione di matrice di Hadamard e dal fatto che $I_m \otimes I_n = I_{mn}$. □

Applicando ripetutamente questo teorema a $H_2 := \begin{pmatrix} + & + \\ + & - \end{pmatrix}$, troviamo una successione di matrici di Hadamard che indicheremo con H_n, dove $n = 2^m$, $m = 1, 2, \ldots$.

Passiamo ora a un metodo diretto per costruire matrici di conferenza, che potremo poi utilizzare con i Teoremi 18.2 e 18.3 per costruire matrici di Hadamard. Nel seguito, q è una potenza di un primo dispari. Sul campo $\mathbb{F}_q$ definiamo una funzione χ, un cosiddetto *carattere*, mediante

$$\chi(x) := \begin{cases} 0 & \text{se } x = 0, \\ 1 & \text{se } x \text{ è un quadrato non nullo}, \\ -1 & \text{se } x \text{ non è un quadrato}. \end{cases}$$

Per ogni $x, y \in \mathbb{F}_q$ abbiamo $\chi(x)\chi(y) = \chi(xy)$; inoltre, poiché i quadrati non nulli sono tanti quanti i non quadrati,

$$\sum_{x \in \mathbb{F}_q} \chi(x) = 0. \tag{18.3}$$

Sia ora $0 \neq c \in \mathbb{F}_q$. Da (18.3) segue

$$\sum_{b \in \mathbb{F}_q} \chi(b)\chi(b+c) = -1. \tag{18.4}$$

Per vederlo, trascuriamo il termine con $b = 0$, che è nullo, e scriviamo $\chi(b+c) = \chi(b)\chi(1+cb^{-1})$, osservando che $\chi(b)^2 = 1$ se $b \neq 0$. Al variare di b fra tutti gli elementi non nulli del campo, $1 + cb^{-1}$ assume tutti i valori tranne 1.

Numeriamo gli elementi di $\mathbb{F}_q$ come $0 = a_0, a_1, \ldots, a_{q-1}$. Definiamo una matrice Q di dimensioni $q \times q$ mediante

$$q_{ij} := \chi(a_i - a_j), \qquad 0 \leq i, j < q.$$

Si osservi che Q è simmetrica se $q \equiv 1 \pmod 4$ e antisimmetrica se $q \equiv 3 \pmod 4$. Dalle proprietà elementari di χ e da (18.4) segue direttamente che $QQ^{\mathsf{T}} = qI - J$ e $QJ = JQ = O$. Definiamo una matrice C di dimensioni $(q+1) \times (q+1)$ mediante

Orig. 203

$$C := \left(\begin{array}{c|ccc} 0 & 1 & \cdots & 1 \\ \hline \pm 1 & & & \\ \vdots & & Q & \\ \pm 1 & & & \end{array}\right), \tag{18.5}$$

dove i segni dei termini ± 1 sono scelti in modo che C sia simmetrica oppure antisimmetrica. Dalle proprietà di Q segue ora che C è una matrice di conferenza di ordine $q+1$. Questa costruzione è dovuta a Paley (1933) e le matrici di conferenza di questo tipo si chiamano solitamente *matrici di Paley*. Nel caso particolare in cui q è primo, Q è una matrice circolante. Riassumiamo le costruzioni in un teorema.

Teorema 18.5. Se q è una potenza di un primo dispari, esiste una matrice di Hadamard di ordine $q+1$ quando $q \equiv 3 \pmod 4$ e di ordine $2(q+1)$ quando $q \equiv 1 \pmod 4$.

+	+	+	+	+	+	+	+	+	+	+	+
−	+	+	−	+	+	+	−	−	−	+	−
−	−	+	+	−	+	+	+	−	−	−	+
−	+	−	+	+	−	+	+	+	−	−	−
−	−	+	−	+	+	−	+	+	+	−	−
−	−	−	+	−	+	+	−	+	+	+	−
−	−	−	−	+	−	+	+	−	+	+	+
−	+	−	−	−	+	−	+	+	−	+	+
−	+	+	−	−	−	+	−	+	+	−	+
−	+	+	+	−	−	−	+	−	+	+	−
−	−	+	+	+	−	−	−	+	−	+	+
−	+	−	+	+	+	−	−	−	+	−	+

Figura 18.1

Orig. 204

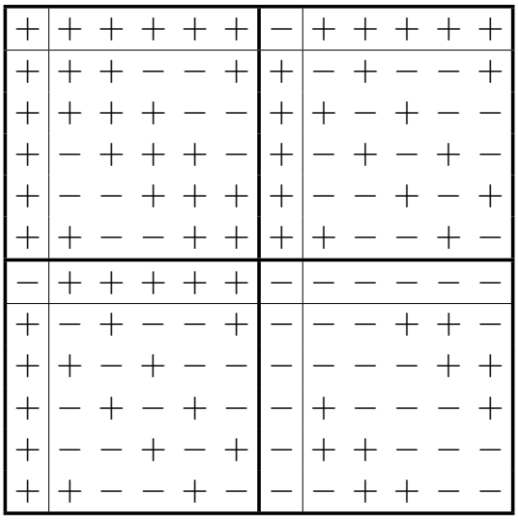


Figura 18.2

Le Figure 18.1 e 18.2 illustrano matrici di Hadamard di ordine 12 costruite a partire da matrici di Paley di ordine rispettivamente $11+1$ e $5+1$.

Problema 18C. Dimostrare che esiste una matrice di Hadamard di ordine n per $n \equiv 0 \pmod 4$, $n \le 100$, con la possibile eccezione di $n = 92$.

Trascorsero trent'anni fra il risultato di Paley e la scoperta di una matrice di Hadamard di ordine 92 da parte di L. D. Baumert, S. W. Golomb e M. Hall. Il metodo utilizzato era stato sviluppato da Williamson nel 1944, ma fu necessaria una ricerca al calcolatore per trovare effettivamente la matrice. Il metodo di Williamson si basa sull'osservazione seguente. Siano A_i, $1 \le i \le 4$, matrici simmetriche di ordine n, con n dispari, e supponiamo che commutino fra loro. Consideriamo la matrice H definita da

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix}. \tag{18.6}$$

Abbiamo allora

$$HH^{\mathsf{T}} = I_4 \otimes (A_1^2 + A_2^2 + A_3^2 + A_4^2). \tag{18.7}$$

Per costruire in questo modo una matrice di Hadamard dobbiamo trovare matrici A_i che soddisfino le condizioni appena indicate, abbiano elementi ± 1 e soddisfino inoltre Orig. 205

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n. \tag{18.8}$$

Sia U la matrice di permutazione di ordine n corrispondente alla permutazione $(12\cdots n)$, cioè $u_{ij} = 1$ se e solo se $j - i \equiv 1 \pmod n$. Allora $U^n = I$ e ogni matrice circolante è una combinazione lineare di potenze di U. Se supponiamo che le matrici A_i abbiano la forma $A_i = \sum_{j=0}^{n-1} a_{ij}U^j$, con $a_{i0} = 1$ e $a_{ij} = a_{i,n-j}$, esse commutano effettivamente fra loro e sono simmetriche. D'ora in poi supponiamo anche che tutti gli a_{ij} siano ± 1 e che valga (18.8). Un semplice esempio di matrice di Hadamard costruita in questo modo si ottiene prendendo $n = 3$, $A_1 = J$ e $A_i = J - 2I$, $i = 2, 3, 4$. Si trova una matrice di Hadamard di ordine 12, riportata nella Figura 18.3.[1]

[1]Nota di traduzione: in questo esempio $J - 2I$ ha diagonale -1, contrariamente alla convenzione $a_{i0} = 1$ appena adottata. La matrice illustrata è comunque una valida matrice di Hadamard; per rispettare anche quella convenzione si possono cambiare i segni dei tre blocchi, prendendo $A_i = 2I - J$.

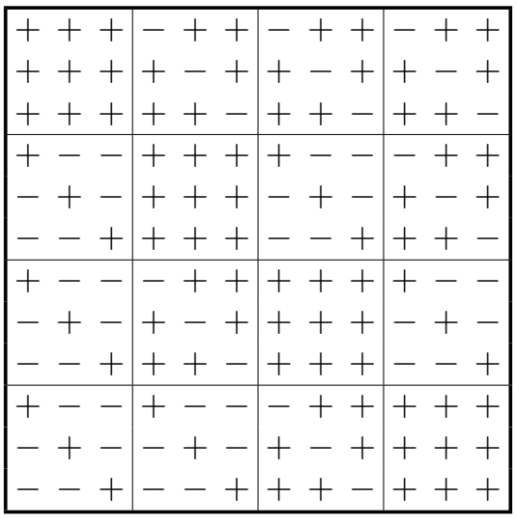


Figura 18.3

Esempio 18.1. La nostra costruzione implica che A_i abbia somma di riga costante a_i, dispari; da (18.8) segue $a_1^2 + \cdots + a_4^2 = 4n$. Se vogliamo usare questo metodo per trovare una matrice di Hadamard di ordine 20, scriviamo anzitutto 20 come somma di quattro quadrati dispari: $20 = 9 + 9 + 1 + 1$. Vediamo così che due delle matrici A_i devono essere $2I - J$; non è poi difficile vedere che le altre due hanno come prima riga rispettivamente $+\ -\ +\ +\ -$ e $+\ +\ -\ -\ +$. Per analizzare ulteriormente la situazione introduciamo le matrici W_i e P_i mediante Orig. 206

$$2W_i := (A_1 + \cdots + A_4) - 2A_i, \tag{18.9}$$

$$A_i = 2P_i - J. \tag{18.10}$$

Le convenzioni sui coefficienti a_{ij} implicano che, definendo p_i mediante $p_i J := P_i J$, p_i sia un intero dispari. Inoltre (18.8) e (18.9) implicano

$$W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4nI. \tag{18.11}$$

Sostituendo (18.10) in (18.8) troviamo

$$\sum_{i=1}^{4} P_i^2 = \left(\sum_{i=1}^{4} p_i - n \right) J + nI. \tag{18.12}$$

Supponiamo che il termine U^k, $k \neq 0$, compaia in α delle matrici P_i. Considerando (18.12) modulo 2, troviamo U^{2k} a sinistra con coefficiente α e a destra con coefficiente 1. Dunque α è dispari; ciò implica che U^k compaia in esattamente una delle matrici W_i, con coefficiente ± 2. Dall'Esempio 18.1 e da (18.9) vediamo che le somme di riga costanti w_i delle matrici W_i soddisfano $w_1^2 + \cdots + w_4^2 = 4n$. Questi fatti riducono le possibilità per le matrici W_i che soddisfano anche (18.11) abbastanza da rendere praticabile una ricerca al calcolatore. Le A_i si ricavano poi da (18.9). Elenchiamo le prime righe delle quattro matrici di ordine 23 che produssero la prima matrice di Hadamard di ordine 92:

$$\begin{aligned}
A_1 &: \quad + + - - - + - - - + - + + - + - - - + - - - + \\
A_2 &: \quad + - + + - + + - - + + + + + + - - + + - + + - \\
A_3 &: \quad + + + - - - + + - + - + + - + - + + - - - + + \\
A_4 &: \quad + + + - + + + - + - - - - - - + - + + + - + +
\end{aligned}$$

Problema 18D. Costruire una matrice di Hadamard di ordine 28 usando il metodo di Williamson.

Consideriamo un altro problema sulle matrici di Hadamard. Se una matrice di Hadamard di ordine n è normalizzata, allora evidentemente ha esattamente n elementi $+1$ in più rispetto agli elementi -1. Orig. 207

Definiamo l'*eccedenza* di una matrice di Hadamard come la somma di tutti i suoi elementi; definiamo poi $\sigma(n)$ come il massimo valore dell'eccedenza fra tutte le matrici di Hadamard di ordine n. La seguente limitazione, dovuta a Best (1977), mostra che $\sigma(n)$ cresce come $n^{3/2}$.

Teorema 18.6. $n^2 2^{-n}\binom{n}{n/2} \le \sigma(n) \le n\sqrt{n}$.

DIMOSTRAZIONE. (a) Sia H una matrice di Hadamard di ordine n. Sia s_k la somma della colonna k di H e sia $\mathbf{c}_i$ la riga i di H, $1 \le i \le n$. Calcoliamo $\sum_{1\le i,j\le n}\langle \mathbf{c}_i, \mathbf{c}_j\rangle$ in due modi. Per la definizione di matrice di Hadamard, la somma vale n^2. D'altra parte,

$$\sum_{1\le i,j\le n}\sum_{k=1}^{n} c_{ik}c_{jk} = \sum_{k=1}^{n} s_k^2.$$

Da questa identità e dalla disuguaglianza di Cauchy–Schwarz segue

$$\sum_{k=1}^{n} s_k \le \left(n\sum_{k=1}^{n} s_k^2\right)^{1/2} = n\sqrt{n},$$

quindi $\sigma(n) \le n\sqrt{n}$.

(b) Sia $\mathbf{x}$ un vettore qualsiasi di $\{+1,-1\}^n$. Moltiplichiamo la colonna j di H per x_j, $1 \le j \le n$. Successivamente moltiplichiamo per -1 le righe che contengono più termini -1 che termini $+1$. Chiamiamo $H_{\mathbf{x}}$ la matrice risultante e definiamo $\sigma(H_{\mathbf{x}}) := \sum_{i=1}^{n} |\langle \mathbf{x}, \mathbf{c}_i\rangle|$. Chiaramente $\sigma(n)$ è almeno il valore medio di $\sigma(H_{\mathbf{x}})$. Troviamo dunque

$$\begin{aligned}
\sigma(n) &\ge 2^{-n}\sum_{\mathbf{x}\in\{+1,-1\}^n} \sigma(H_{\mathbf{x}}) = 2^{-n}\sum_{\mathbf{x}}\sum_{i=1}^{n} |\langle \mathbf{x}, \mathbf{c}_i\rangle| \\
&= 2^{-n}\sum_{i=1}^{n}\sum_{d=0}^{n}\sum_{\mathbf{x}:\, d(\mathbf{x},\mathbf{c}_i)=d} |n-2d| \\
&= 2^{-n} n\sum_{d=0}^{n}\binom{n}{d}|n-2d| = n^2 2^{-n}\binom{n}{n/2}.
\end{aligned}$$

□ Orig. 208

Corollario. $2^{-1/2}n^{3/2} \le \sigma(n) \le n^{3/2}$.

DIMOSTRAZIONE. Dalla formula di Stirling segue che il membro sinistro della disuguaglianza del Teorema 18.6 è asintoticamente equivalente a $2^{1/2}\pi^{-1/2}n^{3/2}$. Per ottenere una disuguaglianza valida per ogni n, dobbiamo sostituire la costante con $2^{-1/2}$. □

Esempio 18.2. Consideriamo un quadrato 4×4, diviso in 16 caselle numerate da 1 a 16. Definiamo una matrice A con righe $\mathbf{a}_i$, $1 \le i \le 16$, ponendo $a_{ij} = -1$ se j si trova nel quadrato nella stessa riga o colonna di i, ma $j \ne i$; negli altri casi poniamo $a_{ij} = 1$. Due righe qualsiasi di A hanno due posizioni nelle quali entrambe hanno elemento -1. Ne segue che A è una matrice di Hadamard di ordine 16 con eccedenza 64: per questa matrice vale cioè l'uguaglianza nella limitazione superiore del Teorema 18.6.

Questa matrice di Hadamard si può costruire anche così. Definiamo $H := J - 2I$, una matrice di Hadamard di ordine 4 con eccedenza massima, pari a 8. Ogni riga di H ha lo stesso numero di termini $+1$, cioè 3. La matrice $H \otimes H$ è una matrice di Hadamard di ordine 16, con 10 termini $+1$ in ogni riga e con eccedenza massima 64. Facendo il prodotto di Kronecker di questa matrice con H, troviamo ancora una matrice di Hadamard con somme di riga costanti ed eccedenza massima, e così via. In generale, una matrice di Hadamard di ordine $4u^2$, con tutte le somme di riga uguali a $2u$ e quindi con eccedenza massima, si chiama *matrice di Hadamard regolare*. Sono note altre costruzioni di tali matrici.

Una delle applicazioni più interessanti e riuscite delle matrici di Hadamard è stato il loro impiego come *codici correttori di errori*. Molti lettori avranno visto le eccellenti immagini di Marte, Saturno e altri pianeti riprese da sonde come Mariner, Voyager e altre. Per trasmettere a Terra un'immagine, la si divide anzitutto in quadratini molto piccoli, i *pixel*; per ciascuno si misura il grado di oscurità, esprimendolo, per esempio, su una scala da 0 a 63. Questi numeri vengono rappresentati nel sistema binario: ogni pixel produce quindi una stringa di sei 0 e 1, detti *bit*. I bit sono trasmessi alla stazione ricevente sulla

Terra, il Jet Propulsion Laboratory del Caltech. A causa di varie sorgenti di rumore, fra cui il rumore termico dell'amplificatore, accade talvolta che un segnale trasmesso come 0, rispettivamente come 1, sia interpretato dal ricevitore come 1, rispettivamente come 0. Se ogni sestupla corrispondente a un pixel fosse trasmessa tal quale, gli errori del ricevitore renderebbero le immagini molto scadenti. Poiché il tempo disponibile per trasmettere le immagini è limitato ed è nota l'energia fornita dai pannelli solari, conosciamo l'energia media disponibile per ogni bit d'informazione da usare nella generazione dei segnali da inviare al ricevitore. Da essa possiamo calcolare la probabilità di errore p per bit. Orig. 209

Supponiamo che, per ottenere un'immagine utilizzabile, ogni sestupla possa essere errata con probabilità P_E al più 10^{-4}. Per ottenere questo risultato trasmettendo semplicemente i bit, occorre $p \approx 10^{-4}/6$, poiché $P_E = 1-(1-p)^6 \approx 10^{-4}$. Supponiamo anzitutto che l'energia necessaria sia disponibile e cerchiamo di migliorare l'immagine nel modo seguente. Invece di inviare un bit, per esempio 0, potremmo inviare cinque 0; il ricevitore traduce poi la quintupla ricevuta nel bit che compare più spesso. Diciamo che usiamo un codice, detto *codice a ripetizione*, con due parole di lunghezza 5, cioè 00000 e 11111. Il numero 1/5 si chiama *tasso d'informazione* di questo codice. Il vincolo di potenza ci permette di calcolare l'energia disponibile per ogni bit di canale. Si può quindi calcolare la nuova probabilità di errore p' per bit di canale. Naturalmente $p' > p$ e, nel nostro esempio, si ha in effetti $p' = 0.035$, quasi 2000 volte il valore senza codifica. La codifica ha senso soltanto se la correzione degli errori compensa più che interamente la perdita di energia per bit.

La probabilità che un pixel trasmesso venga ricevuto correttamente diventa ora

$$[(1-p')^5 + 5p'(1-p')^4 + 10(p')^2(1-p')^3]^6,$$

che vale circa 0.997. In altre parole, abbiamo completamente peggiorato la nostra immagine!

Vediamo ora che cosa fu effettivamente fatto nella missione Mariner del 1969. Le 64 possibili stringhe d'informazione, corrispondenti ai possibili gradi di oscurità di un pixel, furono messe in corrispondenza con le righe delle matrici H_{32} e $-H_{32}$. Poiché ora parole del codice di lunghezza 32 rappresentano parole d'informazione di lunghezza 6, il tasso d'informazione è 6/32, quasi uguale a quello del codice a ripetizione.

Due parole qualsiasi di questo codice differiscono in tutte le 32 posizioni oppure in esattamente 16 posizioni. Ne segue che, se una parola ricevuta contiene al più 7 errori, assomiglia alla parola corretta più che a una qualsiasi delle altre 63 parole. Abbiamo sostituito i simboli 0 e 1 con ± 1. Diciamo che questo codice è un *codice correttore di 7 errori*. La nuova probabilità di errore è ora $p' \approx 0.036$, ancora maggiore. La probabilità che una parola ricevuta venga decodificata erroneamente è ora Orig. 210

$$\sum_{i=8}^{32} \binom{32}{i} (p')^i (1-p')^{32-i},$$

pari a circa $1.4 \cdot 10^{-5}$, un ordine di grandezza migliore di P_E.[2]

In pratica non vi era abbastanza energia per trasmettere buone immagini; l'impiego di questo codice risolse il problema.

Abbiamo visto un esempio di una successione di codici a basso tasso d'informazione, detti *codici di Reed–Muller del primo ordine*. Consideriamo ancora la costruzione delle matrici di Hadamard H_n, con $n = 2^m$. La Figura 18.4 mostra H_8.

Nella matrice H_n sostituiamo ogni $+1$ con 0 e ogni -1 con 1. Numeriamo le righe da 0 a $n-1 = 2^m-1$. Che cosa accade nella costruzione mediante prodotto di Kronecker quando passiamo da m a $m+1$, cioè raddoppiamo l'ordine della matrice? Le nuove righe, interpretate ora come vettori di $\mathbb{F}_2^{2n}$, hanno forma $(\mathbf{c}_i, \mathbf{c}_i)$ per $0 \le i < n$ e forma $(\mathbf{c}_i, \mathbf{c}_i + \mathbf{1})$ per $n \le i < 2n$, dove $\mathbf{1}$ indica il vettore con tutte le componenti uguali a 1.[3]

[2] Nota di traduzione: la somma è esattamente la probabilità di almeno 8 errori di canale; per una decodifica a distanza minima costituisce in generale una maggiorazione della probabilità di errore, perché alcune configurazioni con almeno 8 errori possono ancora essere decodificate correttamente.

[3] Nota di traduzione: nell'ultima espressione l'indice della riga di partenza va letto modulo n, ossia $\mathbf{c}_{i-n}$ quando $n \le i < 2n$.

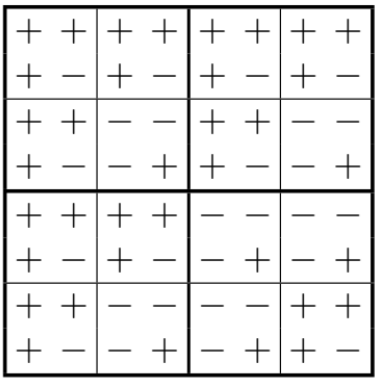


Figura 18.4

Teorema 18.7. Sia $R'(1,m)$ l'insieme dei vettori riga in $\mathbb{F}_2^n$ ottenuti da H_n come descritto sopra. Allora $R'(1,m)$ è un sottospazio di dimensione m di $\mathbb{F}_2^n$. Orig. 211

DIMOSTRAZIONE. Per $m=1$ l'affermazione è banale. Procediamo per induzione. Sia $\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_m$ una base di $R'(1,m)$. L'osservazione precedente mostra che $R'(1,m+1)$ consiste di tutte le combinazioni lineari dei vettori $(\mathbf{v}_i,\mathbf{v}_i)$ e del vettore $(\mathbf{0},\mathbf{1})$. La dimostrazione è così completa. □

Definiamo ora il *codice di Reed–Muller del primo ordine* $R(1,m)$, di lunghezza $n=2^m$ e dimensione $m+1$, come il sottospazio di $\mathbb{F}_2^n$ generato dallo spazio $R'(1,m)$ e dal vettore di lunghezza n con tutte le componenti uguali a 1. In questa terminologia, il codice usato dal Mariner 1969 era $R(1,5)$. Dalle proprietà delle matrici di Hadamard vediamo subito che due parole qualsiasi di $R(1,m)$ differiscono in almeno $n/2$ posizioni. Diciamo che il codice ha *distanza minima* $d=2^{m-1}$. Esso può dunque correggere fino a $2^{m-2}-1$ errori.

Possiamo dare alle parole del codice una bella interpretazione geometrica. Numeriamo i punti dello spazio $\mathbb{F}_2^m$ considerando un vettore come la rappresentazione binaria del suo numero. Per esempio, $(0,1,1,0,1)$ è considerato come il punto P_{22} di $\mathbb{F}_2^5$.[4] Prendiamo queste rappresentazioni come colonne di una matrice $m\times n$ e sia $\mathbf{v}_i$ la riga i di questa matrice, $1\le i\le m$. Dalla Figura 18.4 e dalle osservazioni precedenti vediamo che i vettori $\mathbf{v}_i$ costituiscono la base naturale di $R'(1,m)$. Il vettore di base $\mathbf{v}_i$ è la funzione caratteristica dell'iperpiano $\{(x_1,x_2,\ldots,x_m)\in\mathbb{F}_2^m : x_i=1\}$. Prendendo combinazioni lineari, vediamo che le parole di $R(1,m)$ sono esattamente tutte le funzioni caratteristiche degli iperpiani affini dello spazio vettoriale, insieme con la funzione caratteristica dell'intero spazio, corrispondente a $\mathbf{1}$, e dell'insieme vuoto, corrispondente a $\mathbf{0}$. Due iperpiani affini sono paralleli oppure si intersecano in un sottospazio affine di dimensione $m-2$, in accordo con il fatto che due righe della matrice di Hadamard hanno gli stessi elementi in esattamente metà delle posizioni.

Come suggerisce la notazione $R(1,m)$, nella teoria dei codici correttori di errori si definiscono anche codici di Reed–Muller di ordine superiore. Anche questi hanno un'interpretazione geometrica, che qui non approfondiremo; si veda però l'Esempio 26.4.

Problema 18E. Per $n=2^m$ e $1\le i\le m$ definiamo la matrice $M_n^{(i)}$ mediante Orig. 212

$$M_n^{(i)} := I_{2^{m-i}}\otimes H_2\otimes I_{2^{i-1}}.$$

Dimostrare che

$$H_n = M_n^{(1)}M_n^{(2)}\cdots M_n^{(m)}.$$

Una parola ricevuta $\mathbf{x}$ viene decodificata calcolando $\mathbf{x}H_n^{\mathsf{T}}$. Se gli errori non sono troppi, tutti gli elementi di questo prodotto saranno prossimi a 0 tranne uno, con valore assoluto vicino a n, che ci indica quale fosse il messaggio vero. Una moltiplicazione per ±1 si chiama un'*operazione*. Confrontare il numero di operazioni necessarie alla decodifica usando H_n direttamente e usando la sua rappresentazione come prodotto delle matrici $M_n^{(i)}$. Questo è un esempio della cosiddetta *trasformata veloce di Fourier*.

Problema 18F. Sia $\mathbf{v}_i$, $0\le i\le m$, con $\mathbf{v}_0=\mathbf{1}$, la base di $R(1,m)$ descritta sopra. Consideriamo il sottospazio $R(2,m)$ di $\mathbb{F}_2^n$, con $n=2^m$, generato da tutti i vettori

$$\mathbf{v}_i\cdot\mathbf{v}_j := (v_{i0}v_{j0},\ldots,v_{i,n-1}v_{j,n-1}).$$

[4] Nota di traduzione: la prima coordinata è qui il bit meno significativo; infatti $22=0\cdot2^0+1\cdot2^1+1\cdot2^2+0\cdot2^3+1\cdot2^4$.

Qual è la dimensione di questo spazio? Dimostrare che due vettori distinti di $R(2, m)$ differiscono in almeno $n/4$ posizioni.

Problema 18G. Sia M una matrice $(0, 1)$ di dimensioni $m \times n$, tale che la distanza di Hamming fra due righe distinte sia almeno d. Se M si ottiene sovrapponendo una matrice di Hadamard H a $-H$ e sostituendo i simboli con 0 e 1, si ha un esempio con $m = 2n$ e $d = n/2$.

(1) Contare in due modi le terne ordinate (i, j, k) nelle quali i, j sono gli indici di due righe distinte e k è una colonna in cui $M(i, k) \neq M(j, k)$: un conteggio deve produrre una disuguaglianza che coinvolga d, l'altro le somme delle colonne di M. Dimostrare che, se $2d > n$, allora

$$m \leq \frac{2d}{2d - n}.$$

Questa è nota nella teoria dei codici come *limitazione di Plotkin*. Quali condizioni garantiscono l'uguaglianza? (2) Supporre $d = n/2$. Dimostrare che $m \leq 2n$ e che l'uguaglianza implica l'esistenza di una matrice di Hadamard di ordine n. Orig. 213

Problema 18H. Sia H una matrice di Hadamard di ordine m e sia C una matrice di conferenza simmetrica di ordine n. Sia P la matrice di ordine m della forma $\begin{pmatrix} O & -I \\ I & O \end{pmatrix}$, con blocchi di ordine $m/2$. Dimostrare che $(H \otimes C) + (PH \otimes I)$ è una matrice di Hadamard di ordine mn.

Problema 18I. Sia q una potenza di primo congrua a 1 modulo 4. Sia C la matrice di (18.5). Scegliere H e P come nel Problema 18H. Dimostrare che

$$(H \otimes C \otimes Q) + (PH \otimes C \otimes I_q) + (H \otimes I_{q+1} \otimes J_q)$$

è una matrice di Hadamard di ordine $mq(q + 1)$.

Note

J. Hadamard (1865–1963) fu uno dei principali matematici a cavallo fra il XIX e il XX secolo. I suoi lavori più importanti riguardano la teoria delle funzioni analitiche e la fisica matematica. È noto soprattutto per la dimostrazione del cosiddetto teorema dei numeri primi, insieme a C. J. De La Vallée-Poussin.

R. E. A. C. Paley (1907–1933) morì travolto da una valanga mentre sciava, a 26 anni. Nella sua breve vita produsse 26 articoli di eccellente qualità, principalmente sulla teoria di Fourier.

Una congettura di H. J. Ryser, aperta da molto tempo, afferma che nessuna matrice di Hadamard di ordine $n > 4$ può essere circolante.

J. S. Wallis, nota anche come J. Seberry (1976), dimostrò che, per ogni intero s, esistono matrici di Hadamard di ordine $2^t s$ ogni volta che $t > 2 \log_2(s - 3)$. Non è tuttavia ancora noto se l'insieme degli ordini delle matrici di Hadamard abbia «densità positiva».

Per ulteriori informazioni sui codici correttori di errori si veda il Capitolo 20.

I codici oggi chiamati di Reed–Muller furono effettivamente trattati per la prima volta, forse sorprendentemente, da D. E. Muller (1954) e I. S. Reed (1954).

Per una descrizione dettagliata della codifica e decodifica nelle missioni Mariner si veda E. C. Posner (1968). Orig. 214

Riferimenti bibliografici

L. D. Baumert, S. W. Golomb e M. Hall, Jr. (1962) Discovery of a Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68**, 237–238.

V. Belevitch (1950) Theory of $2n$-terminal networks with applications to conference telephony, *Electrical Communication* **27**, 231–244.

M. R. Best (1977) The excess of a Hadamard matrix, *Proc. Kon. Ned. Akad. v. Wetensch.* **80**, 357–361.

D. E. Muller (1954) Application of Boolean algebra to switching circuit design and to error detection, *IEEE Trans. Computers* **3**, 6–12.

R. E. A. C. Paley (1933) On orthogonal matrices, *J. Math. Phys.* **12**, 311–320.

E. C. Posner (1968) Combinatorial structures in planetary reconnaissance, in: *Error Correcting Codes* (a cura di H. B. Mann), J. Wiley and Sons.

I. S. Reed (1954) A class of multiple-error-correcting codes and the decoding scheme, *IEEE Trans. Information Theory* **4**, 38–49.

J. S. Wallis (1976) On the existence of Hadamard matrices, *J. Combinatorial Theory (A)* **21**, 188–195.

J. Williamson (1944) Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11**, 65–81.

Capitolo 19

Disegni combinatori

In questo capitolo introduciamo un ampio e importante settore della combinatoria, noto come *teoria dei disegni combinatori*. L'oggetto più generale studiato in questa teoria è una cosiddetta *struttura d'incidenza*: una terna $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, dove: Orig. 215

1. $\mathcal{P}$ è un insieme i cui elementi si chiamano *punti*;
2. $\mathcal{B}$ è un insieme i cui elementi si chiamano *blocchi*;
3. $\mathcal{I}$ è una relazione d'incidenza fra $\mathcal{P}$ e $\mathcal{B}$, cioè $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$.

Gli elementi di $\mathcal{I}$ si chiamano *bandiere*.

Se $(p, B) \in \mathcal{I}$, diciamo che il punto p e il blocco B sono *incidenti*. Ammettiamo che due blocchi diversi B_1, B_2 siano incidenti con lo stesso sottoinsieme di punti di $\mathcal{P}$: in questo caso si parla di «blocchi ripetuti». Se ciò non accade, il disegno si dice *semplice* e possiamo considerare i blocchi come sottoinsiemi di $\mathcal{P}$. D'ora in poi lo faremo sempre, avendo cura di ricordare che blocchi diversi possono essere lo stesso sottoinsieme di $\mathcal{P}$. Possiamo così sostituire la notazione $(p, B) \in \mathcal{I}$ con $p \in B$ e diremo spesso che il punto p «appartiene al blocco B», anziché che è incidente con B.

È consuetudine indicare con v la cardinalità di $\mathcal{P}$ e con b quella di $\mathcal{B}$. La struttura d'incidenza consiste dunque di un insieme di v punti e di una famiglia di b sottoinsiemi, non necessariamente distinti, dell'insieme dei punti. La struttura ottenuta sostituendo ogni blocco con il suo complementare si chiama naturalmente *complementare* della struttura: si sostituisce cioè $\mathcal{I}$ con il suo complementare in $\mathcal{P} \times \mathcal{B}$.

Per ottenere una teoria interessante dobbiamo imporre alcune condizioni di regolarità alla struttura $\mathcal{S}$. Come primo esempio menzioniamo le strutture d'incidenza che portano il nome, ambiguo, di «spazi lineari». I blocchi si chiamano solitamente *rette* e le condizioni di regolarità richiedono che ogni retta contenga almeno due punti e che due punti qualsiasi appartengano a esattamente una retta. L'Esempio 19.6 presenta uno spazio lineare semplice ma importante. Il teorema seguente è dovuto a De Bruijn ed Erdős (1948); l'elegante dimostrazione è di Conway. Orig. 216

Teorema 19.1. Per uno spazio lineare si ha $b = 1$ oppure $b \geq v$; in caso di uguaglianza, due rette qualsiasi hanno esattamente un punto incidente con entrambe.

Dimostrazione. Per $x \in \mathcal{P}$, indichiamo con r_x il numero di rette incidenti con x; analogamente, per $B \in \mathcal{B}$, sia k_B il numero di punti di B. Supponiamo che vi sia più di una retta. Se $x \notin L$, allora $r_x \geq k_L$, perché esistono k_L rette che «congiungono» x ai punti di L. Supponiamo $b \leq v$. Allora $b(v - k_L) \geq v(b - r_x)$ e quindi

$$1 = \sum_{x \in \mathcal{P}} \sum_{L \not\ni x} \frac{1}{v(b - r_x)} \geq \sum_{L \in \mathcal{B}} \sum_{x \notin L} \frac{1}{b(v - k_L)} = 1.$$

In tutte le disuguaglianze deve dunque valere l'uguaglianza. Pertanto $v = b$ e $r_x = k_L$ se $x \notin L$. □

Un esempio banale di uguaglianza nel Teorema 19.1 è il cosiddetto *quasi-fascio*: una struttura con una retta contenente tutti i punti tranne uno e, come rette di due punti, tutte le coppie che contengono quel punto. Esempi molto più interessanti sono i piani proiettivi che definiremo più avanti. Queste sono le sole possibilità; si veda il Problema 23C. Il lettore può dimostrarlo per gli spazi lineari come esercizio.

Nel resto del capitolo ci interesseremo a strutture d'incidenza fortemente regolari, dette «t-disegni». Siano v, k, t, λ interi con $v \geq k \geq t \geq 0$ e $\lambda \geq 1$. Un *t-disegno su v punti con blocchi di cardinalità k e indice λ* è una struttura d'incidenza $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ tale che:

(i) $|\mathcal{P}| = v$;

(ii) $|B| = k$ per ogni $B \in \mathcal{B}$;

(iii) per ogni insieme T di t punti esistono esattamente λ blocchi incidenti con tutti i punti di T.

Tutti i blocchi hanno dunque la stessa cardinalità e ogni t-sottoinsieme dell'insieme dei punti è contenuto nello stesso numero di blocchi. Per un tale disegno sono largamente usate due notazioni: t-(v, k, λ) e $S_\lambda(t, k, v)$. Le useremo entrambe. Un *sistema di Steiner* $S(t, k, v)$ è un t-disegno con $\lambda = 1$; nella notazione si omette l'indice. Gran parte della teoria iniziale dei disegni ebbe origine nella statistica, dove i 2-disegni sono utilizzati nella progettazione degli esperimenti per l'analisi statistica. Questi disegni si chiamano spesso *disegni a blocchi incompleti bilanciati* (BIBD). Dalla teoria si escludono solitamente i disegni banali: un disegno con un solo blocco contenente tutti i punti, oppure con tutti i k-sottoinsiemi dell'insieme dei punti come blocchi, è certamente un t-disegno per $t \leq k$, ma non è molto interessante. Orig. 217

Diamo alcuni esempi; altri seguiranno.

Esempio 19.1. Prendiamo come punti i vettori non nulli di $\mathbb{F}_2^4$ e come blocchi tutte le terne $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ con $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. Ogni coppia $\mathbf{x}, \mathbf{y}$, con $\mathbf{x} \neq \mathbf{y}$, determina univocamente un terzo elemento $\mathbf{z}$, diverso da entrambi, che soddisfa questa equazione. Abbiamo dunque costruito un $S(2, 3, 15)$. I blocchi sono i sottospazi bidimensionali di $\mathbb{F}_2^4$ privati di $\mathbf{0}$.

Costruiamo un secondo disegno prendendo tutti i vettori come punti e definendo come blocchi le quadruple $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}\}$ per le quali $\mathbf{w} + \mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. Si ottiene un $S(3, 4, 16)$. Se prendiamo i blocchi contenenti $\mathbf{0}$ ed eliminiamo questo vettore, troviamo i blocchi del disegno precedente.

Esempio 19.2. Prendiamo come punti i dieci spigoli di un K_5. Ogni insieme di quattro spigoli di uno dei tre tipi mostrati nella Figura 19.1 sarà un blocco.

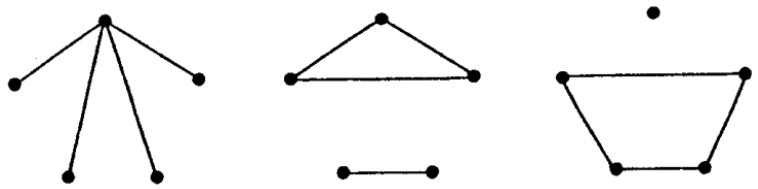


Figura 19.1

Vi sono $5 + 10 + 15 = 30$ blocchi. Nessuna terna di spigoli è contenuta in più di un blocco. I blocchi contengono dunque 120 terne distinte, ossia tutte le terne. Abbiamo costruito un $S(3, 4, 10)$. Orig. 218

Esempio 19.3. Sia H una matrice di Hadamard normalizzata di ordine $4k$. Eliminiamo la prima riga e la prima colonna e identifichiamo i punti con le righe della matrice risultante. Ogni colonna definisce un sottoinsieme delle righe: quelle che hanno un $+$ in quella colonna. Questi sottoinsiemi sono i blocchi. Dal ragionamento del Teorema 18.1 vediamo che ogni coppia di punti è contenuta in esattamente $k-1$ blocchi; chiaramente tutti i blocchi hanno cardinalità $2k-1$. Otteniamo un disegno 2-$(4k-1, 2k-1, k-1)$, detto *2-disegno di Hadamard*.

Consideriamo la stessa matrice H, eliminando ora soltanto la prima riga. Ciascuna delle altre righe determina due $2k$-sottoinsiemi dell'insieme delle colonne. Questa partizione non cambia se cambiamo il segno della riga. Il ragionamento del Teorema 18.1 mostra ora che, per tre colonne qualsiasi, esistono esattamente $k - 1$ di questi sottoinsiemi che contengono tutti e tre gli elementi corrispondenti. Questi $2k$-insiemi sono dunque i blocchi di un disegno 3-$(4k, 2k, k - 1)$, detto *3-disegno di Hadamard*.

Esempio 19.4. Consideriamo una matrice di Hadamard regolare di ordine $4u^2$ (Esempio 18.2). Sostituendo $+$ con 1 e $-$ con 0 otteniamo una matrice $(0, 1)$ con $2u^2 + u$ uni in ogni riga e colonna; inoltre due righe, o due colonne, hanno prodotto scalare $u^2 + u$. Interpretiamo le colonne come funzioni caratteristiche dei blocchi di un disegno su $4u^2$ punti. Le proprietà della matrice mostrano che si tratta di un disegno 2-$(4u^2, 2u^2 + u, u^2 + u)$. Solitamente si preferisce considerarne il complementare, cioè un disegno 2-$(4u^2, 2u^2 - u, u^2 - u)$.

Problema 19A. Ecco altri due esempi nello spirito dell'Esempio 19.2.

(i) Prendere come punti di una struttura d'incidenza gli spigoli di K_6. I blocchi sono tutti gli insiemi di tre spigoli che formano un accoppiamento perfetto oppure un triangolo. Dimostrare che si ottiene un $S(2,3,15)$ e che esso è isomorfo al disegno dell'Esempio 19.1.

(ii) Prendere come punti gli spigoli di K_7. I blocchi sono tutti gli insiemi di cinque spigoli dei tre tipi seguenti: (a) stelle con cinque spigoli incidenti con uno stesso vertice; (b) insiemi degli spigoli di sottografi pentagonali; (c) cinque spigoli che formano un triangolo e due spigoli disgiunti. Dimostrare che si ottiene un $S_3(3,5,21)$.

Diamo ora due teoremi elementari sui t-disegni.

Orig. 219

Teorema 19.2. Il numero dei blocchi di un $S_\lambda(t,k,v)$ è

$$b = \lambda\binom{v}{t}\Big/\binom{k}{t}. \tag{19.1}$$

Dimostrazione. Contiamo in due modi le coppie (T,B), dove T è un t-sottoinsieme di $\mathcal{P}$ e B è un blocco incidente con tutti i punti di T. Troviamo $\lambda\binom{v}{t} = b\binom{k}{t}$. □

Teorema 19.3. Dato i, $0 \le i \le t$, il numero di blocchi incidenti con tutti i punti di un i-sottoinsieme I di $\mathcal{P}$ è

$$b_i = \lambda\binom{v-i}{t-i}\Big/\binom{k-i}{t-i}. \tag{19.2}$$

In altre parole, ogni $S_\lambda(t,k,v)$ è anche un i-disegno per $i \le t$.

Dimostrazione. Contiamo in due modi le coppie (T,B), dove T è un t-sottoinsieme di $\mathcal{P}$ contenente I e B è un blocco incidente con tutti i punti di T. □

Corollario. Se $\mathcal{D}$ è un t-disegno con insieme dei punti $\mathcal{P}$ e insieme dei blocchi $\mathcal{B}$, e $I \subseteq \mathcal{P}$ ha cardinalità $i \le t$, allora l'insieme dei punti $\mathcal{P}\setminus I$ e i blocchi $\{B\setminus I : I \subseteq B\}$ formano un $S_\lambda(t-i,k-i,v-i)$. Questo si chiama *disegno derivato* $\mathcal{D}_I$.

Nell'Esempio 19.1 abbiamo già incontrato un disegno derivato: prendendo $I = \{\mathbf{0}\}$, il derivato di $S(3,4,16)$ è $S(2,3,15)$.

Problema 19B. Dimostrare che, se esiste un $S(3,6,v)$, allora $v \equiv 2$ oppure $6 \pmod{20}$.

Il numero dei blocchi incidenti con un punto, cioè b_1, viene solitamente indicato con r e si chiama *numero di replicazione*. Due casi particolari del Teorema 19.3 danno le relazioni seguenti fra i parametri di un 2-disegno:

$$bk = vr, \tag{19.3}$$

$$\lambda(v-1) = r(k-1). \tag{19.4}$$

Orig. 220

Teorema 19.4. Sia $0 \le j \le t$. Il numero di blocchi di un $S_\lambda(t,k,v)$ che non sono incidenti con nessun punto di un j-sottoinsieme J di $\mathcal{P}$ è

$$b^j = \lambda\binom{v-j}{k}\Big/\binom{v-t}{k-t}. \tag{19.5}$$

Dimostrazione. Per $x \in \mathcal{P}$, sia $\mathcal{B}_x$ l'insieme dei blocchi incidenti con x. Usiamo il principio di inclusione-esclusione, Teorema 10.1, ottenendo

$$b^j = \sum_{i=0}^{j}(-1)^i\binom{j}{i}b_i.$$

Il risultato segue sostituendo (19.2) e usando poi (10.5). È più rapido osservare che b^j non dipende dall'insieme particolare J e contare in due modi le coppie (J,B), dove J è un j-sottoinsieme di $\mathcal{P}$ e $J \cap B = \varnothing$. Si ha $\binom{v}{j}b^j = b\binom{v-k}{j}$; il risultato segue allora dal Teorema 19.2. □

Corollario. Se $i+j \le t$, il numero dei blocchi di un $S_\lambda(t,k,v)$ incidenti con tutti i punti di un insieme di i punti e con nessuno dei punti di un insieme disgiunto di j punti è la costante

$$b_i^j = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}. \tag{19.6}$$

DIMOSTRAZIONE. Basta applicare il Teorema 19.4 al $(t-i)$-disegno $\mathcal{D}_I$, dove I è l'insieme degli i punti. □

Corollario. Se J è un j-sottoinsieme di $\mathcal{P}$, con $j \le t$, l'insieme dei punti $\mathcal{P} \setminus J$ e i blocchi B con $B \cap J = \varnothing$ formano un $S_\mu(t-j,k,v-j)$, detto *disegno residuo* $\mathcal{D}^J$.

Problema 19C. (i) Dimostrare che un $S_\lambda(t,k,v)$ con $v \le k+t$ è banale.

(ii) Dimostrare che il complementare di un $S_\lambda(t,k,v)$ con $v \ge k+t$ è un t-disegno e determinarne i parametri.

Esempio 19.5. Consideriamo un 3-disegno di Hadamard 3-$(4k, 2k, k-1)$ e formiamo il residuo rispetto a un insieme di un solo punto. Troviamo un 2-disegno di Hadamard 2-$(4k-1, 2k, k)$, cioè il complementare del disegno dell'Esempio 19.3. Orig. 221

Una condizione necessaria evidente per l'esistenza di un $S_\lambda(t,k,v)$ è che i numeri b_i di (19.2) siano interi. Essa non è però sufficiente. Un $S(10,16,72)$ non esiste, come mostra il teorema seguente, dovuto a Tits (1964).

Teorema 19.5. In ogni sistema di Steiner non banale $S(t,k,v)$ si ha

$$v \ge (t+1)(k-t+1).$$

DIMOSTRAZIONE. In un sistema di Steiner, due blocchi distinti hanno al più $t-1$ punti in comune. Scegliamo un insieme S di $t+1$ punti non contenuto in alcun blocco. Per ogni insieme $T \subseteq S$ con $|T| = t$, esiste un unico blocco B_T contenente T. Ogni B_T è incidente con $k-t$ punti esterni a S; un punto esterno a S è incidente con al più uno di questi blocchi, perché due di essi hanno già $t-1$ punti di S in comune. L'unione di tutti i blocchi B_T contiene quindi $(t+1)+(t+1)(k-t)$ punti, da cui segue il risultato. □

Data una struttura d'incidenza con $|\mathcal{P}| = v$ e $|\mathcal{B}| = b$, la sua *matrice d'incidenza* N è la matrice $v \times b$ con righe indicizzate dai punti $p \in \mathcal{P}$, colonne indicizzate dai blocchi $B \in \mathcal{B}$ ed elemento $N(p,B) = 1$ se p è incidente con B, e $N(p,B) = 0$ altrimenti. L'elemento di NN^{T} nella riga p e nella colonna q è la somma di $N(p,B)N(q,B)$ su tutti i blocchi B, cioè il numero di blocchi contenenti sia p sia q. Dualmente, l'elemento di $N^{\mathsf{T}}N$ nella riga A e nella colonna B è la cardinalità di $A \cap B$.

Due disegni $\mathcal{D}, \mathcal{D}'$ con matrici d'incidenza N, N' si dicono *isomorfi* o *equivalenti* se esistono matrici di permutazione P, Q tali che $N' = PNQ$.

Identificheremo spesso N con il disegno, chiamando cioè le colonne «blocchi» anziché funzioni caratteristiche dei blocchi.

Se N è la matrice d'incidenza di un 2-disegno, allora NN^{T} ha r in tutte le posizioni diagonali e λ in tutte le altre, cioè

$$NN^{\mathsf{T}} = (r-\lambda)I + \lambda J, \tag{19.7}$$

dove I, J sono matrici $v \times v$. Orig. 222

Problema 19D. Sia N una matrice $(0,1)$ di dimensioni 11×11 con le proprietà seguenti: (i) ogni riga contiene sei uni; (ii) il prodotto scalare di due righe distinte è al più 3. Dimostrare che N è la matrice d'incidenza di un disegno 2-$(11,6,3)$. Dimostrare inoltre che questo disegno è unico a meno di isomorfismi.

Il teorema seguente è noto come *disuguaglianza di Fisher*.

Teorema 19.6. Per un disegno 2-(v,k,λ) con b blocchi e $v > k$ si ha $b \ge v$.

DIMOSTRAZIONE. Poiché $v > k$, da (19.4) segue $r > \lambda$. La matrice J ha un autovalore v e tutti gli altri nulli; pertanto la matrice a destra di (19.7) ha $v-1$ autovalori $r-\lambda$ e un autovalore $(r-\lambda)+\lambda v = rk$. Il suo determinante è quindi $rk(r-\lambda)^{v-1} \ne 0$ e N ha rango v. Ne segue $b \ge v$. □

Dal ragionamento precedente ricaviamo una conclusione molto importante.

Teorema 19.7. Se un disegno 2-(v,k,λ) ha $b = v$ blocchi e v è pari, allora $k-\lambda$ deve essere un quadrato.

DIMOSTRAZIONE. Da $b = v$ segue $r = k$. La matrice N è ora quadrata di ordine v e, per (19.7),

$$(\det N)^2 = k^2(k-\lambda)^{v-1}.$$

Poiché $\det N$ è intero, la dimostrazione è conclusa. □

Il Teorema 19.6 fu generalizzato da A. Ya. Petrenjuk (1968) nella forma $b \geq \binom{v}{2}$ per ogni $S_\lambda(4,k,v)$ con $v \geq k+2$, e infine esteso a t-disegni arbitrari da Ray-Chaudhuri e Wilson (1975).

Teorema 19.8. Per un $S_\lambda(t,k,v)$ con $t \geq 2s$ e $v \geq k+s$ si ha $b \geq \binom{v}{s}$.

DIMOSTRAZIONE. Introduciamo le matrici d'incidenza superiori del t-disegno $\mathcal{D} = S_\lambda(t,k,v)$. Per $i = 0,1,2,\ldots$, sia N_i la matrice $\binom{v}{i} \times b$ con righe indicizzate dagli i-sottoinsiemi dei punti, colonne indicizzate dai blocchi, ed elemento 1 nella riga Y e nella colonna B se $Y \subseteq B$, 0 altrimenti. Per $0 \leq i \leq j \leq v$, indichiamo con W_{ij} la matrice d'incidenza di ordine i della struttura d'incidenza i cui blocchi sono tutti i j-sottoinsiemi di un v-insieme. Dunque W_{ij} è una matrice $\binom{v}{i} \times \binom{v}{j}$. Orig. 223

Affermiamo che

$$N_s N_s^{\mathsf{T}} = \sum_{i=0}^{s} b_{2s-i}^{i} W_{is}^{\mathsf{T}} W_{is}.$$

Per verificarlo, osserviamo che $N_s N_s^{\mathsf{T}}$ ha righe indicizzate dagli s-sottoinsiemi E e colonne indicizzate dagli s-sottoinsiemi F dei punti. Per E,F fissati, il suo elemento (E,F) è il numero di blocchi che contengono sia E sia F, cioè $b_{2s-\mu}$, dove $\mu := |E \cap F|$. L'elemento (E,F) di $W_{is}^{\mathsf{T}} W_{is}$ è il numero di i-sottoinsiemi contenuti sia in E sia in F, ossia $\binom{\mu}{i}$. Pertanto l'elemento (E,F) del membro destro è $\sum_{i=0}^{s} b_{2s-i}^{i}\binom{\mu}{i}$, che per (19.6) è uguale a $b_{2s-\mu}$.[1]

Le matrici $b_{2s-i}^{i} W_{is}^{\mathsf{T}} W_{is}$, di ordine $\binom{v}{s}$, sono tutte semidefinite positive; inoltre $b_s^s W_{ss}^{\mathsf{T}} W_{ss} = b_s^s I$ è definita positiva, perché $b_s^s > 0$ quando $v \geq k+s$. Dunque $N_s N_s^{\mathsf{T}}$ è definita positiva e quindi non singolare. Il rango di $N_s N_s^{\mathsf{T}}$ è uguale a quello di N_s; pertanto N_s ha rango $\binom{v}{s}$, che non può superare il numero b delle sue colonne. □

Se nella disuguaglianza di Wilson–Petrenjuk, Teorema 19.8, vale l'uguaglianza, il $2s$-disegno si dice *stretto*. Gli unici esempi noti con $s > 1$ e $v > k+s$ sono l'unico sistema di Steiner $S(4,7,23)$, che tratteremo nel prossimo capitolo, e il suo complementare.

È utile dare un'idea della storia dei t-disegni. Si conoscono soltanto un numero finito di sistemi di Steiner $S(t,k,v)$ con $t \geq 4$. I più famosi sono i disegni $S(5,8,24)$ e $S(5,6,12)$ trovati da E. Witt (1938), insieme con i 4-disegni derivati; li incontreremo nel prossimo capitolo. R. H. F. Denniston (1976) costruì $S(5,6,24)$, $S(5,7,28)$, $S(5,6,48)$ e $S(5,6,84)$. W. H. Mills (1978) costruì un $S(5,6,72)$. Anche i derivati sono sistemi di Steiner. M. J. Granell e T. S. Griggs (1994) costruirono un $S(5,6,108)$; da allora non ne sono stati trovati altri. Nel 1972 W. O. Alltop costruì la prima successione infinita di 5-disegni senza blocchi ripetuti. È facile mostrare che esistono t-disegni con blocchi ripetuti per ogni t, ma per lungo tempo molti studiosi credettero che non esistessero t-disegni non banali senza blocchi ripetuti per $t > 6$. Il primo 6-disegno semplice fu trovato da D. W. Leavitt e S. S. Magliveras nel 1982; nel 1986 D. L. Kreher e S. P. Radziszowski trovarono il più piccolo 6-disegno semplice possibile, un $S_4(6,7,14)$. Un risultato sensazionale fu l'articolo di L. Teirlinck (1987), che dimostrava l'esistenza di t-disegni semplici non banali per ogni t. La sua costruzione produce disegni con parametri enormi; la costruzione di esempi piccoli rimane quindi un problema aperto. Per vari insiemi particolari di parametri è stata dimostrata la non esistenza dei disegni corrispondenti. Orig. 224

Nel resto del capitolo ci interesseremo soprattutto ai 2-disegni. Quando $t = 2$, omettiamo spesso questo parametro nella notazione «t-(v,k,λ)» e parliamo di disegni (v,k,λ).

Una classe particolarmente interessante è quella dei 2-disegni con $b = v$. In questo caso la matrice d'incidenza N è quadrata e questi disegni dovrebbero chiamarsi *disegni quadrati*. La terminologia standard è però il nome fuorviante di *disegni simmetrici*: si osservi che N non è necessariamente simmetrica. Per un disegno simmetrico 2-(v,k,λ), (19.4) diventa

$$\lambda(v-1) = k(k-1).$$

[1] Nota di traduzione: nell'ultima sommatoria l'originale stampa $i = 1$, ma il termine $i = 0$ è necessario, come nell'identità enunciata immediatamente sopra.

Alcuni autori usano il nome *disegno proiettivo*, derivante dal fatto che un disegno 2-$(v, k, 1)$ con $b = v$ si chiama *piano proiettivo* (Esempio 19.7). Pur non essendo soddisfatti del nome, useremo la terminologia «disegni simmetrici».

Problema 19E. Sia $\mathcal{D}$ un disegno 2-(v, k, λ) con b blocchi e r blocchi per ogni punto. Sia B un blocco qualsiasi. Dimostrare che il numero di blocchi che incontrano B è almeno

$$\frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}.$$

Dimostrare che vale l'uguaglianza se e solo se ogni blocco non disgiunto da B lo incontra in un numero costante di punti.[2]

Esempio 19.6. Prendiamo come punti gli elementi di $\mathbb{Z}_7$ e come blocchi tutte le terne $B_x := \{x, x+1, x+3\}$, con $x \in \mathbb{Z}_7$. È facile verificare che si ottiene un $S(2, 3, 7)$. Si usa spesso la rappresentazione della Figura 19.2. Le rette rappresentano blocchi, ma un blocco deve essere rappresentato dalla circonferenza. Orig. 225

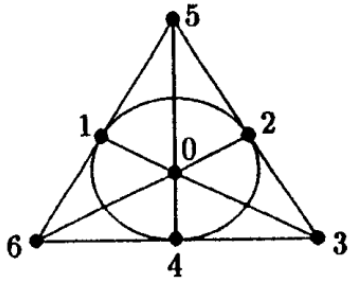


Figura 19.2

Questo disegno è noto come *piano di Fano*. L'idea della costruzione sarà sviluppata nel Capitolo 27. Essa si basa sul fatto che le sei differenze fra gli elementi di $\{0, 1, 3\}$ sono esattamente tutti gli elementi non nulli di $\mathbb{Z}_7$. Se vogliamo trovare, per esempio, il blocco contenente $\{1, 6\}$, osserviamo che $6 - 1 = 1 - 3$; prendiamo quindi $x = 5$ e troviamo $x + 1 = 6$, $x + 3 = 1$: la coppia appartiene effettivamente a B_5. Il lettore non dovrebbe avere difficoltà a trovare allo stesso modo un $S(2, 4, 13)$ usando $\mathbb{Z}_{13}$.

Un disegno simmetrico con $\lambda = 1$ si chiama *piano proiettivo*. Se k è la cardinalità dei blocchi, $n = k-1$ si chiama *ordine* del piano; la ragione di questa scelta sarà chiara nell'Esempio 19.7. In funzione di n, i parametri di un piano proiettivo di ordine n sono

$$v = n^2 + n + 1, \qquad k = n + 1, \qquad \lambda = 1.$$

I blocchi si chiamano solitamente rette. Il piano di Fano è l'unico piano proiettivo di ordine 2.

Esempio 19.7. Consideriamo lo spazio vettoriale $\mathbb{F}_q^3$. Esso contiene $(q^3 - 1)/(q - 1) = q^2 + q + 1$ sottospazi unidimensionali e altrettanti sottospazi bidimensionali. Costruiamo una struttura d'incidenza $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ prendendo queste due classi di sottospazi come $\mathcal{P}$ e $\mathcal{B}$. Un sottospazio unidimensionale e uno bidimensionale si dicono incidenti se il primo è contenuto nel secondo. È immediato che abbiamo così definito un piano proiettivo di ordine q, cioè un disegno 2-$(q^2 + q + 1, q + 1, 1)$. Questo disegno si indica solitamente con $PG(2, q)$ oppure $PG_2(q)$, abbreviazione di *geometria proiettiva di dimensione 2 e ordine* q. Orig. 226

La costruzione precedente si può applicare anche sostituendo $\mathbb{F}_q$ con $\mathbb{R}$. Si ottiene allora il piano proiettivo reale classico, in cui i punti sono i sottospazi unidimensionali e le rette quelli bidimensionali. Questa geometria differisce dalla geometria affine classica per il fatto che non vi sono rette parallele. Parlando dei disegni appena definiti, usiamo la terminologia geometrica.

Problema 19F. Trovare un sottoinsieme $S = \{s_1, \ldots, s_5\}$ di $\mathbb{Z}_{21}$ tale che gli elementi di $\mathbb{Z}_{21}$ come punti e i 21 blocchi $S + x$, $x \in \mathbb{Z}_{21}$, formino un piano proiettivo di ordine 4. Suggerimento: esiste una soluzione S per la quale $2S = S$.

Problema 19G. Sia $(R, C, S; L)$ un quadrato latino di ordine 6. Definire $\mathcal{P} := R \times C$. Sia $\mathcal{B}$ l'insieme dei blocchi

$$B_{ij} := \{(x, y) \in R \times C : x = i \text{ oppure } y = j \text{ oppure } L(x, y) = L(i, j)\} \setminus \{(i, j)\},$$

[2]Nota di traduzione: nel conteggio e nella condizione di uguaglianza si devono considerare i blocchi diversi da B stesso.

per $(i, j) \in R \times C$.

(1) Dimostrare che si ottiene un disegno 2-$(36, 15, 6)$.

(2) Dimostrare che esiste una matrice di Hadamard regolare di ordine 36.

Problema 19H. Sia $\mathcal{D}$ un disegno 3-(v, k, λ). Supporre che il derivato di $\mathcal{D}$ rispetto a un punto p, cioè il caso $i = 1$ del corollario al Teorema 19.3, sia un disegno simmetrico.

(1) Dimostrare che $\lambda(v-2) = (k-1)(k-2)$.

(2) Dimostrare che due blocchi qualsiasi di $\mathcal{D}$ si incontrano in 0 oppure $\lambda + 1$ punti.

(3) Dimostrare che l'insieme dei punti esterni a un blocco B, insieme con i blocchi disgiunti da B, forma un 2-disegno $\mathcal{D}^B$.

(4) Applicare la disuguaglianza di Fisher a $\mathcal{D}^B$ e dedurre che $v = 2k$, oppure $k = (\lambda+1)(\lambda+2)$, oppure $k = 2(\lambda+1)(\lambda+2)$. Quali sono le possibilità per il disegno $\mathcal{D}$? Conosciamo disegni con queste proprietà?

Problema 19I. Sia O un sottoinsieme dei punti di un piano proiettivo di ordine n tale che nessuna retta contenga tre punti di O. Dimostrare che $|O| \le n+1$ se n è dispari e $|O| \le n+2$ se n è pari. Un insieme di $n+1$ punti, a tre a tre non allineati, si chiama *ovale*; un insieme di $n+2$ punti, a tre a tre non allineati, si chiama *iperovale*. Nell'Esempio 19.7 e nel Problema 19F sono state date due costruzioni di $PG_2(4)$: costruire un'iperovale in ciascun caso. Orig. 227

Problema 19J. Sia O un'iperovale, con $q+2$ punti, in $PG_2(q)$, $q = 2^m$. Per ciascuno dei $q^2 - 1$ punti $p \notin O$ passano esattamente $(q+2)/2$ secanti di O. Prendere cinque punti di O e ripartirli in

$$\{\{p_1, p_2\}, \{p_3, p_4\}, \{p_5\}\}.$$

Ciò si può fare in 15 modi. Le due coppie determinano due secanti che si incontrano in un punto $p \notin O$. La retta per p e p_5 incontra nuovamente O in un punto che chiamiamo p_6. Si definiscono così 15 sestuple, non necessariamente distinte, di punti di O contenenti i cinque punti dati. Si ottiene un $S_\lambda(5, 6, q+2)$, secondo una costruzione dovuta a D. Jungnickel e S. A. Vanstone (1987). Dimostrare che i punti di «coordinate», nel senso dell'Esempio 19.7, $(1, t, t^2)$, $t \in \mathbb{F}_q$, insieme con $(0, 1, 0)$ e $(0, 0, 1)$, formano un'iperovale O in $PG_2(q)$. Dimostrare che una scelta opportuna di $p_1, \dots, p_5$ su O produce, con la costruzione appena descritta, blocchi ripetuti: il 5-disegno non è quindi semplice.

Ogni disegno 2-$(n^2, n, 1)$ si chiama *piano affine*. I punti e le rette del piano, ossia dello spazio vettoriale bidimensionale, $\mathbb{F}_q^2$ formano un piano affine di ordine q. Per un tale disegno usiamo la notazione $AG_2(n)$, *geometria affine bidimensionale di ordine n*.

Esempio 19.8. Sia $\mathcal{D}$ un piano proiettivo di ordine n. Eliminando una retta e tutti i suoi punti si ottiene un piano affine di ordine n.

Problema 19K. Sia $\mathcal{D}$ un piano affine qualsiasi di ordine n. Per due blocchi B_1, B_2, scriviamo $B_1 \sim B_2$ se i blocchi coincidono oppure non hanno punti in comune. Dimostrare che $\sim$ è una relazione d'equivalenza. Una sua classe si chiama *classe di parallelismo*. Dimostrare che esiste un piano proiettivo di ordine n dal quale $\mathcal{D}$ si ottiene mediante la costruzione dell'Esempio 19.8. Mostreremo ora che, se N è la matrice d'incidenza di un disegno simmetrico $\mathcal{D}$, allora anche N^{T} è la matrice d'incidenza di un disegno simmetrico $\mathcal{D}^{\mathsf{T}}$, detto *duale* di $\mathcal{D}$. Orig. 228

Teorema 19.9. Sia N la matrice d'incidenza di un disegno simmetrico 2-(v, k, λ). Allora anche N^{T} è la matrice d'incidenza di un disegno.

Dimostrazione. Consideriamo un blocco B qualsiasi. Per $0 \le i \le k$, sia a_i il numero di blocchi diversi da B che hanno i punti in comune con B. Contando i blocchi, le coppie (p, B') con $p \in B \cap B'$ e le terne (p, q, B') con $p \ne q$ e $\{p, q\} \subseteq B \cap B'$, troviamo

$$\sum_{i=0}^{k} a_i = v - 1, \qquad \sum_{i=0}^{k} i a_i = k(k-1), \qquad \sum_{i=0}^{k} \binom{i}{2} a_i = \binom{k}{2}(\lambda - 1).$$

Ne ricaviamo $\sum_{i=0}^{k} (i-\lambda)^2 a_i = 0$. Pertanto ogni blocco $B' \ne B$ ha λ punti in comune con B, cioè $N^{\mathsf{T}} N = (k-\lambda) I + \lambda J$. □

Nell'Esempio 19.7 non era necessario precisare se l'insieme $\mathcal{P}$ fosse costituito dai sottospazi unidimensionali o da quelli bidimensionali. Nel secondo caso si ottiene il duale del primo. In molti casi $\mathcal{D}$ e $\mathcal{D}^{\mathsf{T}}$ non sono isomorfi.

Sia $\mathcal{D}$ un disegno simmetrico 2-(v, k, λ). Vi sono altri due modi di ottenere un disegno da $\mathcal{D}$. I due disegni si chiamano *derivato* e *residuo* di $\mathcal{D}$. Ciò potrebbe creare confusione, perché abbiamo già introdotto questa terminologia; preciseremo sempre quale delle due accezioni intendiamo. Prendiamo un blocco B qualsiasi di $\mathcal{D}$. Il residuo di $\mathcal{D}$ rispetto a B ha come punti $\mathcal{P} \setminus B$ e come blocchi tutti gli insiemi $B' \setminus B$ con $B' \neq B$: è un disegno 2-$(v-k, k-\lambda, \lambda)$. Il derivato ha come punti B e come blocchi tutti gli insiemi $B' \cap B$, con $B' \neq B$: è un disegno 2-$(k, \lambda, \lambda-1)$. Se un disegno con parametri v, k, b, r, λ è il residuo di un disegno simmetrico, allora $r = k + \lambda$. Ogni 2-disegno per il quale vale questa equazione si chiama *quasiresiduo*. Se non è il residuo di un disegno simmetrico, si dice *non immergibile*. L'affermazione del Problema 19K è che ogni piano affine è immergibile in un piano proiettivo. Un teorema di W. S. Connor (1952), che rinviamo al Capitolo 21, afferma che ogni disegno quasiresiduo con $\lambda = 2$ è immergibile.

Orig. 229

Esempio 19.9. Sia $C := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ e sia E_i la matrice 3×3 con uni nella colonna i e zeri altrove. Allora

$$N := \begin{pmatrix} E_1 & I & I & I \\ E_2 & I & C & C^2 \\ E_3 & I & C^2 & C \end{pmatrix}$$

è la matrice d'incidenza 9×12 di $AG_2(3)$. Definiamo

$$A := \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&0&0 \\ 1&1&1&0&0&0&0&0&0&1&1&1 \\ 0&0&0&1&1&1&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0&0&1&1&1 \\ 0&0&0&0&0&0&1&1&1&1&1&1 \end{pmatrix}, \quad B := \begin{pmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&0&1&0 \\ 1&0&1&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 1&0&0&1 \\ 1&0&0&1 \end{pmatrix}.$$

Formiamo la matrice 24×16

$$D := \begin{pmatrix} A & O \\ N & B \\ N & J - B \end{pmatrix}.$$

Si verifica facilmente che D^{T} è la matrice d'incidenza 16×24 di un disegno 2-$(16, 6, 3)$. È un disegno quasiresiduo. Non può però essere il residuo di un disegno simmetrico 2-$(25, 9, 3)$, perché il prodotto scalare della riga $i+6$ e della riga $i+15$ di D, per $1 \leq i \leq 9$, vale 4, mentre per il Teorema 19.9 il prodotto scalare delle colonne della matrice d'incidenza di un disegno 2-$(25, 9, 3)$ vale 3. Esistono dunque disegni non immergibili con $\lambda = 3$.

La combinazione di un argomento di conteggio con una forma quadratica opportuna, usata nella dimostrazione del Teorema 19.9, è molto comune in combinatoria. Talvolta, però, è più semplice usare metodi algebrici, come illustreremo nel teorema seguente, dovuto a Ryser. Il lettore può provare a dimostrarlo con argomenti di conteggio.

Orig. 230

Teorema 19.10. Sia $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ una struttura d'incidenza con $|\mathcal{P}| = |\mathcal{B}| = v$, blocchi di cardinalità k e tale che due blocchi qualsiasi si incontrino in λ punti. Allora $\mathcal{D}$ è un 2-disegno simmetrico.

Dimostrazione. Sia N la matrice d'incidenza di $\mathcal{D}$. Si ha

$$N^{\mathsf{T}} N = (k - \lambda) I + \lambda J \tag{19.8}$$

e

$$JN = kJ. \tag{19.9}$$

Per il Teorema 19.9, basta mostrare che $NJ = kJ$. Da (19.8) vediamo che N è non singolare, e quindi (19.9) si può scrivere come $J = kJN^{-1}$. Da (19.8) ricaviamo $JN^{\mathsf{T}}N = (k - \lambda + \lambda v)J$, perciò

$$JN^{\mathsf{T}} = (k - \lambda + \lambda v) JN^{-1} = (k - \lambda + \lambda v) k^{-1} J.$$

La matrice N ha dunque somme di riga costanti, che devono allora essere uguali a k. Ciò dimostra il teorema e dà $(k-\lambda+\lambda v)k^{-1}=k$, come ci si attendeva da (19.3) e (19.4). □

Per prepararci al più noto teorema di non esistenza per i disegni, occorrono due risultati, entrambi di Lagrange. Per il primo, consideriamo la matrice H di (18.6) con $n=1$, cioè $A_i=(a_i)$. Definiamo $\mathbf{y}=(y_1,y_2,y_3,y_4)$ mediante $\mathbf{y}:=\mathbf{x}H$, dove $\mathbf{x}=(x_1,x_2,x_3,x_4)$. Da (18.7) ricaviamo

$$(a_1^2+a_2^2+a_3^2+a_4^2)(x_1^2+x_2^2+x_3^2+x_4^2)=y_1^2+y_2^2+y_3^2+y_4^2. \tag{19.10}$$

Usando questa identità, Lagrange dimostrò che ogni intero non negativo è somma di quattro quadrati. Chiaramente l'identità mostra che basta dimostrarlo per i numeri primi. Per un'elegante dimostrazione del fatto che un primo è somma di quattro quadrati rinviamo a Chandrasekharan (1968).

Il seguente risultato di non esistenza è noto come *teorema di Bruck–Ryser–Chowla*.

Teorema 19.11. Se v,k,λ sono interi tali che $\lambda(v-1)=k(k-1)$, condizioni necessarie per l'esistenza di un disegno simmetrico 2-(v,k,λ) sono:

(i) se v è pari, $k-\lambda$ è un quadrato;

(ii) se v è dispari, l'equazione $z^2=(k-\lambda)x^2+(-1)^{(v-1)/2}\lambda y^2$ ha una soluzione intera (x,y,z) non identicamente nulla.

Orig. 231

Dimostrazione. L'affermazione (i) è stata dimostrata nel Teorema 19.7. Supponiamo dunque v dispari. Sia $\mathcal{D}$ un disegno simmetrico 2-(v,k,λ) con matrice d'incidenza $N=(n_{ij})$ e poniamo $n:=k-\lambda$. Introduciamo v forme lineari L_i nelle variabili $x_1,\dots,x_v$ mediante

$$L_i:=\sum_{j=1}^{v} n_{ij}x_j, \qquad 1\le i\le v.$$

L'equazione $N^{\mathsf{T}}N=(k-\lambda)I+\lambda J$ implica

$$L_1^2+\cdots+L_v^2=n(x_1^2+\cdots+x_v^2)+\lambda(x_1+\cdots+x_v)^2. \tag{19.11}$$

Per il teorema di Lagrange possiamo scrivere $n=a_1^2+\cdots+a_4^2$. Usando (19.10) possiamo quindi prendere quattro variabili x_j e scrivere

$$n(x_i^2+x_{i+1}^2+x_{i+2}^2+x_{i+3}^2)=y_i^2+y_{i+1}^2+y_{i+2}^2+y_{i+3}^2, \tag{19.12}$$

dove ogni y_j è una forma lineare nelle quattro variabili $x_i,\dots,x_{i+3}$.

Supponiamo anzitutto $v\equiv 1 \pmod 4$. Applicando questa trasformazione a (19.11), quattro variabili alla volta, e introducendo $w:=x_1+\cdots+x_v$, riduciamo (19.11) a

$$L_1^2+\cdots+L_v^2=y_1^2+\cdots+y_{v-1}^2+nx_v^2+\lambda w^2. \tag{19.13}$$

Poiché la matrice H di (18.6) è invertibile, possiamo esprimere le variabili x_j, $1\le j\le v-1$, come forme lineari nelle corrispondenti y_j; anche w è dunque una forma lineare in queste variabili e in x_v. Riduciamo ora il numero delle variabili nel modo seguente. Se la forma lineare L_1, espressa in $y_1,\dots,y_{v-1},x_v$, non ha coefficiente $+1$ per y_1, poniamo $L_1=y_1$; se invece il coefficiente è $+1$, poniamo $L_1=-y_1$. In entrambi i casi risolviamo l'equazione rispetto a y_1, esprimendola linearmente nelle rimanenti y_j e in x_v, e sostituiamo nell'espressione di w. L'equazione (19.11) si è così ridotta a

$$L_2^2+\cdots+L_v^2=y_2^2+\cdots+y_{v-1}^2+nx_v^2+\lambda w^2.$$

Procediamo allo stesso modo per $y_2,\dots,y_{v-1}$. A ogni passo w viene sostituita da un'altra forma lineare nelle variabili rimanenti; alla fine otteniamo

$$L_v^2=nx_v^2+\lambda w^2,$$

nella quale sia L_v sia w sono multipli razionali di x_v. Eliminando i denominatori comuni dei coefficienti troviamo un'equazione

Orig. 232

$$z^2=(k-\lambda)x^2+\lambda y^2$$

in interi. L'affermazione è così dimostrata per $v\equiv 1 \pmod 4$. Se $v\equiv 3 \pmod 4$, applichiamo lo stesso procedimento dopo aver aggiunto a entrambi i membri nx_{v+1}^2, con x_{v+1} nuova variabile. L'equazione si

riduce infine a $nx_{v+1}^2 = y_{v+1}^2 + \lambda w^2$; eliminando ancora i denominatori comuni troviamo un'equazione della forma

$$(k-\lambda)x^2 = z^2 + \lambda y^2,$$

come richiesto da (ii). □

Esempio 19.10. Dall'Esempio 19.7 sappiamo che esiste un piano proiettivo di ordine n per $2 \le n \le 9$, con la possibile eccezione di $n = 6$. Per il Teorema 19.11, una condizione necessaria per l'esistenza di un piano proiettivo di ordine 6 è che $z^2 = 6x^2 - y^2$ abbia una soluzione non banale. Se una tale soluzione esiste, ne esiste anche una nella quale x, y, z non abbiano alcun fattore primo comune; in tal caso z e y sono entrambi dispari. Quindi z^2 e y^2 sono entrambi congrui a 1 modulo 8. Poiché $6x^2$ modulo 8 vale 0 oppure 6, l'equazione ha soltanto la soluzione banale $(0, 0, 0)$. Un piano proiettivo di ordine 6 non esiste.

Se proviamo lo stesso ragionamento per un piano di ordine 10, troviamo $z^2 = 10x^2 - y^2$, che ha la soluzione $x = 1, y = 1, z = 3$. In questo caso il Teorema 19.11 non dice nulla. Nel 1989 Lam e collaboratori annunciarono che una ricerca al calcolatore, durata parecchie centinaia di ore su un Cray 1, aveva escluso l'esistenza di un piano proiettivo di ordine 10. Questo è l'unico caso in cui la non esistenza di un 2-disegno simmetrico sia stata dimostrata con un metodo diverso dal Teorema 19.11.

Corollario. Se esiste un piano proiettivo di ordine $n \equiv 1$ oppure $2 \pmod 4$, allora n è somma di due quadrati interi.

Dimostrazione. La condizione $n \equiv 1$ oppure $2 \pmod 4$ implica $v = n^2+n+1 \equiv 3 \pmod 4$. Il Teorema 19.11 afferma che n è somma di due quadrati razionali. È noto che ciò avviene se e solo se n è somma di due quadrati interi. Questo segue dal fatto che n è somma di due quadrati interi se e solo se nessun divisore primo della sua parte libera da quadrati è congruo a 3 modulo 4. □ Orig. 233

Problema 19L. Dimostrare che non esiste un disegno simmetrico 2-$(29, 8, 2)$.

Problema 19M. Sia M una matrice quadrata razionale di ordine v con $MM^{\mathsf{T}} = mI$. Dimostrare che, se v è dispari, m è un quadrato. Dimostrare che, se $v \equiv 2 \pmod 4$, m è somma di due quadrati razionali.

Una conseguenza dell'ultimo risultato è che l'esistenza di una matrice di conferenza di ordine $n \equiv 2 \pmod 4$ implica che $n - 1$ sia somma di due quadrati.

Molto lavoro è stato dedicato alla costruzione dei 2-disegni. Tratteremo soltanto alcuni esempi per dare un'idea dei metodi usati. La più piccola coppia non banale (k, λ) da considerare è $(3, 1)$. Un disegno 2-$(v, 3, 1)$ si chiama *sistema di terne di Steiner* e si indica con $STS(v)$. Per (19.3) e (19.4), una condizione necessaria per la sua esistenza è $v \equiv 1 \pmod 6$ oppure $v \equiv 3 \pmod 6$. Dimostreremo che questa condizione è anche sufficiente mediante costruzioni dirette negli Esempi 19.11 e 19.15. È però utile vedere alcuni esempi di un approccio più elaborato. I metodi che illustreremo servono anche a costruire disegni diversi dai sistemi di terne di Steiner. Inoltre permettono di produrre disegni con determinati sottodisegni (Problema 19N) o con gruppo di automorfismi prescritto. L'idea è trovare costruzioni dirette di piccoli esempi e alcune costruzioni ricorsive, poi mostrare che, per ogni v che soddisfa le condizioni necessarie, si può costruire un $STS(v)$ ricorsivamente usando l'elenco dei piccoli esempi noti. Vedremo che ciò si riduce a un problema di teoria dei numeri non molto difficile. Come detto, ci limiteremo ad alcuni esempi. Il lettore può provare a mostrare che essi bastano a trovare un $STS(v)$ per tutti i valori possibili di v, senza usare gli Esempi 19.11 e 19.15.

Consideriamo il disegno banale con un unico blocco di cardinalità 3 come $STS(3)$. Abbiamo già visto costruzioni di $STS(7) = PG_2(2)$ e $STS(9) = AG_2(3)$; nell'Esempio 19.1 abbiamo costruito un $STS(15)$. Orig. 234

Esempio 19.11. Sia $n = 2t + 1$. Definiamo $\mathcal{P} := \mathbb{Z}_n \times \mathbb{Z}_3$. Prendiamo come blocchi tutte le terne $\{(x, 0), (x, 1), (x, 2)\}$, con $x \in \mathbb{Z}_n$, e tutte le terne $\{(x, i), (y, i), (\frac{1}{2}(x+y), i+1)\}$, con $x \neq y$ in $\mathbb{Z}_n$ e $i \in \mathbb{Z}_3$. Questa semplice costruzione fornisce un $STS(6t + 3)$ per ogni t.

Esempio 19.12. Sia $q = 6t + 1$ una potenza di primo e sia α un elemento primitivo di $\mathbb{F}_q$, cioè $\mathbb{F}_q^*$ è il gruppo ciclico generato da α. Definiamo

$$B_{i,\xi} := \{\alpha^i + \xi, \alpha^{2t+i} + \xi, \alpha^{4t+i} + \xi\}, \quad 0 \le i < t, \quad \xi \in \mathbb{F}_q. \tag{19.14}$$

Affermiamo che gli elementi di $\mathbb{F}_q$ come punti e i blocchi $B_{i,\xi}$ formano un $STS(q)$. L'idea della dimostrazione è la stessa dell'Esempio 19.6. Si osservi che $\alpha^{6t} = 1$, $\alpha^{3t} = -1$; definiamo s mediante $\alpha^s = \alpha^{2t} - 1$.

Le sei differenze fra coppie di elementi di $B_{0,0}$ sono

$$\begin{aligned} \alpha^{2t}-1 &= \alpha^{s}, & -(\alpha^{2t}-1) &= \alpha^{s+3t},\\ \alpha^{4t}-\alpha^{2t} &= \alpha^{s+2t}, & -(\alpha^{4t}-\alpha^{2t}) &= \alpha^{s+5t},\\ \alpha^{6t}-\alpha^{4t} &= \alpha^{s+4t}, & -(1-\alpha^{4t}) &= \alpha^{s+t}. \end{aligned}$$

Per ogni $\eta \neq 0$ in $\mathbb{F}_q$ esiste dunque un unico i, $0 \leq i < t$, tale che η compaia come differenza di due elementi di $B_{i,0}$. Pertanto, per ogni coppia di elementi distinti x, y di $\mathbb{F}_q$, esistono un unico i e un unico $\xi \in \mathbb{F}_q$ tali che la coppia x, y appartenga a $B_{i,\xi}$. □

Il metodo degli Esempi 19.6 e 19.12 è noto come *metodo delle differenze*. L'Esempio 19.15 ne mostrerà un uso più complesso.

Ora sappiamo che esiste un $STS(v)$ per $v = 13, 19, 25, 31, 37, 43, 49$, oltre ai valori già menzionati. Questi comprendono tutti i $v \equiv 1 \pmod 6$ minori di 50. In effetti, conosciamo ormai almeno un $STS(v)$ per ogni valore ammissibile di v minore di 100, tranne $v = 55, 85, 91$.

Orig. 235

Esempio 19.13. Supponiamo dato un $STS(v_i)$ sull'insieme dei punti V_i, per $i = 1, 2$. Prendiamo $V_1 \times V_2$ come nuovo insieme dei punti e definiamo come blocchi tutte le terne $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ per le quali:

1. $x_1 = x_2 = x_3$ e $\{y_1, y_2, y_3\}$ è un blocco di $STS(v_2)$;
2. $\{x_1, x_2, x_3\}$ è un blocco di $STS(v_1)$ e $y_1 = y_2 = y_3$;
3. $\{x_1, x_2, x_3\}$ è un blocco di $STS(v_1)$ e $\{y_1, y_2, y_3\}$ è un blocco di $STS(v_2)$.

È praticamente evidente che si ottiene un $STS(v_1 v_2)$. Il lettore verifichi che abbiamo definito il numero corretto di blocchi. Questa costruzione ci fornisce un $STS(91)$.

Esempio 19.14. Presentiamo una costruzione leggermente più elaborata. Supponiamo di avere un $STS(v_1)$ sull'insieme $V_1 = \{1, 2, \ldots, v_1\}$ con insieme dei blocchi $\mathcal{S}_1$; supponiamo inoltre che i blocchi completamente contenuti in $V = \{s+1, \ldots, v_1\}$, dove $s = v_1 - v$, formino un $STS(v)$. Sia $\mathcal{S}_2$ l'insieme delle terne di un $STS(v_2)$ sull'insieme $V_2 = \{1, 2, \ldots, v_2\}$.

Consideriamo il nuovo insieme dei punti

$$\mathcal{P} := V \cup \{(x, y) : 1 \leq x \leq s,\ 1 \leq y \leq v_2\},$$

che ha $v + v_2(v_1 - v)$ punti. Introduciamo un insieme $\mathcal{B}$ di quattro tipi di blocchi:

1. quelli del sottosistema $STS(v)$;
2. $\{(a, y), (b, y), c\}$, con $c \in V$, $\{a, b, c\} \in \mathcal{S}_1$ e $y \in V_2$;
3. $\{(a, y), (b, y), (c, y)\}$, con $\{a, b, c\}$ blocco di $\mathcal{S}_1$ privo di punti in V e $y \in V_2$;
4. $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$, dove $\{y_1, y_2, y_3\}$ è un blocco di $\mathcal{S}_2$ e gli interi x_1, x_2, x_3 soddisfano $x_1 + x_2 + x_3 \equiv 0 \pmod s$.

Anche qui si verifica facilmente che due punti qualsiasi di $\mathcal{P}$ determinano univocamente un blocco di $\mathcal{B}$. Quindi $\mathcal{P}$ e $\mathcal{B}$ sono i punti e i blocchi di un sistema di terne di Steiner su $v + v_2(v_1 - v)$ punti. Un esempio semplice si ottiene prendendo come sottosistema un solo blocco, cioè $v = 3$. Con $v_1 = 7$, $v_2 = 13$ troviamo un $STS(55)$.

Abbiamo così costruito un $STS(v)$ per ogni valore ammissibile di v minore di 100, tranne $v = 85$.

Orig. 236

Problema 19N. (a) Dimostrare che, se esistono un $STS(v_1)$ e un $STS(v_2)$, esiste un $STS(v_1 v_2 - v_2 + 1)$. Usare questa costruzione per trovare un $STS(85)$.

(b) Costruire un $STS(15)$ sull'insieme $\{0, 1, \ldots, 14\}$ contenente come sottosistema un piano di Fano su $\{0, 1, \ldots, 6\}$.

Esempio 19.15. Consideriamo l'insieme dei punti $(\mathbb{Z}_{2t} \times \mathbb{Z}_3) \cup \{\infty\}$. La somma è definita coordinata per coordinata, con la convenzione aggiuntiva $\infty + (x, i) = \infty$. Per comodità scriviamo talvolta la seconda coordinata come indice: x_i al posto di (x, i). Definiamo quattro tipi di «blocchi di base»:

1. $\{0_0, 0_1, 0_2\}$;
2. $\{\infty, 0_0, t_1\}$, $\{\infty, 0_1, t_2\}$, $\{\infty, 0_2, t_0\}$;
3. $\{0_0, i_1, (-i)_1\}$, $\{0_1, i_2, (-i)_2\}$, $\{0_2, i_0, (-i)_0\}$, per $i = 1, \ldots, t-1$;
4. $\{t_0, i_1, (1-i)_1\}$, $\{t_1, i_2, (1-i)_2\}$, $\{t_2, i_0, (1-i)_0\}$, per $i = 1, \ldots, t$.

Abbiamo $6t+1$ blocchi di base. Per $a = 0, 1, \ldots, t-1$ aggiungiamo $(a, 0)$, ossia a_0, a ciascun elemento di ogni blocco di base, producendo così $t(6t+1)$ blocchi. Affermiamo che essi sono le terne di un $STS(6t+1)$. È immediato che i blocchi di base di tipo 2 producono una famiglia in cui ogni coppia contenente ∞ compare esattamente una volta. La natura ciclica della definizione dei blocchi di base mostra che basta verificare che tutte le coppie $\{a_0, b_0\}$ con $a \neq b$ e tutte le coppie $\{a_0, b_1\}$ compaiano nelle terne definite. Se $a < b$ e $b - a = 2s$, la coppia $\{a_0, b_0\}$ compare nella terna ottenuta da $\{0_2, s_0, (-s)_0\}$ «traslata» di $(b-s, 0)$. Analogamente, se $b - a$ è dispari, troviamo la coppia cercata traslando un blocco di base di tipo 4. Consideriamo ora $\{a_0, b_1\}$. Se $a = b \leq t-1$, troviamo la coppia traslando il blocco di tipo 1 di $(a, 0)$. Se $a \neq b$ e $a < t$, dobbiamo cercarla in una traslata di un blocco di tipo 2 o 3. Cerchiamo quindi un blocco di base in cui la differenza $b - a$ compaia come $y - x$ per due elementi y_1, x_0. Per il tipo 2 la differenza è t; nei blocchi $\{0_0, i_1, (-i)_1\}$ troviamo le differenze i, $1 \leq i \leq t-1$, e $-i = 2t-i$, $1 \leq i \leq t-1$: proprio ogni differenza una volta. I dettagli rimanenti si possono lasciare per esercizio.

Questo esempio mostra che, se $v = 6t+1$, esiste un $STS(v)$. Insieme con l'Esempio 19.11, dà una costruzione per ogni valore ammissibile di v. Concludiamo il capitolo con una divertente applicazione del piano di Fano. Attualmente l'idea non è usata in pratica, ma il problema ha origine pratica e forse un giorno saranno utilizzate generalizzazioni del metodo seguente. Supponiamo di voler memorizzare uno degli interi da 1 a 7 in una cosiddetta «memoria a scrittura unica». È una memoria binaria, inizialmente piena di zeri, nella quale si possono trasformare alcuni bit in uni, ma non riportarli a zero: lo stato 1 è permanente. Ciò accade, per esempio, con il nastro di carta perforato o con i compact disc, nei quali un laser crea cavità in determinate posizioni. In entrambi i casi non possiamo cancellare ciò che è stato scritto nella memoria. Per memorizzare gli interi da 1 a 7 bastano tre bit. Ma se vogliamo utilizzare la memoria quattro volte consecutive? La soluzione più semplice è una memoria di 12 bit suddivisa in quattro sezioni da tre bit, una per ogni uso. Supponiamo che la memoria sia molto costosa e desideriamo usarne una più corta per lo stesso scopo. Mostreremo che bastano sette bit, con un risparmio superiore al 40%.

Orig. 237

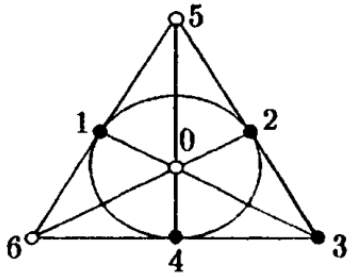


Figura 19.3

Sia $\mathcal{P} = \{1, 2, \ldots, 7\}$ l'insieme dei punti di $PG_2(2)$ e sia $\mathcal{L}$ l'insieme delle rette. Per memorizzare un intero da 1 a 7 in una memoria con posizioni numerate da 1 a 7 usiamo le regole seguenti. Regola generale: se vogliamo memorizzare i e la memoria si trova già, per un uso precedente, in uno stato corrispondente a i, non facciamo nulla. Negli altri casi:

1. se la memoria è vuota, memorizziamo i mettendo 1 nella posizione i;
2. per memorizzare j quando la memoria è nello stato i, mettiamo 1 nella posizione k, dove $\{i, j, k\} \in \mathcal{L}$;
3. per memorizzare i quando la memoria contiene due uni che non corrispondono a i, aggiungiamo altri due uni in modo che i sia una delle quattro posizioni

Orig. 238

occupate e le altre tre formino una retta di $\mathcal{L}$. Qualunque fossero i due uni originari, ciò è possibile, talvolta in due modi.

4. se la memoria contiene quattro uni, possiamo supporre di trovarci nella situazione della Figura 19.3. Per memorizzare 3 non facciamo nulla, per la regola generale; per memorizzare uno dei numeri mancanti, mettiamo uni nelle altre due posizioni; per memorizzare 1, 2 oppure 4, mettiamo un 1 nella posizione vuota sulla retta passante per 3 e per il numero che vogliamo memorizzare.

Lasciamo al lettore il compito di formulare le regole di lettura della memoria. La memoria permette di leggere univocamente l'intero attualmente memorizzato, ma non rivela quante volte un intero sia stato memorizzato né quale fosse quello dell'uso precedente.[3]

Problema 19O. (i) Sia $\mathcal{A}$ una famiglia di sottoinsiemi di un n-insieme X, ciascuno di cardinalità dispari, tale che due membri distinti si incontrino in un numero pari di punti. Dimostrare che $|\mathcal{A}| \le n$.

(ii) Supporre che i membri di $\mathcal{A}$ abbiano cardinalità pari ma che due qualsiasi si incontrino in un numero dispari di punti. Dimostrare che $|\mathcal{A}| \le n+1$. Trovare esempi nei quali valga l'uguaglianza.

Problema 19P. Considerare disegni 2-$(v, k, \lambda = 2)$ con $v = \binom{k+1}{2}$.

(i) Trovare un esempio con $k = 3$. Si può provare con cinque punti su una circonferenza e uno al centro.

(ii) Siano $A_1, A_2, \dots, A_b$ i blocchi e, per $i = 2, 3, \dots, b$, sia $\mu_i = |A_i \cap A_1|$. Calcolare

$$\sum_{i=2}^{b} \mu_i, \qquad \sum_{i=2}^{b} \mu_i(\mu_i - 1), \qquad \sum_{i=2}^{b} (\mu_i - 1)(\mu_i - 2)$$

in funzione di k. Che cosa si può dire dei μ_i?

Problema 19Q. Un *sistema di Steiner generalizzato* è una struttura d'incidenza con un insieme dei punti $\mathcal{P}$ di cardinalità v e un insieme $\mathcal{B}$ di sottoinsiemi di $\mathcal{P}$, ancora detti blocchi, con $|\mathcal{B}| = b$, tale che ogni t-sottoinsieme di $\mathcal{P}$ appartenga a un unico blocco. Non richiediamo che i blocchi abbiano cardinalità costante, ma escludiamo il caso banale $b = 1$. Indichiamo con $b_{t,v}$ il minimo valore di b per un sistema di Steiner generalizzato non banale. Dimostrare che, per $t \ge 2$, Orig. 239

$$b_{t,v}(b_{t,v} - 1) \ge t\binom{v}{t}.$$

Per $t = 2$ questo risultato coincide con il Teorema 19.1. Sono note limitazioni molto più forti, ma non altrettanto facili da ricavare.

Problema 19R. Diremo che un punto del piano di Fano è un rappresentante di una retta se è incidente con essa. Quanti SDR possiede il piano di Fano?

Problema 19S. Costruire disegni 3-$(2^k, 4, 1)$ per ogni $k \ge 2$.

Problema 19T. Un disegno si dice *estendibile* se è il derivato di un disegno, detto *disegno esteso*. Dimostrare che, se un disegno simmetrico può essere esteso due volte, deve essere un disegno 2-$(21, 5, 1)$.

Problema 19U. Considerare il grafo G del Problema 1J. Definire una struttura d'incidenza $\mathcal{I}$ avente come punti i vertici di G e come rette gli insiemi $\Gamma(x)$, per i vertici x di G. Dimostrare che le proprietà di G implicano che $\mathcal{I}$ sia un piano proiettivo. Confrontare il Problema 21Q.

Problema 19V. Usiamo le ipotesi e la notazione introdotte nella dimostrazione del Teorema 19.8.

(i) Verificare che $W_{is}N_s = \binom{k-i}{s-i}N_i$.

(ii) Dimostrare che il prodotto di due qualsiasi delle matrici $W_{is}^{\mathsf{T}}W_{is}$, $i = 0, 1, \dots, s$, è una combinazione lineare di queste $s+1$ matrici. Il loro spazio lineare generato $\mathcal{A}$ è quindi chiuso rispetto alla moltiplicazione.

(iii) Supporre che nel Teorema 19.8 valga l'uguaglianza, cosicché N_s è quadrata. Allora $N_s^{\mathsf{T}}M^{-1}N_s = I$, dove $M := \sum_{i=0}^{s} b_{2s-i}^{i} W_{is}^{\mathsf{T}}W_{is}$. Poiché $M \in \mathcal{A}$, la parte (ii) implica $M^{-1} \in \mathcal{A}$. Usare questo fatto per dimostrare che esiste un polinomio $f(x)$ di grado s tale che $f(|A \cap B|) = 0$ per tutti i blocchi distinti A, B. Vi sono dunque al più s «numeri d'intersezione». Questo generalizza il Teorema 19.9.

[3] Nota di traduzione: la figura originale usa le etichette $0, 1, \dots, 6$, mentre il testo usa $1, 2, \dots, 7$. Per accordare figura e testo basta rinominare il punto 0 come 7; gli altri nomi restano invariati.

Note

La prima comparsa di un 2-disegno potrebbe essere quella di $AG_2(3)$ in un articolo di Plücker (1839). Solitamente l'introduzione dei sistemi di Steiner è attribuita a Woolhouse (1844), certamente non a Steiner! Spesso si dice che essi abbiano origine da un problema di T. P. Kirkman (1847). T. P. Kirkman (1806–1895), autodidatta, era un ministro della Chiesa d'Inghilterra. Matematico dilettante, diede molti contributi alla disciplina. Il più noto è probabilmente il problema delle 15 scolare. Si tratta di disporre 15 scolare in gruppi di tre per passeggiate in sette giorni, in modo che ogni coppia passeggi insieme esattamente una volta. Questo equivale a costruire un $STS(15)$ il cui insieme di terne sia suddivisibile in sette «classi di parallelismo». Orig. 240

Jakob Steiner (1796–1863) fu un importante geometra del suo tempo. Si interessò a ciò che oggi chiamiamo sistemi di Steiner nel 1853, studiando la configurazione delle 28 bitangenti di una curva quartica piana.

Sir Ronald A. Fisher (1890–1962) è considerato uno dei più eminenti statistici. Oltre agli importanti contributi alla statistica, in particolare all'analisi multivariata, e alla genetica, è noto per il lavoro sull'applicazione della teoria statistica all'agricoltura e alla progettazione degli esperimenti. Le applicazioni agli esperimenti agricoli spiegano l'uso di v per il numero di punti di un disegno, da *varieties*, e di r per il numero di blocchi per un punto, da *replication number*.

Il Teorema 19.7 è dovuto a M. P. Schutzenberger (1949).

R. A. Fisher non fu l'unico statistico a contribuire alla teoria matematica dei disegni. Anzi, dovremmo probabilmente considerare il matematico indiano R. C. Bose (1901–1987) come il più importante. Molti dei metodi di costruzione descritti in questo capitolo, fra cui quello delle differenze, sono dovuti a lui.

G. Fano (1871–1952), il cui nome è associato al piano $PG_2(2)$, ebbe un ruolo importante nella scuola italiana di geometria proiettiva.

I piani proiettivi su campi finiti furono studiati per la prima volta da K. G. C. von Staudt (1798–1867) nel suo libro *Geometrie der Lage* (1856).

Il primo esempio di disegno quasiresiduo non immergibile fu dato da Bhattacharya (1944). Anche quello era un disegno 2-$(16, 6, 3)$, ma l'Esempio 19.9 è molto più semplice.

J. L. Lagrange (1736–1813) nacque e si formò in Italia, ma è considerato un matematico francese, che studiò a Berlino. Oltre ai numerosi contributi importanti all'analisi, è noto per vari teoremi di teoria dei numeri. Orig. 241

Il teorema di Bruck–Ryser–Chowla, Teorema 19.11, è tanto noto da essere spesso chiamato semplicemente BRC.

L'idea dell'Esempio 19.15 è dovuta a Skolem (1958), il cui metodo era in realtà leggermente diverso. Da esso deriva il termine *successioni di Skolem*, che hanno altre applicazioni, per esempio in radioastronomia. Ecco l'idea: ripartire l'insieme $\{1, 2, \ldots, 2n\}$ in coppie $\{a_i, b_i\}$ tali che $b_i - a_i = i$, $1 \leq i \leq n$. Questa è una successione di Skolem. Per esempio, $\{9, 10\}, \{2, 4\}, \{5, 8\}, \{3, 7\}, \{1, 6\}$ è una tale partizione per $n = 5$. Formiamo ora le terne $\{0, a_i + n, b_i + n\}$ e consideriamole come blocchi di base modulo $6n + 1$. Poiché tutte le differenze $1, 2, \ldots, 3n$ e i loro opposti compaiono esattamente una volta, i blocchi formano un $STS(6n + 1)$.

Per un'interessante applicazione del codice di Golay (Capitolo 20) alle memorie a scrittura unica si veda Cohen e collaboratori (1986). Essi mostrano la possibilità di tre scritture successive di 11 bit su 23 posizioni.

Riferimenti bibliografici

W. O. Alltop (1972) An infinite class of 5-designs, *J. Combinatorial Theory (A)* **12**, 390–395.

K. N. Bhattacharya (1944) A new balanced incomplete block design, *Science and Culture* **9**, 108.

R. H. Bruck e H. J. Ryser (1949) The non-existence of certain finite projective planes, *Canad. J. Math.* **1**, 88–93.

N. G. de Bruijn e P. Erdős (1948) On a combinatorial problem, *Proc. Kon. Ned. Akad. v. Wetensch.* **51**, 1277–1279.

K. Chandrasekharan (1968) *Introduction to Analytic Number Theory*, Springer-Verlag.

S. Chowla e H. J. Ryser (1950) Combinatorial problems, *Canad. J. Math.* **2**, 93–99.

G. D. Cohen, P. Godlewski e F. Merkx (1986) Linear binary codes for write-once memories, *IEEE Trans. Information Theory* **32**, 697–700.

W. S. Connor, Jr. (1952) On the structure of balanced incomplete block designs, *Ann. Math. Stat.* **23**, 57–71; correzione, ibid. **24**, 135.

Orig. 242

R. H. F. Denniston (1976) Some new 5-designs, *Bull. London Math. Soc.* **8**, 263–267.

G. Fano (1892) *Giornale di Matimatiche* **30**, 114–124.

M. J. Granell e T. S. Griggs (1994) A Steiner system $S(5, 6, 108)$, *Discrete Mathematics* **125**, 183–186.

D. Jungnickel e S. A. Vanstone (1987) Hyperfactorizations of graphs and 5-designs, *J. Univ. Kuwait (Sci)* **14**, 213–223.

T. P. Kirkman (1847) On a problem in combinations, *Cambridge and Dublin Math. J.* **2**, 191–204.

D. L. Kreher e S. P. Radziszowski (1986) The existence of simple 6-(14,7,4) designs, *J. Combinatorial Theory (A)* **41**, 237–243.

C. W. Lam, S. Swiercz e L. Thiel (1989) The nonexistence of finite projective planes of order 10, *Canad. J. Math.* **41**, 1117–1123.

D. W. Leavitt e S. S. Magliveras (1982) Simple 6-(33,8,36)-designs from $P\Gamma L_2(32)$, pp. 337–352, in: *Computational Group Theory*, Proc. Durham 1982.

W. H. Mills (1978) A new 5-design, *Ars Combinatoria* **6**, 193–195.

A. Ya. Petrenjuk (1968) On Fisher's inequality for tactical configurations (in russo), *Mat. Zametki* **4**, 417–425.

D. K. Ray-Chaudhuri e R. M. Wilson (1975) On t-designs, *Osaka J. Math.* **12**, 737–744.

H. J. Ryser (1963) *Combinatorial Mathematics*, Carus Math. Monograph **14**.

M. P. Schutzenberger (1949) A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugenics* **14**, 286–287.

Th. Skolem (1958) Some remarks on the triple systems of Steiner, *Math. Scand.* **6**, 273–280.

J. Steiner (1853) Combinatorische Aufgabe, *J. f. d. reine u. angew. Mathematik* **45**, 181–182.

L. Teirlinck (1987) Nontrivial t-designs without repeated blocks exist for all t, *Discrete Math.* **65**, 301–311.

J. Tits (1964) Sur les systèmes de Steiner associés aux trois «grands» groupes de Mathieu, *Rend. Math. e Appl. (5)* **23**, 166–184.

E. Witt (1938) Die 5-fach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Univ. Hamburg* **12**, 256–264.

Orig. 243

W. S. B. Woolhouse (1844) Prize question 1733, *Lady's and Gentleman's Diary.*

Capitolo 20

Codici e disegni

Introduciamo altri termini della teoria dei codici correttori di errori. Nel senso più generale, un *codice* di lunghezza n è semplicemente un sottoinsieme $C \subseteq S^n$, dove S è un insieme finito, detto *alfabeto*. Gli elementi di C si chiamano *parole di codice*. Un codice *binario* ha alfabeto $S = \{0, 1\}$; un codice *ternario* ha alfabeto $S = \{0, 1, 2\}$. La distanza $d(\mathbf{x}, \mathbf{y})$ fra due parole, o vettori, $\mathbf{x}$ e $\mathbf{y}$ di S^n è il numero di posizioni nelle quali esse differiscono: Orig. 244

$$d(\mathbf{x}, \mathbf{y}) := |\{i : 1 \le i \le n,\ x_i \ne y_i\}|. \tag{20.1}$$

Questa è effettivamente una distanza nel senso usuale: si verifichi che soddisfa la disuguaglianza triangolare.

Il concetto di distanza ha portato all'uso di una terminologia geometrica: per esempio, l'insieme $B_r(\mathbf{x}) := \{\mathbf{y} \in \mathbb{F}_q^n : d(\mathbf{x}, \mathbf{y}) \le r\}$ si chiama *sfera* di raggio r e centro $\mathbf{x}$, anche se «palla» sarebbe un termine più appropriato.

La *distanza minima* d del codice C è

$$d := \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C,\ \mathbf{y} \in C,\ \mathbf{x} \ne \mathbf{y}\}. \tag{20.2}$$

Gran parte della teoria dei codici riguarda i codici lineari. Per *codice q-ario* $[n, k]$ intendiamo un sottospazio lineare C di dimensione k dello spazio vettoriale $\mathbb{F}_q^n$.

Il *peso* $w(\mathbf{x})$ di $\mathbf{x}$ è definito da

$$w(\mathbf{x}) := d(\mathbf{x}, \mathbf{0}). \tag{20.3}$$

Questa definizione ha senso ogni volta che 0 è uno dei simboli dell'alfabeto, ma è particolarmente significativa per i codici lineari. Quando C è lineare, la distanza fra le parole $\mathbf{x}$ e $\mathbf{y}$ è il peso di $\mathbf{x} - \mathbf{y}$, che è ancora una parola di codice. La distanza minima di C coincide quindi con il *peso minimo*, cioè con il minimo dei pesi delle parole non nulle. Usiamo la notazione codice $[n, k, d]$ per un codice $[n, k]$ di distanza minima almeno d. Se $d = 2e + 1$, C si chiama *codice correttore di e errori*. Orig. 245

Il *raggio di ricoprimento* $\rho(C)$ è il minimo R per cui le sfere di raggio R centrate nelle parole di codice ricoprono S^n, cioè

$$\rho(C) := \max\{\min\{d(\mathbf{x}, \mathbf{c}) : \mathbf{c} \in C\} : \mathbf{x} \in S^n\}. \tag{20.4}$$

Nel capitolo 18 abbiamo menzionato il codice di ripetizione in $\{0, 1\}^n$, ossia il sottospazio unidimensionale di $\mathbb{F}_2^n$ costituito soltanto da $\mathbf{0}$ e $\mathbf{1}$. Se $n = 2e + 1$, ogni parola ha distanza $\le e$ da esattamente una parola di codice. Il raggio di ricoprimento è quindi e. Le due sfere di raggio e centrate nelle due parole di codice sono disgiunte e ricoprono lo spazio.

In generale chiamiamo *codice perfetto*, correttore di e errori, un codice $C \subseteq S^n$, non necessariamente lineare, con $|C| > 1$, per cui ogni $\mathbf{x} \in S^n$ abbia distanza $\le e$ da esattamente una parola di codice. Ciò equivale a richiedere distanza minima $d = 2e + 1$ e raggio di ricoprimento e. I codici perfetti sono evidentemente oggetti interessanti dal punto di vista combinatorio, ma sono estremamente rari.

Teorema 20.1. Se C è un codice in S^n con distanza $d \ge 2e + 1$, ponendo $q = |S|$ si ha

$$|C| \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \le q^n. \tag{20.5}$$

DIMOSTRAZIONE. La somma al membro sinistro della (20.5) conta le parole contenute in una sfera di raggio e. □

Il limite dato da questo teorema si chiama *limite dell'impacchettamento di sfere* oppure *limite di Hamming*. Se vale l'uguaglianza, il codice è perfetto.

Problema 20A. Mostrare che, se esiste un codice binario $[23, 12, 7]$, esso è perfetto. Orig. 246

Problema 20B. Per la (20.5), un codice binario di lunghezza 6 e distanza minima 3 ha al più 9 parole. Mostrare che l'uguaglianza è impossibile. Tuttavia 8 parole sono possibili.

Due codici si dicono *equivalenti* se uno si ottiene dall'altro mediante una permutazione delle coordinate in S^n. Talvolta si estende la definizione ammettendo anche una permutazione degli elementi di S, per esempio lo scambio di $+1$ e -1 quando $S = \mathbb{F}_3$.

Una matrice G di dimensione $k \times n$ si chiama *matrice generatrice* del codice $[n, k]$ C se le sue righe generano C. L'algebra lineare elementare mostra che C è equivalente a un codice con matrice generatrice $G = (I_k \ P)$, dove P è una matrice $k \times (n-k)$. Questa si chiama *forma a scala ridotta* di una matrice generatrice.

Il *duale* $C^\perp$ di C è definito da

$$C^\perp := \{\mathbf{x} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0 \text{ per ogni } \mathbf{c} \in C\}. \tag{20.6}$$

Se H è una matrice generatrice di $C^\perp$, chiaramente

$$C = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x}H^\mathsf{T} = \mathbf{0}\}. \tag{20.7}$$

H si chiama *matrice di controllo di parità* di C. Se $G = (I_k \ P)$ è una matrice generatrice, $H = (-P^\mathsf{T} \ I_{n-k})$ è una matrice di controllo di parità. Se $C = C^\perp$, il codice si dice *autoduale*; se $C \subseteq C^\perp$, si dice *autoortogonale*.

Se C è un codice lineare in $\mathbb{F}_q^n$, il *codice esteso* $\overline{C}$ è definito da

$$\overline{C} := \{(c_1, \dots, c_n, c_{n+1}) : (c_1, \dots, c_n) \in C,\ c_1 + \cdots + c_{n+1} = 0\}. \tag{20.8}$$

Il simbolo c_{n+1} si chiama *simbolo di controllo di parità*.

Esempio 20.1. Sia $n = (q^k - 1)/(q-1)$. Consideriamo una matrice H di dimensione $k \times n$ a entrate in $\mathbb{F}_q$, le cui colonne siano a due a due linearmente indipendenti. Questo è il massimo valore di n per cui ciò è possibile. Allora H è chiaramente la matrice di controllo di parità di un codice $[n, n-k]$ di distanza minima 3. Un tale codice si chiama *codice di Hamming q-ario*. Se $\mathbf{c}$ è una parola di codice, $|B_1(\mathbf{c})| = 1 + n(q-1) = q^k$. Poiché $|C| = q^{n-k}$, per la (20.5) il codice è perfetto. Orig. 247

Problema 20C. Sia H il codice di Hamming ternario $[4, 2]$. Definire un codice ternario non lineare C di lunghezza 9, con parole

$$(x_0, x_1, \dots, x_4; y_1, \dots, y_4),$$

richiedendo $\sum_{i=0}^4 x_i \neq 0$ e $(y_1 - x_1, \dots, y_4 - x_4) \in H$. Mostrare che C ha raggio di ricoprimento 1. Non è noto alcun codice ternario di lunghezza 9, raggio di ricoprimento 1 e meno di $2 \cdot 3^6$ parole.

Esempio 20.2. Consideriamo il codice binario di Hamming C di lunghezza $n = 2^k - 1$. Per definizione, il duale $C^\perp$ ha come matrice generatrice la matrice $k \times n$ le cui colonne sono tutti i vettori non nulli di lunghezza k. L'estensione di $C^\perp$ è quindi il codice $R'(1, k)$ del capitolo 18. $C^\perp$ si chiama di solito *codice simplesso* di lunghezza n. Osserviamo che il codice binario di Hamming esteso $[8, 4]$ è autoduale.

Problema 20D. Mostrare che il raggio di ricoprimento di $R(1, 2k)$ è $2^{2k-1} - 2^{k-1}$. Suggerimento: usare la rappresentazione ± 1 anziché $(0, 1)$ e lavorare su $\mathbb{Q}$ per mostrare che il raggio di ricoprimento è al più questo valore. Per ottenere l'uguaglianza, considerare la parola $\mathbf{z}$ che è la funzione caratteristica di

$$\{\mathbf{x} \in \mathbb{F}_2^{2k} : x_1x_2 + \cdots + x_{2k-1}x_{2k} = 1\}.$$

Enunciamo un limite di facile dimostrazione per codici arbitrari, noto come *limite di Singleton*.

Teorema 20.2. Sia C un codice qualsiasi di lunghezza n e distanza minima d su $\mathbb{F}_q$. Allora $|C| \leq q^{n-d+1}$.

DIMOSTRAZIONE. Da ogni parola di codice eliminiamo gli ultimi $d-1$ simboli. Le parole così «accorciate» sono a due a due distinte. Non possono dunque essercene più di q^{n-d+1}. □ Orig. 248

Esempio 20.3. Diamo un esempio che mostra un bel collegamento con il capitolo 19. Sia $q = 2^a$ e sia S un'iperovale in $PG_2(q)$. Nel linguaggio dell'esempio 19.7, gli elementi di S sono rappresentati da vettori di $\mathbb{F}_q^3$ tali che nessuna terna sia linearmente dipendente. Prendiamo questi vettori come colonne di una matrice H di dimensione $3 \times (q+2)$. Interpretando H come matrice di controllo di parità di un codice $[q+2, q-1]$ su $\mathbb{F}_q$, il codice ha distanza minima almeno 4. Per il teorema 20.2 la distanza è dunque esattamente 4. Questo è uno dei rari esempi di uguaglianza nel teorema 20.2. I codici per cui vale l'uguaglianza nel limite di Singleton si chiamano *codici a distanza massima separabile*, o *codici MDS*: un'altra denominazione poco felice! Vi sono molti problemi aperti su questi codici.

Se C è un codice q-ario $[n,k]$ e A_i indica il numero delle sue parole di peso i, allora

$$A(z) := \sum_{i=0}^{n} A_i z^i \tag{20.9}$$

si chiama *enumeratore dei pesi* di C. Naturalmente $A_0 = 1$ e $A(1) = |C| = q^k$.

Problema 20E. Sia C un codice binario, non necessariamente lineare, di lunghezza 23, distanza minima 7 e cardinalità $|C| = 2^{12}$. Supporre $\mathbf{0} \in C$. Mostrare anzitutto che C è perfetto. Sia il suo enumeratore dei pesi dato dalla (20.9). Contare le coppie $(\mathbf{x}, \mathbf{c})$ con $\mathbf{c} \in C$, $w(\mathbf{x}) = 4$ e $d(\mathbf{x}, \mathbf{c}) = 3$, e mostrare che $A_7 = 253$. Mostrare poi che l'enumeratore dei pesi è interamente determinato dalle condizioni che C sia perfetto e $\mathbf{0} \in C$.

Il teorema seguente, dovuto a F. J. MacWilliams (1963), è uno dei più utili nella teoria dei codici correttori di errori.

Teorema 20.3. Sia C un codice $[n,k]$ su $\mathbb{F}_q$, con enumeratore dei pesi $A(z)$, e sia $B(z)$ l'enumeratore dei pesi di $C^\perp$. Allora

$$B(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right). \tag{20.10}$$

DIMOSTRAZIONE. Diamo la dimostrazione soltanto per $q = 2$. Per gli altri valori di q essa è essenzialmente la stessa: al posto di $(-1)^{\langle \mathbf{u},\mathbf{v}\rangle}$ si deve usare $\chi(\langle \mathbf{u}, \mathbf{v}\rangle)$, dove χ è un carattere additivo non banale di $\mathbb{F}_q$. Definiamo Orig. 249

$$g(\mathbf{u}) := \sum_{\mathbf{v}\in\mathbb{F}_2^n} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} z^{w(\mathbf{v})}.$$

Allora

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = \sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in\mathbb{F}_2^n} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} z^{w(\mathbf{v})} = \sum_{\mathbf{v}\in\mathbb{F}_2^n} z^{w(\mathbf{v})} \sum_{\mathbf{u}\in C} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle}.$$

Se $\mathbf{v} \in C^\perp$, la somma interna è $|C|$; se $\mathbf{v} \notin C^\perp$, metà dei suoi termini valgono $+1$ e metà -1. Pertanto

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = |C| B(z). \tag{20.11}$$

Ora

$$\begin{aligned} g(\mathbf{u}) &= \sum_{(v_1,\dots,v_n)\in\mathbb{F}_2^n} \prod_{i=1}^{n} \left((-1)^{u_i v_i} z^{v_i}\right) \\ &= \prod_{i=1}^{n} (1+(-1)^{u_i} z) = (1-z)^{w(\mathbf{u})}(1+z)^{n-w(\mathbf{u})}. \end{aligned}$$

Sostituendo nella (20.11) otteniamo la tesi. □

Corollario. Se scriviamo $B(z) = \sum_{j=0}^{n} B_j z^j$, per $q = 2$ la (20.10) dà

$$B_j = 2^{-k} \sum_{i=0}^{n} A_i \sum_{l=0}^{j} (-1)^l \binom{i}{l}\binom{n-i}{j-l}. \tag{20.12}$$

Queste relazioni, note come *relazioni di MacWilliams*, sono equazioni linearmente indipendenti nei coefficienti A_i, assegnati i coefficienti B_j.

Molti dei 5-disegni non banali noti furono trovati mediante la seguente elegante applicazione del teorema di MacWilliams, solitamente chiamata *teorema di Assmus–Mattson* (1969). Limitiamo nuovamente la dimostrazione al caso binario. Per altri q il teorema ammette una generalizzazione naturale con una dimostrazione quasi identica. Identifichiamo le posizioni di un codice di lunghezza n con $P := \{1, 2, \dots, n\}$. Possiamo così interpretare una parola di un codice binario come un sottoinsieme di P, cioè come la sua funzione caratteristica. Il *supporto* di una parola è l'insieme delle posizioni in cui essa è non nulla. Orig. 250

Problema 20F. Sia C un codice binario perfetto correttore di e errori, di lunghezza n. Supporre che 0 sia un simbolo e $\mathbf{0}$ una parola di codice. Mostrare che P, con i supporti delle parole di peso $d = 2e + 1$, è un $S(e + 1, 2e + 1, n)$.

Teorema 20.4. Sia A un codice binario $[n, k, d]$ e sia $B := A^\perp$ il duale, di parametri $[n, n - k]$. Sia $t < d$. Supponiamo che il numero dei pesi non nulli presenti in B e non maggiori di $n - t$ sia $\le d - t$. Allora, per ogni peso w, i supporti delle parole di peso w in A formano un t-disegno e lo stesso vale per B.

Dimostrazione. Per un codice qualsiasi C, fissato un sottoinsieme $T \subseteq P$ di cardinalità t, indichiamo con C' il codice di lunghezza $n - t$ ottenuto eliminando dalle parole di C le coordinate in T. Indichiamo con C_0 il sottocodice di C' ottenuto eliminando tali coordinate dalle sole parole di C che hanno zeri in tutte le posizioni di T.

La dimostrazione si svolge in quattro passi.

(i) Sia T un sottoinsieme di P di cardinalità t. Poiché t è minore della distanza minima di A, il codice A' ha tante parole quante A, quindi ha ancora dimensione k. Inoltre A' ha distanza minima $\ge d - t$. Il duale $(A')^\perp$ ha perciò dimensione $n - k - t$. Chiaramente B_0 è un sottocodice di $(A')^\perp$. Poiché la dimensione di B_0 è almeno $n - k - t$, deve essere $B_0 = (A')^\perp$.

(ii) Siano $\sum \alpha_i z^i$ e $\sum \beta_i z^i$ gli enumeratori dei pesi di A' e B_0. Affermiamo che essi non dipendono dallo specifico sottoinsieme T, ma soltanto dai numeri t, n, k e dai pesi delle parole di B.

Siano $0 < \ell_1 < \ell_2 < \cdots < \ell_r \le n - t$, con $r \le d - t$, i pesi non nulli di B che non superano $n - t$. Questi sono gli unici possibili pesi non nulli di B_0. La (20.12) dà quindi Orig. 251

$$|B_0|\alpha_j = \binom{n-t}{j} + \sum_{i=1}^{r} \beta_{\ell_i} \sum_{m=0}^{j} (-1)^m \binom{\ell_i}{m} \binom{n-t-\ell_i}{j-m}.$$

Per ipotesi la distanza minima di A' è $\ge r$; conosciamo dunque α_j per $j < r$: $\alpha_0 = 1$ e $\alpha_1 = \cdots = \alpha_{r-1} = 0$. Abbiamo così r equazioni lineari nelle r incognite β_{ℓ_i}. Esse sono determinate univocamente se la matrice dei coefficienti M, di ordine r, con entrata (i, j) uguale a $p_j(\ell_i)$, dove

$$p_j(x) := \sum_{m=0}^{j} (-1)^m \binom{x}{m} \binom{n-t-x}{j-m}, \qquad 1 \le i \le r, \quad 0 \le j \le r - 1,$$

è non singolare. Ma $p_j(x)$ è un polinomio in x di grado esattamente j, con coefficiente di x^j uguale a $(-1)^j 2^j / j!$. Operazioni elementari sulle colonne riducono quindi M alla matrice di Vandermonde

$$\begin{pmatrix} 1 & \ell_1 & \ell_1^2 & \cdots & \ell_1^{r-1} \\ 1 & \ell_2 & \ell_2^2 & \cdots & \ell_2^{r-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \ell_r & \ell_r^2 & \cdots & \ell_r^{r-1} \end{pmatrix},$$

che è non singolare perché gli ℓ_i sono distinti.

L'enumeratore $\sum \beta_i z^i$ non dipende dunque dalla scelta di T. Poiché A' è il duale di B_0, anche $\sum \alpha_i z^i$ è indipendente da T.

(iii) Sia $\mathcal{E}$ la famiglia delle parole di peso w in B, interpretate come sottoinsiemi di P. Il numero degli elementi di $\mathcal{E}$ disgiunti da T è il numero delle parole di peso w in B_0, e non dipende da T. Il complementare di $(P, \mathcal{E})$ è dunque un t-disegno. Per il problema 19C anche gli insiemi di $\mathcal{E}$ formano i blocchi di un t-disegno. Questo dimostra il secondo asserto. Osservazione: si potrebbe obiettare che

l'argomento non vale per $w > n-t$. In tal caso, applicandolo a $t' := n-w$, si vede che o ogni sottoinsieme di cardinalità w è supporto di una parola di codice, oppure nessuno lo è. Le parole di peso w, se ve ne sono, formano quindi un t-disegno banale. (iv) Per il primo asserto procediamo per induzione. Partiamo da $w = d$. Sia $\mathcal{D}$ la famiglia delle parole di peso d in A. Il numero degli insiemi di $\mathcal{D}$ che contengono un dato sottoinsieme T di cardinalità t è il numero delle parole di peso $d-t$ in A'; come abbiamo visto, esso non dipende da T. Quindi $\mathcal{D}$ è un t-disegno. Sia ora $w > d$ e supponiamo l'asserto vero per ogni w' con $d \le w' < w$.[1] Sia $\mathcal{D}$ la famiglia delle parole di peso w in A. Il numero dei suoi insiemi che contengono T è il numero delle parole di peso $w-t$ in A' corrispondenti a parole di peso w in A. Per (ii), il numero totale delle parole di peso $w-t$ in A' è indipendente da T.[2] Per l'ipotesi induttiva e per la (19.6), anche il numero di quelle corrispondenti a parole di peso minore di w in A non dipende da T. Ne segue l'asserto. □ Orig. 252

Problema 20G. Qual è l'enumeratore dei pesi del duale del codice binario di Hamming di lunghezza $2^r - 1$? Ricavare un'espressione per l'enumeratore dei pesi del codice di Hamming stesso.

Esempio 20.4. Sia A il codice binario di Hamming esteso $[8, 4]$. Sappiamo che $A = A^{\perp}$. Nella notazione del teorema 20.4 abbiamo $d = 4$. Prendiamo $t = 3$: le ipotesi del teorema sono soddisfatte. Le parole di peso 4 formano quindi un 3-disegno, precisamente il disegno di Hadamard 3-$(8, 4, 1)$ corrispondente a $R(1, 3)$.

Esempio 20.5. Dopo il prossimo esempio tratteremo il famoso codice binario di Golay e mostreremo che il codice esteso corrispondente G_{24} è un codice autoduale $[24, 12, 8]$ con pesi 0, 8, 12, 16 e 24. Per il teorema 20.4 le parole di peso 8 formano quindi un 5-disegno. Dal problema 20E sappiamo che i blocchi sono 759, e la (19.1) dà $\lambda = 1$. Ciò segue anche dal fatto che il codice ha distanza 8, per cui due blocchi hanno al più quattro punti in comune. È il disegno di Witt $S(5, 8, 24)$ menzionato nel capitolo 19. Anche le parole degli altri pesi danno 5-disegni.

Esempio 20.6. I seguenti 5-disegni, e diversi altri, furono trovati da V. Pless (1972). Consideriamo la matrice di Paley C, di ordine 18, data dalla (18.5). Consideriamo un codice ternario $[36, 18]$, indicato con Sym_{36}, con generatrice $G = (I_{18}\ C)$. Un tale codice si chiama *codice di simmetria*. Poiché C è una matrice di Paley, $GG^{\mathsf{T}} = O$, dunque Sym_{36} è autoduale. Ne segue che tutti i pesi del codice sono divisibili per 3. Affermiamo che ogni parola non nulla di Sym_{36} ha peso almeno 12. Poiché C è simmetrica, la matrice $(-C\ I_{18})$ è una matrice di controllo di parità e, per l'autodualità, è anche una matrice generatrice. Se $(\mathbf{a}, \mathbf{b})$, con $\mathbf{a}, \mathbf{b} \in \mathbb{F}_3^{18}$, è una parola di codice, lo è anche $(-\mathbf{b}, \mathbf{a})$. Pertanto, se esiste una parola di peso minore di 12, ne esiste una che è combinazione lineare di al più quattro righe di G. Queste combinazioni si controllano facilmente a mano nel modo seguente; il lettore dovrebbe farlo per esercizio. Il fatto che C sia una matrice di Paley e l'argomento della dimostrazione del teorema 18.1, usato anche nel problema 18B, mostrano che una combinazione lineare di una, due o tre righe di G, con coefficienti non nulli, ha peso rispettivamente 18, 12, oppure 12 o 15. Restano le combinazioni di quattro righe. Si usi ora il fatto che Q nella (18.5) è ciclica, per cui occorre esaminare soltanto poche combinazioni essenzialmente diverse. Si può anche aggiungere una riga allo schieramento usato nella dimostrazione del teorema 18.1. Entrambi i metodi richiedono poco lavoro e mostrano che il peso minimo è 12. Originariamente il controllo fu eseguito al calcolatore. Orig. 253

Applichiamo ora la generalizzazione del teorema 20.4 ai codici ternari. Prendendo le parole di un peso fissato in Sym_{36} — la generalizzazione vale per i pesi 12, 15, 18 e 21 — e sostituendo ciascuna parola con il suo supporto, otteniamo 5-disegni. Poiché $\mathbf{c}$ e $2\mathbf{c}$ danno lo stesso insieme, lo consideriamo un solo blocco.

Veniamo ora al più famoso dei codici binari: il *codice binario di Golay* G_{23}. Ne esistono moltissime costruzioni, alcune eleganti e corredate da brevi dimostrazioni delle proprietà. Ne mostreremo soltanto una, legata alla teoria dei disegni.

Consideriamo la matrice di incidenza N dell'unico disegno 2-$(11, 6, 3)$; si veda il problema 19D. Abbiamo $NN^{\mathsf{T}} = 3I + 3J$. Considerando N su $\mathbb{F}_2$, otteniamo $NN^{\mathsf{T}} = I + J$. Quindi N ha rango 10 e l'unico vettore non nullo $\mathbf{x}$ con $\mathbf{x}N = \mathbf{0}$ è $\mathbf{1}$. Le proprietà del disegno implicano immediatamente che ogni riga ha peso 6 e che la somma di due righe di N ha peso 6. Sappiamo inoltre che la somma di tre o quattro righe di N non è nulla. Sia ora G la matrice 12×24 su $\mathbb{F}_2$ data da $G = (I_{12}\ P)$, dove Orig. 254

[1] Nota di traduzione: l'originale inverte gli estremi dell'ipotesi induttiva scrivendo $w \ge w' > d$.

[2] Nota di traduzione: il rinvio originale è a (iii); il risultato sull'enumeratore dei pesi di A' è dimostrato in (ii).

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & N & \\ 1 & & & \end{pmatrix}. \tag{20.13}$$

Ogni riga di G ha peso congruo a 0 modulo 4. Due righe qualsiasi hanno prodotto scalare 0. Ne segue che ogni combinazione lineare delle righe di G ha peso congruo a 0 modulo 4; lo si dimostri per induzione. Le osservazioni su N mostrano allora che ogni combinazione lineare non nulla delle righe di G ha peso almeno 8. Chiamiamo G_{24} il codice generato da G. Eliminando una coordinata qualsiasi otteniamo un codice binario $[23, 12]$ di distanza minima almeno 7. Per il problema 20A la distanza minima è esattamente 7 e, inoltre, il codice è perfetto! Lo indichiamo con G_{23}. Giustificheremo queste notazioni mostrando l'unicità di G_{24}, il *codice binario di Golay esteso*, dalla quale si può dedurre l'unicità di G_{23}.

Teorema 20.5. Se C è un codice binario di lunghezza 24, con $|C| = 2^{12}$, distanza minima 8 e $\mathbf{0} \in C$, allora C è equivalente a G_{24}.

Dimostrazione. (i) La parte difficile consiste nel mostrare che C deve essere lineare. Eliminando una coordinata qualsiasi si ottiene un codice C' di lunghezza 23 e distanza 7, con $|C'| = 2^{12}$. Per il problema 20E, l'enumeratore dei pesi di questo codice perfetto è determinato:

$$A_0 = A_{23} = 1, \quad A_7 = A_{16} = 253, \quad A_8 = A_{15} = 506, \quad A_{11} = A_{12} = 1288.$$

Poiché ciò vale qualunque sia la posizione eliminata, tutte le parole di C hanno peso 0, 8, 12, 16 oppure 24. Inoltre, cambiando l'origine, ossia sommando una parola fissata a tutte le parole del codice, deduciamo che anche la distanza fra due parole qualsiasi appartiene a $\{0, 8, 12, 16, 24\}$. Poiché tutti i pesi e tutte le distanze sono divisibili per 4, due parole qualsiasi hanno prodotto scalare 0. Le parole di C generano dunque un codice autoortogonale. Un tale codice può però avere al più 2^{12} parole. Pertanto C stesso è lineare e autoduale. (ii) Costruiamo una matrice generatrice di C scegliendo come prima riga una parola qualsiasi di peso 12. Dopo una permutazione delle posizioni abbiamo

Orig. 255

$$G = \left(\begin{array}{ccc|ccc} 1 & \cdots & 1 & 0 & \cdots & 0 \\ & A & & & B & \end{array} \right).$$

Sappiamo che ogni combinazione lineare non banale delle righe di B ha peso pari e non nullo; B ha quindi rango 11. Il codice generato da B è perciò il codice $[12, 11, 2]$ delle parole di peso pari. Possiamo dunque supporre che B sia I_{11} affiancata da una colonna di uni. Un'altra permutazione delle colonne dà una generatrice G' della forma $(I_{12}\ P)$, con P della stessa forma della (20.13). Che cosa sappiamo della matrice N? Ogni sua riga deve chiaramente avere peso 6. Inoltre la somma di due righe ha peso almeno 6. Per il problema 19D, N è la matrice di incidenza dell'unico disegno 2-$(11, 6, 3)$: dunque C è equivalente a G_{24}. □

Come abbiamo visto nell'esempio 20.5, le parole di peso 8 in G_{24} formano i blocchi del disegno di Witt $\mathcal{D} = S(5, 8, 24)$. Indichiamo con $\{0, 1, \ldots, 23\}$ il suo insieme dei punti e consideriamo $I = \{21, 22, 23\}$. Per il corollario al teorema 19.3, $\mathcal{D}_I$ è un $S(2, 5, 21)$, cioè un piano proiettivo di ordine 4, anch'esso noto essere unico. Il problema seguente mostra la bella struttura combinatoria di $\mathcal{D}$.

Problema 20H. Sia B un blocco di $\mathcal{D}$ con $|B \cap I| = \alpha$ e sia $B^* := B \setminus I$. Abbiamo visto che, per $\alpha = 3$, B^* è una retta di $PG_2(4)$. Mostrare che:

(i) se $\alpha = 2$, B^* è un'iperovale in $PG_2(4)$;

(ii) se $\alpha = 0$, B^* è la differenza simmetrica di due rette.

Il lettore ambizioso potrà mostrare che, per $\alpha = 1$, i sette punti di B^*, insieme alle rette di $PG_2(4)$ che contengono almeno due di essi, formano un piano di Fano. Un tale piano si chiama *sottopiano di Baer* di $PG_2(4)$.

Contando le iperovali, le coppie di rette e così via si può mostrare che ciascuna delle configurazioni geometriche menzionate è uno degli insiemi B^*. Una nota costruzione di $S(5, 8, 24)$ parte proprio da questi oggetti e produce il disegno aggiungendo opportuni sottoinsiemi di I. Se non si usa il gruppo degli automorfismi di $PG_2(4)$, questa costruzione è un problema combinatorio non banale. Ancora una volta, il lettore ambizioso dovrebbe cimentarvisi.

Orig. 256

Problema 20I. Sia $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$. Sia C il codice $[6, 3]$ su $\mathbb{F}_4$ con parole della forma

$$(a, b, c, f(1), f(\omega), f(\overline{\omega})),$$

dove $f(x) := ax^2 + bx + c$.

(i) Mostrare che C ha peso minimo 4 e nessuna parola di peso 5.

(ii) Sia G il codice binario le cui parole sono tutte le matrici $(0,1)$ A, di dimensione 4×6, con righe $\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_\omega, \mathbf{a}_{\overline{\omega}}$, tali che:

(1) ogni colonna di A abbia la stessa parità della prima riga $\mathbf{a}_0$;

(2) $\mathbf{a}_1 + \omega\mathbf{a}_\omega + \overline{\omega}\mathbf{a}_{\overline{\omega}} \in C$.

Mostrare che G è un codice $[24, 12, 8]$, cioè $G = G_{24}$ a meno di equivalenza.

Problema 20J. Come nell'esempio 20.6, costruire un codice ternario Sym_{12} usando la matrice di Paley C di ordine 6. Mostrare che Sym_{12} è autoduale con parametri $[12, 6, 6]$. Perforare il codice, cioè eliminarne una coordinata, ottenendo un codice ternario G_{11} con parametri $[11, 6, 5]$. Mostrare che è perfetto. È il *codice ternario di Golay.*

Abbiamo dato diversi esempi di disegni costruiti mediante un codice adatto. Invertiamo ora il procedimento e studiamo i codici generati dalle funzioni caratteristiche dei blocchi di un disegno. Sia N la matrice di incidenza di un piano proiettivo di ordine n. Consideriamo il sottospazio C di $\mathbb{F}_2^v$, con $v = n^2 + n + 1$, generato dalle righe di N. Se n è dispari, C non è molto interessante. Sommando infatti le righe di N che hanno un 1 in una posizione fissata, si ottiene una riga con 0 in quella posizione e 1 in tutte le altre. Questi vettori generano il codice $[v, v-1, 2]$ delle parole di peso pari, che deve coincidere con C, poiché C non ha parole di peso dispari. Per n pari il problema diventa più interessante. Ci limitiamo a $n \equiv 2 \pmod 4$.

Teorema 20.6. Se $n \equiv 2 \pmod 4$, le righe della matrice di incidenza N di un piano proiettivo di ordine n generano un codice binario C di dimensione $\frac{1}{2}(n^2 + n + 2)$.

Dimostrazione. (i) Poiché n è pari, il codice esteso $\overline{C}$ è autoortogonale: ogni retta ha un numero dispari di punti e due rette si incontrano in un punto. Quindi $\dim C \le \frac{1}{2}(n^2 + n + 2)$. (ii) Sia $\dim C = r$ e sia $k := n^2 + n + 1 - r = \dim C^\perp$. Sia H una matrice di controllo di parità di C. Supponiamo di aver permutato le coordinate in modo che $H = (I_k \ P)$. Definiamo

Orig. 257

$$A := \begin{pmatrix} I_k & P \\ O & I_r \end{pmatrix}.$$

Interpretiamo le matrici $(0,1)$ N e A come matrici su $\mathbb{Q}$. Allora, a meno del segno del determinante,

$$|\det NA^{\mathsf{T}}| = |\det N| = (n+1)n^{\frac{1}{2}(n^2+n)}.$$

[3] Poiché tutte le entrate delle prime k colonne di NA^{T} sono interi pari, $\det N$ è divisibile per 2^k. Quindi $\frac{1}{2}(n^2 + n) \ge k$, ossia $r \ge \frac{1}{2}(n^2 + n + 2)$. Il risultato segue da (i) e (ii). □

Il teorema mostra che il codice C generato dalle righe di N ha la proprietà che $\overline{C}$ è autoduale. Mostreremo ora una proprietà ancora più interessante: dal codice si può ricostruire il piano.

Teorema 20.7. Il codice C del teorema 20.6 ha peso minimo $n + 1$ e ogni parola di peso minimo corrisponde a una retta del piano di ordine n.

Dimostrazione. Come prima, interpretiamo una parola come un sottoinsieme del piano. Sarà quindi chiaro che cosa significhi dire che un punto appartiene alla parola $\mathbf{c}$. Sia $\mathbf{c}$ una parola di peso d. Poiché n è pari, le parole corrispondenti alle rette hanno simbolo di controllo di parità uguale a 1 nel codice esteso $\overline{C}$. Quest'ultimo è autoduale, perciò:

(1) se d è dispari, $\mathbf{c}$ incontra ogni retta almeno una volta;

(2) se d è pari e $\mathbf{c} \neq \mathbf{0}$, ogni retta per un punto fissato di $\mathbf{c}$ incontra $\mathbf{c}$ in un secondo punto.

Nel caso (2) vediamo subito che $d > n + 1$. Nel caso (1) troviamo $(n+1)d \ge n^2 + n + 1$, dunque $d \ge n + 1$. Se $w(\mathbf{c}) = n + 1$, esiste una retta L che incontra $\mathbf{c}$ in almeno tre punti. Se un punto di L non appartenesse a $\mathbf{c}$, ogni retta diversa da L passante per quel punto dovrebbe incontrare $\mathbf{c}$, per (1). Ne seguirebbe $d \ge n + 3$. Dunque $\mathbf{c}$ coincide con L. □

Ricordiamo che, in un piano proiettivo di ordine pari n, un'iperovale è un insieme di $n + 2$ punti, nessuna terna dei quali è allineata.

Orig. 258

[3] Nota di traduzione: l'originale scrive il determinante senza valore assoluto; il suo segno dipende dall'ordinamento di punti e rette e non influisce sull'argomento di divisibilità.

Teorema 20.8. Le parole di peso $n+2$ nel codice C del teorema 20.6 sono precisamente tutte le iperovali del piano.

DIMOSTRAZIONE. (i) Sia $\mathbf{v} \in C$ di peso $n+2$. Ogni retta incontra $\mathbf{v}$ in un numero pari di punti. Sia L una retta che ha $2a$ punti in comune con $\mathbf{v}$. Se $a > 0$, ciascuna delle n rette diverse da L per uno di questi punti incontra $\mathbf{v}$ almeno un'altra volta. Pertanto $2a + n \leq n + 2$, ossia $a = 1$; le sole possibilità sono dunque $a = 0$ e $a = 1$.

(ii) Sia V un'iperovale e sia S l'insieme delle sue $\binom{n+2}{2}$ secanti. Ogni punto non appartenente a V si trova su $\frac{1}{2}(n+2)$ secanti, mentre ogni punto di V si trova su $n+1$ secanti. Poiché $n \equiv 2 \pmod 4$, la somma delle parole corrispondenti alle secanti è la funzione caratteristica di V, che è quindi una parola di codice. □

Teoremi come questi due fornirono informazioni sufficienti sul codice corrispondente a un piano proiettivo di ordine 10 da rendere possibile la ricerca al calcolatore menzionata in precedenza. Il primo passo importante fu compiuto da F. J. MacWilliams, N. J. A. Sloane e J. G. Thompson (1973), che mostrarono che un tale codice non può avere parole di peso 15. Attualmente l'unico piano proiettivo noto di ordine $n \equiv 2 \pmod 4$ è il piano di Fano.

Problema 20K. Trovare una matrice 4×39 di 0, 1 e -1 tale che: (i) nessuna colonna sia nulla e nessuna sia uguale a un'altra moltiplicata per ± 1; (ii) ogni riga contenga 13 occorrenze di ciascuno dei simboli 0, 1, -1.

Generalizzare costruendo matrici di dimensione $r \times \left(\frac{1}{2}(3^r - 1) - 1\right)$ con le proprietà (i) e (ii), sostituendo 13 con il valore opportuno.

La matrice può essere usata per il seguente rompicapo. Fra 39 monete ve n'è una falsa che pesa più o meno delle altre. Si dispone di una bilancia a due piatti: collocando alcune monete su ciascun piatto si può stabilire quale sottoinsieme abbia peso totale maggiore. Occorre individuare la moneta falsa e stabilire se sia più leggera o più pesante mediante quattro pesate complessive.

Problema 20L. Körner e Simonyi chiamarono *trifferente* un codice su un alfabeto di $q > 2$ simboli le cui parole non siano soltanto distinte, ma tali che per ogni terna di parole esista una posizione in cui esse abbiano tre simboli diversi. Sia $F(n, q)$ il massimo numero di parole in un codice trifferente di lunghezza n. Dimostrare che $F(n, q) \geq 6^{-1/2}(q/3)^{n/2}$. Suggerimento: usare il teorema 3.6. Considerare un codice casuale con N parole. Per ogni sottoinsieme S di cardinalità 3 di $\{1, 2, \ldots, N\}$, sia A_S l'evento che le tre parole con indici in S non siano tutte distinte o non siano trifferenti. Mostrare che A_S ha probabilità $(3q(q-1)+q)^n/q^{3n}$, ecc.[4] Orig. 259

Note

In questo capitolo non ci siamo occupati delle proprietà di correzione degli errori. Per una trattazione sistematica della teoria dei codici rimandiamo a Van Lint (1999). Molto altro materiale sui rapporti fra teoria dei disegni e teoria dei codici si trova in Cameron e Van Lint (1991). Il miglior testo di riferimento sulla teoria dei codici è MacWilliams e Sloane (1977).

Per la storia delle origini della teoria dei codici rimandiamo a Thompson (1983). Vi sono controversie sulle priorità, ma è chiaro che sia R. W. Hamming sia M. J. E. Golay contribuirono alla «scoperta» di questa affascinante disciplina nel 1947 e 1948. Il fondamentale lavoro di C. E. Shannon (1948) diede realmente avvio agli sviluppi. Pare che Hamming fosse irritato dal fatto che il suo calcolatore continuasse a fermarsi ogni volta che rilevava un errore. Decise, giustamente, che se era capace di rilevare gli errori avrebbe dovuto anche individuarli e correggerli, per poi proseguire il lavoro! Golay pubblicò i due codici che portano il suo nome fornendone le matrici generatrici, ma senza dimostrarne le proprietà.

E. F. Assmus (1931–1998) morì tragicamente durante un convegno su codici e disegni in un luogo che amava, il Mathematisches Forschungsinstitut di Oberwolfach. Gran parte di questo capitolo si basa sui suoi numerosi contributi ai rapporti fra teoria dei codici e teoria dei disegni, spesso scritti con H. F. Mattson.

M. J. E. Golay (1902–1989) fu un fisico svizzero attivo in molti settori. È noto per i lavori sulla spettroscopia infrarossa e per l'invenzione della colonna capillare, ma ai matematici soprattutto per la scoperta dei due codici di Golay.

[4] Nota di traduzione: nell'originale l'insieme degli indici è scritto $\{1, \ldots, n\}$, ma le parole del codice sono N; si è corretto in $\{1, \ldots, N\}$.

Per ulteriori informazioni sui codici MDS rimandiamo a MacWilliams e Sloane (1977).

F. J. MacWilliams (1917–1990) diede molti contributi alla teoria dei codici, fra cui il più importante è il teorema che porta il suo nome. Il libro scritto con N. J. A. Sloane è il principale testo di riferimento della disciplina. Come molti importanti studiosi di teoria dei codici, trascorse gran parte della carriera ai Bell Laboratories. Orig. 260

Come abbiamo già osservato, il codice di Golay G_{24} ammette molte costruzioni. Ognuna mostra che un certo gruppo di permutazioni è contenuto nel gruppo degli automorfismi del codice. Per esempio, una delle costruzioni più comuni mette in evidenza un automorfismo di ordine 23. Poiché il codice è unico, il suo gruppo completo degli automorfismi deve contenere tutti questi gruppi come sottogruppi. In tal modo si può dimostrare che esso è il famoso *gruppo di Mathieu* M_{24}. Questo gruppo ha ordine $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$ e agisce in modo 5-transitivo sulle 24 posizioni delle parole di codice.

È stato dimostrato che non esistono altri codici perfetti correttori di e errori, con $e > 2$, oltre a quelli menzionati in questo capitolo. Per approfondimenti si veda Van Lint (1999); si veda anche il capitolo 30.

Bibliografia

E. F. Assmus, Jr. e H. F. Mattson, Jr. (1969), New 5-designs, *J. Combinatorial Theory* **6**, 122–151.

P. J. Cameron e J. H. van Lint (1991), *Designs, Graphs, Codes and their links*, London Math. Soc. Student Texts **22**, Cambridge University Press.

J. H. van Lint (1999), *Introduction to Coding Theory*, terza edizione, Springer-Verlag.

F. J. MacWilliams (1963), A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42**, 79–94.

F. J. MacWilliams e N. J. A. Sloane (1977), *The Theory of Error-Correcting Codes*, North-Holland.

F. J. MacWilliams, N. J. A. Sloane e J. G. Thompson (1973), On the existence of a projective plane of order 10, *J. Combinatorial Theory (A)* **14**, 66–78.

V. Pless (1972), Symmetry codes over GF(3) and new 5-designs, *J. Combinatorial Theory (A)* **12**, 119–142.

C. E. Shannon (1948), A mathematical theory of communication, *Bell Syst. Tech. J.* **27**, 379–423 e 623–656.

T. M. Thompson (1983), *From Error-Correcting Codes through Sphere Packings to Simple Groups*, Carus Math. Monograph **21**.

Capitolo 21

Grafi fortemente regolari e geometrie parziali

Un *grafo fortemente regolare* $\mathrm{srg}(v,k,\lambda,\mu)$ è un grafo con v vertici, regolare di grado k, che gode delle proprietà seguenti: Orig. 261

1. Per ogni coppia di vertici adiacenti x,y, vi sono esattamente λ vertici adiacenti sia a x sia a y.
2. Per ogni coppia di vertici non adiacenti x,y, vi sono esattamente μ vertici adiacenti sia a x sia a y.

Un esempio banale è il pentagono, un $\mathrm{srg}(5,2,0,1)$. Forse l'esempio più famoso è il grafo della Fig. 1.4, il *grafo di Petersen*, un $\mathrm{srg}(10,3,0,1)$.

È chiaro che un grafo formato dall'unione di m grafi completi K_k è un $\mathrm{srg}(km,k-1,k-2,0)$. Talvolta escluderemo gli esempi banali richiedendo che un grafo fortemente regolare e il suo complementare siano connessi, ossia supporremo

$$0<\mu<k<v-1. \tag{21.1}$$

(Osserviamo che il fatto che $\mu=0$ implichi che il grafo è un'unione di grafi completi si vede più facilmente dalla (21.4) qui sotto.) Non è difficile verificare che il complementare $\overline{G}$ di un $\mathrm{srg}(v,k,\lambda,\mu)$ G è un

$$\mathrm{srg}(v,v-k-1,v-2k+\mu-2,v-2k+\lambda), \tag{21.2}$$

e, poiché i parametri sono non negativi, otteniamo una semplice condizione sui parametri, precisamente

$$v-2k+\mu-2\geq 0. \tag{21.3}$$

Un'altra relazione fra i parametri si trova facilmente nel modo seguente. Consideriamo un vertice qualunque x e suddividiamo gli altri vertici nell'insieme $\Gamma(x)$ dei vertici uniti a x e nell'insieme $\Delta(x)$ dei vertici non uniti a x. Per la definizione di grafo fortemente regolare, $\Gamma(x)$ contiene k vertici, ciascuno dei quali è unito a λ vertici di $\Gamma(x)$. Ogni vertice di $\Delta(x)$ è unito a μ vertici di $\Gamma(x)$. Contando in due modi gli spigoli con un estremo in $\Gamma(x)$ e uno in $\Delta(x)$, troviamo Orig. 262

$$k(k-\lambda-1)=\mu(v-k-1). \tag{21.4}$$

Problema 21A. Mostrare che un grafo fortemente regolare è estremale nel senso seguente. Sia G un grafo con v vertici, ciascuno di grado al più k. Supponiamo che ogni coppia di vertici adiacenti, rispettivamente non adiacenti, abbia almeno λ, rispettivamente μ, vicini comuni. Allora

$$k(k-1-\lambda)\geq\mu(v-k-1),$$

e l'uguaglianza implica che G è fortemente regolare.

Prima di addentrarci nell'affascinante teoria di questi grafi, menzioniamo alcune classi di esempi.

Esempio 21.1. Il *grafo triangolare* $T(m)$, $m\geq 4$, ha come vertici i sottoinsiemi di due elementi di un insieme di cardinalità m; due vertici distinti sono adiacenti se e solo se non sono disgiunti. $T(m)$ è un $\mathrm{srg}\big(\binom{m}{2},2(m-2),m-2,4\big)$. Il grafo di Petersen è $\overline{T(5)}$ (si veda il Problema 1A).

Esempio 21.2. Il *grafo reticolare* $L_2(m)$, $m \geq 2$, ha come insieme dei vertici $S \times S$, dove S è un insieme di cardinalità m; due vertici distinti sono adiacenti se e solo se hanno una coordinata in comune. $L_2(m)$ è un $\mathrm{srg}(m^2, 2(m-1), m-2, 2)$. $L_2(2)$ è un quadrilatero, che costituisce un esempio banale perché il suo complementare non è connesso.

Esempio 21.3. Sia q una potenza di un primo con $q \equiv 1 \pmod 4$. Il *grafo di Paley* $P(q)$ ha come vertici gli elementi di $\mathbb{F}_q$; due vertici sono adiacenti se e solo se la loro differenza è un quadrato non nullo in $\mathbb{F}_q$. Il fatto che questo sia un $\mathrm{srg}\big(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1)\big)$ è una conseguenza diretta della (18.4), ma è più semplice dimostrarlo usando la matrice Q della (18.5), come vedremo qui sotto. Si noti che $P(5)$ è il pentagono. Orig. 263

Esempio 21.4. Il *grafo di Clebsch* ha come vertici tutti i sottoinsiemi di cardinalità pari dell'insieme $\{1, \dots, 5\}$; due vertici sono uniti se e solo se la loro differenza simmetrica ha cardinalità 4. Questo è un $\mathrm{srg}(16, 5, 0, 2)$. Si possono anche descrivere i vertici come le parole di peso pari in $\mathbb{F}_2^5$, con uno spigolo quando la distanza è 4. Per ogni vertice x, il sottografo indotto su $\Delta(x)$ è il grafo di Petersen. Si veda la Fig. 21.1 qui sotto.

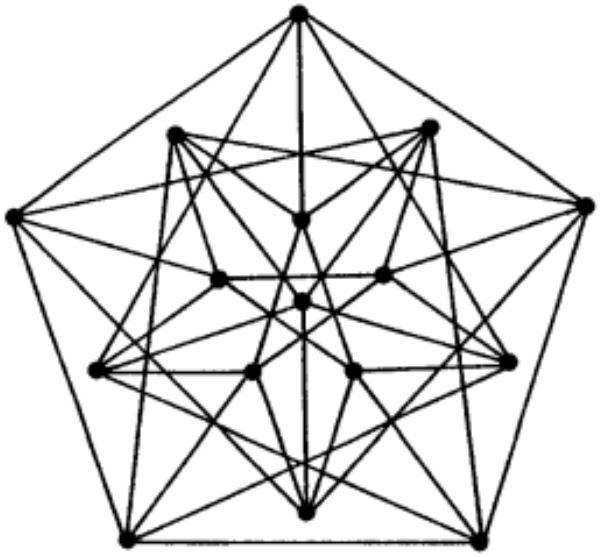


Figura 21.1

Definiamo la *matrice di adiacenza* A di un grafo G con v vertici $1, \dots, v$ come la matrice $(0,1)$ di ordine v con $a_{ij} = a_{ji} = 1$ se e solo se i vertici i e j sono uniti. Chiaramente A è simmetrica e ha zeri sulla diagonale. L'affermazione che G sia un $\mathrm{srg}(v, k, \lambda, \mu)$ equivale a

$$AJ = kJ, \qquad A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J. \tag{21.5}$$

Se Q è la matrice che compare nella (18.5), allora, per la (18.4), abbiamo $Q^2 = qI - J$, e la matrice di adiacenza del grafo $P(q)$ definito nell'Esempio 21.3 è $A = \frac{1}{2}(Q + J - I)$. Dunque A soddisfa la (21.5) con $k = \frac{1}{2}(q-1)$, $\lambda = \frac{1}{4}(q-5)$, $\mu = \frac{1}{4}(q-1)$.

Abbiamo già incontrato un collegamento fra i grafi fortemente regolari e gli argomenti trattati nei capitoli precedenti. Ne seguiranno diversi altri. La teoria dei grafi fortemente regolari mostra un aspetto della teoria dei grafi completamente diverso da quello studiato nei Capitoli 1–4 e 8. Ora faremo ampio ricorso a metodi algebrici. Vogliamo nondimeno illustrare anche alcuni eleganti argomenti di conteggio che si impiegano in questa teoria. Orig. 264

Definiamo l'*algebra di Bose–Mesner* $\mathcal{A}$ di un grafo fortemente regolare G come l'algebra tridimensionale delle combinazioni lineari di I, J e A. Che si tratti effettivamente di un'algebra è conseguenza della (21.5). Questa algebra è formata da matrici simmetriche che commutano fra loro, e pertanto esiste una matrice ortogonale che le diagonalizza simultaneamente. Ciò si può anche vedere in modo elementare dalla (21.5). Nel prossimo teorema vedremo infatti che A ha tre distinti autospazi in $\mathbb{R}^v$ e che ciascuno di essi è un autospazio per ogni elemento di $\mathcal{A}$.

Teorema 21.1. Se esiste un $\mathrm{srg}(v,k,\lambda,\mu)$, i numeri

$$f := \frac{1}{2}\left(v-1+\frac{(v-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right)$$

e

$$g := \frac{1}{2}\left(v-1-\frac{(v-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right)$$

sono interi non negativi.

DIMOSTRAZIONE. Sia A la matrice di adiacenza del grafo. Per la (21.5), il vettore tutto uno $\mathbf{j} := (1,1,\ldots,1)^\top$ è un autovettore di A con autovalore k, ed è naturalmente anche un autovettore di I e di J. Applicando la (21.5) si ottiene una seconda dimostrazione della (21.4). La molteplicità di questo autovalore è uno, perché il grafo è connesso. Ogni altro autovettore, diciamo con autovalore x, è ortogonale a $\mathbf{j}$, e quindi dalla (21.5) ricaviamo

$$x^2+(\mu-\lambda)x+(\mu-k)=0.$$

Questa equazione ha due soluzioni

$$r,s = \frac{1}{2}\left(\lambda-\mu\pm\sqrt{(\lambda-\mu)^2+4(k-\mu)}\right). \tag{21.6}$$

Siano f e g le molteplicità di r e s come autovalori di A. Allora

Orig. 265

$$1+f+g=v \qquad \text{e} \qquad \mathrm{tr}(A)=k+fr+gs=0.$$

Risolvendo queste due equazioni lineari si ottiene l'asserto del teorema. □

Si noti che le molteplicità si possono esprimere anche come

$$f=\frac{-k(s+1)(k-s)}{(k+rs)(r-s)}, \qquad g=\frac{k(r+1)(k-r)}{(k+rs)(r-s)}. \tag{21.7}$$

Dalla (21.6) possiamo trarre un'ulteriore, sorprendente conclusione. Se $f\neq g$, la radice quadrata al denominatore delle espressioni di f e di g deve essere un intero, ossia $(\mu-\lambda)^2+4(k-\mu)$ è un quadrato perfetto. Dalla (21.6) segue allora che gli autovalori r e s sono interi!

L'altro caso, cioè quello in cui $f=g$, è solitamente chiamato *caso a metà* (*half-case*). Abbiamo allora un $\mathrm{srg}(4\mu+1,2\mu,\mu-1,\mu)$. I grafi di Paley ne sono esempi. Nel suo articolo sulla telefonia per conferenze, menzionato nel Capitolo 18, Belevitch osservò che una condizione necessaria per l'esistenza di una matrice di conferenza di ordine n è che $n-1$ sia somma di due quadrati. Si veda il Problema 19M. Notiamo che i parametri $v=21$, $k=10$, $\lambda=4$, $\mu=5$ soddisfano tutte le condizioni necessarie all'esistenza di un grafo fortemente regolare enunciate finora, ma il grafo non esiste: usando la (18.5), esso implicherebbe l'esistenza di una matrice di conferenza di ordine 22, e ciò è impossibile poiché 21 non è somma di due quadrati.

La condizione del Teorema 21.1 è nota come *condizione di integralità*. Chiameremo *ammissibile* un insieme di parametri (v,k,λ,μ) che soddisfi queste condizioni e le precedenti condizioni necessarie.

Problema 21B. Mostrare che, se esiste un $\mathrm{srg}(k^2+1,k,0,1)$, allora $k=1,2,3,7$ oppure 57. (Si vedano le note al Capitolo 4.)

Abbiamo visto che la matrice di adiacenza di un $\mathrm{srg}(v,k,\lambda,\mu)$ ha tre autovalori, uno dei quali è k. Vale un parziale viceversa: se G è un grafo connesso e regolare di grado k, la cui matrice di adiacenza A ha esattamente tre autovalori distinti, allora G è fortemente regolare. Questo è il Problema 31F del Capitolo 31. Per ottenere altri esempi di grafi fortemente regolari, consideriamo un ulteriore collegamento con un argomento già incontrato: i disegni combinatori. L'idea è dovuta a J.-M. Goethals e J. J. Seidel (1970). Un 2-disegno si dice *quasisimmetrico* se la cardinalità dell'intersezione di due blocchi distinti assume soltanto due valori distinti, diciamo $x>y$. Introduciamo un grafo, detto *grafo dei blocchi* del disegno: i vertici sono i blocchi del disegno e due vertici sono adiacenti se e solo se la loro intersezione ha cardinalità y.

Orig. 266

Teorema 21.2. Il grafo dei blocchi di un disegno quasisimmetrico è fortemente regolare.

DIMOSTRAZIONE. Sia N la matrice di incidenza $v \times b$ del disegno e sia A la matrice di adiacenza del suo grafo dei blocchi G. Usando i parametri v, k, b, r, λ del 2-disegno, abbiamo

$$NN^\top = (r-\lambda)I + \lambda J, \qquad N^\top N = kI + yA + x(J - I - A).$$

(La prima equazione è la (19.7), la seconda è la definizione di A.) Sappiamo che sia $NN^\top$ sia $N^\top N$ hanno autovettori tutto uno $\mathbf{j}$ (di lunghezze diverse!) con autovalore kr. Sappiamo inoltre che $NN^\top$ ha su $\mathbf{j}^\perp$ il solo autovalore $r-\lambda$, con molteplicità $v-1$. Pertanto $N^\top N$ ha questo stesso autovalore, con la stessa molteplicità, e l'autovalore 0 con molteplicità $b-v$. Poiché $x \neq y$, A è una combinazione lineare di I, J e $N^\top N$. Quindi A ha autovettore $\mathbf{j}$ e soltanto due autovalori sullo spazio $\mathbf{j}^\perp$. Essi sono $(r-\lambda+k+x)/(y-x)$ con molteplicità $v-1$ e $(x-k)/(y-x)$ con molteplicità $b-v$.[1] Per l'osservazione fatta sopra, G è fortemente regolare. □

Ora che sappiamo che G è fortemente regolare, è facile calcolarne i parametri. Omettiamo le poco gradevoli formule.

Esempio 21.5. Consideriamo l'$S(5,8,24)$ del Capitolo 20. Fissiamo due punti e consideriamo il disegno residuo rispetto a questi due punti.[2] È un 3-$(22,6,1)$. Dal Problema 20F sappiamo che i 21 blocchi di questo disegno contenenti un punto fissato sono le rette di $PG_2(4)$, una volta rimosso quel punto, e che i 56 blocchi che non lo contengono sono iperovali di questo piano. Essi formano un disegno 2-$(21,6,4)$. Dalle proprietà di $S(5,8,24)$ segue che due qualsiasi di queste iperovali si intersecano in 0 o in 2 punti. Orig. 267
Pertanto questo disegno derivato è quasisimmetrico. Dal Teorema 21.2 segue che il suo grafo dei blocchi è un $\mathrm{srg}(56,k,\lambda,\mu)$. Qui $k=10$, perché vi sono $45 = (4-1)\binom{6}{2}$ iperovali che intersecano un'iperovale data in 2 punti. Dalle proprietà del disegno, oppure dalle condizioni sui grafi fortemente regolari, si ricava poi facilmente che $\lambda = 0$ e $\mu = 2$. Il grafo costruito in questo esempio è noto come *grafo di Gewirtz*. Si noti che, se A è la sua matrice di adiacenza, per la (21.5) abbiamo $(I+A)^2 = 9I + 2J$: ciò significa che $N := I + A$ è la matrice di incidenza di un disegno 2-$(56,11,2)$, un cosiddetto *biplano*. Dunque, in questo caso, dal grafo fortemente regolare troviamo anche un nuovo disegno.

Problema 21C. Sia $D := (\mathcal{P}, \mathcal{B}, \mathcal{I})$ il disegno 3-$(22,6,1)$ menzionato sopra; esso è unico. Formiamo un grafo il cui insieme dei vertici è $\mathcal{P} \cup \mathcal{B} \cup \{\infty\}$. Il vertice ∞ è unito a ogni elemento di $\mathcal{P}$. Un elemento di $\mathcal{P}$ è unito a un elemento di $\mathcal{B}$ se essi sono incidenti. Infine, due elementi di $\mathcal{B}$ sono uniti se e solo se i blocchi sono disgiunti. Mostrare che così si definisce un $\mathrm{srg}(100,22,0,6)$. Questo grafo è chiamato *grafo di Higman–Sims*.

Se a questo punto compilassimo un elenco degli insiemi ammissibili di parametri dei grafi fortemente regolari, esso conterrebbe molti insiemi che non corrispondono a un grafo di questo tipo. Dimostreremo alcuni dei teoremi che li escludono. Ancora una volta i metodi sono algebrici. Come preparazione, il lettore provi a svolgere il problema seguente con argomenti puramente combinatori.

Problema 21D. Mostrare che non esiste un $\mathrm{srg}(28,9,0,4)$.

La non esistenza di questo grafo è una conseguenza del prossimo teorema, noto come *condizione di Krein*.

Teorema 21.3. Sia G un grafo fortemente regolare con matrice di adiacenza A, avente autovalori k, r, s. Allora

$$(r+1)(k+r+2rs) \leq (k+r)(s+1)^2,$$

e

$$(s+1)(k+s+2sr) \leq (k+s)(r+1)^2.$$

Orig. 268

DIMOSTRAZIONE. Sia $B := J - I - A$. Sappiamo che le matrici di $\mathcal{A}$ hanno tre autospazi comuni, rispettivamente di dimensioni $1, f, g$. Chiamiamoli V_0, V_1, V_2. Qui V_0 è lo spazio generato da $\mathbf{j}$, mentre V_1 e V_2 corrispondono agli autovalori r e s di A. Per $i = 0,1,2$, sia E_i la matrice della proiezione su V_i, cioè E_i ha autovalore 1 su V_i e 0 sugli altri due autospazi. Queste matrici costituiscono quella che si chiama una base di idempotenti minimali di $\mathcal{A}$.

[1] Nota redazionale: l'originale stampa $r-\lambda+k+x$. Dall'identità precedente $N^\top N = (k-x)I + (y-x)A + xJ$ si ottiene invece $r-\lambda-k+x$ al numeratore. Qui è mantenuta la formula stampata, segnalando esplicitamente il refuso.

[2] Nota redazionale: qui l'originale dice *residual*; l'operazione descritta, che produce un 3-$(22,6,1)$, è la derivazione rispetto ai due punti. La terminologia originale è conservata e il disallineamento è segnalato.

Consideriamo ora lo stesso insieme $\mathcal{A}$, ma prendiamo come moltiplicazione il prodotto di Hadamard (si veda il Problema 21E). È evidente che due matrici distinte fra I, A, B hanno prodotto O. Ogni matrice $(0,1)$ è idempotente per la moltiplicazione di Hadamard. Concludiamo quindi che $\mathcal{A}$ è chiusa rispetto a tale moltiplicazione e che le matrici I, A, B formano una base di idempotenti minimali.

Si noti che la definizione di E_i $(i = 0, 1, 2)$ implica

$$I = E_0 + E_1 + E_2, \qquad A = kE_0 + rE_1 + sE_2,$$

e

$$B = (v - k - 1)E_0 + (-r - 1)E_1 + (-s - 1)E_2.$$

Da queste relazioni possiamo esprimere le E_i in termini di I, A, B.

Consideriamo il comportamento delle matrici E_i rispetto al prodotto di Hadamard. Poiché formano una base di $\mathcal{A}$, abbiamo

$$E_i \circ E_j = \sum_{k=0}^{2} q_{ij}^k E_k,$$

dove q_{ij}^k è l'autovalore di $E_i \circ E_j$ su V_k. Il calcolo è laborioso, ma i numeri q_{ij}^k si possono esprimere in termini dei parametri di G usando le relazioni precedenti.

A questo punto ci occorre il risultato del Problema 21E. Il prodotto di Hadamard $E_i \circ E_j$ è una sottomatrice principale del prodotto di Kronecker $E_i \otimes E_j$. Quest'ultima matrice è idempotente, quindi i suoi autovalori sono 0 e 1. Per il teorema richiamato nel Problema 21E, gli autovalori q_{ij}^k devono essere compresi fra 0 e 1. Una volta eseguiti tutti i calcoli, risulta che tutte le disuguaglianze così ottenute, tranne due, sono già soddisfatte. Le due rimanenti sono $q_{11}^1 \geq 0$ e $q_{22}^2 \geq 0$: sono le due disuguaglianze dell'asserto. □

Orig. 269

Problema 21E. Siano A e B due matrici simmetriche $n \times n$, con autovalori rispettivamente $\lambda_1, \ldots, \lambda_n$ e $\mu_1, \ldots, \mu_n$. Determinare gli autovalori di $A \otimes B$. Definiamo il *prodotto di Hadamard* $A \circ B$ come la matrice di elementi $a_{ij}b_{ij}$. Mostrare che $A \circ B$ è una sottomatrice principale di $A \otimes B$. Che cosa si può concludere sugli autovalori di $A \circ B$?

Per apprezzare il prossimo teorema, il lettore si convinca anzitutto che l'insieme di parametri $(50, 21, 4, 12)$ è ammissibile e soddisfa le condizioni di Krein. Che cosa si dovrebbe contare per dimostrare che, nondimeno, esso non corrisponde a un grafo fortemente regolare?

Teorema 21.4. Siano k, r, s gli autovalori della matrice di adiacenza A di un $\mathrm{srg}(v, k, \lambda, \mu)$ e siano $1, f, g$ le loro molteplicità. Allora

$$v \leq \frac{1}{2}f(f+3) \qquad \text{e} \qquad v \leq \frac{1}{2}g(g+3).$$

Dimostrazione. Sia $B = J - I - A$ e siano E_i $(i = 0, 1, 2)$ le matrici della dimostrazione precedente. Poniamo

$$E_1 = \alpha I + \beta A + \gamma B.$$

Poiché E_1 è simmetrica, esiste una matrice ortogonale $(H_1\ K_1)$ tale che

$$E_1 = (H_1\ K_1)\begin{pmatrix} I & O \\ O & O \end{pmatrix}\begin{pmatrix} H_1^\top \\ K_1^\top \end{pmatrix} = H_1 H_1^\top.$$

Qui H_1 è una matrice $v \times f$ con $H_1^\top H_1 = I$. Consideriamo le righe di H_1 come v vettori in $\mathbb{R}^f$. Ne segue che ciascuno di questi vettori ha lunghezza $\alpha^{1/2}$ e che due vettori distinti di questo insieme, che chiameremo S, hanno prodotto scalare β oppure γ. Un insieme di questo tipo si chiama *insieme sferico a due distanze*, perché possiamo interpretare S come un insieme di punti su una sfera con soltanto due distanze angolari distinte. Dobbiamo mostrare che la cardinalità di S è al più $\frac{1}{2}f(f+3)$.

Normalizzando otteniamo un insieme S' di v vettori sulla sfera unitaria Ω di $\mathbb{R}^f$, con soltanto due prodotti scalari, diciamo b e c. Per ogni $\mathbf{v} \in S'$ definiamo una funzione $f_\mathbf{v} : \Omega \to \mathbb{R}$ mediante

$$f_\mathbf{v}(\mathbf{x}) := \frac{(\langle \mathbf{v}, \mathbf{x}\rangle - b)(\langle \mathbf{v}, \mathbf{x}\rangle - c)}{(1-b)(1-c)}.$$

Queste funzioni sono polinomi di grado 2 nelle coordinate di $\mathbf{x}$. Se $\mathbf{v}, \mathbf{w} \in S$ e $\mathbf{v} \neq \mathbf{w}$, allora $f_\mathbf{v}(\mathbf{v}) = 1$

Orig. 270

e $f_{\mathbf{v}}(\mathbf{w}) = 0$.[3] Pertanto queste funzioni sono linearmente indipendenti. Gli spazi delle forme omogenee lineari e quadratiche su Ω hanno dimensioni rispettivamente f e $\frac{1}{2}f(f+1)$; poiché $x_1^2 + \cdots + x_f^2 = 1$ su Ω, possiamo esprimere le costanti mediante forme di grado 2 e 1. Dall'indipendenza lineare delle funzioni $f_{\mathbf{v}}$ segue che ve ne possono essere al più $f + \frac{1}{2}f(f+1) = \frac{1}{2}f(f+3)$. □

Questo teorema è noto come *limite assoluto*. A. Neumaier (1980) dimostrò che esso si può migliorare in

$$v \le \frac{1}{2}f(f+1) \quad \text{a meno che } q_{11}^1 = 0,$$

e analogamente per l'altra disuguaglianza.

Prima di passare alla relazione fra grafi fortemente regolari e certe strutture d'incidenza, mostriamo che anche eleganti argomenti di conteggio hanno un ruolo in questo ambito.

Teorema 21.5. Sia G un grafo fortemente regolare con gli stessi parametri di $T(n)$, ossia $G = \mathrm{srg}\binom{n}{2}, 2(n-2), n-2, 4\big)$. Se $n > 8$, allora G è isomorfo a $T(n)$.

Dimostrazione. Fissiamo un vertice x e indichiamo con Γ il sottografo indotto su $\Gamma(x)$. È un grafo regolare su $2(n-2)$ vertici, di grado $n-2$. Siano y e z vertici non adiacenti di Γ e siano m i vertici di Γ adiacenti a entrambi. Poiché $\mu = 4$ e x è adiacente a y e a z, abbiamo $m \le 3$. Nel grafo Γ vi sono $n-2-m$ vertici adiacenti a y ma non a z, e altrettanti adiacenti soltanto a z. Vi sono dunque $m-2$ vertici adiacenti a nessuno dei due. Quindi $m \ge 2$. Supponiamo $m = 3$. Consideriamo l'unico vertice w adiacente né a y né a z. Ogni vertice adiacente a w in Γ è adiacente a y oppure a z, il che implica $n-2 \le 3+3 = 6$, una contraddizione. Pertanto $m = 2$, e vediamo anche che il complementare $\overline{\Gamma}$ non contiene triangoli.

Mostriamo ora che $\overline{\Gamma}$ è bipartito. Supponiamo, per assurdo, che contenga un circuito di lunghezza dispari. Scegliamo un tale circuito $C = (x_0, x_1, \ldots, x_k = x_0)$ con k minimo. Dall'argomento precedente sappiamo che $k \ne 3$. Nel grafo Γ i vertici x_0 e x_1 non sono adiacenti e sono entrambi adiacenti a $x_3, x_4, \ldots, x_{k-2}$. Per quanto appena mostrato, $k \le 6$ e, poiché k è dispari, $k = 5$. Il vertice x_0 ha grado $n-3$ in $\overline{\Gamma}$, ossia è adiacente a $n-5$ vertici oltre a x_1 e x_4. Questi devono essere non adiacenti in $\overline{\Gamma}$ sia a x_1 sia a x_4. Un'affermazione analoga per x_2 fornisce $n-5$ vertici esterni a C non adiacenti in $\overline{\Gamma}$ sia a x_1 sia a x_3. Vi sono esattamente $n-4$ vertici esterni a C non adiacenti a x_1; vi sono quindi almeno $n-6$ vertici non adiacenti in $\overline{\Gamma}$ sia a x_3 sia a x_4. Il risultato del primo paragrafo implica $n-6 \le 1$, una contraddizione. Orig. 271

Il risultato del secondo paragrafo significa che Γ contiene due cricche disgiunte, cioè insiemi di vertici a due a due adiacenti, di cardinalità $n-2$. Poiché x era arbitrario, abbiamo mostrato che ogni vertice di G appartiene a due cricche di cardinalità $n-1$, che chiameremo *grandi cricche*. Lo stesso argomento mostra che ogni spigolo appartiene a una di esse. Il numero delle grandi cricche è $2\binom{n}{2}/(n-1) = n$. Poiché due grandi cricche hanno al più un vertice in comune, devono averne esattamente uno. Se consideriamo le grandi cricche come "punti" e i vertici come "blocchi", abbiamo appena mostrato che essi formano un disegno 2-$(n, 2, 1)$, cioè il disegno banale costituito da tutte le coppie di un insieme di n elementi. G è il grafo dei blocchi di questo disegno, ed è dunque effettivamente isomorfo a $T(n)$. □

Osserviamo che il teorema si può dimostrare, per analisi dei casi, anche per $n < 8$, e che per $n = 8$ esistono altri tre grafi con i parametri di $T(8)$, noti come *grafi di Chang*.

Problema 21F. Sia G un grafo fortemente regolare con gli stessi parametri di $L_2(n)$, ossia $G = \mathrm{srg}(n^2, 2(n-1), n-2, 2)$. Dimostrare che, se $n > 4$, allora G è isomorfo a $L_2(n)$.

R. C. Bose (1963) studiò le grandi cricche in grafi fortemente regolari più generali. Ciò lo condusse al concetto di *geometria parziale*. Una geometria parziale $\mathrm{pg}(K, R, T)$ è una struttura d'incidenza di punti e rette con le proprietà seguenti:

1. ogni retta contiene K punti e ogni punto appartiene a R rette;
2. due punti qualsiasi sono incidenti con al più una retta;
3. se il punto p non appartiene alla retta L, vi sono esattamente T rette per p che intersecano L.

Se due punti x, y appartengono a una retta, diciamo che sono *collineari* e scriviamo $x \sim y$. Orig. 272

Problema 21G. Determinare il numero di punti e di rette di una geometria parziale $\mathrm{pg}(K, R, T)$.

[3] Nota redazionale: dopo la normalizzazione, l'insieme pertinente è S'; l'originale torna qui alla lettera S.

Scambiando i ruoli di punti e rette in una $\mathrm{pg}(K,R,T)$ otteniamo la cosiddetta *geometria parziale duale*, una $\mathrm{pg}(R,K,T)$.

Introduciamo il *grafo dei punti* di una geometria parziale: i vertici sono i punti della geometria e $\{x,y\}$ è uno spigolo se e solo se $x \sim y$.

Problema 21H. Mostrare che il grafo dei punti di una $\mathrm{pg}(K,R,T)$ è un $\mathrm{srg}(v,k,\lambda,\mu)$, eventualmente banale, con

$$\begin{aligned} v &= K\left(1+\frac{(K-1)(R-1)}{T}\right), & k &= R(K-1),\\ \lambda &= (K-2)+(R-1)(T-1), & \mu &= RT,\\ r &= K-1-T, & s &= -R. \end{aligned}$$

Se un grafo fortemente regolare ha parametri tali da poter essere il grafo dei punti di una geometria parziale, lo si chiama *pseudogeometrico*; lo si dice *geometrico* se è effettivamente il grafo dei punti di una geometria parziale. L'idea, usata sopra, di introdurre grandi cricche e poi mostrare che esse e i punti formano un disegno fu impiegata da Bose per dimostrare il teorema seguente.

Teorema 21.6. Se un grafo fortemente regolare è pseudogeometrico, corrispondente a $\mathrm{pg}(K,R,T)$, e se

$$2K > R(R-1)+T(R+1)(R^2-2R+2),$$

allora il grafo è geometrico.

Non ne diamo qui la dimostrazione. Le idee della dimostrazione furono estese da A. Neumaier (1979); dopo un miglioramento dovuto ad A. E. Brouwer, il suo risultato assunse la forma seguente, nota come *limite della zampa* (*claw bound*).

Orig. 273

Teorema 21.7. Se, per un grafo fortemente regolare con i consueti parametri, $\mu \neq s^2$ e $\mu \neq s(s+1)$, allora $2(r+1) \leq s(s+1)(\mu+1)$.

L'idea della dimostrazione è mostrare, mediante argomenti di conteggio, che se r è grande il grafo è il grafo dei punti di una geometria parziale. Si applicano poi il limite assoluto e le condizioni di Krein al grafo dei punti della geometria parziale duale. Ne segue la disuguaglianza che afferma che r non può essere troppo grande.

I parametri $(2058, 242, 91, 20)$ sono ammissibili e soddisfano tutte le altre condizioni necessarie enunciate in questo capitolo, ma non il limite della zampa. Dunque un grafo con questi parametri non esiste.

Problema 21I. Considerare un $\mathrm{srg}(v,k,\lambda,1)$. Mostrare che il sottografo indotto su $\Gamma(x)$ è un'unione di cricche. Contare le cricche di cardinalità $\lambda+2$ del grafo. Mostrare così che sia $k/(\lambda+1)$ sia $vk/\{(\lambda+1)(\lambda+2)\}$ sono interi. Applicare il risultato all'insieme $(209, 16, 3, 1)$.

Le geometrie parziali si possono suddividere in quattro classi:

1. Una geometria parziale con $T = K$ è un disegno 2-$(v,K,1)$.
2. Una geometria parziale con $T = R-1$ si chiama *rete*; dualmente, se $T = K-1$, si parla di *disegno trasversale*.
3. Una geometria parziale con $T = 1$ si chiama *quadrangolo generalizzato*; per una $\mathrm{pg}(K,R,1)$ si usa comunemente la notazione $GQ(K-1,R-1)$.
4. Se $1 < T < \min\{K-1, R-1\}$, la geometria parziale si dice *propria*.

Esempio 21.6. Consideriamo il piano affine $AG_2(n)$. Dal Problema 19K sappiamo che le rette si possono suddividere in classi di equivalenza di rette parallele, ciascuna contenente n rette. Consideriamo tutti i punti del piano e prendiamo le rette di m classi di parallelismo. È chiaro che esse formano una $\mathrm{pg}(n,m,m-1)$, cioè una rete.

Esempio 21.7. Consideriamo un quadrato latino di ordine n. Prendiamo le sue n^2 celle come vertici di un grafo; due vertici sono uniti da uno spigolo se e solo se si trovano nella stessa riga, nella stessa colonna, oppure contengono lo stesso simbolo. Il grafo è regolare di grado $3(n-1)$. Se due vertici sono uniti, possiamo supporre senza perdita di generalità che si trovino nella stessa riga: basta pensare al

quadrato latino come a un $OA(n,3)$. Essi hanno allora $n-2$ vicini comuni.[4] Se due vertici non sono uniti, è chiaro che hanno sei vicini comuni. Si tratta dunque di un $\mathrm{srg}(n^2, 3(n-1), n-2, 6)$. Questo si chiama *grafo di un quadrato latino* e si indica con $L_3(n)$, in accordo con la notazione dell'Esempio 21.2. In un capitolo successivo ne incontreremo generalizzazioni. Il grafo $L_3(n)$ è geometrico e corrisponde a una geometria parziale $\mathrm{pg}(n,3,2)$, cioè a una rete. Naturalmente le rette corrispondono alle righe, alle colonne e ai simboli del quadrato. Vedremo nel Capitolo 22 che reti e schieramenti ortogonali sono in effetti concetti equivalenti. Orig. 274

Esempio 21.8. Un quadrilatero soddisfa le condizioni di una geometria parziale. È una $\mathrm{pg}(2,2,1)$, il che spiega il nome di quadrangolo generalizzato.

Consideriamo un'iperovale $\mathcal{O}$ in $PG_2(4)$. Prendiamo come insieme dei punti i 15 punti del piano che non appartengono a $\mathcal{O}$, e come rette le secanti di $\mathcal{O}$. Ogni retta contiene allora 3 punti e ogni punto appartiene a 3 rette. Si tratta effettivamente di una $\mathrm{pg}(3,3,1)$, ossia $GQ(2,2)$.

Si noti che la stessa costruzione, applicata a $PG_2(q)$ per q pari, fornisce una $\mathrm{pg}\big(q-1, \frac{1}{2}(q+2), \frac{1}{2}(q-2)\big)$.

Esempio 21.9. Consideriamo $PG_2(q)$, con q pari. Come nell'Esempio 19.7, si tratta di una struttura d'incidenza i cui oggetti sono i sottospazi di dimensione 1 e 2 di $\mathbb{F}_q^3$. Sia di nuovo $\mathcal{O}$ un'iperovale nel piano proiettivo. Prendiamo come rette tutti i sottospazi unidimensionali appartenenti a $\mathcal{O}$ e le loro classi laterali in $\mathbb{F}_q^3$; i punti sono quelli dello spazio vettoriale. Ogni retta contiene q punti e ogni punto appartiene a $q+2$ rette. Il fatto che $\mathcal{O}$ sia un'iperovale implica che per ogni punto p esterno a una retta L esiste un'unica retta per p che incontra L. Abbiamo dunque definito un $GQ(q-1, q+1)$.

Esempio 21.10. Consideriamo il sottogruppo G di $\mathbb{Z}_3^6$ generato dall'elemento $(1,1,1,1,1,1)$. Per ogni classe laterale $\mathbf{a}+G$, la somma delle coordinate dei punti è una costante i. Diciamo che la classe è di *tipo* i. Sia A_i l'insieme delle classi laterali di G di tipo i. Definiamo un grafo tripartito Γ unendo la classe $\mathbf{a}+G$ alla classe $\mathbf{a}+\mathbf{b}+G$ per ogni $\mathbf{b}$ con una sola coordinata non nulla. Chiaramente ogni elemento di A_i ha sei vicini in A_{i+1} e sei in A_{i+2}. Costruiamo una geometria parziale prendendo un A_i come insieme dei punti e una delle altre due classi A_j come insieme delle rette. L'incidenza corrisponde all'adiacenza. Che $K = R = 6$ è chiaro; mostrare che $T = 2$ è un facile esercizio. Si definisce così una $\mathrm{pg}(6,6,2)$. Orig. 275

Diamo ora un'elegante applicazione del Teorema 21.5. Dimostreremo il teorema, citato senza dimostrazione nel Capitolo 19, secondo cui un disegno quasiresiduo con $\lambda = 2$ è un disegno residuo. Poiché i casi $k \le 6$ richiedono un trattamento separato, ci limitiamo a blocchi di cardinalità maggiore di 6.

Teorema 21.8. Sia D un disegno 2-$(v,k,2)$ con $k > 6$ e $v = \frac{1}{2}k(k+1)$, dunque quasiresiduo. Allora D è un residuo di un 2-disegno simmetrico.

Dimostrazione. Sia B un blocco e sia a_i il numero dei blocchi diversi da B che intersecano B in i punti. Come nel Teorema 19.9 troviamo

$$\sum a_i = \frac{1}{2}k(k+3), \quad \sum i a_i = k(k+1), \quad \sum i(i-1)a_i = k(k-1).$$

Ne segue $\sum (i-1)(i-2)a_i = 0$. Quindi due blocchi distinti si intersecano in 1 o in 2 punti, ossia D è quasisimmetrico. Dal Teorema 21.2 ricaviamo che il grafo dei blocchi G di D è fortemente regolare. Il calcolo dei parametri mostra che G ha gli stessi parametri di $T(k+2)$. Per il Teorema 21.5, G è dunque isomorfo a $T(k+2)$. Ciò significa che possiamo etichettare i blocchi di D con sottoinsiemi di due elementi di $S := \{1, 2, \ldots, k+2\}$, in modo che due blocchi si intersechino in i punti quando le loro etichette si intersecano in $2-i$ punti $(i = 1, 2)$. Aggiungiamo S all'insieme dei punti di D e a ciascun blocco aggiungiamo la sua etichetta, un sottoinsieme di due elementi di S. Infine consideriamo S come nuovo blocco. Otteniamo così il disegno simmetrico richiesto, con $\lambda = 2$, che ha D come residuo rispetto al blocco S. □

Elenchiamo qui sotto gli insiemi ammissibili di parametri con $v < 30$ e quanto abbiamo appreso su di essi in questo capitolo. L'unico lasciato come sfida al lettore è il n. 14, cioè $GQ(2,4)$, di cui non abbiamo dato una costruzione. Il grafo corrispondente è noto come grafo di Schläfli.[5] Orig. 276

[4] Nota redazionale: l'originale omette qui due vicini comuni esterni alla riga. Il valore corretto è n; coerentemente, nella formula successiva va letto $\lambda = n$ anziché $n-2$. Il refuso si riscontra anche confrontando il caso $L_3(5)$ nella tabella di p. 276, dove compare correttamente $\lambda = 5$.

[5] Nota redazionale: nella terminologia usuale il grafo di Schläfli ha parametri $(27, 16, 10, 8)$ ed è il complementare del grafo dei punti di $GQ(2,4)$, che ha parametri $(27, 10, 1, 5)$. È conservata l'attribuzione dell'originale.

N.	v	k	λ	μ	Esempio
1	5	2	0	1	$P(5)$
2	9	4	1	2	$L_2(3)$
3	10	3	0	1	Petersen, $\overline{T(5)}$
4	13	6	2	3	$P(13)$
5	15	6	1	3	$GQ(2,2)$
6	16	5	0	2	Clebsch
7	16	6	2	2	$L_2(4)$
8	17	8	3	4	$P(17)$
9	21	10	3	6	$\overline{T(7)}$
10	21	10	4	5	non esiste, matrice di conferenza
11	25	8	3	2	$L_2(5)$
12	25	12	5	6	$L_3(5)$
13	26	10	3	4	$STS(13)$, Teorema 21.2
14	27	10	1	5	$GQ(2,4)$
15	28	9	0	4	non esiste, Teoremi 21.3, 21.4
16	28	12	6	4	$T(8)$
17	29	14	6	7	$P(29)$

Diamo alcune osservazioni sui grafi orientati fortemente regolari e alcuni problemi.

La condizione sui cammini di lunghezza 2 nella definizione di grafo fortemente regolare si vede meglio scrivendo la (21.5) nella forma

$$AJ = kJ, \qquad A^2 = kI + \lambda A + \mu(J - I - A). \tag{21.5'}$$

A. Duval (1988) generalizzò la definizione ai grafi orientati. Consideriamo un grafo orientato G senza cappi né spigoli multipli. Se vi è uno spigolo da a a b, scriviamo $a \to b$. Ammettiamo spigoli in entrambe le direzioni, indicati con $a \leftrightarrow b$; in tal caso chiamiamo (a, b) uno spigolo non orientato. La generalizzazione della (21.5') resta la stessa per quanto riguarda i cammini di lunghezza 2, ma ora richiediamo che ogni vertice abbia grado entrante k, grado uscente k e che fra questi spigoli vi siano t spigoli non orientati, che producono cammini di lunghezza 2 da un vertice a se stesso. Dunque G si chiama *grafo orientato fortemente regolare* se la sua matrice di adiacenza A soddisfa

$$AJ = JA = kJ, \qquad A^2 = tI + \lambda A + \mu(J - I - A). \tag{21.8}$$

Per un tale grafo su v vertici useremo la notazione $\mathrm{dsrg}(v; k, t; \lambda, \mu)$.

Orig. 277

Esempio 21.11. Sia G il grafo su sei vertici formato dal triangolo orientato $1 \to 2 \to 3 \to 1$, dal triangolo orientato $1' \to 3' \to 2' \to 1'$ e dagli spigoli non orientati (i, i'), $i = 1, 2, 3$. Se C è la matrice circolante 3×3 con $c_{ij} = 1$ per $(i, j) = (1, 2), (2, 3), (3, 1)$ e 0 altrimenti, la matrice di adiacenza di G è

$$A = \begin{pmatrix} C & I \\ I & C^2 \end{pmatrix}.$$

Si verifica facilmente che A soddisfa la (21.8) con $k = 2$, $t = 1$, $\lambda = 0$, $\mu = 1$. Dunque G è un $\mathrm{dsrg}(6; 2, 1; 0, 1)$.

Problema 21J. Enunciare e dimostrare un analogo del Teorema 21.1 per i grafi orientati fortemente regolari.

Problema 21K. Escludere i grafi fortemente regolari e i grafi con matrice di adiacenza $J - A$. Mostrare che gli autovalori calcolati nel Problema 21J conducono a un analogo del "caso a metà" se $(\mu-\lambda)^2+4(t-\mu)$ non è il quadrato di un intero. Dimostrare che in questo caso la matrice di adiacenza A del dsrg è del tipo della matrice Q della (18.5).[6]

Problema 21L. Considerare il caso $\mu = 1$, $\lambda = 0$, $t = k - 1$. Dimostrare che sono possibili soltanto tre valori di v. Mostrare che, nel secondo caso, si può ottenere un esempio da $K_{3,3}$ sostituendo opportunamente i vertici con triangoli orientati e gli spigoli con copie del grafo dell'Esempio 21.11.

Diamo ora alcuni commenti e problemi sui *grafi con intorni regolari*.

[6] Nota redazionale: la formulazione dell'originale è riprodotta fedelmente, ma richiede cautela: $J - A$ ha diagonale uno quando A ha diagonale nulla, e la Q della (18.5) è una matrice con segni. Il testo non chiarisce qui la normalizzazione o la trasformazione intesa.

In un grafo fortemente regolare G, gli intorni $\Gamma(x)$ e $\Delta(x)$ di x rispettivamente in G e nel complementare $\overline{G}$ sono grafi regolari. C. D. Godsil e B. D. McKay (1979) chiamarono *grafo con intorni regolari* ogni grafo che possiede questa proprietà. Non è difficile mostrare che un grafo con intorni regolari, se è anche regolare, è in effetti fortemente regolare. Se G o $\overline{G}$ non è connesso, si presentano situazioni banali. Nei problemi seguenti supponiamo che G abbia intorni regolari, che non sia regolare e che G e $\overline{G}$ siano connessi.

Orig. 278

Problema 21M.

(i) Mostrare che il grado di $\Gamma(x)$ non dipende da x. Indicare tale numero con a.

(ii) Mostrare che esiste un numero $\overline{a}$ tale che, per ogni x, il grado di $\overline{\Delta(x)}$ è $\overline{a}$.

Problema 21N. Se X e Y sono sottoinsiemi dell'insieme dei vertici di G, indichiamo con $|XY|$ il numero degli spigoli (x, y) di G con $x \in X$ e $y \in Y$. Siano x_1 e x_2 due vertici non adiacenti di G,[7] di gradi rispettivamente k_1 e k_2, con $k_1 \neq k_2$. Sia $d_i := \deg \Delta(x_i)$, $i = 1, 2$. Si noti che $d_1 \neq d_2$. Considerare i sottoinsiemi

$$A := \Gamma(x_1) \cap \Delta(x_2), \quad B := \Gamma(x_2) \cap \Delta(x_1),$$
$$C := \Gamma(x_1) \cap \Gamma(x_2), \quad D := \Delta(x_1) \cap \Delta(x_2).$$

(i) Trovare relazioni fra i numeri $|XY|$ e $|X|$, dove X, Y sono fra B, C, D.

(ii) Dedurre che $|DD| = (a + \overline{a} + 1)d_1 - d_1^2 - a|C| + |CC|$.

(iii) Dimostrare che $d_1 + d_2 = a + \overline{a} + 1$.

(iv) Mostrare che tutti i vertici di G hanno grado k_1 oppure k_2.

Esempio 21.12. Sia G l'ottagono sui vertici da 1 a 8, con le due diagonali (15) e (26). È un grafo con intorni regolari, con $k_1 = 2$, $k_2 = 3$, $a = 0$, $\overline{a} = 2$, $d_1 = 1$ e $d_2 = 2$.

Problema 21O. Dato un sistema di terne di Steiner S su n punti, definire un grafo G i cui vertici sono le terne $\mathcal{A}$ del sistema, e nel quale $A, B \in \mathcal{A}$ sono adiacenti quando $|A \cap B| = 1$.

(i) Mostrare con mezzi elementari, senza usare il Teorema 21.2 o metodi matriciali, che G è fortemente regolare e calcolarne i parametri.

(ii) Mostrare che, se C è una cricca di G e $|C| > 7$, allora C è un sottoinsieme delle terne contenenti un punto fissato x di S.

(iii) Usare questo risultato per mostrare che, se i grafi G_1 e G_2 provenienti da due sistemi di terne di Steiner su $n > 15$ punti sono isomorfi, allora anche i due sistemi sono isomorfi. Osserviamo che vi sono più di 163929929318400 sistemi di terne di Steiner non isomorfi su 25 punti, si veda R. M. Wilson (1973/74); abbiamo quindi almeno altrettanti grafi fortemente regolari non isomorfi su 100 vertici.

Orig. 279

Problema 21P. Mostrare che nel Problema 4H l'uguaglianza non può verificarsi a meno che $n = 3$.

Problema 21Q. Dimostrare il cosiddetto *teorema dell'amicizia*: a una festa con n persone, $n > 3$, ogni coppia di persone ha esattamente un amico comune. Allora vi è un'unica persona alla festa che è amica di tutte le altre. Usare il Problema 1J.

Note

I grafi fortemente regolari e le geometrie parziali furono introdotti da R. C. Bose nel 1963. Un concetto molto più generale, quello di schema di associazione, era stato introdotto da Bose e Shimamoto nel 1952; si vedano il Capitolo 30 di questo libro e Cameron e Van Lint (1991), Capitolo 17.

[7] Nota redazionale: l'originale dice "edges", ma qui si tratta evidentemente di vertici. È inoltre chiusa nella formula di D una parentesi mancante nell'originale.

Per una rassegna dei metodi di costruzione dei grafi fortemente regolari, si vedano Hubaut (1975) e Brouwer e Van Lint (1982).

Il grafo di Clebsch si può definire mediante le 16 rette della superficie quartica di Clebsch, dichiarando adiacenti due rette se e solo se sono sghembe. Alfred Clebsch (1833–1872) fu un matematico e fisico che lavorò a Karlsruhe, Giessen e Göttingen. Fu uno dei fondatori della celebre rivista *Mathematische Annalen*.

L'algebra $\mathcal{A}$ fu introdotta da R. C. Bose e D. M. Mesner nel 1959.

Il lavoro di Goethals e Seidel (1970) contiene, oltre al Teorema 21.2, molti collegamenti interessanti fra grafi fortemente regolari e altri disegni combinatori. Matrici di Hadamard, sistemi di Steiner e codice di Golay contribuiscono tutti alla teoria. Per questi collegamenti si veda ancora Cameron e Van Lint (1991).

Il grafo di Higman–Sims è connesso al loro famoso gruppo semplice finito (si veda Higman e Sims (1968)).

Il Teorema 21.3 divenne noto come condizione di Krein perché L. L. Scott ne dimostrò un caso particolare applicando a un problema sui gruppi finiti un risultato di M. G. Krein riguardante i gruppi topologici. La semplice dimostrazione data in questo capitolo è dovuta a D. G. Higman (1975) e P. Delsarte (1973). Il caso di uguaglianza nelle condizioni di Krein fu trattato da Delsarte, Goethals e Seidel (1977) e da Cameron, Goethals e Seidel (1978). Orig. 280

L'idea della dimostrazione del Teorema 21.4 è dovuta a T. H. Koornwinder (1976).

Il Teorema 21.5 fu dimostrato più volte: si vedano, per esempio, L. C. Chang (1959), W. S. Connor (1958), A. J. Hoffman (1960). I tre grafi eccezionali per $n = 8$ sono noti come grafi di Chang.

Per rassegne sulle geometrie parziali, si vedano Van Lint (1983), De Clerck e Van Maldeghem (1995), e De Clerck (2000).

Le reti furono introdotte da R. H. Bruck nel 1951. Il risultato di Bose sui grafi pseudogeometrici fu ispirato dal lavoro di Bruck, per esempio per l'idea delle grandi cricche.

Per tutto ciò che si desidera sapere sui quadrangoli generalizzati, e anche di più, rimandiamo al libro *Finite Generalized Quadrangles* di S. E. Payne e J. A. Thas (1984).

Sono note soltanto tre geometrie parziali proprie con $T = 2$. La geometria $\mathrm{pg}(6, 6, 2)$ dell'Esempio 21.9[8] fu costruita per la prima volta da Van Lint e Schrijver (1981); la costruzione che abbiamo descritto è dovuta a Cameron e Van Lint (1982). Gli altri esempi noti sono una $\mathrm{pg}(5, 18, 2)$ dovuta a Haemers e una $\mathrm{pg}(8, 20, 2)$ trovata da Mathon con l'aiuto di un calcolatore.

Un importante passo verso la dimostrazione della non esistenza di un piano proiettivo di ordine 10, menzionata nel Capitolo 19, fu la dimostrazione della non esistenza di una $\mathrm{pg}(6, 9, 4)$. Ciò implicava, si veda l'Esempio 21.8, che se il piano fosse esistito non avrebbe contenuto iperovali.

Riferimenti bibliografici

R. C. Bose (1963)
Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.* **13**, 389–419.

R. C. Bose and D. M. Mesner (1959)
On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Stat.* **30**, 21–38.

A. E. Brouwer and J. H. van Lint (1982)
Strongly regular graphs and partial geometries, in: *Enumeration and Design* (D. M. Jackson and S. A. Vanstone, eds.), Academic Press.

R. H. Bruck (1951)
Finite nets I, *Canad. J. Math.* **3**, 94–107.

R. H. Bruck (1963)
Finite nets II, *Pacific J. Math.* **13**, 421–457.

Orig. 281

[8] Nota redazionale: il rinvio corretto è all'Esempio 21.10. Le affermazioni sullo stato delle conoscenze sono quelle dell'edizione originale.

P. J. Cameron (1978)
Strongly regular graphs, in: *Selected Topics in Graph Theory* (L. W. Beineke and R. J. Wilson, eds.), Academic Press.

P. J. Cameron, J.-M. Goethals, and J. J. Seidel (1978)
The Krein condition, spherical designs, Norton algebras and permutation groups, *Proc. Kon. Ned. Akad. v. Wetensch.* **81**, 196–206.

P. J. Cameron and J. H. van Lint (1991)
Designs, Graphs, Codes and their links, London Math. Soc. Student Texts **22**, Cambridge University Press.

P. J. Cameron and J. H. van Lint (1982)
On the partial geometry pg$(6, 6, 2)$, *J. Combinatorial Theory (A)* **32**, 252–255.

L. C. Chang (1959)
The uniqueness and nonuniqueness of triangular association schemes, *Sci. Record Peking Math.* **3**, 604–613.

F. De Clerck and H. Van Maldeghem (1995)
Some classes of rank 2 geometries. In F. Buekenhout (editor), *Handbook of Incidence geometry, Buildings and Foundations*, North-Holland.

F. De Clerck (2000)
Partial and semipartial geometries: an update, *Combinatorics 2000* (Gaeta, Italy).

W. S. Connor (1958)
The uniqueness of the triangular association scheme, *Ann. Math. Stat.* **29**, 262–266.

P. Delsarte (1973)
An algebraic approach to the association schemes of coding theory, *Philips Res. Repts. Suppl.* **10**.

P. Delsarte, J.-M. Goethals and J. J. Seidel (1977)
Spherical codes and designs, *Geometriae Dedicata* **6**, 363–388.

A. M. Duval (1988)
A Directed Graph Version of Strongly Regular Graphs, *J. Combinatorial Theory (A)* **47**, 71–100.

A. Gewirtz (1969)
The uniqueness of $g(2, 2, 10, 56)$, *Trans. New York Acad. Sci.* **31**, 656–675.

C. D. Godsil and B. D. McKay (1979)
Graphs with Regular Neighborhoods, *Combinatorial Mathematics VII*, 127–140, Springer.

J.-M. Goethals and J. J. Seidel (1970)
Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22**, 597–614.

D. G. Higman (1975)
Invariant relations, coherent configurations and generalized polygons, in: *Combinatorics* (M. Hall, Jr. and J. H. van Lint, eds.), D. Reidel.

D. G. Higman and C. C. Sims (1968)
A simple group of order 44,352,000, *Math. Z.* **105**, 110–113.

Orig. 282

A. J. Hoffman (1960)
On the uniqueness of the triangular association scheme, *Ann. Math. Stat.* **31**, 492–497.

X. Hubaut (1975)
Strongly regular graphs, *Discrete Math.* **13**, 357–381.

T. H. Koornwinder (1976)
A note on the absolute bound for systems of lines, *Proc. Kon. Ned. Akad. v. Wetensch.* **79**, 152–153.

J. H. van Lint (1983)
Partial geometries, *Proc. Int. Congress of Math.*, Warsaw.

J. H. van Lint and A. Schrijver (1981)
Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* **1**, 63–73.

J. H. van Lint and J. J. Seidel (1969)
Equilateral point sets in elliptic geometry, *Proc. Kon. Ned. Akad. v. Wetensch.* **69**, 335–348.

A. Neumaier (1979)
Strongly regular graphs with smallest eigenvalue $-m$, *Archiv der Mathematik* **33**, 392–400.

A. Neumaier (1980)
New inequalities for the parameters of an association scheme, in: *Combinatorics and Graph Theory*, Lecture Notes in Math. **885**, Springer-Verlag.

S. E. Payne and J. A. Thas (1984)
Finite Generalized Quadrangles, Pitman.

R. M. Wilson (1973/74)
Nonisomorphic Steiner triple systems, *Math. Z.* **135**, 303–313.

Capitolo 22

Quadrati latini ortogonali

Due quadrati latini $L_1 : R \times C \to S$ e $L_2 : R \times C \to T$, con gli stessi insiemi di righe e colonne, si dicono *ortogonali* se per ogni coppia ordinata $(s,t) \in S \times T$ esiste un'unica cella $(x,y) \in R \times C$ tale che Orig. 283

$$L_1(x,y) = s \qquad \text{e} \qquad L_2(x,y) = t.$$

L'uso della parola "ortogonale" è forse poco felice, poiché essa ha altri significati in matematica, ma è ormai troppo diffuso per tentare di cambiarlo.

Per esempio, siano

$$A := \begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix}, \qquad B := \begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix}.$$

Figura 22.1

Qui $R = C = \{1,2,3,4\}$, $S = \{A,K,Q,J\}$, $T = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$. L'ortogonalità di A e B diventa evidente sovrapponendo i due quadrati: vediamo che ogni elemento di $S \times T$ compare esattamente una volta.

$$\begin{bmatrix} A\spadesuit & K\heartsuit & Q\diamondsuit & J\clubsuit \\ Q\clubsuit & J\diamondsuit & A\heartsuit & K\spadesuit \\ J\heartsuit & Q\spadesuit & K\clubsuit & A\diamondsuit \\ K\diamondsuit & A\clubsuit & J\spadesuit & Q\heartsuit \end{bmatrix}$$

L'ortogonalità non dipende dal particolare insieme di simboli usato. Potremmo sostituire i semi delle carte del nostro esempio con quattro simboli qualsiasi, in un ordine qualunque, e il quadrato risultante resterebbe ortogonale ad A. Abbiamo usato lettere latine per i simboli di A; se avessimo usato lettere greche per B, sarebbe stato chiaro perché la sovrapposizione di due quadrati latini ortogonali si chiama spesso *quadrato greco-latino*. Orig. 284

L'esempio con le carte da gioco è simile a quello noto come *problema dei 36 ufficiali di Eulero*. Secondo la tradizione, Caterina la Grande, presso la cui corte Eulero risiedeva, gli avrebbe chiesto di disporre 36 ufficiali, appartenenti a sei reggimenti diversi e aventi sei gradi diversi, uno per ogni grado e reggimento, in una disposizione 6×6, in modo che ogni riga e ogni colonna contenesse un ufficiale di ciascun grado e uno di ciascun reggimento. Una soluzione richiede una coppia di quadrati latini ortogonali di ordine 6.

Sorprendentemente, non vi è soluzione. Che Caterina glielo avesse chiesto o no, Eulero considerò effettivamente il problema nel 1779 e si convinse della sua impossibilità. Era capace di calcoli monumentali, ma non è chiaro se avesse davvero esaminato tutti i casi. G. Tarry lo fece sistematicamente nel 1900. Oggi un calcolatore può farlo facilmente. D. R. Stinson (1984) ne diede una dimostrazione breve, che richiede comunque l'analisi di diversi casi.

Eulero sapeva che esisteva una coppia di quadrati latini ortogonali di ordine n per tutti i valori dispari di n e per tutti gli $n \equiv 0 \pmod 4$; si veda il Teorema 22.3 qui sotto. Per ottenere esempi di ordine dispari n, sia G un gruppo qualsiasi di ordine n e definiamo due quadrati L_1, L_2, aventi G come insieme delle righe, delle colonne e dei simboli, mediante

$$L_1(x,y) := xy, \qquad L_2(x,y) := x^{-1}y.$$

Per ragioni del tutto banali non esiste una coppia di quadrati latini ortogonali di ordine 2. Eulero affermò di ritenere che tale impossibilità per $n = 2, 6$ si estendesse anche a $n = 10, 14, 18, \ldots$, ossia agli ordini $n \equiv 2 \pmod 4$. Questa affermazione fu nota come "congettura di Eulero" per 177 anni, fino a quando Bose, Parker e Shrikhande la confutarono improvvisamente e completamente. Dimostreremo più avanti il loro teorema: esistono coppie di quadrati latini ortogonali di ogni ordine n, eccetto $n = 2, 6$.

In epoche diverse è stata posta una domanda più generale: si possono trovare insiemi di molti quadrati latini, a due a due ortogonali? Indicheremo con $N(n)$ il massimo intero k per il quale esistono k quadrati latini di ordine n a due a due ortogonali. Per esempio, possiamo aggiungere ai quadrati della Fig. 22.1 Orig. 285

$$C := \begin{bmatrix} 0 & \alpha & \beta & \gamma \\ \alpha & 0 & \gamma & \beta \\ \beta & \gamma & 0 & \alpha \\ \gamma & \beta & \alpha & 0 \end{bmatrix},$$

la tavola di addizione del gruppo di Klein di ordine quattro, ottenendo tre quadrati latini di ordine 4 a due a due ortogonali; dunque $N(4) \geq 3$. Osserviamo che la definizione di ortogonalità è banale o vacua per $n = 1$ o 0, perciò $N(1) = N(0) = \infty$.

Ecco una costruzione che dimostra $N(q) \geq q - 1$ quando q è una potenza di un primo. Tutti gli insiemi delle righe, delle colonne e dei simboli sono gli elementi del campo $\mathbb{F}_q$. Per ogni elemento non nullo $a \in \mathbb{F}_q$, definiamo $L_a(x, y) := ax + y$; questi $q - 1$ quadrati sono a due a due ortogonali. Come tutti sappiamo, i sistemi

$$\begin{cases} ax + by = s, \\ cx + dy = t \end{cases}$$

hanno un'unica soluzione (x, y) quando $ad - bc \neq 0$, quindi è facile stabilire quando due quadrati definiti da equazioni lineari sono ortogonali. Ecco i quadrati per $q = 5$:

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}.$$

Teorema 22.1. Per $n \geq 2$ vale $1 \leq N(n) \leq n - 1$.

Dimostrazione. In un insieme di k quadrati latini a due a due ortogonali $\{L_i\}_{i=1}^k$, possiamo sostituire, per comodità di notazione, tutti gli insiemi delle righe, delle colonne e dei simboli con $\{1, 2, \ldots, n\}$, e rinominare se necessario i simboli in modo che la prima riga di ogni quadrato sia $1, 2, \ldots, n$ in quest'ordine. Orig. 286 Consideriamo gli elementi

$$L_1(2, 1), L_2(2, 1), \ldots, L_k(2, 1)$$

nella seconda riga e prima colonna. Nessuno è 1, poiché 1 compare già nella prima colonna. Essi sono distinti: se, per esempio, $L_i(2, 1) = L_j(2, 1) = s$, il fatto che anche $L_i(1, s) = L_j(1, s) = s$ contraddirebbe l'ortogonalità di L_i e L_j. Ne segue il limite superiore. □

Alla luce della costruzione con i campi finiti e del semplice teorema precedente, abbiamo

$$N(q) = q - 1 \quad \text{se } q \text{ è una potenza di un primo.} \tag{22.1}$$

A questo punto vogliamo mostrare che il concetto di quadrati latini a due a due ortogonali equivale a qualcosa che il lettore ha già incontrato nel capitolo precedente! L'asserto del teorema risulterà più immediato se notiamo dapprima che la proprietà di essere un quadrato latino si può essa stessa descrivere in termini di ortogonalità. Per esempio, un quadrato di ordine 5 è latino se e solo se è ortogonale ai due

quadrati

$$\begin{bmatrix} 0&0&0&0&0\\ 1&1&1&1&1\\ 2&2&2&2&2\\ 3&3&3&3&3\\ 4&4&4&4&4 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0&1&2&3&4\\ 0&1&2&3&4\\ 0&1&2&3&4\\ 0&1&2&3&4\\ 0&1&2&3&4 \end{bmatrix}.$$

Teorema 22.2. Esiste un insieme di k quadrati latini di ordine n a due a due ortogonali se e solo se esiste una rete $(n, k+2)$.

DIMOSTRAZIONE. Supponiamo che $L_i : R \times C \to S_i$, $1 \le i \le k$, siano quadrati latini a due a due ortogonali. Sia $\mathcal{P} = R \times C$ l'insieme delle n^2 celle. In termini intuitivi prendiamo come rette le righe, le colonne e le rette "a simbolo costante" in ciascun quadrato. Più formalmente, poniamo

$$\mathcal{A}_1 = \{\{(x,b) : b \in C\} : x \in R\},$$

Orig. 287

$$\mathcal{A}_2 = \{\{(a,y) : a \in R\} : y \in C\},$$

$$\mathcal{A}_{i+2} = \{\{(x,y) : L_i(x,y) = c\} : c \in S_i\}, \quad 1 \le i \le k,$$

e $\mathcal{B} = \bigcup_{i=1}^{k+2} \mathcal{A}_i$. Che $(\mathcal{P}, \mathcal{B})$ sia una rete $(n, k+2)$ segue dalle definizioni di quadrato latino e di ortogonalità.

Data una rete $(n, k+2)$ $(\mathcal{P}, \mathcal{B})$, dove $\mathcal{B} = \bigcup_{i=1}^{k+2} \mathcal{A}_i$ è la partizione in classi di parallelismo, definiamo $L_i : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}_{i+2}$ ponendo $L_i(A,B)$ uguale all'unica retta di $\mathcal{A}_{i+2}$ che contiene il punto d'intersezione di A e B. Come al solito lasciamo al lettore i dettagli della verifica che questi quadrati siano latini e ortogonali. □

Corollario. $N(n) = n-1$ se e solo se esiste un piano proiettivo, o affine, di ordine n.

Il valore di $N(n)$ ci dice, in un senso molto impreciso, quanto possiamo avvicinarci all'esistenza di un piano proiettivo di ordine n. Ma sappiamo terribilmente poco di questa funzione. L'unico valore di n, diverso dalle potenze di primi, per il quale $N(n)$ sia noto è $n = 6$.

Problema 22A. (i) Considerare il complementare del grafo di una rete (n,n) e dimostrare che $N(n) \ge n-2$ implica $N(n) = n-1$.

(ii) Usare il risultato del Problema 21F per dimostrare che, se $n > 4$, allora $N(n) \ge n-3$ implica $N(n) = n-1$.

Teorema 22.3.

(i) $N(nm) \ge \min\{N(n), N(m)\}$.

(ii) Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ è la fattorizzazione di n in potenze di primi, allora $N(n) \ge \min_{1 \le i \le r}(p_i^{e_i} - 1)$.

DIMOSTRAZIONE. La parte (ii) segue dalla parte (i) e dalla (22.1), applicate induttivamente.

Per dimostrare (i), definiamo anzitutto nel modo naturale un prodotto di quadrati simile al prodotto di Kronecker. Dati $L_i : R_i \times C_i \to S_i$, $i = 1, 2$, definiamo

$$L_1 \otimes L_2 : (R_1 \times R_2) \times (C_1 \times C_2) \to (S_1 \times S_2)$$

mediante

$$(L_1 \otimes L_2)((x_1, x_2), (y_1, y_2)) := (L_1(x_1, y_1), L_2(x_2, y_2)).$$

È immediato verificare che, se $\{A_i\}_{i=1}^k$ sono quadrati latini di ordine n a due a due ortogonali e $\{B_i\}_{i=1}^k$ sono quadrati latini di ordine m a due a due ortogonali, allora $\{A_i \otimes B_i\}_{i=1}^k$ sono quadrati latini di ordine nm a due a due ortogonali. Lasciamo questo compito al lettore, ma gli consigliamo di proseguire semplicemente nella lettura senza preoccuparsene. □ Orig. 288

Il Teorema 22.3 è noto come *teorema di MacNeish*. Nel 1922 MacNeish congetturò che nel Teorema 22.3(ii) valesse l'uguaglianza. Ciò implicherebbe la congettura di Eulero. Ma i problemi combinatori di questo tipo hanno raramente risposte così semplici.

La congettura di MacNeish fu confutata dapprima per $n = 21$, quando si costruirono tre quadrati latini di ordine 21 con l'aiuto del piano proiettivo di ordine 4, avente 21 punti; si veda l'Esempio 22.1. Si trattava di un esempio dei *metodi di composizione*, che fornirono anche il primo controesempio alla congettura di Eulero, per $n = 22$. Parker trovò la prima coppia di quadrati latini ortogonali di ordine 10 con quelli che potremmo chiamare *metodi delle differenze*. Discutiamo dapprima i metodi di composizione, rivelatisi più potenti per grandi valori di n.

Bose, Parker e Shrikhande diedero molte costruzioni di insiemi di quadrati latini ortogonali. Scegliamo di descriverne due fondamentali ed eleganti in termini di quasigruppi. Ricordiamo che un quasigruppo è un quadrato latino i cui insiemi delle righe, delle colonne e dei simboli coincidono con uno stesso insieme X. Un quasigruppo L si dice *idempotente* se $L(x, x) = x$ per ogni $x \in X$. Per esempio, se X è il campo finito $\mathbb{F}_q$, allora

$$L_a(x, y) := ax + (1 - a)y$$

definisce un quasigruppo idempotente L_a se $a \neq 0, 1$. Due quadrati distinti di questa forma sono ortogonali.

Problema 22B. Per una potenza di primo $q \geq 4$, costruire due quadrati latini A, S di ordine q, con insiemi delle righe e delle colonne uguali a $\mathbb{F}_q$, in modo che A sia ortogonale alla propria trasposta e a S, che deve essere simmetrico. Fare inoltre in modo che S sia idempotente se q è dispari e "unipotente", cioè con diagonale costante, se q è pari.

Supponiamo di avere uno spazio lineare, si confronti il Capitolo 19, sull'insieme di punti X, con insieme delle rette $\mathcal{A}$. Supponiamo inoltre che per ogni retta $A \in \mathcal{A}$ vi siano k quasigruppi idempotenti a due a due ortogonali $L_1^A, L_2^A, \ldots, L_k^A$ sull'insieme A. Possiamo allora costruire k quasigruppi idempotenti a due a due ortogonali $L_1, L_2, \ldots, L_k$ sull'intero insieme X ponendo, per ogni $i = 1, 2, \ldots, k$, $L_i(x, x) := x$ per $x \in X$ e, per $x, y \in X$ distinti, $L_i(x, y) := L_i^A(x, y)$, dove A è l'unica retta di $\mathcal{A}$ che contiene x e y. È semplice verificare che $L_1, L_2, \ldots, L_k$ siano quadrati latini e siano ortogonali; per esempio, dati i, j, s, t, con $s \neq t$, esiste una cella (x, y) tale che

Orig. 289

$$L_i(x, y) = s \qquad \text{e} \qquad L_j(x, y) = t,$$

e x, y si possono trovare nella retta B contenente s, t, grazie all'ortogonalità di L_i^B e L_j^B.

Teorema 22.4. Per ogni spazio lineare con insieme delle rette $\mathcal{A}$ su un insieme X di n elementi, vale

$$N(n) \geq \min_{A \in \mathcal{A}} \{N(|A|) - 1\}.$$

Dimostrazione. Sia k il minimo indicato. Ciò significa che disponiamo di almeno $k + 1$ quasigruppi a due a due ortogonali su ogni $A \in \mathcal{A}$. Descriveremo come ricavarne k quasigruppi idempotenti a due a due ortogonali su ciascun A. La costruzione precedente darà allora $N(n) \geq k$.

In generale, siano $H_1, H_2, \ldots, H_{k+1}$ quasigruppi a due a due ortogonali su un insieme B di m elementi. Scegliamo un $b \in B$. Vi saranno m celle (x, y) per le quali $H_{k+1}(x, y) = b$, una in ciascuna riga e una in ciascuna colonna. Permutiamo simultaneamente, per esempio, le colonne di tutti i quadrati affinché queste celle si trovino sulla diagonale del $(k + 1)$-esimo quadrato. L'ortogonalità implica che, per ogni $i \leq k$, tutti gli m simboli compaiono sulla diagonale dell'i-esimo quadrato. Infine permutiamo i simboli indipendentemente in ciascuno dei primi k quadrati, in modo da renderli idempotenti. □

Teorema 22.5. Se $\mathcal{A}$ è l'insieme delle rette di uno spazio lineare su un insieme X di n elementi e $\mathcal{B} \subseteq \mathcal{A}$ è un insieme di rette a due a due disgiunte, allora

$$N(n) \geq \min\big(\{N(|A|) - 1 : A \in \mathcal{A} \setminus \mathcal{B}\} \cup \{N(|B|) : B \in \mathcal{B}\}\big).$$

Dimostrazione. Sia k il minimo indicato. Come abbiamo visto nella dimostrazione precedente, su ogni $A \in \mathcal{A} \setminus \mathcal{B}$ esistono k quasigruppi idempotenti L_i^A a due a due ortogonali. Se necessario aggiungiamo singoletti a $\mathcal{B}$ affinché esso diventi una partizione di X. Su ogni $B \in \mathcal{B}$ abbiamo k quasigruppi L_i^B a due a due ortogonali, non necessariamente idempotenti. Definiamo $L_1, L_2, \ldots, L_k$ sull'intero insieme X ponendo, per ogni $i = 1, 2, \ldots, k$, $L_i(x, x) := L_i^B(x, x)$, dove B è l'unico membro di $\mathcal{B}$ contenente x; per x, y distinti poniamo $L_i(x, y) := L_i^A(x, y)$, dove A è l'unica retta di $\mathcal{A}$, appartenente o meno a $\mathcal{B}$, che contiene entrambi. I quasigruppi L_i sono ortogonali, i facili dettagli sono lasciati al lettore, e dunque $N(n) \geq k$. □

Orig. 290

Esempio 22.1. Sia $n = 21$ e consideriamo il piano proiettivo di ordine 4, con 21 rette di cardinalità 5. Il Teorema 22.4 implica $N(21) \geq 3$, e ciò confuta la congettura di MacNeish. Eliminiamo tre punti non collineari. Abbiamo uno spazio lineare con 18 punti e rette di cardinalità 5, 4 e 3; le tre rette di cardinalità 3 sono a due a due disgiunte. Il Teorema 22.5 implica $N(18) \geq 2$, e ciò confuta la congettura di Eulero.

Esempio 22.2. Per vedere quanto Eulero si sbagliasse, consideriamo altri due valori di $n \equiv 2 \pmod 4$. Eliminiamo tre punti non collineari da un piano proiettivo di ordine 8: otteniamo uno spazio lineare su 70 punti, con rette di cardinalità 9, 8 e 7, queste ultime a due a due disgiunte. Il Teorema 22.5 mostra che $N(70) \geq 6$. Nel piano costruito su $\mathbb{F}_8$ è possibile trovare sette punti senza tre punti collineari, e addirittura dieci, si veda il Problema 19I. Eliminandoli otteniamo uno spazio lineare al quale possiamo applicare il Teorema 22.4 per ricavare $N(66) \geq 5$.

La prossima costruzione sarebbe difficile da descrivere senza i disegni trasversali. Essi forniscono un linguaggio compatto e concettualmente comodo per manipolare insiemi di quadrati latini a due a due ortogonali. Forniscono anche una vasta famiglia di spazi lineari utili per costruire altri disegni combinatori o ulteriori quadrati latini ortogonali. Un $TD(n,k)$ si può definire come la struttura d'incidenza duale di una rete (n,k), cioè come una geometria parziale $(n,k,k-1)$.[1] Vi sono dunque nk punti e n^2 blocchi: parlando di disegni trasversali useremo "blocchi" anziché "rette". Ogni punto appartiene a n blocchi e ogni blocco contiene k punti. I punti si suddividono in k classi di equivalenza di cardinalità n, chiamate, con una certa ambiguità, *gruppi*: due punti dello stesso gruppo non appartengono a uno stesso blocco, mentre due punti di gruppi diversi appartengono a esattamente un blocco. In particolare, ogni blocco contiene esattamente un punto di ciascun gruppo. Dobbiamo riferirci ai gruppi tanto spesso che li includiamo nella notazione e parliamo di un disegno trasversale $(X, \mathcal{G}, \mathcal{A})$, le cui tre coordinate sono rispettivamente gli insiemi dei punti, dei gruppi e dei blocchi. $(X, \mathcal{G} \cup \mathcal{A})$ è uno spazio lineare con blocchi di cardinalità k e n. Orig. 291

Esempio 22.3. Ecco un $TD(2,3)$:

$$\begin{aligned} &\text{Gruppi: } \{a_1,a_2\},\ \{b_1,b_2\},\ \{c_1,c_2\};\\ &\text{Blocchi: } \{a_1,b_1,c_1\},\ \{a_1,b_2,c_2\},\ \{a_2,b_1,c_2\},\ \{a_2,b_2,c_1\}. \end{aligned}$$

Per il Teorema 22.2, l'esistenza di un $TD(n,k+2)$ equivale a quella di k quadrati latini a due a due ortogonali. A rischio di annoiare qualche lettore, riprendiamo il collegamento descrivendo rapidamente come ottenere i quadrati da un $TD(n,k+2)$: numeriamo i gruppi $\{G_1, G_2, \ldots, G_{k+2}\}$ e definiamo $L_i : G_1 \times G_2 \to G_{i+2}$ ponendo $L_i(x,y)$ uguale al punto d'intersezione di G_{i+2} con il blocco contenente x e y.

Un $TD(n,k)$ si dice *risolubile* se l'insieme $\mathcal{A}$ dei blocchi si può suddividere in n classi di parallelismo $\mathcal{A}_1, \ldots, \mathcal{A}_n$: ciascuna $\mathcal{A}_i$ è quindi un insieme di n blocchi di cardinalità k che partizionano X. Da un $TD(n,k)$ $(X, \mathcal{G}, \mathcal{A})$ possiamo sempre costruire un $TD(n,k-1)$ risolubile eliminando gli n punti di un gruppo $G_0 = \{x_1, x_2, \ldots, x_n\}$,[2] il che toglie esattamente un punto a ciascun blocco. Per ogni i, i blocchi dai quali è stato tolto x_i formano una classe di parallelismo sull'insieme di punti $X \setminus G_0$ del $TD(n,k-1)$. Viceversa, un $TD(n,k-1)$ risolubile si può estendere a un $TD(n,k)$.

Teorema 22.6. Se $0 \leq u \leq t$, allora

$$N(mt+u) \geq \min\{N(m), N(m+1), N(t)-1, N(u)\}.$$

Dimostrazione. Sia k il membro destro aumentato di 2. Ciò significa che esistono disegni trasversali $TD(m,k)$, $TD(m+1,k)$, $TD(t,k+1)$ e $TD(u,k)$; per dimostrare il teorema dobbiamo costruire un $TD(mt+u,k)$.

Poiché la costruzione è piuttosto tecnica, cominciamo descrivendo la costruzione di un $TD(mt,k)$ a partire da un $TD(t,k)$ e da vari $TD(m,k)$. Si tratta del caso degenere $u = 0$ del teorema. Questa costruzione non richiede un $TD(m+1,k)$ né un $TD(t,k+1)$ e fornisce quindi una nuova dimostrazione del Teorema 22.3(i). Orig. 292

Sia $(X, \mathcal{G}, \mathcal{A})$ un $TD(t,k)$. A ogni $x \in X$ associamo un insieme M_x di m nuovi elementi, in modo che tali insiemi siano a due a due disgiunti. Per $S \subseteq X$, poniamo $M_S := \bigcup_{x \in S} M_x$.

[1] Nota redazionale: con la convenzione $\mathrm{pg}(K,R,T)$ del Capitolo 21, il duale della rete $\mathrm{pg}(n,k,k-1)$ è $\mathrm{pg}(k,n,k-1)$. L'originale mantiene qui erroneamente l'ordine $(n,k,k-1)$; i conteggi immediatamente successivi usano correttamente k punti per blocco e n blocchi per punto.

[2] Nota redazionale: nell'originale il secondo elemento dell'elenco è ripetuto come x_1; è stato reso x_2.

Costruiamo un $TD(mt,k)$ sull'insieme di punti M_X, di cardinalità kmt, con gruppi $\{M_G : G \in \mathcal{G}\}$, ciascuno di cardinalità mt; i blocchi $\mathcal{B}$ si ottengono così. Per ogni $A \in \mathcal{A}$, scegliamo blocchi $\mathcal{B}_A$ tali che

$$(M_A, \{M_x : x \in A\}, \mathcal{B}_A)$$

sia un $TD(m,k)$, e poniamo $\mathcal{B} = \bigcup_{A\in\mathcal{A}} \mathcal{B}_A$. La verifica è immediata.

Torniamo al caso generale. Ricordiamo che l'esistenza di un $TD(t,k+1)$ implica quella di un $TD(t,k)$ risolubile. Abbiamo dunque un $TD(t,k)$ $(X,\mathcal{G},\mathcal{A})$ nel quale $\mathcal{A}$ ammette una partizione in classi di parallelismo $\mathcal{A}_1,\dots,\mathcal{A}_t$. Trattiamo in un modo i blocchi delle prime u classi di parallelismo e in un altro quelli di $\mathcal{B} := \bigcup_{i=u+1}^{t} \mathcal{A}_i$.

Sia $(U,\mathcal{H},\mathcal{C})$ un $TD(u,k)$. Ci occorre anche una partizione di U in u sottoinsiemi di cardinalità k, $\{K_1,\dots,K_u\}$, ciascuno formato da esattamente un punto di ogni $H \in \mathcal{H}$; non si richiede però che questi sottoinsiemi siano blocchi di $\mathcal{C}$.

Numeriamo i gruppi come $\mathcal{G} = \{G_1,\dots,G_k\}$ e $\mathcal{H} = \{H_1,\dots,H_k\}$. Costruiamo un $TD(mt+u,k)$ con insieme di punti $Y := M_X \cup U$ e gruppi

$$\mathcal{J} := \{M_{G_1} \cup H_1, M_{G_2} \cup H_2, \dots, M_{G_k} \cup H_k\}.$$

I blocchi si ottengono come segue. Per ogni $B \in \mathcal{B}$, come prima, sia

$$(M_B, \{M_x : x \in B\}, \mathcal{D}_B)$$

un $TD(m,k)$. Per ogni blocco $A \in \mathcal{A}_i$, con $1 \le i \le u$, sia

$$\big(M_A \cup K_i, \{(M_A \cap M_{G_j}) \cup (K_i \cap H_j) : j = 1,\dots,k\}, \mathcal{D}_A\big)$$

un $TD(m+1,k)$ nel quale K_i compare come blocco, e sia $\mathcal{D}'_A$ l'insieme dei rimanenti $(m+1)^2-1$ blocchi. Affermiamo allora che $(Y,\mathcal{J},\mathcal{E})$ è il $TD(mt+u,k)$ richiesto, dove

$$\mathcal{E} := \mathcal{C} \cup \left(\bigcup_{B\in\mathcal{B}} \mathcal{D}_B\right) \cup \left(\bigcup_{A\in\mathcal{A}_1\cup\cdots\cup\mathcal{A}_u} \mathcal{D}'_A\right).$$

La verifica richiede di considerare diversi casi. □ Orig. 293

Esempio 22.4. Ponendo $m = 3$ nel Teorema 22.6, otteniamo

$$N(3t+u) \ge 2 \quad \text{se } 0 \le u \le t,\ N(t) \ge 3,\ N(u) \ge 2. \tag{22.2}$$

Possiamo prendere $(t,u) = (5,3),(7,1),(7,5),(9,3)$, ottenendo $N(n) \ge 2$ per $n = 18,22,26,30$.

Teorema 22.7. $N(n) \ge 2$ per ogni $n \ne 2,6$.

Dimostrazione. Occorre considerare soltanto $n \equiv 2 \pmod 4$. Per $n = 10,14$ si vedano gli Esempi 22.6 e 22.7 più avanti. Per $n = 18,22,26,30$ si veda l'Esempio 22.4. Supponiamo ora $n \ge 34$. Uno dei numeri

$$n-1, n-3, n-5, n-7, n-9, n-11$$

è divisibile per 3 ma non per 9, quindi possiamo scrivere $n = 3t+u$, dove $u = 1,3,5,7,9$ oppure 11 e t non è divisibile per 3. Poiché n è pari, t è anche dispari, dunque $N(t) \ge 4$ per il Teorema 22.3(ii). Da $n \ge 34$ segue $t \ge 11$,[3] perciò $0 \le u \le t$, e la (22.2) dà $N(n) \ge 2$. □

Teorema 22.8. $N(n) \to \infty$ quando $n \to \infty$.

Dimostrazione. Sia x un intero positivo. Affermiamo che $N(n) \ge x-1$ ogni volta che

$$n \ge 2\left(\prod_{p\le x} p\right)^{2x+1}, \tag{22.3}$$

[3]Nota redazionale: la scelta va precisata perché $t \ge 11$ non segue da qualunque u ammissibile. Per $n = 34,38,42$, con $n \equiv 2 \pmod 4$, si possono scegliere rispettivamente $(t,u) = (11,1),(11,5),(13,3)$; per $n \ge 46$ vale automaticamente $t \ge (n-11)/3 > 11$.

dove il prodotto è esteso a tutti i primi $p \le x$.

Dato n che soddisfa la (22.3), scegliamo m, mediante il teorema cinese dei resti, in modo che $0 \le m \le (\prod_{p\le x} p)^x$ e che, per ogni primo $p \le x$,

$$m \equiv \begin{cases} -1 \pmod{p^x} & \text{se } p \text{ divide } n, \\ 0 \pmod{p^x} & \text{se } p \text{ non divide } n. \end{cases}$$

Scegliamo poi un intero $t \equiv 1 \pmod{\prod_{p\le x} p}$ tale che

$$0 \le u := n - mt < \left(\prod_{p\le x} p\right)^{x+1}.$$

Il resto della dimostrazione è fornito dal Problema 22C. □

Orig. 294

Problema 22C. Con m, t, u scelti come sopra, mostrare che $u \le t$ e che il Teorema 22.3(ii) implica $N(mt + u) \ge x - 1$.

* * *

Nel Capitolo 19 abbiamo incontrato costruzioni mediante i cosiddetti metodi delle differenze. Qui usiamo quest'idea per costruire quadrati latini. Conviene descrivere le costruzioni in termini di schieramenti ortogonali. Un $OA(n, k)$ è uno schieramento $k \times n^2$, o, come preferiamo pensarlo qui, un insieme di n^2 vettori colonna di altezza k, poiché l'ordine delle colonne non conta, i cui elementi appartengono a un insieme S di n simboli, tale che per ogni coppia i, j di indici distinti, $1 \le i, j \le k$, e per ogni coppia di simboli $s, t \in S$, esiste un'unica colonna con coordinata i uguale a s e coordinata j uguale a t. Ciò generalizza gli $OA(n, 3)$ introdotti nel Capitolo 17.

È un'ulteriore formulazione equivalente dell'ortogonalità: l'esistenza di un $OA(n, k + 2)$ equivale a quella di k quadrati latini a due a due ortogonali. Per esempio, per ottenere lo schieramento dai quadrati $L_1, \dots, L_k$, supponiamo senza perdita di generalità che tutti gli insiemi delle righe, delle colonne e dei simboli siano uno stesso insieme S, e prendiamo tutte le colonne

$$[i, j, L_1(i, j), L_2(i, j), \dots, L_k(i, j)]^\top, \qquad i, j \in S.$$

Il lettore dovrebbe saper ricavare immediatamente due quadrati ortogonali dall'$OA(3, 4)$ della Fig. 22.2; naturalmente, qualunque coppia di righe può essere usata per assegnare le coordinate ai quadrati.

$$\begin{bmatrix} x & x & x & y & y & y & z & z & z \\ x & y & z & x & y & z & x & y & z \\ x & y & z & z & x & y & y & z & x \\ x & y & z & y & z & x & z & x & y \end{bmatrix}$$

Figura 22.2

Esempio 22.5. La seguente matrice di elementi di $\mathbb{Z}_{15}$ fu trovata con l'aiuto di un calcolatore da Schellenberg, Van Rees e Vanstone (1978):

Orig. 295

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 2 & 5 & 7 & 9 & 12 & 4 & 1 & 14 & 11 & 3 & 6 & 8 & 10 & 13 \\ 0 & 6 & 3 & 14 & 10 & 7 & 13 & 4 & 11 & 2 & 8 & 5 & 1 & 12 & 9 \\ 0 & 10 & 6 & 1 & 11 & 2 & 7 & 12 & 3 & 8 & 13 & 4 & 14 & 9 & 5 \end{bmatrix}.$$

Essa ha la proprietà che, per ogni coppia di righe, le differenze fra le coordinate di quelle due righe comprendono tutti gli elementi di $\mathbb{Z}_{15}$, ciascuno una sola volta. Ne segue che otteniamo un $OA(15, 5)$ prendendo tutte le traslate di queste colonne per gli elementi di $\mathbb{Z}_{15}$. Si possono quindi costruire tre quadrati latini di ordine 15 a due a due ortogonali. Ma l'$OA(15, 5)$ è risolubile: le 15 traslate di ogni colonna hanno la proprietà che, in ciascuna coordinata, tutti i simboli compaiono una volta. Come per i disegni trasversali, possiamo aggiungere una nuova riga ottenendo un $OA(15, 6)$, e quindi quattro quadrati latini di ordine 15 a due a due ortogonali. Non è noto se $N(15) \ge 5$.

Le ultime tre righe della matrice precedente sono quelli che chiameremo fra poco ortomorfismi a due a due ortogonali di $\mathbb{Z}_{15}$.

Nel 1960 Johnson, Dulmage, Mendelsohn e un calcolatore dimostrarono con questo metodo che $N(12) \geq 5$, usando il gruppo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Il gruppo ciclico di ordine 12 non serve allo scopo; si veda il Teorema 22.9.

Esempio 22.6. Descriviamo una costruzione che dimostra

$$N(m) \geq 2 \quad \Longrightarrow \quad N(3m+1) \geq 2.$$

Sia G un gruppo abeliano di ordine $2m+1$ e sia M un sistema di rappresentanti delle coppie $\{i,-i\}$, $i \neq 0$, in G. Dunque $|M| = m$ e $G = \{0\} \cup M \cup (-M)$. Per ogni $i \in M$ introduciamo un nuovo simbolo ∞_i e prendiamo $S := G \cup \{\infty_i : i \in M\}$ come insieme dei simboli per un $OA(3m+1,4)$.

Consideriamo tutti i vettori colonna ottenuti da

$$\left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} \infty_i \\ 0 \\ i \\ -i \end{bmatrix}, \begin{bmatrix} 0 \\ \infty_i \\ -i \\ i \end{bmatrix}, \begin{bmatrix} i \\ -i \\ \infty_i \\ 0 \end{bmatrix}, \begin{bmatrix} -i \\ i \\ 0 \\ \infty_i \end{bmatrix} : i \in M \right\}$$

traslandoli per gli elementi di G, con la convenzione che i simboli ∞ rimangano fissi, ossia $\infty_i + g = \infty_i$. Otteniamo così $(4m+1)(2m+1)$ colonne. Aggiungiamo le m^2 colonne di un $OA(m,4)$ per ottenere un $OA(3m+1,4)$. Orig. 296

Per rendere esplicito il caso $m = 3$, usiamo i simboli $\mathbb{Z}_7 \cup \{x,y,z\}$ e $M = \{1,2,3\}$. Prendiamo le sette traslate delle seguenti 13 colonne e aggiungiamo l'$OA(3,4)$ della Fig. 22.2:

$$\begin{bmatrix} 0 & x & 0 & 1 & 6 & y & 0 & 2 & 5 & z & 0 & 3 & 4 \\ 0 & 0 & x & 6 & 1 & 0 & y & 5 & 2 & 0 & z & 4 & 3 \\ 0 & 1 & 6 & x & 0 & 2 & 5 & y & 0 & 3 & 4 & z & 0 \\ 0 & 6 & 1 & 0 & x & 5 & 2 & 0 & y & 4 & 3 & 0 & z \end{bmatrix}.$$

La verifica della costruzione richiede un'attenzione particolare ai simboli x,y,z, che abbiamo usato al posto degli ∞_i, e l'osservazione che le differenze fra due righe qualsiasi, quando entrambe le coordinate appartengono a $\mathbb{Z}_7$, comprendono tutti gli elementi di $\mathbb{Z}_7$, ciascuno una sola volta. I quadrati risultanti sono riportati qui sotto.

$$\begin{bmatrix} 0 & z & 1 & y & 2 & x & 3 & 6 & 5 & 4 \\ 4 & 1 & z & 2 & y & 3 & x & 0 & 6 & 5 \\ x & 5 & 2 & z & 3 & y & 4 & 1 & 0 & 6 \\ 5 & x & 6 & 3 & z & 4 & y & 2 & 1 & 0 \\ y & 6 & x & 0 & 4 & z & 5 & 3 & 2 & 1 \\ 6 & y & 0 & x & 1 & 5 & z & 4 & 3 & 2 \\ z & 0 & y & 1 & x & 2 & 6 & 5 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & x & y & z \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & z & x & y \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & y & z & x \end{bmatrix} \quad \begin{bmatrix} 0 & 4 & x & 5 & y & 6 & z & 1 & 2 & 3 \\ z & 1 & 5 & x & 6 & y & 0 & 2 & 3 & 4 \\ 1 & z & 2 & 6 & x & 0 & y & 3 & 4 & 5 \\ y & 2 & z & 3 & 0 & x & 1 & 4 & 5 & 6 \\ 2 & y & 3 & z & 4 & 1 & x & 5 & 6 & 0 \\ x & 3 & y & 4 & z & 5 & 2 & 6 & 0 & 1 \\ 3 & x & 4 & y & 5 & z & 6 & 0 & 1 & 2 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 & x & y & z \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 & y & z & x \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & z & x & y \end{bmatrix}.$$

Esempio 22.7. Descriviamo un $OA(14,4)$ sui simboli $\mathbb{Z}_{11} \cup \{x,y,z\}$. Prendiamo le 11 traslate, per gli elementi di $\mathbb{Z}_{11}$, delle seguenti 17 colonne e aggiungiamo l'$OA(3,4)$ della Fig. 22.2:

$$\begin{bmatrix} 0 & 0 & 6 & 4 & 1 & x & 1 & 4 & 0 & y & 2 & 6 & 0 & z & 8 & 9 & 0 \\ 0 & 1 & 0 & 6 & 4 & 0 & x & 1 & 4 & 0 & y & 2 & 6 & 0 & z & 8 & 9 \\ 0 & 4 & 1 & 0 & 6 & 4 & 0 & x & 1 & 6 & 0 & y & 2 & 9 & 0 & z & 8 \\ 0 & 6 & 4 & 1 & 0 & 1 & 4 & 0 & x & 2 & 6 & 0 & y & 8 & 9 & 0 & z \end{bmatrix}.$$

Ancora una volta la verifica richiede un'attenzione particolare ai simboli x,y,z, usati al posto degli ∞_i, e l'osservazione che le differenze fra due righe qualsiasi dello schieramento precedente, quando entrambe le coordinate appartengono a $\mathbb{Z}_{11}$, comprendono tutti gli elementi di $\mathbb{Z}_{11}$, ciascuno una sola volta. Orig. 297

Problema 22D. Mostrare che l'esistenza di k quasigruppi idempotenti a due a due ortogonali equivale all'esistenza di un $TD(n,k+2)$ nel quale si possa trovare una classe di parallelismo di blocchi.

Un *ortomorfismo* di un gruppo abeliano G è una permutazione σ degli elementi di G tale che anche

$$x \longmapsto \sigma(x) - x$$

sia una permutazione di G. Il lettore può verificare che il quadrato $L(x, y) := \sigma(x) + y$ è latino se e solo se σ è una permutazione, ed è ortogonale alla tavola di addizione $A(x, y) := x + y$ di G se e solo se σ è un ortomorfismo.

Osserviamo che, se A ammette un qualunque quadrato ortogonale, allora esiste un ortomorfismo. Infatti le celle nelle posizioni in cui un quadrato ortogonale ad A contiene un simbolo fissato sono esattamente una per riga e per colonna; sono quindi della forma $(x, \tau(x))$, $x \in G$, per una permutazione τ. Poiché queste celle devono contenere simboli diversi in A, l'applicazione σ definita da $\sigma(x) := x + \tau(x)$ è una permutazione. Alla luce di questa osservazione, il prossimo teorema dimostra che i quadrati ciclici di ordine pari non ammettono un quadrato latino ortogonale.

Teorema 22.9. Se un gruppo abeliano G ammette un ortomorfismo, allora il suo ordine è dispari oppure il suo 2-sottogruppo di Sylow non è ciclico.

DIMOSTRAZIONE. Se il 2-sottogruppo di Sylow è ciclico e non banale, vi è esattamente un elemento $z \in G$ di ordine 2. Sommando tutti gli elementi di G, ogni elemento si accoppia con il proprio opposto tranne z e 0; pertanto la somma di tutti gli elementi di G è z. Ma, se σ fosse un ortomorfismo, avremmo

$$z = \sum_{x \in G} (\sigma(x) - x) = \sum_{x \in G} \sigma(x) - \sum_{x \in G} x = z - z = 0,$$

in contraddizione con la scelta di z. □

Orig. 298

Osservazioni. Se G è abeliano e ha ordine dispari, possiede automorfismi che fissano soltanto l'identità; ciò vale anche per alcuni gruppi abeliani di ordine pari. Tali automorfismi sono ortomorfismi. Anche se G non è abeliano si possono definire ortomorfismi, detti anche *applicazioni complete*, e resta vero che essi non esistono se il 2-sottogruppo di Sylow è ciclico e non banale: si veda Hall e Paige (1955), dove si dimostra anche l'esistenza di applicazioni complete per i gruppi risolubili con 2-sottogruppi di Sylow banali o non ciclici.

* * *

H. B. Mann (1950) osservò che un quadrato latino di ordine $4t+1$ con un sottoquadrato di ordine $2t$ non ammette quadrati ortogonali. Analogamente, un quadrato latino di ordine $4t + 2$ con un sottoquadrato di ordine $2t + 1$ non ammette quadrati ortogonali. Entrambi i risultati sono corollari della parte (ii) del teorema seguente, che dimostra anche che nessuna delle coppie di quadrati ortogonali di ordine $12t + 10$ costruite nell'Esempio 22.6 può essere estesa a un insieme di tre o più quadrati latini a due a due ortogonali. Lasciamo al lettore il compito di convincersi che ai sottoquadrati corrispondono sottodisegni trasversali.

Teorema 22.10. Sia $(X, \mathcal{G}, \mathcal{A})$ un $TD(n, k)$ che contiene un sotto-$TD(m, k)$ $(Y, \mathcal{H}, \mathcal{B})$, con $m < n$. Ciò significa $Y \subseteq X$, $\mathcal{H} = \{G \cap Y : G \in \mathcal{G}\}$ e $\mathcal{B} \subseteq \mathcal{A}$. Allora

(i) $m(k - 1) \leq n$;

(ii) se $(X, \mathcal{G}, \mathcal{A})$ è risolubile, allora

$$m^2 \geq n \left\lceil \frac{mk - n}{k - 1} \right\rceil .$$

DIMOSTRAZIONE. Scegliamo un punto $x_0 \in X \setminus Y$ e supponiamo che appartenga a $G_0 \in \mathcal{G}$. Per ciascuno degli $m(k - 1)$ punti $y \in Y \setminus G_0$, esiste un unico blocco $A_y \in \mathcal{A}$ con $\{x_0, y\} \subseteq A_y$. Un blocco contenente due punti di Y deve appartenere a $\mathcal{B}$, e non potrebbe contenere x_0; questi $m(k - 1)$ blocchi sono quindi distinti. Il loro numero non può superare quello totale dei blocchi per x_0, che è n.

Supponiamo che $(X, \mathcal{G}, \mathcal{A})$ sia risolubile e che $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ sia una partizione di $\mathcal{A}$ in classi di parallelismo. Sia s_i il numero dei blocchi di $\mathcal{A}_i$ contenuti in Y e sia t_i il numero di quelli che incontrano Y in esattamente un punto. Allora

Orig. 299

$$ks_i + t_i = |Y| = mk \qquad \text{e} \qquad s_i + t_i \leq n,$$

da cui $(k-1)s_i \geq mk-n$, ossia

$$s_i \geq \left\lceil \frac{mk-n}{k-1} \right\rceil .$$

La parte (ii) segue ora da $m^2 = |\mathcal{B}| = \sum_{i=1}^{n} s_i$. □

Problema 22E. Dimostrare che $N(24) \geq 3$ e $N(33) \geq 3$.

Problema 22F. Supponiamo di avere $c-1$ quadrati latini mutuamente ortogonali di ordine k. Abbiamo allora un $OA(k, c+1)$, che rappresentiamo così:

$$\left(\begin{array}{cccc|cccc|c|cccc} 1 & 1 & \cdots & 1 & 2 & 2 & \cdots & 2 & \cdots & k & k & \cdots & k \\ 1 & 2 & \cdots & k & & & & & & & & & \\ \vdots & & & & & A_1 & & & \cdots & & A_{k-1} & & \\ 1 & 2 & \cdots & k & & & & & & & & & \end{array}\right),$$

dove ogni riga di ciascuna matrice A_i è una permutazione di $1, 2, \ldots, k$. Sia A la matrice $c \times k(k-1)$ formata dalle matrici A_i. Usare questa matrice e la matrice S del Problema 19U per dimostrare il teorema seguente.

Teorema. Se esiste un disegno simmetrico $(v, k, 1)$, allora $N(v) \geq N(k)$.

Problema 22G. Generalizzare il Teorema 22.6 nel modo seguente.

Teorema. Se $0 \leq u \leq t$ e $0 \leq v \leq t$, allora

$$N(mt+u+v) \geq \min\{N(m), N(m+1), N(m+2), N(t)-2, N(u), N(v)\}.$$

Problema 22H. Mostrare che $N(21) \geq 4$.

Problema 22I. Mostrare che $N(51) \geq 4$.

Orig. 300

Problema 22J. Supponiamo di aver mostrato, dando esempi, che $N(n) \geq 3$ per $a \leq n \leq 7a+3$. Mostrare che $N(n) \geq 3$ per $7a \leq n \leq 7^2 a$ e concludere che $N(n) \geq 3$ per $n \geq a$.

Note

Sono d'uso comune l'espressione "quadrati latini mutuamente ortogonali", anziché "a due a due ortogonali", e l'acronimo inglese "MOLS".

Abbiamo già menzionato Eulero nelle note al Capitolo 1. Il suo articolo del 1782 aveva il titolo "Un nuovo tipo di quadrato magico", perché Eulero aveva notato che da una coppia di quadrati latini ortogonali si ricavano particolari quadrati magici. Per esempio, cambiamo gli insiemi dei simboli di A e B nella Fig. 22.1 rispettivamente in $\{4, 3, 2, 1\}$ e $\{12, 8, 4, 0\}$, e sommiamo invece di sovrapporre. Otteniamo

$$\begin{pmatrix} 16 & 11 & 6 & 1 \\ 2 & 5 & 12 & 15 \\ 9 & 14 & 3 & 8 \\ 7 & 4 & 13 & 10 \end{pmatrix}.$$

Ogni riga e ogni colonna di questa matrice ha somma 34. La proprietà latina non implica in generale che anche le diagonali abbiano per somma il "numero magico", ma il nostro esempio è un quadrato particolarmente gradevole: le diagonali, i quattro angoli e molti altri insiemi di quattro elementi hanno somma 34.

Gli autori sono consapevoli che nella Fig. 22.1 "A" viene usato sia come nome di una matrice sia come elemento della stessa matrice. Vogliamo soltanto verificare che il lettore sia attento.

I quadrati latini ortogonali, spesso nella forma di schieramenti ortogonali, sono di grande importanza nella teoria statistica del disegno degli esperimenti.

L'articolo di MacNeish del 1922 contiene in realtà una dimostrazione errata della congettura di Eulero.

Il collegamento fra quadrati latini ortogonali e piani proiettivi finiti fu osservato da R. C. Bose (1938).

Molti risultati sui quadrati latini ortogonali erano stati anticipati da E. H. Moore (1896), come R. D. Baker ha fatto notare agli autori. Purtroppo, nell'articolo di Moore non compare mai l'espressione "quadrato latino", per cui i suoi risultati passarono inosservati per molto tempo. Fra essi figurano casi particolari dei Teoremi 22.3 e 22.4, sebbene in forme completamente diverse, e descrizioni di piani proiettivi il cui ordine è una potenza di primo; egli avrebbe quindi potuto confutare la congettura di MacNeish se l'avesse conosciuta. Orig. 301

Il Teorema 22.6 è un caso particolare di una costruzione di Wilson (1974), a sua volta generalizzata in diversi modi. Si veda T. Beth, D. Jungnickel e H. Lenz (1986).

Usando metodi simili a quello del Problema 22J, il secondo autore di questo libro dimostrò che $N(n) \geq 3$ per $n \geq 47$. Attualmente è noto che $N(n) \geq 3$ per $n > 10$. Per limiti inferiori recenti di $N(n)$ per vari n si veda Colbourn e Dinitz (1996).

Il Teorema 22.8 è dovuto a Chowla, Erdős e Straus (1960). Essi dimostrarono di più: $N(n) \geq n^{1/91}$ per n sufficientemente grande. Il loro lavoro è di natura aritmetica e si basa sulle costruzioni di Bose–Parker–Shrikhande. Il risultato è stato migliorato più volte, ma il migliore risultato a oggi è quello di T. Beth (1983). Ciò sembra ben lontano dalla verità effettiva. È del tutto possibile che, per esempio, $N(n) \geq n/10$ per tutti i valori di n, o per tutti tranne un numero finito, ma al momento sembra incredibilmente difficile dimostrarlo.[4]

Riferimenti bibliografici

T. Beth (1983)
Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, *Abh. Math. Sem. Hamburg* **53**, 284–288.

T. Beth, D. Jungnickel, and H. Lenz (1986)
Design Theory, Bibliographisches Institut.

R. C. Bose (1938)
On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, *Sanhkya* **3**, 323–338.

R. C. Bose, S. S. Shrikhande, and E. T. Parker (1960)
Further results in the construction of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Canad. J. Math.* **12**, 189–203.

S. Chowla, P. Erdős, and E. G. Straus (1960)
On the maximal number of pairwise orthogonal Latin squares of a given order, *Canad. J. Math.* **12**, 204–208.

C. J. Colbourn and J. H. Dinitz, editors (1996)
The CRC Handbook of Combinatorial Designs, CRC Press.

Orig. 302

A. L. Dulmage, D. Johnson, and N. S. Mendelsohn (1961)
Orthomorphisms of groups and orthogonal Latin squares, *Canadian J. Math.* **13**, 356–372.

M. Hall and L. J. Paige (1955)
Complete mappings of finite groups, *Pacific J. Math.* **5**, 541–549.

H. F. MacNeish (1922)
Euler squares, *Ann. Math.* **23**, 221–227.

H. B. Mann (1950)
On orthogonal Latin squares, *Bull. Amer. Math. Soc.* **50**, 249–257.

E. H. Moore (1896)
Tactical memoranda I–III, *Amer. J. Math.* **18**, 264–303.

[4]Nota redazionale: "attualmente", "recente" e "a oggi" in queste note si riferiscono all'epoca della seconda edizione originale, non alla data della traduzione.

P. J. Schellenberg, G. M. J. Van Rees, and S. A. Vanstone (1978)
Four pairwise orthogonal Latin squares of order 15, *Ars Comb.* **6**, 141–150.

D. R. Stinson (1984)
Nonexistence of a Pair of Orthogonal Latin Squares of Order Six, *J. Combinatorial Theory (A)* **36**, 373–376.

R. M. Wilson (1974)
Concerning the number of mutually orthogonal Latin squares, *Discrete Math.* **9**, 181–198.

Capitolo 23

Geometrie proiettive e combinatorie

Una *geometria combinatoria* è una coppia $(X, \mathcal{F})$, dove X è un insieme di punti e $\mathcal{F}$ è una famiglia di sottoinsiemi di X, chiamati *sottospazi chiusi* (*flats*), tale che: Orig. 303

1. $\mathcal{F}$ è chiusa rispetto all'intersezione di due elementi;
2. nell'insieme parzialmente ordinato $\mathcal{F}$ non vi sono catene infinite;
3. $\mathcal{F}$ contiene l'insieme vuoto, tutti i singoletti $\{x\}$, $x \in X$, e lo stesso insieme X;
4. per ogni sottospazio chiuso $E \in \mathcal{F}$, $E \neq X$, i sottospazi chiusi che coprono E in $\mathcal{F}$ partizionano i punti rimanenti.

Qui dire che F *copre* E in $\mathcal{F}$ significa che $E, F \in \mathcal{F}$, $E \subsetneq F$, ma non esiste $G \in \mathcal{F}$ con $E \subsetneq G \subsetneq F$. L'ultima proprietà dovrebbe essere familiare al lettore dalla geometria: le rette che contengono un punto dato partizionano i punti rimanenti; i piani che contengono una retta data partizionano i punti rimanenti.

Un esempio banale di geometria consiste in un insieme finito X, con tutti i suoi sottoinsiemi come sottospazi chiusi. È l'algebra booleana su X.

Osserviamo che (1) e (2) implicano che $\mathcal{F}$ sia chiusa rispetto a intersezioni arbitrarie.

Esempio 23.1. Ogni spazio lineare, come introdotto nel Capitolo 19, dà una geometria combinatoria sul proprio insieme di punti X, prendendo come sottospazi chiusi $\varnothing$, tutti i singoletti $\{x\}$, tutte le rette e X stesso. Il fatto che le rette per un punto dato partizionino i punti rimanenti è un altro modo di dire che due punti determinano una retta unica.

Esempio 23.2. Ogni sistema di Steiner $S(t, k, v)$ dà una geometria combinatoria sul proprio insieme di punti X, prendendo come sottospazi chiusi tutti i sottoinsiemi di cardinalità minore di t, tutti i blocchi e X. Per ottenere una geometria con questa costruzione non occorre che tutti i blocchi abbiano la stessa cardinalità, ma soltanto che ogni sottoinsieme di t elementi sia contenuto in un unico blocco; si confronti il Problema 19R, dove abbiamo chiamato queste strutture sistemi di Steiner generalizzati. Orig. 304

Esempio 23.3. Sia V uno spazio vettoriale di dimensione n su un campo $\mathbb{F}$. Per *sottospazio affine* di V intendiamo l'insieme vuoto oppure una classe laterale, cioè una traslata, di un sottospazio ordinario, ossia lineare, di V nel gruppo additivo. Per esempio, per $a, b \in \mathbb{F}$, il sottoinsieme $\{(x, y) : y = ax + b\}$ è un sottospazio affine di $\mathbb{F}^2$. L'insieme V con tutti i suoi sottospazi affini forma una geometria combinatoria chiamata *geometria affine* $AG_n(\mathbb{F})$. Scriviamo $AG_n(q)$ per $AG_n(\mathbb{F}_q)$; il caso $n = 2$ è stato introdotto nel Capitolo 19.

Esempio 23.4. La *geometria proiettiva* $PG_n(\mathbb{F})$, pur essendo più fondamentale di $AG_n(\mathbb{F})$, può essere un po' più scomoda da definire. Sia V uno spazio vettoriale di dimensione $n+1$ su un campo $\mathbb{F}$. L'insieme dei punti X di $PG_n(\mathbb{F})$ è costituito da tutti i sottospazi lineari unidimensionali di V. Per esempio, se $\mathbb{F} = \mathbb{F}_q$ è il campo con q elementi, il numero dei punti proiettivi di $PG_n(\mathbb{F}_q)$ è

$$\frac{q^{n+1} - 1}{q - 1} = q^n + \cdots + q^2 + q + 1.$$

A ogni sottospazio lineare W di V associamo un sottospazio chiuso F_W, costituito da tutti i sottospazi unidimensionali di V contenuti in W, e prendiamo come $\mathcal{F}$ la famiglia di tutti questi F_W. Scriviamo $PG_n(q)$ per $PG_n(\mathbb{F}_q)$; il caso $n = 2$ è stato introdotto nel Capitolo 19.

Le geometrie proiettive $PG_n(\mathbb{F})$ si possono definire anche quando $\mathbb{F}$ è un anello con divisione, nel quale la moltiplicazione non è necessariamente commutativa; si veda Crawley e Dilworth (1973).

Sia Y un sottoinsieme qualsiasi dell'insieme di punti X di una geometria combinatoria $(X, \mathcal{F})$ e poniamo

$$\mathcal{E} := \{F \cap Y : F \in \mathcal{F}\}.$$

Allora anche $(Y, \mathcal{E})$ è una geometria combinatoria, la *sottogeometria su* Y. Per esempio, $AG_n(\mathbb{F})$ è una sottogeometria di $PG_n(\mathbb{F})$. Esiste un'immersione standard dell'insieme dei punti di $AG_n(\mathbb{F})$ nell'insieme dei punti di $PG_n(\mathbb{F})$: a ogni vettore $\mathbf{x}$ di uno spazio vettoriale V di dimensione n associamo il sottospazio unidimensionale generato da $(\mathbf{x}, 1)$ nello spazio $V \times \mathbb{F}$, di dimensione $n + 1$. L'immagine è costituita da tutti i punti proiettivi non contenuti nell'iperpiano $V \times 0$. Orig. 305

L'insieme $\mathcal{F}$ dei sottospazi chiusi di una geometria combinatoria, ordinato per inclusione, ha diverse proprietà importanti.

Un *reticolo* L è un insieme parzialmente ordinato nel quale ogni sottoinsieme finito $S \subseteq L$ ha un *estremo inferiore*, cioè un elemento $b \in L$ tale che

$$(\forall a \in S \quad b \le a) \qquad \text{e} \qquad (\forall a \in S \quad c \le a) \Longrightarrow c \le b,$$

e un *estremo superiore*, cioè un elemento $b \in L$ tale che

$$(\forall a \in S \quad b \ge a) \qquad \text{e} \qquad (\forall a \in S \quad c \ge a) \Longrightarrow c \ge b.$$

Gli estremi inferiore e superiore di un insieme di due elementi $\{x, y\}$ si indicano rispettivamente con $x \wedge y$ e $x \vee y$. Si vede facilmente che $\wedge$ e $\vee$ sono operazioni binarie commutative, associative e idempotenti; inoltre, se tutti i sottoinsiemi di due elementi hanno estremi inferiore e superiore, ogni sottoinsieme finito li possiede.

I reticoli che considereremo non hanno catene infinite. Un tale reticolo ha un unico elemento minimo, che indichiamo con 0_L: l'assenza di catene infinite permette infatti di trovare un elemento minimale m, e ogni elemento minimale è minimo, poiché, se $m \not\le a$, allora $m \wedge a$ sarebbe minore di m. Analogamente, esiste un unico elemento massimo 1_L.

Per due elementi a, b di un insieme parzialmente ordinato, diciamo che a *copre* b, e scriviamo $a \gtrdot b$, se $a > b$ ma non esiste c con $a > c > b$. Per esempio, per sottospazi lineari U, W di uno spazio vettoriale, $U \gtrdot W$ quando $U \supseteq W$ e $\dim U = \dim W + 1$. Ricordiamo che una catena in un insieme parzialmente ordinato P è un sottoinsieme totalmente ordinato di P. Una catena finita può dunque essere pensata come una successione $a_0 < a_1 < \cdots < a_n$. Un *punto* di un reticolo L con elemento minimo 0_L è un elemento che copre 0_L.

Un *reticolo geometrico* è un reticolo L senza catene infinite tale che:

1. L è atomico, cioè ogni elemento è l'estremo superiore di punti di L;
2. L è semimodulare, cioè, se a, b sono distinti e coprono entrambi c in L, allora $a \vee b$ copre sia a sia b.

Orig. 306

Teorema 23.1. L'insieme dei sottospazi chiusi di una geometria combinatoria, ordinato per inclusione, è un reticolo geometrico. Viceversa, dato un reticolo geometrico L con insieme dei punti X, la coppia $(X, \{F_y : y \in L\})$ è una geometria combinatoria, dove

$$F_y := \{x \in X : x \le y\}.$$

Dimostrazione. Poiché la famiglia $\mathcal{F}$ dei sottospazi chiusi di una geometria combinatoria è chiusa rispetto all'intersezione, il suo insieme parzialmente ordinato è un reticolo atomico: l'estremo inferiore di due sottospazi chiusi è la loro intersezione e l'estremo superiore è l'intersezione di tutti i sottospazi chiusi che li contengono entrambi. Supponiamo che F_1 e F_2 coprano un sottospazio chiuso E. Sia $x \in F_1 \setminus F_2$. Esiste un sottospazio chiuso G_2 che copre F_2 e contiene x. Esso contiene F_1, altrimenti avremmo $E \subsetneq F_1 \cap G_2 \subsetneq F_1$. Ma, per un argomento simmetrico, esiste un sottospazio chiuso G_1 che copre F_1 e contiene anch'esso F_1 e F_2. L'estremo superiore $F_1 \vee F_2$ deve essere contenuto sia in G_1 sia in G_2. Poiché G_i copre F_i, abbiamo $F_1 \vee F_2 = G_1 = G_2$.

Sia L un reticolo geometrico e definiamo i sottospazi chiusi F_y come sottoinsiemi dell'insieme di punti X secondo l'enunciato. È chiaro che l'insieme vuoto, ogni singoletto e X sono sottospazi chiusi, scegliendo y rispettivamente uguale a 0_L, a un punto di L o a 1_L. Poiché $x \le y$ e $x \le z$ se e solo se $x \le y \wedge z$, vale $F_y \cap F_z = F_{y\wedge z}$; dunque $\mathcal{F} := \{F_y : y \in L\}$ è chiusa rispetto all'intersezione. Nessun punto x esterno a F_y può appartenere a due sottospazi chiusi che coprono F_y, quindi resta soltanto da mostrare che un sottospazio chiuso che copre F_y contiene x. Completiamo la dimostrazione mostrando che $F_{x\vee y}$ copre F_y.

Ciò equivale a mostrare che $x \vee y \gtrdot y$ in L quando $x \not\le y$ e x è un punto di L. Scegliamo una catena massimale

$$0_L \lessdot y_1 \lessdot y_2 \lessdot \cdots \lessdot y_k = y.$$

Poiché x e y_1 coprono 0_L, $x \vee y_1$ copre y_1. Poiché $x \vee y_1$ e y_2 coprono y_1, $x \vee y_2$ copre y_2, essendo chiaramente $x \vee y_1 \vee y_2 = x \vee y_2$. Per induzione otteniamo che $x \vee y_k$ copre y_k. □

In un certo senso la differenza fra reticoli geometrici e geometrie combinatorie è la stessa che intercorre fra strutture d'incidenza, da un lato, e famiglie di sottoinsiemi di un insieme, dall'altro. Strutture d'incidenza e reticoli sono più astratti e vanno usati in certi casi per evitare confusione, per esempio discutendo dualità o intervalli; per molti argomenti preferiamo però il linguaggio e la notazione degli insiemi e dei sottoinsiemi. Orig. 307

Per esempio, per elementi a, b di un insieme parzialmente ordinato, l'*intervallo* $[a, b]$ è definito da $[a, b] := \{x : a \le x \le b\}$. Ogni intervallo di un reticolo è ancora un reticolo. Il lettore verifichi che ogni intervallo di un reticolo geometrico è ancora un reticolo geometrico. Sarebbe scomodo enunciare il fatto corrispondente in termini di geometrie combinatorie.

Per il Teorema 23.1, o più precisamente per le semplici corrispondenze descritte nella dimostrazione, è spesso comodo, anche se talvolta fonte di confusione, mescolare notazione e linguaggio delle geometrie combinatorie e dei reticoli geometrici. Per esempio, possiamo usare lo stesso simbolo $PG_n(\mathbb{F})$ per la geometria combinatoria e per il corrispondente reticolo dei sottospazi di uno spazio vettoriale.

Problema 23A. (i) Ogni intervallo di $PG_n(\mathbb{F})$ è isomorfo, come insieme parzialmente ordinato, a $PG_m(\mathbb{F})$ per qualche $m \le n$. (ii) $PG_n(\mathbb{F})$ è isomorfo al proprio insieme parzialmente ordinato duale, nel quale l'ordine è invertito.

Esempio 23.5. I *reticoli delle partizioni* Π_n, i cui elementi sono tutte le partizioni di un insieme X di n elementi, forniscono un'altra famiglia di reticoli geometrici e quindi di geometrie combinatorie. Le partizioni sono ordinate per raffinamento: $\mathcal{A}$ è un raffinamento di $\mathcal{B}$ se ogni blocco di $\mathcal{B}$ è unione di blocchi di $\mathcal{A}$. L'elemento minimo, la partizione più fine, è quindi la famiglia di tutti i singoletti $\{\{x\} : x \in X\}$, e l'elemento massimo è $\{X\}$, formato da un unico blocco. Un momento di riflessione mostra che una partizione ne copre un'altra se si ottiene da essa fondendo due blocchi in uno solo. I punti sono le partizioni costituite da un blocco di cardinalità 2 e da $n-2$ singoletti.

Per esempio, Π_4 ha 15 elementi:

$$\{1234\},$$
$$\{123,4\},\{124,3\},\{134,2\},\{234,1\},\{12,34\},\{13,24\},\{14,23\},$$
$$\{12,3,4\},\{13,2,4\},\{14,2,3\},\{23,1,4\},\{24,1,3\},\{34,1,2\},$$
$$\{1,2,3,4\}.$$

Per semplificare la notazione, abbiamo scritto, per esempio, $\{123,4\}$ al posto di $\{\{1,2,3\},\{4\}\}$. Orig. 308

Esempio 23.6. I punti di Π_n sono in corrispondenza biunivoca con gli spigoli di K_n. Dato un grafo semplice G su n vertici, otteniamo un reticolo geometrico $L(G)$ i cui punti corrispondono all'insieme degli spigoli $E(G)$ nel modo seguente. Gli elementi di L sono tutte le partizioni $\mathcal{A}$ di $V(G)$ per le quali il sottografo di G indotto da ogni blocco di $\mathcal{A}$ è connesso. Tali partizioni sono esattamente quelle che si ottengono come estremo superiore, in Π_n, di punti di Π_n corrispondenti a un sottoinsieme degli spigoli di G. I reticoli $L(G)$ sono talvolta chiamati *reticoli delle contrazioni* di G; si veda il Capitolo 33.

La Fig. 23.1 cerca di illustrare le geometrie combinatorie $L(K_4)$ e $L(K_5)$. Per esempio, $L(K_5)$ ha dieci punti; il punto della figura etichettato 12 rappresenta il punto, ossia la partizione, $\{12,3,4,5\}$. Le partizioni del tipo $\{123,4,5\}$ contengono tre punti e sono rappresentate da segmenti; le rette con due punti non sono disegnate. Si noti che $L(K_4)$, con sei punti e sette rette, è la geometria ottenuta eliminando un punto dalla configurazione di Fano.

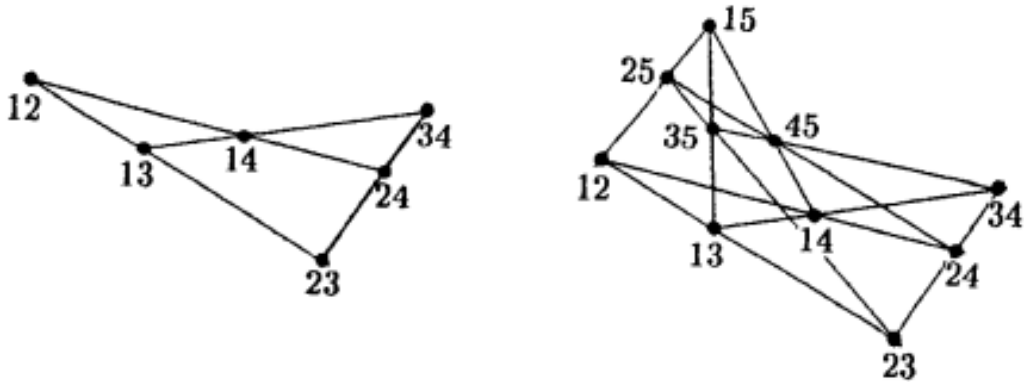


Figura 23.1

Per un sottoinsieme S dei punti di una geometria combinatoria, la *chiusura* $\overline{S}$ è l'intersezione di tutti i sottospazi chiusi contenenti S. Per esempio, in uno spazio lineare la chiusura di un insieme di due punti è la retta che li contiene. Esercizio: mostrare che $S \subseteq \overline{S}$, che $A \subseteq B \Longrightarrow \overline{A} \subseteq \overline{B}$ e che $\overline{\overline{S}} = \overline{S}$. Talvolta converrà usare il simbolo dell'estremo superiore nel reticolo dei sottospazi chiusi; si noti che

$$E \vee F := \overline{E \cup F}.$$

Un sottoinsieme $S \subseteq X$ è *indipendente* se per ogni $x \in S$ vale $x \notin \overline{S \setminus \{x\}}$. Nell'Esempio 23.1, tre punti di uno spazio lineare sono indipendenti se e solo se non sono contenuti in una retta; nessun insieme di quattro punti è indipendente. Un insieme di punti di $PG_n(\mathbb{F})$ è indipendente se e solo se i vettori rappresentanti sono linearmente indipendenti. Un insieme di punti di $AG_n(\mathbb{F})$ è indipendente se e solo se i vettori sono affinemente indipendenti. Un modo di vedere le geometrie combinatorie è considerarle come lo studio dell'"indipendenza astratta". Orig. 309

Per *rango* di una geometria combinatoria con insieme di punti X intendiamo la massima cardinalità di un sottoinsieme indipendente di X. Sia $PG_n(\mathbb{F})$ sia $AG_n(\mathbb{F})$ hanno rango $n+1$. Eviteremo la parola *dimensione*; se però dimenticassimo questa convenzione e la usassimo, essa significherà il rango meno uno. La massima cardinalità di un sottoinsieme indipendente di un sottospazio chiuso F è il rango di F. I sottospazi chiusi di rango 1 si chiamano punti, quelli di rango 2 rette, quelli di rango 3 piani. Quelli il cui rango è uno meno di $\operatorname{rank}(X)$ si chiamano *iperpiani* o *copunti*. Talvolta ci occorrerà il termine *coretta* per un sottospazio chiuso di rango $\operatorname{rank}(X) - 2$.

Da ogni geometria combinatoria $(X, \mathcal{F})$ otteniamo uno spazio lineare $(X, \mathcal{L})$, dove $\mathcal{L}$ è la famiglia di tutte le rette, cioè dei sottospazi chiusi di rango 2.

Nella Fig. 23.1 due punti qualsiasi determinano una retta che può avere due o tre punti; soltanto queste ultime sono disegnate. I piani di $L(K_5)$ hanno quattro oppure sei punti; quelli con sei punti contengono quattro rette di tre punti.

Raccogliamo alcuni fatti semplici.

Lemma 23.2.

1. Se $x \notin \overline{A}$ ma $x \in \overline{A \cup \{y\}}$, allora $y \in \overline{A \cup \{x\}}$: è l'*assioma di scambio*.
2. Se S è un insieme indipendente di punti di una geometria e $x \notin \overline{S}$, allora $\{x\} \cup S$ è indipendente.
3. Se $F = \overline{S}$, allora $F = \overline{A}$ per ogni sottoinsieme indipendente massimale A di S.

Dimostrazione. $F_1 := \overline{A \cup \{x\}}$ è il sottospazio chiuso che copre $E := \overline{A}$ e contiene x; $F_2 := \overline{A \cup \{y\}}$ è quello che copre E e contiene y. Se $x \in F_2$, deve essere $F_1 = F_2$. Ciò dimostra (1).

Se $\{x\} \cup S$ non è indipendente, esiste un $y \in S$ tale che $y \in \overline{(S \cup \{x\}) \setminus \{y\}}$. Poniamo $A := S \setminus \{y\}$. Poiché S è indipendente, $y \notin \overline{A}$. Ma (1) implica allora $x \in \overline{A \cup \{y\}}$, cioè $x \in \overline{S}$. Ciò dimostra (2). Orig. 310

Supponiamo $F = \overline{S}$ e che A sia un sottoinsieme indipendente di S massimale rispetto a tale proprietà. Se $S \nsubseteq \overline{A}$, per (2) potremmo trovare un sottoinsieme indipendente di S più grande. Dunque $S \subseteq \overline{A}$ e, poiché F è il più piccolo sottospazio chiuso contenente S, $F \subseteq \overline{A}$. Ciò dimostra (3). □

Una *base* di un sottospazio chiuso F è un sottoinsieme indipendente $B \subseteq F$ tale che $\overline{B} = F$, ossia un sottoinsieme indipendente massimale di F. Come esercizio, il lettore verifichi che avremmo potuto

definire una base di F anche come un insieme generatore minimale, cioè un sottoinsieme B con $\overline{B} = F$ minimale rispetto a questa proprietà.

Problema 23B. Sia G un grafo semplice connesso. Mostrare che le basi della geometria combinatoria $L(G)$ sono esattamente gli insiemi di spigoli degli alberi ricoprenti di G.

Teorema 23.3. Tutte le basi di un sottospazio chiuso F di una geometria combinatoria hanno la stessa cardinalità finita, chiamata rango di F. Per sottospazi chiusi E, F,

$$\operatorname{rank}(E) + \operatorname{rank}(F) \geq \operatorname{rank}(E \cap F) + \operatorname{rank}(E \vee F). \tag{23.1}$$

Dimostrazione. Dovrebbe essere chiaro che l'assenza di catene infinite di sottospazi chiusi costringe tutti gli insiemi indipendenti a essere finiti.

Se non fosse vero che tutte le basi di F hanno la stessa cardinalità, scegliamo una coppia ordinata (B_1, B_2) di basi con $|B_1| > |B_2|$, ma con $|B_2 \setminus B_1|$ minimo fra le coppie che soddisfano tale vincolo. Scegliamo $x \in B_1 \setminus B_2$. Allora $B_1 \setminus \{x\}$ è indipendente e ha una chiusura che non contiene F, e quindi non contiene B_2. Scegliamo $y \in B_2 \setminus B_1$ tale che $y \notin \overline{B_1 \setminus \{x\}}$. Per il Lemma 23.2, $(B_1 \setminus \{x\}) \cup \{y\}$ è indipendente ed è contenuto in una base B_3 di F. Abbiamo ora una coppia ordinata (B_3, B_2)[1] di basi con $|B_3| > |B_2|$, mentre $B_2 \setminus B_3$ è un sottoinsieme proprio di $B_2 \setminus B_1$, una contraddizione.

Per dimostrare la seconda parte, osserviamo anzitutto che il Lemma 23.2(2) implica che una base di un sottospazio chiuso E si può estendere a una base di qualunque sottospazio chiuso E' contenente E.

Sia ora B una base di $E \cap F$. Estendiamo B a basi B_1, B_2 di E, F rispettivamente. Ogni sottospazio chiuso contenente $B_1 \cup B_2$ contiene E e F, quindi $\overline{E \cup F}$: ossia $\overline{B_1 \cup B_2} = \overline{E \cup F}$, e $B_1 \cup B_2$ contiene una base di $\overline{E \cup F}$. Pertanto Orig. 311

$$\begin{aligned} \operatorname{rank}(\overline{E \cup F}) &\leq |B_1 \cup B_2| = |B_1| + |B_2| - |B_1 \cap B_2| \\ &= \operatorname{rank}(E) + \operatorname{rank}(F) - \operatorname{rank}(E \cap F). \end{aligned}$$

□

La disuguaglianza (23.1) si chiama *legge semimodulare*.

Osserviamo che la dimostrazione del Teorema 23.3 mostra che tutti i sottoinsiemi indipendenti massimali di un qualunque sottoinsieme S, non necessariamente chiuso, hanno la stessa cardinalità. Ciò è comunque un corollario dell'enunciato per i sottospazi chiusi, poiché possiamo applicare il Teorema 23.3[2] alla sottogeometria su S.

Come esercizio, assicurarsi di comprendere quanto segue: siano $E \subseteq F$ sottospazi chiusi di una geometria. Se $\operatorname{rank}(E) = \operatorname{rank}(F)$, allora $E = F$; F copre E se e solo se $\operatorname{rank}(F) = \operatorname{rank}(E) + 1$.

Per le geometrie affini $AG_n(q)$, il numero di punti di un sottospazio chiuso di rango r è q^r. Per le geometrie proiettive $PG_n(q)$ il numero di punti di un sottospazio chiuso di rango r è

$$\frac{q^{r+1} - 1}{q - 1} = q^r + \cdots + q^2 + q + 1. \tag{23.2}$$

[3]

Teorema 23.4. Supponiamo che ogni sottospazio chiuso di rango i in una geometria combinatoria su v punti abbia esattamente k_i punti, per $i = 0, 1, \ldots, n$. Allora il numero totale di sottospazi chiusi di rango r è

$$\prod_{i=0}^{r-1} \frac{v - k_i}{k_r - k_i}. \tag{23.3}$$

Inoltre i punti, insieme alla famiglia dei sottospazi chiusi di rango r, formano un 2-disegno.

Dimostrazione. Poiché i sottospazi chiusi di rango $r+1$ contenenti un dato sottospazio chiuso di rango r partizionano i $v - k_r$ punti rimanenti in insiemi di cardinalità $k_{r+1} - k_r$, ve ne sono esattamente

[1] Nota redazionale: l'originale stampa qui (B_3, B_1), ma i confronti successivi riguardano B_2; è stato corretto il secondo indice.

[2] Nota redazionale: l'originale rinvia al Teorema 23.4, ma il risultato pertinente è il Teorema 23.3.

[3] Nota redazionale: in questo paragrafo l'originale confonde rango e dimensione. Con il rango definito a p. 309, i due numeri corretti sono rispettivamente q^{r-1} e $(q^r - 1)/(q - 1)$ per $r \geq 1$. Le formule stampate sopra sono quelle originali e valgono usando r come dimensione.

$(v - k_r)/(k_{r+1} - k_r)$. La formula (23.3) segue per induzione su r, contando le coppie ordinate (E, F) di sottospazi chiusi di ranghi r e $r+1$ con $E \subseteq F$. Si noti che $k_0 = 0$ e $k_1 = 1$, quindi la (23.3) vale per $r = 1$. Ogni coppia di punti è contenuta in un unico sottospazio chiuso di rango 2. L'argomento precedente implica che ogni sottospazio chiuso di rango 2 sia contenuto nello stesso numero di sottospazi chiusi di rango r. Questi ultimi danno dunque un 2-disegno. □ Orig. 312

I numeri dei sottospazi chiusi di rango r di $PG_n(q)$ si chiamano *numeri gaussiani*; si veda il Capitolo 24. Le equazioni (23.2) e (23.3) implicano che i numeri dei punti e degli iperpiani di $PG_n(q)$ siano uguali, cosa che si può vedere anche in altri modi. Abbiamo quindi il corollario seguente.

Corollario. I punti e gli iperpiani della geometria proiettiva $PG_n(q)$ formano un disegno simmetrico (v, k, λ) con

$$v = \frac{q^{n+1} - 1}{q - 1}, \qquad k = \frac{q^n - 1}{q - 1}, \qquad \lambda = \frac{q^{n-1} - 1}{q - 1}.$$

Problema 23C. Mostrare che la struttura d'incidenza i cui punti sono quelli di $AG_r(2)$ e i cui blocchi sono i piani di $AG_r(2)$ è un sistema di Steiner $S(3, 4, 2^r)$.

Il teorema seguente è dovuto a C. Greene (1970).

Teorema 23.5. In una geometria combinatoria finita il numero degli iperpiani è almeno uguale al numero dei punti.

Dimostrazione. La dimostrazione sarà simile a quella del Teorema 19.1. Mostriamo anzitutto, per induzione sul rango, che se un punto x non appartiene a un iperpiano H, il numero r_x degli iperpiani per x è almeno pari al numero k_H dei punti di H. L'asserto è banale per geometrie di rango al più 2. Per l'ipotesi induttiva sappiamo che il numero degli iperpiani della sottogeometria su H, cioè delle corette C contenute in H, è almeno k_H. Per ogni tale coretta C otteniamo però un iperpiano per x, l'estremo superiore di C e x.

Riprendiamo ora la dimostrazione del Teorema 19.1. Siano $\mathcal{H}$ l'insieme degli iperpiani, $v := |X|$ e $b := |\mathcal{H}|$. Supponiamo $b \le v$. Allora

$$1 = \sum_{x \in X} \sum_{\substack{H \in \mathcal{H} \\ x \notin H}} \frac{1}{v(b - r_x)} \ge \sum_{H \in \mathcal{H}} \sum_{x \notin H} \frac{1}{b(v - k_H)} = 1.$$

Ne segue che in tutte le disuguaglianze deve valere l'uguaglianza, e quindi $v = b$. □ Per il caso di uguaglianza nel Teorema 23.5, si veda l'osservazione che segue il Lemma 23.8. Orig. 313

Nello studio di $PG_n(\mathbb{F})$ ha un ruolo cruciale la formula delle dimensioni

$$\dim(U \cap W) + \dim(U + W) = \dim U + \dim W$$

per sottospazi lineari di uno spazio vettoriale. Equivalentemente,

$$\operatorname{rank}(E \cap F) + \operatorname{rank}(E \vee F) = \operatorname{rank}(E) + \operatorname{rank}(F) \tag{23.4}$$

per sottospazi chiusi E, F di $PG_n(\mathbb{F})$. Questa è una versione più forte della legge semimodulare. Una geometria combinatoria nella quale vale la (23.4) si dice infatti *modulare*. Per esempio, in una geometria combinatoria modulare la (23.4) implica che due rette contenute in un piano abbiano intersezione non vuota; si confronti il Teorema 19.1.

Problema 23D. Sia $(X, \mathcal{B})$ lo spazio lineare costituito dai punti e dalle rette di una geometria combinatoria modulare finita di rango 3. Mostrare che $(X, \mathcal{B})$ è un quasifascio, come definito dopo il Teorema 19.1, oppure un piano proiettivo, come definito nel Capitolo 19: cioè mostrare che tutte le rette hanno la stessa cardinalità $n + 1$ e che vi sono esattamente $n^2 + n + 1$ punti, per un intero $n \ge 2$.

Abbiamo introdotto le geometrie proiettive $PG_n(\mathbb{F})$ e definito i piani proiettivi nel Capitolo 19. Ecco la definizione generale: una *geometria proiettiva* è una geometria combinatoria modulare *connessa*, nel senso che l'insieme dei punti non si può esprimere come unione di due sottospazi chiusi propri.

Non abbiamo qui lo spazio né il tempo per dimostrare il seguente risultato fondamentale. Per una dimostrazione si vedano Veblen e Young (1907) oppure Crawley e Dilworth (1973).

Teorema 23.6. Ogni geometria proiettiva di rango $n \geq 4$ è isomorfa a $PG_n(\mathbb{F})$ per un opportuno anello con divisione $\mathbb{F}$.[4]

Le geometrie combinatorie di rango al più 2 non presentano grande interesse, ma sono tutte modulari e, eccetto la retta con due punti, sono geometrie proiettive. Le geometrie proiettive di rango 3, per il Problema 23D, sono equivalenti ai piani proiettivi introdotti nel Capitolo 19; i quasifasci non sono connessi. Orig. 314

Ogni geometria combinatoria modulare si può assemblare a partire da geometrie proiettive. È il contenuto del problema seguente.

Problema 23E.

(i) Siano $(X_1, \mathcal{F}_1)$ e $(X_2, \mathcal{F}_2)$ geometrie combinatorie modulari, con $X_1 \cap X_2 = \varnothing$. Mostrare che $(X_1 \cup X_2, \{F_1 \cup F_2 : F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2\})$ è una geometria combinatoria modulare.

(ii) Sia $(X, \mathcal{F})$ una geometria combinatoria modulare nella quale X è unione di due sottospazi chiusi X_1, X_2 con $X_1 \cap X_2 = \varnothing$. Posto $\mathcal{F}_i := \{F \cap X_i : F \in \mathcal{F}\}$, $i = 1, 2$, mostrare che $(X_i, \mathcal{F}_i)$ sono geometrie combinatorie modulari e che $\mathcal{F} = \{F_1 \cup F_2 : F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2\}$.

Problema 23F. Dimostrare che ogni sottospazio chiuso F di una geometria combinatoria $(X, \mathcal{F})$ ha un *complemento modulare*: esiste cioè un sottospazio chiuso E tale che $E \cap F = \varnothing$, $E \vee F = X$ e $\operatorname{rank}(E) + \operatorname{rank}(F) = \operatorname{rank}(X)$.

Gli spazi lineari costituiti dai punti e dalle rette di geometrie combinatorie modulari soddisfano la seguente condizione, nota come *assioma di Pasch*: una retta che incontra due lati di un triangolo incontra anche il terzo. Più precisamente, siano A, B, C rette distinte e a, b, c punti distinti con le incidenze indicate nella Fig. 23.2. Richiediamo che ogni retta L contenente un punto della retta C diverso da a, b e un punto della retta B diverso da a, c contenga anche un punto della retta A diverso da b, c. Si veda la Fig. 23.2. Per verificare ciò in una geometria modulare, si osservi che L e A devono essere entrambe contenute nel piano $P = \overline{\{a, b, c\}}$, e che la legge modulare implica che due rette di un piano si incontrino.

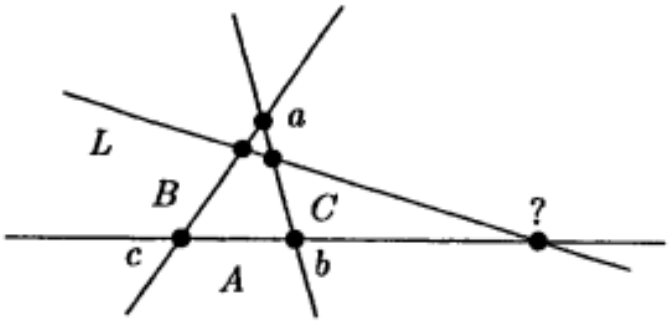


Figura 23.2

Orig. 315

Problema 23G. Considerare la struttura d'incidenza i cui punti sono i sottospazi di dimensione k di uno spazio vettoriale V e le cui rette sono i sottospazi di dimensione $k + 1$, con l'incidenza data dal contenimento. Mostrare che questa struttura soddisfa l'assioma di Pasch.

Teorema 23.7. Uno spazio lineare finito $(X, \mathcal{A})$ nel quale vale l'assioma di Pasch è costituito dai punti e dalle rette di una geometria combinatoria modulare su X.

Dimostrazione. Supponiamo che valga l'assioma di Pasch. Dobbiamo costruire i sottospazi chiusi di una geometria combinatoria e lo facciamo così: un sottoinsieme $S \subseteq X$ è un sottospazio chiuso se, per ogni retta L,

$$|L \cap S| \geq 2 \quad \Longrightarrow \quad L \subseteq S.$$

Indichiamo con $\mathcal{F}$ la famiglia di tutti questi sottospazi chiusi; essa contiene l'insieme vuoto, tutti i singoletti, X e tutte le rette di $\mathcal{A}$. Verificare che la definizione implica che l'intersezione di una famiglia qualsiasi di sottospazi chiusi sia ancora un sottospazio chiuso.

[4] Nota redazionale: con le convenzioni di questo capitolo, $PG_n(\mathbb{F})$ ha rango $n + 1$. L'enunciato deve quindi recare $PG_{n-1}(\mathbb{F})$ quando n denota il rango.

Sia x un punto non appartenente a un sottospazio chiuso S, e sia T l'unione di tutte le rette che congiungono x ai punti $s \in S$. Affermiamo che questa semplice costruzione produce un sottospazio chiuso T che copre S.

A tal fine sia L una retta contenente due punti t_1, t_2 di T. Vogliamo mostrare $L \subseteq T$. Se t_1, t_2 appartengono entrambi a una delle rette per x, allora L è quella retta e dunque $L \subseteq T$. Se invece entrambi appartengono a S, si ha ancora $L \subseteq T$; possiamo quindi supporre $t_1 \notin S$. Allora t_1, t_2 appartengono a rette distinte M_1, M_2 per x. Sia s_i il punto in cui M_i incontra S, $i = 1, 2$, e sia N la retta che congiunge s_1, s_2. Abbiamo $N \subseteq S$. L'assioma di Pasch garantisce che L incontra N in un punto $z \in S$.

Consideriamo un altro punto $t_3 \in L$ e sia M_3 la retta che congiunge x a t_3. Poiché M_3 incontra due lati del triangolo avente lati M_1, L, N e vertici z, t_1, s_1, deve incontrare il terzo lato N in un punto $s_3 \in S$. Dunque M_3 è una delle rette che congiungono x a punti di S, e $t_3 \in T$. Abbiamo dimostrato che T è un sottospazio chiuso.

È facile vedere che T copre S: se U è un sottospazio chiuso con $S \subsetneq U \subseteq T$, scegliamo $y \in U \setminus S$. Per costruzione, la retta che congiunge x e y è una delle rette per x che incontrano S; contiene due punti di U ed è quindi contenuta in U. Ne segue $x \in U$, da cui $T \subseteq U$. Poiché ogni punto appartiene a un sottospazio chiuso che copre S, $(X, \mathcal{F})$ è una geometria combinatoria. L'ipotesi che X sia finito serve soltanto qui, per garantire l'assenza di catene infinite di sottospazi chiusi. Orig. 316

Sia x un punto su una retta L e sia H un iperpiano qualsiasi. Se x non è già in H, l'estremo superiore di H e x deve essere X, perciò L deve essere una delle rette per x che incontrano H. Dunque ogni retta L e ogni iperpiano H hanno intersezione non vuota. Il Lemma 23.8 qui sotto implica allora la modularità. □

Lemma 23.8. Una geometria combinatoria è modulare se e solo se ogni retta e ogni iperpiano hanno intersezione non vuota.

Dimostrazione. La legge modulare (23.4) mostra che un sottospazio chiuso di rango 2 e uno di rango $n-1$ in una geometria di rango n si intersecano in un sottospazio chiuso di rango almeno 1.

Per il viceversa procediamo per induzione sul rango. Supponiamo che tutte le rette e tutti gli iperpiani di una geometria combinatoria di rango n si incontrino. Sia H un iperpiano e supponiamo che esistano una retta $L \subseteq H$ e un sottospazio chiuso $C \subseteq H$ di rango $n-2$ disgiunti. Allora, per un punto qualunque $x \notin H$, l'iperpiano $C \vee \{x\}$ sarebbe disgiunto dalla retta L. Per induzione, la sottogeometria su ogni iperpiano H è dunque modulare.

Quindi, se esiste una coppia di sottospazi chiusi E, F che fornisce un controesempio alla legge modulare (23.4), $E \vee F$ deve essere l'intero insieme dei punti X. Sia H un iperpiano contenente E e poniamo $F' := H \cap F$. Allora $E \vee F' \subseteq H$. Ma $\operatorname{rank}(F') \geq \operatorname{rank}(F) - 1$: altrimenti un complemento modulare di F' in F avrebbe rango almeno 2 e conterrebbe quindi una retta disgiunta da H. Vediamo allora che E, F' forniscono un controesempio alla (23.4) contenuto in H, contraddicendo la modularità della sottogeometria su H. □

Osservazione. Supponiamo che il numero degli iperpiani di una geometria combinatoria finita $(X, \mathcal{F})$ sia uguale a quello dei punti. Riesaminando la dimostrazione del Teorema 23.5, abbiamo $r_x = k_H$ quando $x \notin H$. Applicando il Teorema 23.5 all'intervallo $[\{x\}, X]$ in una qualunque geometria combinatoria, troviamo $r_x \geq l_x$, dove l_x è il numero delle rette contenenti x, poiché tali rette sono i punti del reticolo geometrico $[\{x\}, X]$. Per $x \notin H$ è evidente che $l_x \geq k_H$, essendo distinte le rette $\{x\} \vee \{y\}$, $y \in H$. In sintesi, l'uguaglianza nel Teorema 23.5 implica $l_x = k_H$ quando $x \notin H$. Ciò significa che ogni retta incontra ogni iperpiano e dunque $(X, \mathcal{F})$ è modulare per il Lemma 23.8. Orig. 317

Due triangoli $\{a_1, b_1, c_1\}$ e $\{a_2, b_2, c_2\}$ si dicono *prospettivi rispetto a un punto* se esiste un punto p, il *centro di prospettività*, tale che $\{p, a_1, a_2\}$, $\{p, b_1, b_2\}$ e $\{p, c_1, c_2\}$ siano terne collineari. Si dicono *prospettivi rispetto a una retta* se esiste una retta L, l'*asse di prospettività*, tale che $\{L, A_1, A_2\}$, $\{L, B_1, B_2\}$ e $\{L, C_1, C_2\}$ siano terne di rette concorrenti. Qui con "triangolo" intendiamo tre punti non collineari, e con A_i, B_i, C_i indichiamo i lati del triangolo opposti rispettivamente ad a_i, b_i, c_i. Ossia $A_i := \overline{\{b_i, c_i\}}$, $i = 1, 2$, e così via.

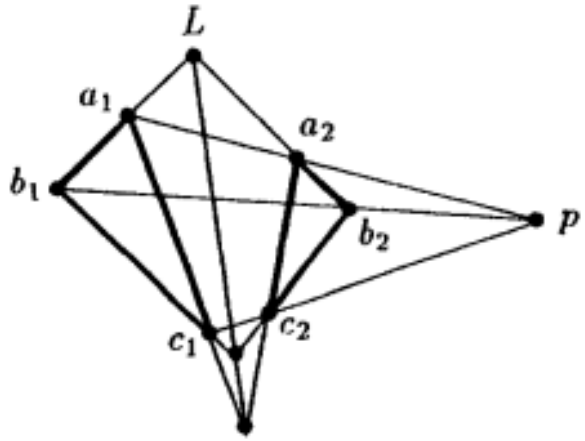


Figura 23.3

Nella Fig. 23.3 i triangoli sono prospettivi sia rispetto al punto p sia rispetto alla retta L. La struttura d'incidenza così illustrata, con dieci punti e dieci rette, ogni retta su tre punti e ogni punto su tre rette, si chiama *configurazione di Desargues*. I triangoli non devono necessariamente giacere in un piano. Il diagramma a destra della Fig. 23.1 è isomorfo, come struttura d'incidenza, a quello della Fig. 23.3! Il primo è più facile da immaginare tridimensionale. Lo si può leggere in molti modi, per esempio vedendovi che i triangoli $\{25, 35, 45\}$ e $\{12, 13, 14\}$ sono prospettivi rispetto al punto 15 e alla retta $\{23, 24, 34\}$.

Se scegliamo una base dello spazio vettoriale di dimensione $n+1$ i cui sottospazi costituiscono $PG_n(\mathbb{F})$, possiamo descrivere i punti proiettivi mediante le cosiddette *coordinate omogenee*. Con $\langle x_0, x_1, \ldots, x_n\rangle$ intendiamo il sottospazio unidimensionale generato dal vettore $(x_0, x_1, \ldots, x_n)$. Il punto proiettivo $\langle x_0, x_1, \ldots, x_n\rangle$ coincide con $\langle y_0, y_1, \ldots, y_n\rangle$ se e solo se $(y_0, y_1, \ldots, y_n)$ è un multiplo scalare non nullo di $(x_0, x_1, \ldots, x_n)$. Anche gli iperpiani si possono descrivere mediante $(n+1)$-uple omogenee: $[c_0, c_1, \ldots, c_n]$ indicherà l'iperpiano dei punti con coordinate omogenee $\langle x_0, x_1, \ldots, x_n\rangle$ tali che $c_0x_0+x_1c_1+\cdots+x_nc_n = 0$. Orig. 318

Teorema 23.9 (teorema di Desargues). In $PG_n(\mathbb{F})$, se due triangoli sono prospettivi rispetto a un punto, allora sono prospettivi rispetto a una retta.

Dimostrazione. Siano $\{a_1, b_1, c_1\}$ e $\{a_2, b_2, c_2\}$ prospettivi rispetto a un punto p. Supporremo che nessuna terna fra p, a_1, b_1, c_1 sia collineare, per non dedicare troppo tempo ai dettagli. Supporremo inoltre che tutti i punti giacciano in un piano, cioè dimostreremo il teorema per $PG_2(\mathbb{F})$. Gli altri casi sono lasciati al lettore.

Scegliamo una base di uno spazio vettoriale tridimensionale in modo che i vettori di base $\mathbf{x}, \mathbf{y}, \mathbf{z}$ generino rispettivamente i sottospazi unidimensionali a_1, b_1, c_1. Le coordinate omogenee di questi punti sono allora $\langle 1, 0, 0\rangle$, $\langle 0, 1, 0\rangle$, $\langle 0, 0, 1\rangle$. Il punto p ha coordinate $\langle \alpha, \beta, \gamma\rangle$, tutte non nulle. Sostituiamo i vettori di base con $\alpha\mathbf{x}, \beta\mathbf{y}, \gamma\mathbf{z}$: i punti a_1, b_1, c_1 restano rappresentati dalle stesse coordinate, mentre p ha ora coordinate $\langle 1, 1, 1\rangle$. Ciò semplificherà i calcoli.

Segue che $a_2 = \langle \alpha, 1, 1\rangle$, $b_2 = \langle 1, \beta, 1\rangle$, $c_2 = \langle 1, 1, \gamma\rangle$ per opportuni $\alpha, \beta, \gamma \in \mathbb{F}$. La retta che congiunge a_1, b_1 è $[0, 0, 1]$; quella che congiunge a_2, b_2 è $[1-\beta, 1-\alpha, \alpha\beta-1]$: verificare che entrambi i punti vi appartengano. Il punto comune alle due rette è $\langle 1-\beta, \alpha-1, 0\rangle$. Analogamente, il punto d'intersezione della retta per b_1, c_1 con quella per b_2, c_2 risulta $\langle 0, 1-\alpha, \gamma-1\rangle$, mentre il punto d'intersezione della retta per c_1, a_1 con quella per c_2, a_2 risulta $\langle \beta-1, 0, 1-\gamma\rangle$.[5] I tre punti d'intersezione sono collineari perché le loro coordinate sono linearmente dipendenti.

Con la dovuta attenzione la dimostrazione dovrebbe funzionare anche per anelli con divisione $\mathbb{F}$. □

Problema 23H. Dimostrare che lo spazio lineare di $PG_n(\mathbb{F})$ soddisfa anche il *teorema di Pappo* quando $\mathbb{F}$ è un campo commutativo. L'enunciato è il seguente. Siano a_i, b_i, c_i punti collineari su una retta L_i, per $i = 1, 2$. Supponiamo che L_1, L_2 si incontrino in un punto diverso dai sei nominati. Allora le rette $\overline{\{a_1, b_2\}}$ e $\overline{\{a_2, b_1\}}$ si incontrano in un punto c; le rette $\overline{\{b_1, c_2\}}$ e $\overline{\{b_2, c_1\}}$ in un punto a; le rette $\overline{\{a_1, c_2\}}$ e $\overline{\{a_2, c_1\}}$ in un punto b. I tre punti a, b, c sono collineari. Orig. 319

[5] Nota redazionale: le coordinate stampate nell'originale in questo passaggio contengono scambi di parametri. Le tre intersezioni corrette sono, rispettivamente, $\langle 1-\alpha, \beta-1, 0\rangle$, $\langle 0, 1-\beta, \gamma-1\rangle$ e $\langle \alpha-1, 0, 1-\gamma\rangle$. I tre vettori rappresentanti hanno somma zero, il che dimostra la collinearità. La prima intersezione dell'originale non soddisfa in generale l'equazione della retta $[1-\beta, 1-\alpha, \alpha\beta-1]$.

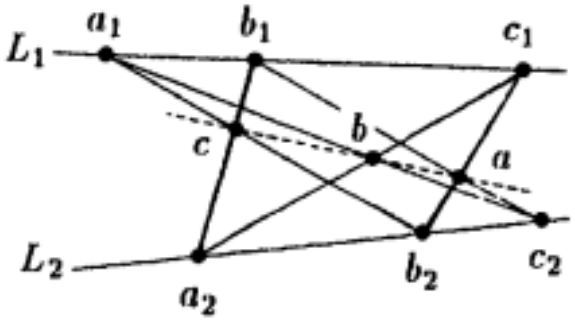


Figura 23.4

I piani proiettivi nei quali vale l'enunciato del Teorema 23.9, cioè due triangoli prospettivi rispetto a un punto sono prospettivi rispetto a una retta, si chiamano *piani desarguesiani*. Quelli nei quali vale la conclusione del Problema 23H si chiamano *piani pappiani*. Non abbiamo qui lo spazio né il tempo per dimostrare il seguente ulteriore risultato fondamentale. Si veda Crawley e Dilworth (1973).

Teorema 23.10.

1. Una geometria proiettiva di rango 3 è isomorfa a $PG_2(\mathbb{E})$ per un anello con divisione $\mathbb{E}$ se e solo se è un piano desarguesiano.
2. Una geometria proiettiva di rango 3 è isomorfa a $PG_2(\mathbb{F})$ per un campo $\mathbb{F}$ se e solo se è un piano pappiano.

Un corollario del Teorema 23.10 è che ogni piano pappiano è desarguesiano. Per una dimostrazione sintetica, cioè senza coordinate, del fatto che il teorema di Pappo implica quello di Desargues, si veda D. Pedoe (1963). Osserviamo che ogni anello con divisione finito è un campo, per il teorema di Wedderburn; quindi ogni piano desarguesiano finito è pappiano. Si veda M. Hall, Jr. (1972).

Descriviamo un metodo per ottenere piani proiettivi finiti non desarguesiani. Sia G un gruppo abeliano di ordine n^2 e supponiamo che esistano sottogruppi $H_0, H_1, \ldots, H_n$ di ordine n che partizionano gli elementi non nulli di G, ossia tali che $H_i \cap H_j = \{0\}$ per $i \neq j$ e quindi Orig. 320

$$\bigcup_{i=0}^{n} (H_i \setminus \{0\}) = G \setminus \{0\}.$$

Affermiamo che la struttura d'incidenza i cui punti sono gli elementi di G e le cui rette sono tutte le classi laterali, cioè le traslate, dei sottogruppi H_i è un piano affine. In generale, l'intersezione di classi laterali di due sottogruppi H, K è vuota oppure è una classe laterale di $H \cap K$; dunque due rette si incontrano in al più un punto. Potremmo ora contare le coppie coperte per mostrare che due punti distinti appartengono a una retta, ma è altrettanto semplice notare che, dati $x, y \in G$, la classe $H_* + y$ li contiene entrambi, dove H_* è il sottogruppo contenente $x - y$. Un piano affine ottenuto in questo modo da un gruppo G e da $n+1$ sottogruppi si chiama *piano affine di traslazione*. È noto che, affinché tali sottogruppi esistano, G deve essere abeliano elementare; si veda J. André (1954). Il piano affine si può completare a un piano proiettivo come nel Problema 19K; un piano proiettivo così ottenuto si chiama *piano di traslazione*.

Esempio 23.7. Ecco una partizione degli elementi non nulli di $\mathbb{F}_3^4$ in dieci sottogruppi $H_0, H_1, \ldots, H_9$. Abbiamo indicato gli elementi come stringhe, omettendo virgole e parentesi.

$$\{0000, 1000, 2000, 0100, 0200, 1100, 2200, 2100, 1200\}$$
$$\{0000, 0010, 0020, 0001, 0002, 0011, 0022, 0021, 0012\}$$
$$\{0000, 1010, 2020, 0101, 0202, 1111, 2222, 2121, 1212\}$$
$$\{0000, 2010, 1020, 0201, 0102, 2211, 1122, 1221, 2112\}$$
$$\{0000, 0110, 0220, 2001, 1002, 2111, 1222, 2221, 1112\}$$
$$\{0000, 0210, 0120, 1001, 2002, 1211, 2122, 1121, 2212\}$$
$$\{0000, 1110, 2220, 2101, 1202, 0211, 0122, 1021, 2012\}$$
$$\{0000, 2210, 1120, 1201, 2102, 0111, 0222, 2021, 1012\}$$
$$\{0000, 2110, 1220, 2201, 1102, 1011, 2022, 0121, 0212\}$$
$$\{0000, 1210, 2120, 1101, 2202, 2011, 1022, 0221, 0112\}.$$

Il piano affine corrispondente a questa *partizione in sottospazi* (*spread*) è il piano desarguesiano. Ma si Orig. 321

noti che gli elementi, per esempio, dei primi quattro sottogruppi si possono ripartire in sottogruppi in un altro modo, come indicato dalle colonne seguenti:

$$\begin{array}{llll}
\{0000, & \{0000, & \{0000, & \{0000, \\
1000, 2000, & 0100, 0200, & 1100, 2200, & 2100, 1200, \\
0010, 0020, & 0001, 0002, & 0011, 0022, & 0021, 0012, \\
1010, 2020, & 0101, 0202, & 1111, 2222, & 2121, 1212, \\
2010, 1020\} & 0201, 0102\} & 2211, 1122\} & 1221, 2112\}.
\end{array}$$

L'esempio precedente è il caso particolare $q = 3$ della costruzione che ora descriviamo. Sia V uno spazio vettoriale bidimensionale su $\mathbb{F}_{q^2}$ e siano $H_0, H_1, \ldots, H_{q^2}$ i suoi sottospazi unidimensionali su $\mathbb{F}_{q^2}$. Se consideriamo V come spazio vettoriale quadridimensionale su $\mathbb{F}_q$, i sottospazi H_i hanno dimensione 2 su $\mathbb{F}_q$; formano uno *spread* di rette in $PG_3(q)$, si veda il Teorema 24.3. Sia U un sottospazio bidimensionale su $\mathbb{F}_q$ diverso da tutti gli H_i. Allora U incontra ogni H_i in $\{0\}$ oppure in un sottospazio unidimensionale su $\mathbb{F}_q$. Supponiamo che incontri $H_0, H_1, \ldots, H_q$ in q punti ciascuno e $H_{q+1}, H_{q+2}, \ldots, H_{q^2}$ soltanto nel vettore nullo. Consideriamo i sottospazi su $\mathbb{F}_q$ della forma αU, al variare di α fra gli elementi non nulli di $\mathbb{F}_{q^2}$. Poiché la moltiplicazione per un elemento non nullo di $\mathbb{F}_q$ lascia fisso U, vi sono soltanto $(q^2-1)/(q-1)$ sottospazi distinti di questa forma, diciamo $U_0, U_1, \ldots, U_q$. Questi $q+1$ sottospazi si incontrano a due a due soltanto nel vettore nullo e la loro unione è $H_0 \cup H_1 \cup \cdots \cup H_q$. Quindi

$$U_0, U_1, \ldots, U_q, H_{q+1}, H_{q+2}, \ldots, H_{q^2}$$

è un'altra partizione di V in sottogruppi di ordine q^2.

Non dimostreremo qui che i piani proiettivi risultanti da questa costruzione non sono desarguesiani, per $q > 2$. Si veda il Teorema 10.9 di D. R. Hughes e F. C. Piper (1973). Il lettore può trovare a mano controesempi al teorema di Desargues nell'Esempio 23.7.

Concludiamo il capitolo dimostrando un passaggio importante della difficile dimostrazione del Teorema 23.6. Ci serve un'osservazione preliminare.

Proposizione 23.11. La sottogeometria su ogni sottospazio chiuso di una geometria proiettiva è ancora una geometria proiettiva.

Dimostrazione. Che la legge modulare valga nella sottogeometria su un sottospazio chiuso di una geometria proiettiva modulare è immediato. Dobbiamo mostrare che tali sottogeometrie siano connesse. A tal fine basta mostrare che, se H è un iperpiano di una geometria proiettiva con insieme dei punti X, la sottogeometria su H è connessa. Orig. 322

Se non lo fosse, $H = E \cup F$ con E, F sottospazi chiusi. Per la (23.4), $\operatorname{rank}(E) + \operatorname{rank}(F) = n - 1$, dove $n := \operatorname{rank}(X)$. Siano $E_1, \ldots, E_s$ e $F_1, \ldots, F_t$ i sottospazi chiusi che coprono rispettivamente E e F e contengono punti esterni a H; ciascuna famiglia partiziona i punti esterni a H. Supponiamo $s, t \geq 2$. Per la (23.4), esiste $x_i \in E_i \cap F_i$, $i = 1, 2$. La retta $\overline{\{x_1, x_2\}}$, sempre per la (23.4), incontra H in un punto $e \in E$. Ma allora x_2, appartenendo alla retta che congiunge e a x_1, deve appartenere a E_1: una contraddizione. Pertanto uno fra s, t è uguale a 1, diciamo $s = 1$, e allora X è l'unione dei sottospazi chiusi disgiunti F ed E_1, in contraddizione con la connessione della geometria proiettiva originaria. □

Un corollario della Proposizione 23.11 è che ogni retta di una geometria proiettiva ha almeno tre punti, poiché una retta di due punti non è connessa. Questo fatto viene usato in un passaggio cruciale della dimostrazione seguente. Osserviamo che, con l'aiuto del Problema 23D, è facile vedere che tutte le rette di una geometria proiettiva finita hanno la stessa cardinalità $n + 1$.

Teorema 23.12. Il teorema di Desargues vale in ogni geometria proiettiva di rango almeno 4.

Dimostrazione. Consideriamo due triangoli $\{a_1, b_1, c_1\}$ e $\{a_2, b_2, c_2\}$ prospettivi rispetto a un punto p.[6]

Supponiamo anzitutto che i piani P_1, P_2 generati rispettivamente da $\{a_1, b_1, c_1\}$ e $\{a_2, b_2, c_2\}$ siano distinti. Poniamo $T := \overline{\{p, a_1, b_1, c_1\}}$. Le rette $\overline{\{p, a_1\}}$, $\overline{\{p, b_1\}}$ e $\overline{\{p, c_1\}}$ contengono rispettivamente a_2, b_2, c_2, perciò P_1, P_2 sono contenuti in T, che ha evidentemente rango 4. Per la legge modulare, P_1, P_2 devono quindi intersecarsi in una retta L. Affermiamo che i due triangoli originali sono prospettivi rispetto a L.

Il piano $Q := \overline{\{p, a_1, b_1\}}$ contiene a_2, b_2 e dunque entrambe le rette $\overline{\{a_1, b_1\}}$ e $\overline{\{a_2, b_2\}}$, che si intersecano quindi in un punto, diciamo q. Il punto q appartiene sia a P_1 sia a P_2, dunque $q \in L$. Analogamente le

[6] Nota redazionale: all'inizio della dimostrazione l'originale chiama il centro x, ma prosegue poi usando p. Qui è uniformato a p.

rette $\overline{\{b_i, c_i\}}$, $i = 1, 2$, si incontrano in un punto di L, e lo stesso vale per $\overline{\{a_i, c_i\}}$, $i = 1, 2$. I due triangoli sono pertanto prospettivi rispetto a L.

Supponiamo ora che i due triangoli originari giacciano in un piano P. Sia x_1 un punto esterno a P e sia x_2 un altro punto della retta contenente x_1 e p.[7] Le rette $\overline{\{x_1, a_1\}}$ e $\overline{\{x_2, a_2\}}$ sono contenute nel piano $\overline{\{p, x_1, a_1\}}$ e si incontrano quindi in un punto a^*. Analogamente, le rette $\overline{\{x_1, b_1\}}$ e $\overline{\{x_2, b_2\}}$ si incontrano in b^*, e le rette $\overline{\{x_1, c_1\}}$ e $\overline{\{x_2, c_2\}}$ in c^*. Il piano $P^* := \overline{\{a^*, b^*, c^*\}}$ e P sono contenuti in un sottospazio chiuso di rango 4 e si incontrano dunque nella retta $L := P \cap P^*$. Orig. 323

I triangoli $\{a_1, b_1, c_1\}$ e $\{a^*, b^*, c^*\}$ sono prospettivi rispetto al punto x_1 e giacciono in piani distinti, quindi sono prospettivi rispetto alla retta L. Analogamente, i triangoli $\{a_2, b_2, c_2\}$ e $\{a^*, b^*, c^*\}$ sono prospettivi rispetto a x_2 e quindi rispetto a L. La retta $\overline{\{a_1, b_1\}}$ incontra L nello stesso punto della retta $\overline{\{a^*, b^*\}}$, e così fa la retta $\overline{\{a_2, b_2\}}$; pertanto $\overline{\{a_1, b_1\}}$ e $\overline{\{a_2, b_2\}}$ si incontrano in un punto di L. Analogamente gli altri lati corrispondenti dei due triangoli originari si incontrano in punti di L. In conclusione, i triangoli originari sono prospettivi rispetto a L. □

Problema 23I. Determinare il numero dei sottospazi chiusi di rango $n - k$ nel reticolo delle partizioni Π_n.

Problema 23J. Per un disegno a blocchi arbitrario, con parametri v, k, λ, b, r, definiamo una retta come l'intersezione di tutti i blocchi contenenti una coppia di punti x, y. Dimostrare:

(i) due punti qualsiasi appartengono a un'unica retta;

(ii) se L è una retta, allora $2 \leq |L| \leq (b - \lambda)/(r - \lambda)$;

(iii) se una retta incontra un blocco in due punti, è contenuta nel blocco.

Note

Girard Desargues (1593–1662) fu architetto e ingegnere militare, e introdusse il termine *involuzione* nel suo lavoro sulla prospettiva. Lavorò a Lione e a Parigi. L'opera di Pappo di Alessandria, attivo intorno al 320, l'ultimo importante geometra greco, era molto anteriore. La disciplina matematica della geometria proiettiva non si sviluppò prima del XIX secolo.

Moritz Pasch era inizialmente un algebrista, ma si interessò poi alla geometria non euclidea. Giunse a Giessen all'età di 27 anni come *Privatdozent* e vi rimase fino alla morte, sessant'anni dopo. Fu rettore dell'università nel 1893–1894. Un'interessante famiglia di geometrie combinatorie, chiamate *geometrie trasversali*, si ottiene dai grafi bipartiti; si veda Crapo e Rota (1970). Gli insiemi indipendenti di queste geometrie sono quei sottoinsiemi di una parte X di una bipartizione (X, Y) che possono essere accoppiati a vertici di Y. Orig. 324

Abbiamo visto che i concetti di geometria combinatoria e reticolo geometrico sono "criptomorfi", cioè costituiscono essenzialmente sistemi di assiomi diversi per le stesse strutture. Crapo e Rota (1970) ne danno altre versioni criptomorfe. Per esempio, i "matroidi" sono più o meno la stessa cosa delle geometrie combinatorie, sebbene l'accento posto dalla teoria dei matroidi sia diverso.

Alcune caratterizzazioni del disegno simmetrico formato dai punti e dagli iperpiani di uno spazio proiettivo finito si trovano nella Sezione 2.1 di P. Dembowski (1968).

Riferimenti bibliografici

J. André (1954)
Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe, *Math. Zeitschr.* **60**, 156–186.

L. M. Batten (1986)
Combinatorics of Finite Geometries, Cambridge University Press.

H. Crapo and G.-C. Rota (1970)
Combinatorial Geometries, MIT Press.

[7] Nota redazionale: si sceglie x_2 distinto sia da x_1 sia da p; la possibilità è garantita dal fatto che ogni retta ha almeno tre punti.

P. Crawley and R. P. Dilworth (1973)
Algebraic Theory of Lattices, Prentice-Hall.

P. Dembowski (1968)
Finite Geometries, Springer-Verlag.

C. Greene (1970)
A rank inequality for finite geometric lattices, *J. Combinatorial Theory* **9**, 357–364.

M. Hall, Jr. (1972)
The Theory of Groups, 2nd edn., Chelsea.

D. R. Hughes and F. C. Piper (1973)
Projective Planes, Springer-Verlag.

D. Pedoe (1963)
An Introduction to Projective Geometry, Macmillan.

O. Veblen and J. W. Young (1907)
Projective Geometries (2 vols.), Ginn Co.

Capitolo 24

Numeri gaussiani e q-analoghi

Esistono molte analogie fra l'insieme parzialmente ordinato di tutti i sottoinsiemi di un insieme finito e quello di tutti i sottospazi di uno spazio vettoriale finito. La ragione principale è che entrambi sono esempi di "disegni matroidali", come definiti nel capitolo precedente. Orig. 325

Indichiamo con $V_n(q)$ uno spazio vettoriale di dimensione n sul campo $\mathbb{F}_q$ con q elementi. Usiamo il termine *k-sottospazio* come abbreviazione di sottospazio di dimensione k.

Cominciamo con un conteggio. Per ottenere una catena massimale, cioè una catena di cardinalità $n+1$ contenente un sottospazio per ogni dimensione possibile, nell'insieme parzialmente ordinato di tutti i sottospazi di $V_n(q)$, partiamo dallo 0-sottospazio. Dopo aver scelto un i-sottospazio U_i, con $0 \le i < n$, possiamo scegliere un $(i+1)$-sottospazio U_{i+1} che contenga U_i in $(q^n - q^i)/(q^{i+1} - q^i)$ modi: possiamo infatti prendere lo spazio generato da U_i e da uno qualsiasi dei $q^n - q^i$ vettori non appartenenti a U_i, ma ogni $(i+1)$-sottospazio compare esattamente $q^{i+1} - q^i$ volte in questo modo. In sintesi, il numero delle catene massimali di sottospazi di $V_n(q)$ è

$$M(n,q) = \frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^2-1)(q-1)}{(q-1)^n}.$$

Per ogni intero n possiamo considerare $M(n,q)$ come un polinomio in q. Sostituendo all'indeterminata q una potenza di primo, otteniamo il numero delle catene massimali nell'insieme parzialmente ordinato $PG_n(q)$.[1] Ponendo $q = 1$ abbiamo $M(n,1) = n!$, il numero delle catene massimali nell'insieme parzialmente ordinato dei sottoinsiemi di un insieme di n elementi.

Il *numero gaussiano* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ si può definire come il numero dei k-sottospazi di $V_n(q)$. Alcuni autori li chiamano *coefficienti gaussiani*, per sottolineare l'analogia con i coefficienti binomiali. Per trovare un'espressione di $\begin{bmatrix} n \\ k \end{bmatrix}_q$, contiamo il numero N delle coppie (U, C), dove U è un k-sottospazio e C una catena massimale contenente U. Naturalmente ogni catena massimale contiene esattamente un sottospazio di dimensione k, quindi $N = M(n,q)$. D'altra parte, ciascuna di queste catene si ottiene in modo unico concatenando una catena massimale nell'insieme parzialmente ordinato dei sottospazi di U, per la quale vi sono $M(k,q)$ scelte, con una catena massimale nell'insieme parzialmente ordinato dei sottospazi di $V_n(q)$ contenenti U. Per quest'ultima vi sono $M(n-k,q)$ scelte, poiché $\{W : U \subseteq W \subseteq V\}$ è isomorfo all'insieme parzialmente ordinato dei sottospazi dello spazio quoziente V/U, di dimensione $n-k$. Pertanto Orig. 326

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{M(n,q)}{M(k,q)M(n-k,q)} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Per certi scopi è meglio pensare a $\begin{bmatrix} n \\ k \end{bmatrix}_q$ come a un polinomio nell'indeterminata q, anziché come a una funzione di una potenza di primo. Che la funzione razionale precedente sia effettivamente un polinomio si può vedere in vari modi. Per esempio, è un facile esercizio mostrare che una funzione razionale in x che assume valori interi per infiniti valori interi di x deve essere un polinomio in x. Forse *polinomio gaussiano* è un termine migliore di numero o coefficiente gaussiano. Per esempio,

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_q = q^9 + q^8 + 2q^7 + 3q^6 + 3q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1.$$

[1] Nota redazionale: con le convenzioni del Capitolo 23, il reticolo dei sottospazi di $V_n(q)$ corrisponde a $PG_{n-1}(q)$; l'indice n dell'originale è qui maggiore di uno.

Ponendo $q = 1$ in $\begin{bmatrix} n \\ k \end{bmatrix}_q$, otteniamo $\binom{n}{k}$. Ciò spiega una piccola parte della tendenza dei risultati sugli spazi vettoriali finiti a ridursi ai corrispondenti risultati sugli insiemi quando q viene sostituito con 1. Si possono anche formulare i cosiddetti *q-analoghi* di risultati sugli insiemi, cercando di sostituire "sottoinsieme di k elementi" con "k-sottospazio". Talvolta tali enunciati sono veri e hanno dimostrazioni simili a quelle dei risultati sugli insiemi.

Il seguente è il q-analogo del teorema di Sperner, Teorema 6.3.

Orig. 327

Teorema 24.1. Se $\mathcal{A}$ è un'anticatena nell'insieme parzialmente ordinato di tutti i sottospazi di $V_n(q)$, allora

$$|\mathcal{A}| \le \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q.$$

Dimostrazione. Sia $\mathcal{A}$ un'anticatena e contiamo il numero N delle coppie (U, C), dove $U \in \mathcal{A}$ e C è una catena massimale contenente U. Ogni catena massimale contiene al più un sottospazio di $\mathcal{A}$, dunque $N \le M(n, q)$. D'altra parte, ogni k-sottospazio di $\mathcal{A}$ appartiene a esattamente $M(k, q)M(n-k, q)$ catene massimali. Quindi

$$M(n, q) \ge N = \sum_{k=0}^{n} c_k M(k, q) M(n-k, q),$$

dove c_k è il numero dei sottospazi di dimensione k appartenenti a $\mathcal{A}$. La dimostrazione si completa in modo analogo a quella del Teorema 6.3 se accettiamo che $\begin{bmatrix} n \\ k \end{bmatrix}_q \le \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q$ per ogni k; la verifica è lasciata al lettore. □

Il prossimo teorema fornisce un'interpretazione combinatoria dei coefficienti di $\begin{bmatrix} n \\ k \end{bmatrix}_q$ come polinomio in q, dimostrando così che sono tutti interi positivi.

Teorema 24.2. Sia

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\ell=0}^{k(n-k)} a_\ell q^\ell.$$

Il coefficiente a_ℓ è il numero delle partizioni di ℓ i cui diagrammi di Ferrers stanno in un rettangolo di dimensioni $k \times (n-k)$.

Dimostrazione. Possiamo lavorare nello spazio vettoriale $\mathbb{F}_q^n$ delle n-uple su $\mathbb{F}_q$. È noto che ogni k-sottospazio di $\mathbb{F}_q^n$ si presenta in modo unico come lo spazio delle righe di una matrice $k \times n$ su $\mathbb{F}_q$ che (i) ha rango k e (ii) è in *forma a scala ridotta per righe*. Ciò significa che il primo elemento non nullo di ciascuna riga è 1, che sopra ciascun 1 iniziale vi sono zeri e che il primo 1 della riga i è più a destra del primo 1 della riga $i-1$, per $i = 2, 3, \ldots, k$. Supponiamo che il primo 1 della riga i sia nella colonna c_i, $i = 1, 2, \ldots, k$. Allora

Orig. 328

$$(n-k+1-c_1, n-k+2-c_2, \ldots, n-1-c_{k-1}, n-c_k)$$

è una successione non crescente di numeri non negativi; eliminando gli zeri finali, essa corrisponde quindi a una partizione di un certo numero in al più k parti, ciascuna di cardinalità al più $n-k$. Viceversa, una tale partizione dà le posizioni degli 1 iniziali in una classe di forme a scala.

Per esempio, nel caso $n = 6$, $k = 3$, vi sono 20 classi di forme a scala; si veda la Fig. 24.1.

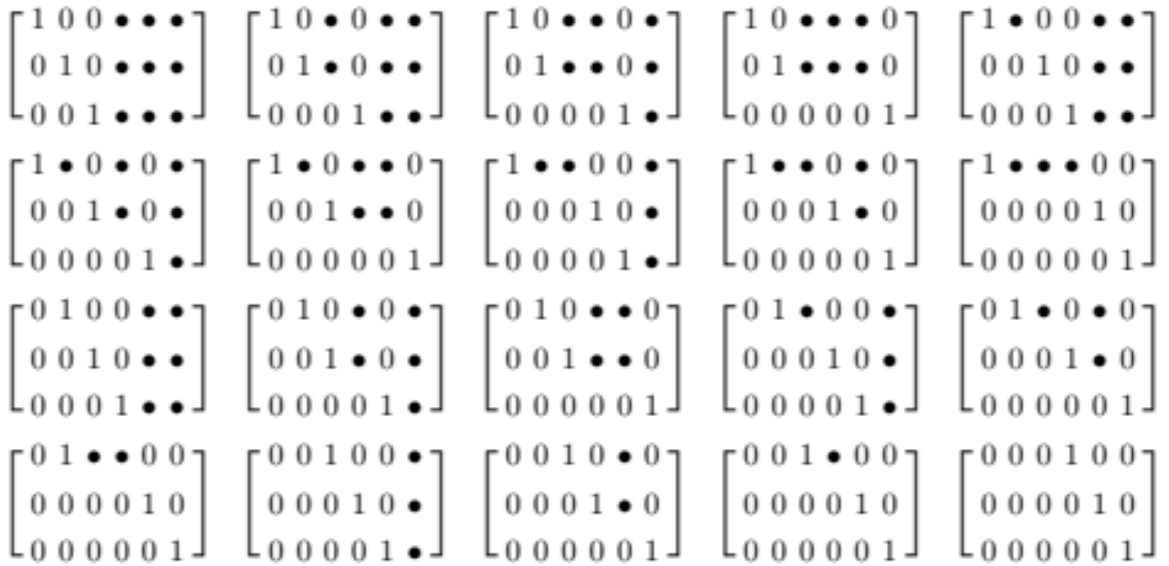


Figura 24.1

In ogni matrice della Fig. 24.1, le posizioni dei punti, eliminando le colonne intermedie e riflettendo rispetto a un asse verticale, descrivono il diagramma di Ferrers di una partizione di un numero al più 9, che sta in un rettangolo 3×3. La classe rappresentata dall'ultima matrice della prima riga, per esempio, contiene q^7 forme a scala.

In generale, la classe delle forme a scala nelle quali il primo 1 della riga i si trova nella colonna c_i, $i = 1, \ldots, k$, contiene q^ℓ matrici per un certo ℓ, poiché le posizioni che non contengono un 1 e non sono obbligate a contenere 0 possono essere riempite arbitrariamente con elementi di $\mathbb{F}_q$. Precisamente,

$$\ell = (n - k + 1 - c_1) + \cdots + (n - 1 - c_{k-1}) + (n - c_k),$$

perché, per ogni $i = 1, \ldots, k$, vi sono $n - (k - i) - c_i$ posizioni della riga i che possono essere riempite arbitrariamente. La classe consta dunque di q^ℓ matrici, dove la partizione in al più k parti di cardinalità al più $n - k$ corrispondente alla classe è proprio una partizione del numero ℓ. Orig. 329

Se definiamo quindi a_ℓ come il numero delle partizioni di ℓ il cui diagramma di Ferrers sta in un rettangolo $k \times (n - k)$, il polinomio $\sum_{\ell=0}^{k(n-k)} a_\ell q^\ell$ coincide con $\begin{bmatrix} n \\ k \end{bmatrix}_q$ quando viene valutato in qualunque potenza di primo q; i due polinomi sono dunque uguali. □

Osserviamo che, ponendo $q = 1$ nell'enunciato del Teorema 24.2, otteniamo come corollario che il numero totale delle partizioni il cui diagramma di Ferrers sta in un rettangolo $k \times (n - k)$ è $\binom{n}{k}$.

Problema 24A. Mostrarlo direttamente.

Ricaviamo ora una ricorrenza, la (24.1), per i numeri gaussiani. Essa fornisce un altro modo di vedere, per esempio per induzione su n, che essi sono polinomi in q. Fissiamo un iperpiano H, cioè un $(n-1)$-sottospazio di $V_n(q)$. Alcuni k-sottospazi sono contenuti in H, e il loro numero è $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$; gli altri incontrano H in un $(k-1)$-sottospazio. Ognuno dei $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ sottospazi di dimensione $k-1$ di H è contenuto in

$$\begin{bmatrix} n-k+1 \\ 1 \end{bmatrix}_q = \frac{q^{n-k+1} - 1}{q - 1}$$

k-sottospazi di V, dei quali

$$\begin{bmatrix} n-k \\ 1 \end{bmatrix}_q = \frac{q^{n-k} - 1}{q - 1}$$

sono contenuti in H. Ne restano q^{n-k} non contenuti in H. Dunque

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q. \tag{24.1}$$

Problema 24B. Determinare gli esponenti e_i, che possono dipendere da m, n, k oltre che da i, affinché valga l'identità

$$\begin{bmatrix} n+m \\ k \end{bmatrix}_q = \sum_{i=0}^{k} q^{e_i} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} m \\ k-i \end{bmatrix}_q .$$

Un modo di risolvere il problema usa le forme a scala; un altro usa la (24.1).

Orig. 330

L'equazione del Problema 24B è un q-analogo dell'identità

$$\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$$

per i coefficienti binomiali. Il q-analogo dell'inclusione-esclusione compare nel prossimo capitolo; per un'applicazione si veda il Teorema 25.2.

Qual è il q-analogo dei t-disegni semplici? Sarebbe una famiglia $\mathcal{B}$ di k-sottospazi di $V_v(q)$ tale che ogni t-sottospazio sia contenuto in esattamente λ membri di $\mathcal{B}$. Non erano noti esempi non banali di tali "q-$S_\lambda(t,k,v)$" con $t \geq 2$ fino al 1986, quando S. Thomas descrisse una famiglia con

$$q = 2, \qquad \lambda = 7, \qquad t = 2, \qquad k = 3, \qquad v \equiv \pm 1 \pmod 6.$$

Il caso $t = \lambda = 1$ è già non banale per gli spazi vettoriali. Per gli insiemi, un $S(1,k,v)$ è una partizione di un insieme di v elementi in sottoinsiemi di k elementi, ed esiste se e solo se k divide v.

Teorema 24.3. Esiste una famiglia di k-sottospazi di $V_v(q)$ tale che ogni 1-sottospazio sia contenuto in esattamente un membro della famiglia, un cosiddetto *spread* di k-sottospazi, se e solo se k divide v.

Dimostrazione. In altre parole, ci interessano famiglie di k-sottospazi che si intersecano a due a due nello 0-sottospazio, ma la cui unione è l'intero spazio vettoriale di dimensione v.

Il numero di k-sottospazi richiesto è il numero totale dei vettori non nulli diviso per quello dei vettori non nulli di un k-sottospazio, cioè $(q^v - 1)/(q^k - 1)$. Questo numero è intero se e solo se k divide v.

Supponiamo $v = km$ con m intero. Come spazio vettoriale di dimensione v su $\mathbb{F}_q$, prendiamo uno spazio vettoriale V di dimensione m su $\mathbb{F}_{q^k}$. Sia $\mathcal{B}$ la famiglia dei suoi sottospazi unidimensionali su $\mathbb{F}_{q^k}$. Ve ne sono quindi $q^{k(m-1)} + q^{k(m-2)} + \cdots + q^k + 1$, ciascuno contenente q^k vettori. Pensiamo ora a V come spazio vettoriale su $\mathbb{F}_q$, sottocampo di $\mathbb{F}_{q^k}$: i membri di $\mathcal{B}$ sono sottospazi di dimensione k su $\mathbb{F}_q$ e danno la partizione richiesta. □

Orig. 331

Problema 24C. Sia $\mathcal{B}$ uno spread di k-sottospazi di $V_v(q)$ e sia $\mathcal{A}$ la famiglia di tutte le classi laterali di tutti i membri di $\mathcal{B}$. Mostrare che $\mathcal{A}$ è l'insieme dei blocchi di un $S(2, q^k, q^v)$ sull'insieme dei punti $V_v(q)$. Il caso $v = 2k$ è particolarmente interessante, perché si ottengono piani affini di ordine q^k. I piani ottenuti da spread si chiamano *piani di traslazione*.

Problema 24D. Dimostrare che

$$\sum_{k=0}^{n} (q^n - 1)\cdots(q^{n-k+1} - 1) q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q = q^{n^2}.$$

Il teorema di Erdős–Ko–Rado, si veda il Teorema 6.4, si può formulare in due modi equivalenti. In una formulazione il limite per m è $\binom{n-1}{k-1}$, nell'altra è $\frac{k}{n}\binom{n}{k}$, dove $\binom{n}{k}$ conta il numero totale dei sottoinsiemi di k elementi di un insieme di n elementi.

Consideriamo ora un possibile q-analogo. Partiamo da una famiglia $\mathcal{A} := \{A_1, \ldots, A_m\}$ di m distinti sottospazi di dimensione k dello spazio vettoriale $V(n,q)$ di dimensione n su $\mathbb{F}_q$, tale che due qualsiasi degli A_i si intersechino in un sottospazio di dimensione almeno 1. Si può allora congetturare che, se $k \leq \frac{1}{2}n$,

$$m \leq \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \qquad \text{oppure} \qquad m \leq \frac{k}{n}\begin{bmatrix} n \\ k \end{bmatrix}_q .$$

In questo caso i limiti sono diversi: il primo è più forte del secondo. Per una dimostrazione del primo si veda W. N. Hsieh (1975). P. Frankl e R. M. Wilson (1986) rafforzarono tale risultato. Il secondo limite si può dimostrare generalizzando la dimostrazione del Teorema 6.4, come richiesto nel prossimo problema.

Problema 24E. Nella situazione appena descritta, facciamo variare $\pi := (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ nell'insieme $\mathcal{B}_n$ di tutte le basi ordinate di $V(n,q)$. Disponiamo π su una circonferenza. Se una sequenza di k vettori consecutivi $\mathbf{x}_i$ sulla circonferenza è una base di A_j, scriviamo $A_j \in \pi$.

(i) Mostrare che per π fissata vale $|\mathcal{A} \cap \pi| \leq k$.

(ii) Per A_j fissato, contare le basi $\pi \in \mathcal{B}_n$ tali che $A_j \in \pi$.

(iii) Dimostrare che $m \leq \frac{k}{n} \begin{bmatrix} n \\ k \end{bmatrix}_q$.

Orig. 332

Note

È stato suggerito di usare per $M(n, q)$ la notazione $nq.$, da leggersi "n q-toriale". Avremmo allora

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{nq.}{kq.\,(n-k)q.}.$$

Si noti inoltre che

$$\lim_{q \to 1} nq. = n1. \qquad \text{cioè } n!.$$

Non sappiamo chi abbia proposto per primo questa notazione.

Il q-analogo del teorema di Ramsey rimase a lungo un problema aperto, fino alla soluzione di R. L. Graham, K. Leeb e B. L. Rothschild nel 1972.

Carl Friedrich Gauss (1777–1855) fu forse il più grande matematico, e scienziato, di tutti i tempi. Diede contributi estremamente importanti alla teoria dei numeri. Fu il primo a studiare le proprietà delle espressioni che oggi chiamiamo polinomi o numeri gaussiani.

Riferimenti bibliografici

P. Frankl and R. M. Wilson (1986)
The Erdős-Ko-Rado theorem for vector spaces, *J. Combinatorial Theory (A)* **43**, 228–236.

R. L. Graham, K. Leeb, B. L. Rothschild (1972)
Ramsey's theorem for a class of categories, *Adv. Math.* **8**, 417–433.

R. L. Graham, B. L. Rothschild, and J. Spencer (1980)
Ramsey Theory, Wiley.

W. N. Hsieh (1975)
Intersection theorems for systems of finite vector spaces, *Discrete Math.* **12**, 1–16.

S. Thomas (1986)
Designs over finite fields, *Geometriae Dedicata* **24**, 237–242.

Capitolo 25

Reticoli e inversione di Möbius

Orig. 333

Una delle tecniche che appartengono ai fondamenti della combinatoria è il principio di inversione di Möbius sugli insiemi parzialmente ordinati. Lo si può considerare tanto una generalizzazione dell'inclusione–esclusione quanto un'estensione dell'inversione mediante la funzione classica di Möbius della teoria dei numeri, discussa nel Capitolo 10.

Sia P un insieme parzialmente ordinato finito. Considereremo matrici α le cui righe e colonne sono indicizzate dagli elementi di P, cioè applicazioni da $P \times P$ nei numeri razionali o complessi. L'*algebra di incidenza* $A(P)$ è costituita da tutte le matrici α tali che $\alpha(x, y) = 0$ a meno che $x \leq y$ in P. Per definizione di moltiplicazione fra matrici,

$$(\alpha\beta)(x, y) = \sum_{z \in P} \alpha(x, z)\beta(z, y).$$

Se $\alpha, \beta \in A(P)$, basta estendere la somma agli z nell'intervallo $[x, y] := \{z : x \leq z \leq y\}$. È facile vedere che $A(P)$ è chiusa rispetto alla moltiplicazione, oltre che all'addizione e alla moltiplicazione per scalari.

Un elemento di $A(P)$ che avrà un ruolo importante nella teoria seguente è ζ, la *funzione zeta* di P, definita da

$$\zeta(x, y) = \begin{cases} 1 & \text{se } x \leq y \text{ in } P, \\ 0 & \text{altrimenti.} \end{cases}$$

Affermiamo che ζ è invertibile e che la sua inversa, chiamata *funzione di Möbius* di P e indicata con μ, ha valori interi e appartiene ad $A(P)$.

La verifica è semplice. L'equazione $\mu\zeta = I$, dove I è l'identità, richiede che

Orig. 334

$$\sum_{x \leq z \leq y} \mu(x, z) = \begin{cases} 1 & \text{se } x = y, \\ 0 & \text{altrimenti,} \end{cases} \tag{25.1}$$

e basta dunque definire μ induttivamente, ponendo $\mu(x, x) := 1$, $\mu(x, y) := 0$ se $x \not\leq y$, e

$$\mu(x, y) := -\sum_{x \leq z < y} \mu(x, z) \qquad \text{per } x < y \text{ in } P. \tag{25.2}$$

Per esempio, se $P = \{1, 2, 3, 4, 6, 12\}$ è il reticolo di tutti i divisori positivi dell'intero 12,

$$\zeta = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

La prima riga di μ è stata calcolata così:

$$\begin{aligned}
\mu(1,1) &= +1,\\
\mu(1,2) &= -\mu(1,1) = -1,\\
\mu(1,3) &= -\mu(1,1) = -1,\\
\mu(1,4) &= -\mu(1,1) - \mu(1,2) = 0,\\
\mu(1,6) &= -\mu(1,1) - \mu(1,2) - \mu(1,3) = +1,\\
\mu(1,12) &= -\mu(1,1) - \mu(1,2) - \mu(1,3) - \mu(1,4) - \mu(1,6) = 0.
\end{aligned}$$

Osserviamo che, considerando invece la relazione $\zeta\mu = I$, si ottiene un'equazione leggermente diversa:

$$\sum_{x\le z\le y} \mu(z,y) = \begin{cases} 1 & \text{se } x = y,\\ 0 & \text{altrimenti.}\end{cases} \tag{25.3}$$

Un altro modo, assai più complicato, di affrontare l'invertibilità di ζ è il seguente. Osserviamo anzitutto che un ordine parziale finito può sempre essere "dominato" da un ordine totale; esiste cioè un'indicizzazione $P = \{x_1, x_2, \ldots, x_n\}$ tale che $x_i \le x_j$ in P implichi $i \le j$. (Dimostrazione: si prenda un qualunque elemento massimale x di P, si indicizzi $P \setminus \{x\}$ per induzione e si collochi x per ultimo.) Rispetto a tale indicizzazione di P, le matrici di $A(P)$ sono triangolari superiori. La funzione zeta ha tutti 1 sulla diagonale, quindi determinante 1 e, per la formula di Cramer, un'inversa a coefficienti interi. Inoltre $\zeta^{-1} = \mu$ appartiene ad $A(P)$, perché l'inversa di una matrice (o di un elemento di un'algebra commutativa di dimensione finita) è un polinomio in quella matrice (o in quell'elemento). Orig. 335

L'equazione (25.2) implica che $\mu(x,y) = -1$ se $x \prec y$. Si osservi anche che $\mu(x,y) = k-1$ se l'intervallo $[x,y]$ è una retta con k punti, cioè se è costituito da x, y e k elementi $z_1, \ldots, z_k$ a due a due non confrontabili, ciascuno con $x \prec z_i \prec y$.

Nel teorema seguente elenchiamo i valori della funzione di Möbius per alcuni insiemi parzialmente ordinati comuni. Rimanderemo la dimostrazione del Teorema 25.1 alla fine del capitolo, perché vogliamo prima discutere le conseguenze dell'inversione di Möbius. I lettori ingegnosi e/o operosi potranno dimostrare alcune parti del Teorema 25.1 con la ricorrenza (25.2) e semplici argomenti induttivi; noi preferiamo attendere di avere a disposizione il teorema di Weisner, Teorema 25.3. Non dimostreremo qui la parte (v): si vedano le note.

Teorema 25.1. (i) Per il reticolo di tutti i sottoinsiemi di un insieme X di n elementi,

$$\mu(A,B) = \begin{cases} (-1)^{|B|-|A|} & \text{se } A \subseteq B,\\ 0 & \text{altrimenti.}\end{cases}$$

(ii) Per il reticolo di tutti i divisori positivi di un intero n,

$$\mu(a,b) = \begin{cases} (-1)^r & \text{se } b/a \text{ è il prodotto di } r \text{ primi distinti},\\ 0 & \text{altrimenti, cioè se } a \nmid b \text{ o } b/a \text{ non è libero da quadrati.}\end{cases}$$

(In altre parole, $\mu(a,b) = \mu(b/a)$, dove l'ultima μ è la funzione classica di una variabile in (10.8).)

(iii) Per il reticolo di tutti i sottospazi di uno spazio vettoriale V di dimensione finita sul campo $\mathbb{F}_q$ di q elementi,

$$\mu(U,W) = \begin{cases} (-1)^k q^{\binom{k}{2}} & \text{se } U \subseteq W \text{ e } \dim W - \dim U = k,\\ 0 & \text{se } U \not\subseteq W.\end{cases}$$

(iv) Per il reticolo Π_n di tutte le partizioni di un insieme X di n elementi, Orig. 336

$$\mu(\mathcal{A},\mathcal{B}) = (-1)^{|\mathcal{A}|-|\mathcal{B}|} \prod_{B\in\mathcal{B}} (n_B - 1)!$$

per elementi $\mathcal{A},\mathcal{B}$ di Π_n con $\mathcal{A} \preceq \mathcal{B}$, dove n_B indica il numero di blocchi di $\mathcal{A}$ contenuti in un blocco B di $\mathcal{B}$.

(v) Per il reticolo delle facce di un politopo convesso,

$$\mu(A,B) = \begin{cases} (-1)^{\dim B - \dim A} & \text{se } A \subseteq B,\\ 0 & \text{altrimenti.}\end{cases}$$

Enunciamo ora il *principio di inversione di Möbius*. Siano P un insieme parzialmente ordinato finito e μ la sua funzione di Möbius. Siano $f, g, h : P \to \mathbb{R}$ (o in un qualsiasi gruppo additivo) funzioni tali che

$$g(x) = \sum_{a:a\le x} f(a), \qquad h(x) = \sum_{b:b\ge x} f(b)$$

per ogni $x \in P$. Allora, per ogni $x \in P$,

$$f(x) = \sum_{a:a\le x} \mu(a,x)g(a), \tag{25.4}$$

e

$$f(x) = \sum_{b:b\ge x} \mu(x,b)h(b). \tag{25.5}$$

Queste formule si verificano facilmente per sostituzione diretta. Per esempio, il secondo membro di (25.4) è

$$\sum_{a:a\le x} \mu(a,x) \left(\sum_{b:b\le a} f(b) \right) = \sum_{b:b\le x} f(b) \left(\sum_{a:b\le a\le x} \mu(a,x) \right).$$

Per (25.3), però, la somma interna a destra è nulla a meno che $b = x$, e rimane soltanto il termine $f(x)$. Oppure, in notazione matriciale, considerando f, g, h come vettori riga o colonna, secondo quanto occorre, con coordinate indicizzate da P, le relazioni assunte per g e h equivalgono a $g = \zeta f$, da cui $f = \mu g$, e $h = f\zeta$, da cui $f = h\mu$.[1] Orig. 337

Applicando il principio di inversione di Möbius al reticolo dei sottoinsiemi di un insieme X, si ritrova l'inclusione–esclusione. Sia $(A_i : i \in I)$ una famiglia finita di sottoinsiemi di un insieme finito X. Per $J \subseteq I$, sia $f(J)$ il numero di elementi di X che appartengono esattamente agli insiemi A_j con $j \in J$ e a nessun altro. (Si pensi alla cardinalità di una delle regioni di un diagramma di Venn degli insiemi.) Sia $g(J)$ il numero di elementi di $\bigcap_{j\in J} A_j$. Allora $g(J) = \sum_{K:J\subseteq K} f(K)$, per cui l'inversione di Möbius dà

$$f(J) = \sum_{K:J\subseteq K} (-1)^{|K\setminus J|} g(K).$$

Nel caso $J = \varnothing$ si può scrivere

$$\left| X \setminus \bigcup_{i\in I} A_i \right| = \sum_{K\subseteq I} (-1)^{|K|} \left| \bigcap_{j\in K} A_j \right|,$$

che è un modo un po' criptico di enunciare l'inclusione–esclusione.

Applicando il principio al reticolo dei divisori positivi di un intero n, si ritrova l'inversione classica di Möbius della teoria dei numeri. Se f e g soddisfano

$$g(m) = \sum_{k|m} f(k) \qquad \text{per ogni } m \text{ che divide } n,$$

l'inversione di Möbius dà

$$f(m) = \sum_{k|m} \mu(k,m)g(k) \qquad \text{per ogni } m \text{ che divide } n;$$

alla luce del Teorema 25.1(ii), ciò equivale al Teorema 10.4.

Diamo un q-analogo dell'Esempio 10.2, nel quale avevamo usato l'inclusione–esclusione per ottenere l'espressione $\sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} k^n$ per il numero di suriezioni da un insieme di n elementi a uno di m elementi. Orig. 338

Teorema 25.2. Il numero di trasformazioni lineari suriettive da uno spazio vettoriale di dimensione n a uno spazio vettoriale V di dimensione m su $\mathbb{F}_q$ è

$$\sum_{k=0}^{m} (-1)^{m-k} q^{nk+\binom{m-k}{2}} \begin{bmatrix} m \\ k \end{bmatrix}_q.$$

[1] Nota di traduzione: nell'originale le due convenzioni sono scambiate. Con $\zeta(x,y) = 1$ per $x \le y$, la relazione per g si scrive $g = f\zeta$ e quindi $f = g\mu$ per vettori riga; quella per h si scrive $h = \zeta f$ e quindi $f = \mu h$ per vettori colonna.

DIMOSTRAZIONE. Per un sottospazio $U \subseteq V$, sia $f(U)$ il numero di trasformazioni lineari la cui immagine è U. Sia $g(U)$ il numero di trasformazioni lineari la cui immagine è contenuta in U. Chiaramente,

$$g(U) = \sum_{W : W \subseteq U} f(W),$$

e $g(U) = q^{nr}$ se $\dim U = r$. Per inversione di Möbius sul reticolo dei sottospazi di V,

$$f(U) = \sum_{W : W \subseteq U} \mu(W, U) q^{n \dim W}.$$

Si prenda $U = V$ e si usi il Teorema 25.1(iii) per ottenere il risultato enunciato. □

Corollario. Il numero di matrici $n \times m$ sul campo $\mathbb{F}_q$ aventi rango r è

$$\begin{bmatrix} m \\ r \end{bmatrix}_q \sum_{k=0}^{r} (-1)^{r-k} q^{nk + \binom{r-k}{2}} \begin{bmatrix} r \\ k \end{bmatrix}_q.$$

Osserviamo che il numero di trasformazioni lineari iniettive ha una forma relativamente semplice. Fissata una base di uno spazio vettoriale di dimensione n, consideriamo le iniezioni in uno spazio vettoriale di dimensione m: l'immagine dell'i-esimo vettore della base va scelta fra i $q^m - q^{i-1}$ vettori che non appartengono al sottospazio generato dalle immagini dei vettori precedenti. In conclusione, vi sono $(q^m - 1)(q^m - q) \cdots (q^m - q^{n-1})$ trasformazioni lineari iniettive. Poiché anche il Teorema 25.2 con $m = n$ fornisce un'espressione per questo numero, abbiamo dimostrato un'identità.

Orig. 339

Problema 25A. (i) Usare l'inversione di Möbius per ricavare un'espressione per il numero di sottospazi di dimensione k che intersecano banalmente un dato sottospazio di dimensione r di uno spazio vettoriale di dimensione n su $\mathbb{F}_q$. Si dovrebbe ottenere un q-analogo di (10.5). (ii) Nel caso particolare $r + k = n$, mostrare da un altro punto di vista che tali sottospazi sono esattamente q^{rk}, considerando matrici $r \times n$ su $\mathbb{F}_q$ della forma $(I\ M)$, dove I è l'identità di ordine r.

Problema 25B. Usare l'inversione di Möbius per ricavare un'espressione per il numero di applicazioni lineari non singolari di uno spazio vettoriale di dimensione n su $\mathbb{F}_q$ in sé che non fissano alcun vettore diverso da 0, cioè che non hanno 1 come autovalore. (Esse saranno ortomorfismi del gruppo additivo; si vedano le osservazioni successive al Teorema 22.9.)

* * *

Gli insiemi parzialmente ordinati menzionati nel Teorema 25.1 sono tutti reticoli. Il seguente utile teorema fu trovato da L. Weisner (1935).

Teorema 25.3. Sia μ la funzione di Möbius di un reticolo finito L e sia $a \in L$ con $a > 0_L$. Allora

$$\sum_{x : x \vee a = 1_L} \mu(0_L, x) = 0.$$

DIMOSTRAZIONE. Fissiamo a e consideriamo

$$S := \sum_{x,y \in L} \mu(0,x)\zeta(x,y)\zeta(a,y)\mu(y,1) = \sum_{x \in L} \sum_{\substack{y \geq x \\ y \geq a}} \mu(0,x)\mu(y,1).$$

Da un lato,

$$S = \sum_{x} \mu(0,x) \sum_{\substack{y \geq x \\ y \geq a}} \mu(y,1).$$

Ma $y \geq a$ e $y \geq x$ se e solo se $y \geq x \vee a$, e la somma interna è

$$\sum_{y \geq x \vee a} \mu(y,1) = \begin{cases} 1 & \text{se } x \vee a = 1, \\ 0 & \text{se } x \vee a < 1. \end{cases}$$

Dunque S è la somma nell'enunciato. D'altro lato,

Orig. 340

$$S = \sum_{y \geq a} \mu(y,1) \sum_{0 \leq x \leq y} \mu(0,x),$$

e la somma interna è sempre 0, poiché $y > 0$. □

Corollario. Per elementi x, y di un reticolo geometrico L con $x \leq y$, $\mu(x,y)$ ha segno $(-1)^{\mathrm{rank}(y)-\mathrm{rank}(x)}$ e, in particolare, non è mai 0.

Dimostrazione. Mostriamo per induzione sul rango di L che $\mu(0_L, 1_L)$ ha segno $(-1)^{\mathrm{rank}(L)}$. Scegliamo un punto $p \in L$. Per semimodularità, $a \vee p = 1_L$ se e solo se $a = 1_L$ oppure a è un copunto non incidente con p; il teorema di Weisner, Teorema 25.3, dà dunque

$$\mu(0_L, 1_L) = - \sum_{\substack{h : h \prec 1_L \\ h \not\geq p}} \mu(0_L, h). \tag{25.6}$$

Per ipotesi induttiva tutti i termini a destra hanno segno $(-1)^{\mathrm{rank}(L)-1}$, e la dimostrazione è conclusa. □

Il numero $\chi_G(x)$ di colorazioni proprie di un grafo G con x colori si può trovare per inversione di Möbius sul reticolo $L(G)$ introdotto nel Capitolo 23, anche se non è necessariamente un metodo molto pratico. Ricordiamo che gli elementi di $L(G)$ sono le partizioni $\mathcal{A}$ dell'insieme dei vertici di G i cui blocchi inducono tutti sottografi connessi di G. Per $\mathcal{A} \in L(G)$, sia $g(\mathcal{A})$ il numero di applicazioni dall'insieme dei vertici di G in un insieme di x colori, cioè di colorazioni, tali che tutti i vertici di ciascun blocco di $\mathcal{A}$ ricevano lo stesso colore. Chiaramente $g(\mathcal{A}) = x^{|\mathcal{A}|}$. Sia $f(\mathcal{A})$ il numero di applicazioni costanti su ogni blocco di $\mathcal{A}$ ma tali che gli estremi di spigoli che uniscono blocchi distinti di $\mathcal{A}$ ricevano colori diversi. Data una colorazione "contata da" $g(\mathcal{A})$, basta riflettere un momento per vedere che esiste un'unica partizione più grossolana $\mathcal{B}$ tale che la colorazione sia "contata da" $f(\mathcal{B})$: si devono fondere due blocchi di $\mathcal{A}$ dello stesso colore se uno spigolo li unisce. Dunque $g(\mathcal{A}) = \sum_{\mathcal{B} \geq \mathcal{A}} f(\mathcal{B})$, e l'inversione di Möbius dà

$$f(\mathcal{A}) = \sum_{\mathcal{B} \geq \mathcal{A}} \mu(\mathcal{A}, \mathcal{B}) g(\mathcal{B}).$$

Il numero di colorazioni proprie è f valutata in $0_{L(G)}$, la partizione in singoletti, ossia

Orig. 341

$$\chi_G(x) = \sum_{\mathcal{B}} \mu(0_{L(G)}, \mathcal{B}) x^{|\mathcal{B}|} = \sum_{k=1}^{n} \left(\sum_{|\mathcal{B}|=k} \mu(0_{L(G)}, \mathcal{B}) \right) x^k.$$

Il polinomio $\chi_G(x)$ si chiama *polinomio cromatico* del grafo. Il corollario precedente conduce direttamente all'enunciato seguente.

Teorema 25.4. Il numero di colorazioni proprie con x colori di un grafo G con n vertici è dato da un polinomio monico $\chi_G(x)$ di grado n i cui coefficienti hanno segni alterni.

Problema 25C. Sia G un grafo semplice con n vertici e m spigoli. Mostrare che il coefficiente di x^{n-1} in $\chi_G(x)$ è $-m$ e che il coefficiente di x^{n-2} è $m(m-1)/2$ meno il numero di triangoli di G.

T. Dowling e R. M. Wilson (1975) dimostrarono il seguente teorema e il suo corollario; quest'ultimo generalizza la disuguaglianza del Teorema 19.1 sugli spazi lineari.

Teorema 25.5. Se L è un reticolo finito tale che $\mu(x, 1_L) \neq 0$ per ogni $x \in L$, esiste una permutazione π degli elementi di L tale che $x \vee \pi(x) = 1_L$ per ogni $x \in L$.

Dimostrazione. Prima di iniziare, osserviamo che una catena con più di due elementi è un esempio di reticolo che non soddisfa la nostra ipotesi. E naturalmente non esiste alcuna permutazione π con la proprietà enunciata. Il reticolo di tutti i sottoinsiemi di un insieme di n elementi, invece, ammette un'unica permutazione con tale proprietà: quella che porta ciascun sottoinsieme nel suo complementare.

Tutte le matrici qui considerate hanno righe e colonne indicizzate da L. Poniamo

$$\eta(x,y) := \begin{cases} 1 & \text{se } x \vee y = 1_L, \\ 0 & \text{altrimenti.} \end{cases}$$

Sia δ_1 la matrice diagonale con $\delta_1(x,x) := \mu(x, 1_L)$. Allora $\zeta \delta_1 \zeta^{\mathsf{T}} = \eta$, perché

Orig. 342

$$(\zeta\delta_1\zeta^{\mathsf{T}})(x,y) = \sum_{a,b} \zeta(x,a)\delta_1(a,b)\zeta(y,b)$$
$$= \sum_{a:a\geq x \text{ e } a\geq y} \delta_1(a,a) = \sum_{a:a\geq x\vee y} \mu(a,1_L),$$

e quest'ultima somma è, per (25.1), 1 se $x \vee y = 1_L$ e 0 altrimenti.[2]

Per l'ipotesi $\mu(x,1_L) \neq 0$, la matrice δ_1 è non singolare. Poiché anche ζ è non singolare, lo è pure η. Pertanto almeno un termine dello sviluppo del suo determinante non si annulla, e ciò implica la conclusione del teorema. □

Corollario. In un reticolo geometrico finito di rango n, il numero di elementi di rango $\geq n-k$ è almeno il numero di elementi di rango $\leq k$, per $0 \leq k \leq n$.

Dimostrazione. Consideriamo una permutazione π come nel Teorema 25.5, applicabile grazie al corollario del Teorema 25.3. La legge semimodulare

$$\operatorname{rank}(x) + \operatorname{rank}(\pi(x)) \geq \operatorname{rank}(x \vee \pi(x)) + \operatorname{rank}(x \wedge \pi(x)) \geq n$$

implica che l'immagine di un elemento di rango $\leq k$ abbia rango $\geq n-k$. □

Diamo ora una dimostrazione matriciale analoga di un teorema di T. Dowling (1977) sulle permutazioni che associano a ogni elemento un suo complemento.

Teorema 25.6. Se L è un reticolo finito tale che $\mu(x,1_L) \neq 0$ e $\mu(0_L,x) \neq 0$ per ogni $x \in L$, esiste una permutazione π degli elementi di L tale che

$$x \vee \pi(x) = 1_L \qquad \text{e} \qquad x \wedge \pi(x) = 0_L$$

per ogni $x \in L$.

Dimostrazione. Sia δ_1 come nella dimostrazione precedente e sia δ_0 la matrice diagonale con $\delta_0(x,x) := \mu(0_L,x)$. Consideriamo $\kappa := \zeta\delta_1\zeta^{\mathsf{T}}\delta_0\zeta$. Le ipotesi implicano che κ è non singolare. Affermiamo che $\kappa(x,y) = 0$ a meno che x e y siano complementi. Allora qualsiasi permutazione corrispondente a un termine non nullo nello sviluppo del determinante di κ avrà la proprietà richiesta. Orig. 343

Per dimostrare l'affermazione, osserviamo anzitutto che $\kappa = \eta\delta_0\zeta$, quindi

$$\kappa(x,y) = \sum_{z:z\vee x=1_L,\ z\leq y} \mu(0_L,z).$$

Se questa somma non è nulla, esiste uno z con $z \vee x = 1_L$ e $z \leq y$, e dunque $y \vee x = 1_L$. Per dualità, $\eta' = \zeta^{\mathsf{T}}\delta_0\zeta$, dove

$$\eta'(x,y) := \begin{cases} 1 & \text{se } x \wedge y = 0_L, \\ 0 & \text{altrimenti.} \end{cases}$$

Ora $\kappa = \zeta\delta_1\eta'$ e, analogamente, $\kappa(x,y) \neq 0$ implica $x \wedge y = 0_L$. □

Diamo infine la dimostrazione promessa all'inizio del capitolo.

Dimostrazione del Teorema 25.1. (i) Poiché l'intervallo $[A,B]$ è isomorfo al reticolo dei sottoinsiemi di $B \setminus A$, basta mostrare che $\mu(\varnothing,C) = (-1)^{|C|}$. Usiamo (25.6) e procediamo per induzione su $|C|$. Sia p un punto di C. C'è un solo copunto non incidente con p, cioè il complementare di $\{p\}$. Quindi (25.6) implica

$$\mu(\varnothing,C) = -\mu(\varnothing,C\setminus\{p\}) = -(-1)^{|C|-1} = (-1)^{|C|}.$$

(ii) Anche qui basta calcolare $\mu(1,m)$; usiamo l'induzione su m. Sia p un divisore primo di m. Il teorema di Weisner afferma che

$$\mu(1,m) = -\sum_{\operatorname{mcm}(a,p)=m,\ a<m} \mu(0,a).$$

[3] Se p^2 divide m, la somma a destra è vuota, dunque $\mu(1,m) = 0$. Se p^2 non divide m, c'è un solo termine, quello con $a = m/p$. (iii) Basta mostrare che $\mu(0,V) = (-1)^k q^{\binom{k}{2}}$ per V di dimensione k. Procediamo Orig. 344

[2] Nota di traduzione: il riferimento pertinente è (25.3), anziché (25.1).

[3] Nota di traduzione: nell'originale compare $\mu(0,a)$; nel reticolo dei divisori il minimo è 1 e va letto $\mu(1,a)$.

per induzione su k. Sia P un sottospazio di dimensione 1 di V. Per il teorema di Weisner,

$$\mu(0,V) = -\sum_{U:U\vee P=V,\ U\neq V} \mu(0,U).$$

Per ipotesi induttiva, ogni termine $\mu(0,U)$ di questa somma è uguale a $(-1)^{k-1}q^{\binom{k-1}{2}}$. Gli unici sottospazi U diversi da V tali che $U\vee P = V$ sono quelli di dimensione $k-1$ che non contengono P; il loro numero è

$$\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q = q^{k-1}.$$

Ciò conclude la dimostrazione della parte (iii).

(iv) Consideriamo due partizioni $\mathcal{A} \preceq \mathcal{B}$. Supponiamo che $\mathcal{B}$ abbia k blocchi che, una volta numerati, siano rispettivamente unioni di $n_1, n_2, \ldots, n_k$ blocchi di $\mathcal{A}$. Allora l'intervallo $[\mathcal{A},\mathcal{B}]$ è isomorfo al prodotto diretto di reticoli di partizioni

$$\Pi_{n_1} \times \Pi_{n_2} \times \cdots \times \Pi_{n_k},$$

perché una partizione $\mathcal{C}$ con $\mathcal{A} \preceq \mathcal{C} \preceq \mathcal{B}$ è specificata da una partizione degli n_i blocchi di $\mathcal{A}$ che stanno nell'i-esimo blocco di $\mathcal{B}$, per ciascun $i = 1, 2, \ldots, k$.

Ricordiamo ora che la funzione di Möbius $\mu_{P\times Q}$ del prodotto diretto di due insiemi parzialmente ordinati è il prodotto di Kronecker, o tensoriale, delle funzioni di Möbius μ_P, μ_Q di P, Q; cioè

$$\mu_{P\times Q}((a_1,b_1),(a_2,b_2)) = \mu_P(a_1,a_2)\mu_Q(b_1,b_2).$$

(Lasciamo al lettore la riflessione: basta verificare che definire $\mu_{P\times Q}$ come sopra produce un'inversa di $\zeta_{P\times Q}$.) Dunque $\mu(\mathcal{A},\mathcal{B})$ è il prodotto dei $\mu(0_{\Pi_{n_i}}, 1_{\Pi_{n_i}})$ per $i = 1, 2, \ldots, k$.

Mostriamo ora per induzione su n che $\mu(0_{\Pi_n}, 1_{\Pi_n}) = (-1)^{n-1}(n-1)!$. Sia P un punto di Π_n, cioè una partizione di un insieme di n elementi in un insieme di due elementi $\{x,y\}$ e $n-2$ singoletti. Le partizioni $\mathcal{A}$ tali che $P \vee \mathcal{A} = 1_{\Pi_n}$ sono le 2^{n-2} partizioni in due blocchi che separano x e y;[4] ve ne sono $\binom{n-2}{i}$ in cui il blocco contenente x ha cardinalità $i+1$ e quello contenente y ha cardinalità $n-1-i$. Da (25.6) e dall'ipotesi induttiva, Orig. 345

$$\begin{aligned}\mu(0_{\Pi_n}, 1_{\Pi_n}) &= -\sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i i! (-1)^{n-2-i}(n-2-i)! \\ &= (-1)^{n-1}(n-1)!.\end{aligned}$$

□

Problema 25D. Il duale del teorema di Weisner, ottenuto applicando il Teorema 25.3 al reticolo duale, afferma

$$\sum_{x:x\wedge a = 0_L} \mu(x, 1_L) = 0 \qquad \text{per ogni } a \in L \text{ con } a < 1_L.$$

Nel reticolo delle partizioni, prendere per a una partizione con un blocco di cardinalità $n-1$ e uno di cardinalità 1 e usare questa formula per dare una dimostrazione un po' diversa di $\mu(0_{\Pi_n}, 1_{\Pi_n}) = (-1)^{n-1}(n-1)!$.

Usiamo l'inversione di Möbius sul reticolo delle partizioni per ottenere un'espressione per il numero di grafi semplici connessi etichettati con n vertici. Sia X un insieme di n elementi. A ogni grafo G con insieme dei vertici X corrisponde la partizione $\mathcal{C}_G$ di X i cui blocchi sono gli insiemi dei vertici delle componenti connesse di G. Indichiamo con $g(\mathcal{B})$ il numero di grafi semplici G con $V(G) = X$ e $\mathcal{C}_G = \mathcal{B}$; con $f(\mathcal{B})$ il numero di grafi semplici G con $V(G) = X$ per i quali $\mathcal{C}_G$ è un raffinamento di $\mathcal{B}$. Chiaramente,

$$f(\mathcal{B}) = \sum_{\mathcal{A}\preceq\mathcal{B}} g(\mathcal{A}).$$

Ci interessa $g(1_{\Pi_n})$, dove 1_{Π_n} è la partizione con un solo blocco. È però $f(\mathcal{B})$ a essere facile da calcolare: un grafo contato da $f(\mathcal{B})$ si ottiene scegliendo arbitrariamente un grafo semplice su ciascun blocco di $\mathcal{B}$. Se dunque $\mathcal{B}$ ha k_i blocchi di cardinalità i,

$$f(\mathcal{B}) = 2^{k_2\binom{2}{2}} 2^{k_3\binom{3}{2}} \cdots 2^{k_n\binom{n}{2}}.$$

Per inversione di Möbius,

Orig. 346

$$g(\mathcal{B}) = \sum_{\mathcal{A} \preceq \mathcal{B}} \mu(\mathcal{A}, \mathcal{B}) f(\mathcal{A}).$$

Ponendo $\mathcal{B} = 1_{\Pi_n}$ otteniamo

$$g(1_{\Pi_n}) = \sum_{\mathcal{A}} \mu(\mathcal{A}, 1_{\Pi_n}) f(\mathcal{A}). \tag{25.7}$$

Ricordiamo che il numero di partizioni di X di tipo $(k_1, k_2, \ldots, k_n)$ è

$$\frac{n!}{(1!)^{k_1} k_1! (2!)^{k_2} k_2! \cdots (n!)^{k_n} k_n!};$$

si confronti (13.3). Usando il Teorema 25.1(iv), troviamo che il numero di grafi connessi etichettati con n vertici è

$$\sum (-1)^{k_1+k_2+\cdots+k_n-1} \frac{n!(k_1+\cdots+k_n-1)!}{(1!)^{k_1} k_1! \cdots (n!)^{k_n} k_n!} 2^{k_2\binom{2}{2}+k_3\binom{3}{2}+\cdots+k_n\binom{n}{2}},$$

dove si somma su tutte le partizioni $(k_1, \ldots, k_n)$ dell'intero n, cioè su tutte le n-uple non negative con $1k_1 + 2k_2 + \cdots + nk_n = n$.

Non intendiamo sostenere che questa sia una risposta particolarmente elegante alla domanda iniziale. Infatti è una somma su una vasta collezione di oggetti, il cui numero supera $e^{\sqrt{n}}$ per n grande. Tuttavia illustra in modo naturale l'inversione di Möbius e riduce notevolmente il problema. Per $n = 5$ abbiamo

partizione di 5	numero di $\mathcal{A}$	$f(\mathcal{A})$	$\mu(\mathcal{A}, 1_{\Pi_5})$
5	1	1024	1
41	5	64	−1
32	10	16	−1
311	10	8	2
221	15	4	2
2111	10	2	−6
11111	1	1	24

Orig. 347

Da questa tabella e da (25.7) vediamo che 728 dei 1024 grafi semplici etichettati con 5 vertici sono connessi.

* * *

Diamo un'applicazione dell'inversione di Möbius alla teoria dei codici. Ricordiamo la definizione di codice MDS nell'Esempio 20.3. Sia C un tale codice, cioè un codice $[n, k, d]$ su $\mathbb{F}_q$ con $d = n - k + 1$. Se consideriamo un insieme di d posizioni e il sottocodice di C che ha zeri in tutte le altre posizioni, esso ha dimensione $\geq k - (n - d) = 1$. Poiché la sua distanza minima è d, per il Teorema 20.2 deve avere dimensione esattamente 1. Ne segue che, per $n \geq d' > d$, fissare d' posizioni e richiedere che le parole siano nulle in tutte le altre definisce un sottocodice di C di dimensione $d' - d + 1$. Lo useremo nella dimostrazione seguente. Mostreremo che l'enumeratore dei pesi di un codice MDS è determinato dai suoi parametri.

Teorema 25.7. Sia C un codice $[n, k]$ su $\mathbb{F}_q$ con distanza $d = n - k + 1$. Allora l'enumeratore dei pesi di C è $1 + \sum_{i=d}^{n} A_i z^i$, dove

$$A_i = \binom{n}{i} (q-1) \sum_{j=0}^{i-d} (-1)^j \binom{i-1}{j} q^{i-j-d}, \qquad i = d, d+1, \ldots, n.$$

Dimostrazione. Sia R un sottoinsieme di $N := \{0, 1, \ldots, n-1\}$.[5] Sia $f(R)$ il numero di parole $(c_0, c_1, \ldots, c_{n-1})$ del codice per le quali $\{i : c_i \neq 0\} = R$. Per $S \subseteq N$, definiamo $g(S) := \sum_{R \subseteq S} f(R)$. Come osservato sopra,

$$g(S) = \begin{cases} 1 & \text{se } |S| \leq d-1, \\ q^{|S|-d+1} & \text{se } n \geq |S| \geq d. \end{cases}$$

La definizione di f implica $A_i = \sum_{R\subseteq N,\ |R|=i} f(R)$. Ora applichiamo l'inversione di Möbius e il Teorema 25.1(i), ottenendo Orig. 348

$$\begin{aligned} A_i &= \sum_{\substack{R\subseteq N\\ |R|=i}} \sum_{S\subseteq R} \mu(S,R)g(S) \\ &= \binom{n}{i}\left\{\sum_{j=0}^{d-1}\binom{i}{j}(-1)^{i-j} + \sum_{j=d}^{i}\binom{i}{j}(-1)^{i-j}q^{j-d+1}\right\} \\ &= \binom{n}{i}\sum_{j=d}^{i}\binom{i}{j}(-1)^{i-j}(q^{j-d+1}-1). \end{aligned}$$

Il risultato segue sostituendo j con $i-j$ e usando poi $\binom{i}{j} = \binom{i-1}{j-1} + \binom{i-1}{j}$. □

Il Teorema 25.7 impone restrizioni piuttosto forti alla cardinalità dell'alfabeto di un codice MDS.

Corollario. Se esiste un codice MDS C su $\mathbb{F}_q$ di lunghezza n e dimensione k, allora

$$\begin{cases} \text{(i)} & q \geq n-k+1 \quad \text{oppure } k \leq 1, \\ \text{(ii)} & q \geq k+1 \quad \text{oppure } d = n-k+1 \leq 2. \end{cases}$$

Dimostrazione. (i) Sia $d = n-k+1$. Dal Teorema 25.7, per $d < n$ troviamo

$$0 \leq A_{d+1} = \binom{n}{d+1}(q-1)(q-d).$$

(ii) Sia $G := (I_k\ P)$ la matrice generatrice di C. Poiché C ha peso minimo d, ogni insieme di $d-1 = n-k$ colonne della matrice di controllo di parità $H := (-P^{\mathsf{T}}\ I_{n-k})$ è linearmente indipendente. Quindi ogni sottomatrice quadrata di H è non singolare.[6] Dunque nessuna parola non nulla di $C^\perp$ ha $n-k$ zeri, cioè anche $C^\perp$ è MDS. Si applichi il risultato di (i) a $C^\perp$. □

Problema 25E. Sia P un insieme parzialmente ordinato. Ricordare che, se $x < y$, una successione $x = x_0 < x_1 < \cdots < x_k = y$ si chiama catena di lunghezza k da x a y. Sia $c_k(x,y)$ il numero di tali catene (quindi $c_1(x,y) = 1$). Dimostrare che

$$\mu(x,y) = \sum_{k\geq 1}(-1)^k c_k(x,y).$$

Orig. 349

Problema 25F. Consideriamo il reticolo dei sottospazi dello spazio vettoriale $V := \mathbb{F}_q^n$. Sia S un altro spazio vettoriale su $\mathbb{F}_q$. Per un sottospazio U definiamo:[7]

$$\begin{aligned} f(U) &:= \text{numero di applicazioni lineari da } V \text{ a } S \text{ con nucleo } U, \\ g(U) &:= \text{numero di applicazioni lineari da } V \text{ a } U \text{ con nucleo } \supseteq U. \end{aligned}$$

(i) Determinare $g(U)$ e applicare poi l'inversione di Möbius a

$$g(U) = \sum_{W:W\supseteq U} f(W).$$

(ii) Mostrare che

$$f(\{0\}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2}} |S|^{n-k}.$$

[4]Nota di traduzione: qui si intendono le partizioni $\mathcal{A} \neq 1_{\Pi_n}$, come nella somma (25.6). Anche la partizione massima soddisfa l'uguaglianza del supremo.

[5]Nota di traduzione: l'originale scrive $N = \{0,1,\ldots,n\}$; l'ultimo indice è stato corretto in $n-1$ per coerenza con le n coordinate delle parole.

[6]Nota di traduzione: questa frase contiene un refuso nell'originale: la proprietà riguarda le sottomatrici quadrate di P (o di P^{T}), non tutte quelle di H, che contiene un blocco identità. Con questa correzione segue la conclusione sul codice duale.

[7]Nota di traduzione: nella definizione di $g(U)$ l'originale reca "da V a U"; per la relazione seguente il codominio deve essere S.

(iii) Dimostrare l'identità polinomiale

$$\prod_{k=0}^{n-1}(x-q^k)=\sum_{k=0}^{n}(-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} x^{n-k}.$$

Note

L'espressione del polinomio cromatico di un grafo mediante la funzione di Möbius di $L(G)$ è dovuta a G.-C. Rota (1964).

Il Teorema 25.1(v) è essenzialmente la formula di Eulero per i politopi:

$$f_0 - f_1 + f_2 - f_3 + \cdots + (-1)^n f_n = 0,$$

dove f_i è il numero di facce di rango i, ossia di dimensione $i-1$ ($f_0 = f_n = 1$). Si veda B. Grünbaum (1967). Si veda anche R. Stanley (1986), dove gli insiemi parzialmente ordinati con la proprietà $\mu(x, y) = (-1)^d$ ogni volta che i ranghi di x e y differiscono di d sono chiamati *insiemi parzialmente ordinati euleriani*.

Riferimenti bibliografici

T. Dowling (1977), A note on complementing permutations, *J. Combinatorial Theory (B)* **23**, 223–226.

T. Dowling and R. M. Wilson (1975), Whitney number inequalities for geometric lattices, *Proc. Amer. Math. Soc.* **47**, 504–512.

Orig. 350

B. Grünbaum (1967), *Convex Polytopes*, J. Wiley (Interscience).

G.-C. Rota (1964), On the foundations of combinatorial theory I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2**, 340–368.

R. P. Stanley (1986), *Enumerative Combinatorics*, Vol. 1, Wadsworth.

L. Weisner (1935), Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.* **38**, 474–484.

Capitolo 26

Disegni combinatori e geometrie proiettive

Le geometrie sui campi finiti sono una ricca fonte di disegni combinatori e di configurazioni combinatorie affini. Cominciamo con due argomenti, archi e sottopiani, che scegliamo di trattare soltanto nei piani proiettivi, prima di passare alle quadriche e ad altre configurazioni negli spazi proiettivi generali. Orig. 351

Un (m,k)-*arco* in un piano proiettivo è un insieme di m punti, nessun $k+1$ dei quali è allineato. Nel Problema 19I ci siamo occupati di $(m,2)$-archi.

Sia A un (m,k)-arco in un piano proiettivo di ordine n e sia $x \in A$. Ognuna delle $n+1$ rette per x contiene al più $k-1$ altri punti di A, quindi

$$m \leq 1 + (n+1)(k-1).$$

Un (m,k)-arco A si dice *perfetto* quando vale l'uguaglianza. Ogni retta contenente un punto di un (m,k)-arco perfetto contiene evidentemente esattamente k punti dell'arco; cioè

$$|L \cap A| = 0 \text{ oppure } k$$

per ogni retta L. Chiaramente, le intersezioni non vuote delle rette con un (m,k)-arco perfetto forniscono i blocchi di un sistema di Steiner $S(2,k,m)$.

Un singolo punto è un $(1,1)$-arco perfetto. L'insieme degli n^2 punti non appartenenti a una retta fissata di un piano proiettivo di ordine n è un (n^2,n)-arco perfetto; il corrispondente sistema di Steiner è un piano affine di ordine n. Le iperovali del Problema 19I sono $(q+2,2)$-archi perfetti. I disegni corrispondenti sono banali. Essi hanno però archi "duali" i cui sistemi di Steiner sono interessanti: si veda il Problema 26A. La costruzione di (m,k)-archi perfetti in piani desarguesiani di ordine pari, nella parte (2) del teorema seguente, è dovuta a R. H. F. Denniston (1969). Al momento non si conoscono esempi di (m,k)-archi perfetti, $1 < k < n$, in piani proiettivi di ordine dispari n.[1] Orig. 352

Teorema 26.1. (1) Se in un piano proiettivo di ordine n esiste un (m,k)-arco perfetto, allora k divide n.

(2) Se q è una potenza di 2 e k divide q, esiste un (m,k)-arco perfetto in $PG_2(q)$.

Dimostrazione. Sia x un punto esterno a un (m,k)-arco perfetto A in un piano proiettivo di ordine n. Le rette per x partizionano i punti rimanenti, ma ciascuna contiene esattamente 0 oppure k punti di A. Quindi k deve dividere $m = 1 + (n+1)(k-1)$, da cui segue che k divide n.

Siano ora q una potenza di 2 e k un divisore di q. Sia $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ una qualsiasi forma quadratica irriducibile su $\mathbb{F}_q$ e sia H un sottogruppo di ordine k del gruppo additivo di $\mathbb{F}_q$. Nel piano affine $AG(2,q)$ poniamo

$$A := \{(x,y) : f(x,y) \in H\}.$$

Affermiamo che ogni retta affine interseca A in 0 oppure k punti. Immergendo il piano affine in $PG_2(q)$, A sarà un (m,k)-arco perfetto.

[1] Nota di traduzione: "al momento" si riferisce alla data dell'edizione originale.

Consideriamo una retta $L = \{(x, y) : y = mx + b\}$ con b, m entrambi non nulli. (Lasciamo al lettore le rette della forma $\{(x, y) : y = mx\}$ e $\{(x, y) : x = c\}$.) L'intersezione $L \cap A$ è l'insieme dei punti $(x, mx + b)$ per cui $\alpha x^2 + \beta x(mx + b) + \gamma(mx + b)^2 \in H$, ossia

$$F(x) \in H, \qquad F(x) := (\alpha + \beta m + \gamma m^2)x^2 + \beta bx + \gamma b^2.$$

Lavoriamo su un campo di caratteristica 2, quindi

$$x \longmapsto (\alpha + \beta m + \gamma m^2)x^2 + \beta bx$$

è un'applicazione lineare;[2] il suo nucleo ha ordine 2, perché l'irriducibilità di $f(x, y)$ assicura che tanto β quanto il coefficiente di x^2 sono non nulli. L'immagine K_F di questa applicazione è dunque un sottogruppo di ordine $q/2$ del gruppo additivo di $\mathbb{F}_q$. L'immagine di F è una classe laterale di K_F, ma, poiché $F(x)$ non è mai 0, ancora per l'irriducibilità di $f(x, y)$, essa è il complementare $\mathbb{F}_q \setminus K_F$. In conclusione, Orig. 353

$$|\{x : F(x) = a\}| = \begin{cases} 2 & \text{se } a \notin K_F, \\ 0 & \text{se } a \in K_F. \end{cases}$$

[3] Dunque $|L \cap A| = 2|H \cap (\mathbb{F}_q \setminus K_F)|$. Il sottogruppo H o è contenuto in K_F, nel qual caso $L \cap A = \varnothing$, oppure interseca K_F in un sottogruppo di ordine $k/2$, nel qual caso $|L \cap A| = k$. □

Come corollario, prendendo $n = 2^{m+1}$ e $k = 2^m$, otteniamo sistemi di Steiner

$$S(2, 2^m, 2^{2m+1} - 2^m).$$

I sistemi di Steiner $S(2, k, v)$ sono per molti aspetti più interessanti quando v è vicino a k^2, come avviene per i piani affini e proiettivi: la disuguaglianza di Fisher, Teorema 19.6, mostra che $v \geq k^2 - k + 1$. Questi esempi hanno $v < 2k^2$, un risultato ancora notevole.

Problema 26A. Sia A un (m, k)-arco perfetto in un piano proiettivo $\mathcal{P}$ di ordine n, $1 \leq k \leq n$. Sia A^* l'insieme delle rette che non incontrano A. Mostrare che A^* è un $(m^*, [n/k])$-arco perfetto nel piano duale $\mathcal{P}^*$ e calcolare m^* in funzione di m, k, n.

Problema 26B. Una classe parallela in un sistema di Steiner $S(2, k, m)$ è un insieme $\mathcal{A}$ di m/k blocchi tale che ogni punto sia incidente con esattamente un blocco di $\mathcal{A}$. Un $S(2, k, m)$ è risolubile quando i blocchi si possono partizionare in classi parallele (cfr. Problema 19K).

Sia A un (m, k)-arco perfetto in un piano proiettivo $\mathcal{P}$ di ordine n. Spiegare perché è risolubile il sistema di Steiner $S(2, k, m)$ i cui blocchi sono le intersezioni non banali delle rette con A.

Un *sottopiano* $\mathcal{S}$ di un piano proiettivo $\mathcal{P}$ è una sottostruttura di $\mathcal{P}$ che è essa stessa un piano proiettivo. Ricordiamo che una sottostruttura di una struttura d'incidenza $(\mathcal{P}, \mathcal{B}, I)$ è una struttura d'incidenza $(\mathcal{P}_0, \mathcal{B}_0, I_0)$ dove $\mathcal{P}_0 \subseteq \mathcal{P}$, $\mathcal{B}_0 \subseteq \mathcal{B}$ e $I_0 = I \cap (\mathcal{P}_0 \times \mathcal{B}_0)$. Dato un automorfismo, o collineazione, α di un piano proiettivo $\mathcal{P}$, la sottostruttura $\mathcal{S}$ costituita dai punti e dalle rette di $\mathcal{P}$ fissati da α ha la proprietà che due suoi punti sono incidenti con un'unica sua retta e due sue rette con un unico suo punto. Se $\mathcal{S}$ contiene quattro punti, nessun terzetto dei quali allineato, è un sottopiano; altrimenti può essere un quasifascio, oppure avere una sola retta o nessuna. Orig. 354

Esempio 26.1. Sia $V := \mathbb{F}_{q^n}^3$. I punti e le rette di $PG_2(q^n)$ sono i sottospazi di dimensione 1 e 2 di V su $\mathbb{F}_{q^n}$. Definiamo una sottostruttura $\mathcal{S}$ di $PG_2(q^n)$ i cui punti e rette siano quei sottospazi su $\mathbb{F}_{q^n}$ di dimensione 1 e 2 che ammettono basi costituite da vettori con coordinate nel sottocampo $\mathbb{F}_q$. Allora $\mathcal{S}$ è un sottopiano. Una sua retta è incidente con $q^n + 1$ punti di $PG_2(q^n)$, ma soltanto $q + 1$ di essi sono punti di $\mathcal{S}$.

Teorema 26.2. Se un piano proiettivo $\mathcal{P}$ di ordine n contiene un sottopiano $\mathcal{S}$ di ordine $m < n$, allora o (i) $n = m^2$, oppure (ii) $n \geq m^2 + m$.

Dimostrazione. Sia L una retta del sottopiano $\mathcal{S}$ e sia x un punto di L in $\mathcal{P}$ ma non in $\mathcal{S}$. Ognuna delle altre n rette per x può contenere al più un punto di $\mathcal{S}$: una retta M di $\mathcal{P}$ contenente almeno due punti di $\mathcal{S}$ dovrebbe infatti appartenere al sottopiano, e allora anche il punto x comune a M, L apparterrebbe al sottopiano. La retta L contiene $m+1$ punti di $\mathcal{S}$, che ha in totale m^2+m+1 punti, ciascuno appartenente a una retta per x. Dunque $m^2 \leq n$.

[2] Nota di traduzione: la linearità qui è su $\mathbb{F}_2$, ossia rispetto alla struttura additiva, non in generale su $\mathbb{F}_q$.

[3] Nota di traduzione: nelle condizioni dell'originale compare x al posto di a; è stato corretto l'indice.

L'uguaglianza implica che ogni retta di $\mathcal{P}$ incontra $\mathcal{S}$, evidentemente in uno oppure $m+1$ punti: se una retta N fosse disgiunta da $\mathcal{S}$, prendendo $x = L \cap N$ ciascuno degli m^2 punti di $\mathcal{S}$ esterni a L apparterrebbe a una di $n-1$ rette.

Supponiamo ora $m^2 < n$; esiste dunque una retta N non incidente con alcun punto di $\mathcal{S}$. Ognuna delle m^2+m+1 rette di $\mathcal{S}$ contiene un punto di N e due di esse non possono contenere lo stesso punto. Quindi $m^2+m+1 \le n+1$. □

Problema 26C. Mostrare che, se $PG_2(\mathbb{F})$ contiene la configurazione di Fano $PG_2(2)$, allora $\mathbb{F}$ ha caratteristica 2. Suggerimento: senza perdita di generalità, quattro punti della configurazione di Fano sono $\langle 1,0,0\rangle$, $\langle 0,1,0\rangle$, $\langle 0,0,1\rangle$, $\langle 1,1,1\rangle$. Calcolare le coordinate omogenee degli altri tre punti, che devono appartenere a una retta.

Orig. 355

Problema 26D. Un insieme bloccante in un piano proiettivo è un insieme S di punti che non contiene alcuna retta, ma tale che ogni retta incontri S in almeno un punto. Mostrare che un insieme bloccante in un piano proiettivo di ordine n contiene almeno $n+\sqrt{n}+1$ punti e che vale l'uguaglianza se e solo se S è l'insieme dei punti di un sottopiano di Baer.

Illustriamo un "metodo polinomiale" con la dimostrazione del seguente teorema su un tipo di insiemi bloccanti affini, dovuto a Brouwer e Schrijver (1978).

Teorema 26.3. Se V è un sottoinsieme di $AG(k,q)$ che incontra tutti gli iperpiani, allora

$$|V| \ge k(q-1)+1.$$

Dimostrazione. Sia A l'insieme bloccante. Senza perdita di generalità $0 \in A$. Poniamo $B := A \setminus \{0\}$. Allora B interseca tutti gli iperpiani che non contengono 0. Essi sono definiti dalle equazioni $w_1x_1+\cdots+w_kx_k=1$, dove w percorre tutti i vettori non nulli. Pertanto

$$F(x_1,x_2,\dots,x_k) := \prod_{b\in B}(b_1x_1+b_2x_2+\cdots+b_kx_k-1)$$

è identicamente nullo sullo spazio, eccetto che in 0.

Si mostra facilmente per induzione che un polinomio identicamente nullo sullo spazio appartiene all'ideale generato dai polinomi $x_i^q - x_i$, $i=1,\dots,k$. Scriviamo

$$F(x_1,\dots,x_k) = \sum_{i=1}^{k} F_i(x_1,\dots,x_k)(x_i^q-x_i) + G(x_1,\dots,x_k),$$

dove il grado massimo di ciascun x_i in G è al più $q-1$. Per ogni i, il polinomio $x_iF(x_1,\dots,x_k)$ è identicamente nullo sullo spazio, e lo stesso vale per $x_iG(x_1,\dots,x_k)$. Quindi G è divisibile per $\prod_i(x_i^{q-1}-1)$. Poiché $F(0)\neq 0$, anche $G(0)\neq 0$, per cui G ha grado $k(q-1)$. Il grado di F, che è $|B|$, deve dunque essere almeno $k(q-1)$. □

Una *forma quadratica* nelle indeterminate $x_1,x_2,\dots,x_n$ su un campo $\mathbb{F}$ è un polinomio omogeneo di grado 2 in tali indeterminate, cioè

$$f(x) = f(x_1,\dots,x_n) = \sum_{i,j=1}^{n} c_{ij}x_ix_j, \tag{26.1}$$

dove $c_{ij}\in\mathbb{F}$. La stessa forma quadratica è definita da più matrici $C=(c_{ij})$, perché contano soltanto i coefficienti diagonali e le somme $c_{ij}+c_{ji}$. Potremmo imporre $c_{ij}=0$ per $i>j$: le forme quadratiche in $x_1,\dots,x_n$ sarebbero allora in corrispondenza biunivoca con le matrici triangolari superiori $n\times n$ su $\mathbb{F}$.

Orig. 356

Una *quadrica* in $PG_n(\mathbb{F})$ è un insieme di punti proiettivi

$$Q = Q(f) := \{\langle x\rangle : f(x)=0\},$$

dove f è una forma quadratica in $n+1$ indeterminate. Per dare questa definizione dobbiamo scegliere una base e identificare i vettori con $(n+1)$-uple su $\mathbb{F}$.

Due forme quadratiche f,g sono *proiettivamente equivalenti* quando g si ottiene da f mediante una sostituzione lineare invertibile; in notazione matriciale, $g(x)=f(xA)$ per una matrice non singolare $n\times n$

A su $\mathbb{F}$. Se dunque f è data da una matrice C come in (26.1), cioè $f(x) = xCx^{\mathsf{T}}$, allora g è data da ACA^{T}. Per esempio, per ogni intero positivo n, la forma $nx_1^2 + nx_2^2 + nx_3^2 + nx_4^2$ è proiettivamente equivalente su $\mathbb{Q}$ a $x_1^2 + x_2^2 + x_3^2 + x_4^2$; si veda (19.12).

La notazione matriciale non si presta bene ai cambiamenti di nome o di numero delle indeterminate, che vogliamo ammettere. Per esempio, sostituire x_1 in una forma quadratica f con $y_1 + y_2$, dove y_1, y_2 sono nuove indeterminate, produce una forma proiettivamente equivalente.

Il *rango* di una forma quadratica è il minimo numero di indeterminate che compaiono con coefficienti non nulli in una forma quadratica proiettivamente equivalente. Per esempio, $(x_1 + \cdots + x_n)^2$ ha rango 1. Forme quadratiche proiettivamente equivalenti hanno lo stesso rango. Una forma quadratica in r indeterminate si dice *non degenere* quando ha rango r.

Esempio 26.2. Consideriamo le forme quadratiche in due indeterminate

$$f(x, y) = ax^2 + bxy + cy^2.$$

La forma ha rango 0 se e solo se $a = b = c = 0$. La quadrica corrispondente contiene tutti i punti di $PG_1(\mathbb{F})$, la retta proiettiva. Se la forma non è nulla, ha rango 1 se e solo se è un multiplo scalare del quadrato di una forma lineare $dx + ey$, il che avviene se e solo se il discriminante $b^2 - 4ac$ è 0.[4] La quadrica corrispondente in $PG_1(\mathbb{F})$ consiste allora in un solo punto. Una forma quadratica di rango 2 in due indeterminate o è irriducibile, oppure è prodotto di due forme lineari distinte. Nel primo caso la quadrica corrispondente in $PG_1(\mathbb{F})$ è vuota, nel secondo consiste di due punti.

Orig. 357

È chiaro che una forma quadratica irriducibile di rango 2 non è proiettivamente equivalente a una riducibile: quest'ultima ha zeri non banali in $\mathbb{F}$, mentre la prima non ne ha. Una forma quadratica riducibile è proiettivamente equivalente a x_1x_2.

Problema 26E. Mostrare che, su un campo $\mathbb{F}$ di caratteristica dispari, una forma quadratica f come in (26.1) è degenere se e solo se la matrice simmetrica $C + C^{\mathsf{T}}$ è singolare. Per un campo $\mathbb{F}$ di caratteristica 2, mostrare che f è degenere se e solo se $C + C^{\mathsf{T}}$ è singolare e $x(C + C^{\mathsf{T}}) = 0$ per qualche x con $f(x) = 0$.[5]

È importante capire che l'intersezione di una quadrica con un sottospazio chiuso U di $PG_n(\mathbb{F})$ è una quadrica in quel sottospazio. Supponiamo per esempio che U sia una retta proiettiva $PG_1(\mathbb{F})$ e che f sia una forma quadratica in $x_0, x_1, \ldots, x_n$. I punti di U hanno coordinate omogenee $\langle ya + zb \rangle$, dove $a = (a_0, \ldots, a_n)$ e $b = (b_0, \ldots, b_n)$ sono vettori linearmente indipendenti. Tali punti corrispondono biunivocamente alle coordinate omogenee $\langle (y, z) \rangle$ dei punti di $PG_1(\mathbb{F})$. Se $f = \sum_{0 \le i \le j \le n} c_{ij} x_i x_j$, allora

$$g(y, z) := \sum_{0 \le i \le j \le n} c_{ij}(ya_i + zb_i)(ya_j + zb_j)$$

è una forma quadratica in y, z e definisce una quadrica in $PG_1(\mathbb{F})$.[6] La forma quadratica g può essere degenere anche se f non lo è. Per l'Esempio 26.2, una retta o è interamente contenuta in una quadrica Q, oppure incontra Q in 0, 1 o 2 punti.

Lemma 26.4. Ogni forma quadratica f di rango $n \ge 3$ è proiettivamente equivalente a

$$x_1x_2 + g(x_3, \ldots, x_n) \tag{26.2}$$

per qualche forma quadratica $g(x_3, \ldots, x_n)$.[7]

Orig. 358

Dimostrazione. Supponiamo anzitutto q dispari. È facile vedere che una forma quadratica f è proiettivamente equivalente a una forma $\sum_{1 \le i \le j \le n} c_{ij} x_i x_j$ con $c_{11} \neq 0$. Poniamo $y := x_1 + \frac{1}{2c_{11}}(c_{12}x_2 + \cdots + c_{1n}x_n)$. Allora $f = c_{11}y^2 + g(x_2, \ldots, x_n)$. Induttivamente, se il rango di f è almeno 3, troviamo che f è proiettivamente equivalente a

$$h(x) = ax_1^2 + bx_2^2 + cx_3^2 + g'(x_4, \ldots, x_n),$$

[4] Nota di traduzione: in caratteristica 2 questa equivalenza richiede un campo perfetto, come tutti i campi finiti considerati nel seguito. Su un campo imperfetto una forma $ax^2 + cy^2$ può avere discriminante nullo senza essere un multiplo di un quadrato lineare.

[5] Nota di traduzione: in quest'ultima condizione si deve richiedere $x \neq 0$; il vettore nullo soddisfa sempre entrambe le equazioni.

[6] Nota di traduzione: nella somma che definisce g l'originale pone $1 \le i$; l'indice iniziale è stato corretto in 0, coerentemente con f e con le coordinate precedenti.

[7] Nota di traduzione: il lemma e i risultati di classificazione successivi sono sui campi finiti $\mathbb{F}_q$, come usa la dimostrazione; l'enunciato non vale su un campo arbitrario.

con a, b, c tutti non nulli. Si può moltiplicare ciascuno dei tre scalari per un quadrato non nullo ottenendo una forma proiettivamente equivalente; due di essi devono differire per un fattore quadrato, per cui possiamo supporre, per esempio, $b = c$.

Affermiamo che esistono $s, t \in \mathbb{F}_q$ tali che $s^2 + t^2 = -b^{-1}a$. Per vederlo si può considerare la tabella di addizione di $\mathbb{F}_q$, che è un quadrato latino. I quadrati di $\mathbb{F}_q$, incluso 0, sono $(q+1)/2$. L'elemento $-b^{-1}a$, come ogni altro, compare $(q-1)/2$ volte nelle $(q-1)/2$ colonne indicizzate dai non quadrati, e altrettante nelle righe indicizzate dai non quadrati; deve dunque comparire almeno una volta nella sottomatrice le cui righe e colonne sono indicizzate dai quadrati. Scelti così s, t, h è proiettivamente equivalente a

$$\begin{aligned} &ax_1^2 + b(sx_2 + tx_3)^2 + b(tx_2 - sx_3)^2 + g'(x_4, \ldots, x_n) \\ &\quad = ax_1^2 - ax_2^2 - ax_3^2 + g'(x_4, \ldots, x_n) \\ &\quad = (ax_1 + ax_2)(x_1 - x_2) - ax_3^2 + g'(x_4, \ldots, x_n), \end{aligned}$$

e quest'ultima è chiaramente proiettivamente equivalente a (26.2).

Il caso q pari è un po' più laborioso; si veda la dimostrazione del Teorema 5.1.7 in J. W. P. Hirschfeld (1979). □

Teorema 26.5. (i) Ogni forma quadratica f di rango dispari n è proiettivamente equivalente a

$$f_0(x) := x_1x_2 + \cdots + x_{n-2}x_{n-1} + cx_n^2 \tag{26.3}$$

per qualche scalare c. (ii) Ogni forma quadratica f di rango pari n è proiettivamente equivalente o a Orig. 359

$$f_1(x) := x_1x_2 + \cdots + x_{n-3}x_{n-2} + x_{n-1}x_n, \tag{26.4}$$

oppure a

$$f_2(x) := x_1x_2 + \cdots + x_{n-3}x_{n-2} + p(x_{n-1}, x_n), \tag{26.5}$$

dove $p(x_{n-1}, x_n)$ è una forma quadratica irriducibile in due indeterminate.

Dimostrazione. Segue dal Lemma 26.3 e dall'induzione.[8] □

Le forme quadratiche, e le corrispondenti quadriche, di rango dispari si chiamano *paraboliche*. Quelle di rango pari proiettivamente equivalenti a (26.4) si chiamano *iperboliche*, quelle equivalenti a (26.5) *ellittiche*. Due forme quadratiche iperboliche dello stesso rango sono entrambe proiettivamente equivalenti a (26.4), quindi tra loro. È anche vero che tutte le forme quadratiche paraboliche di un dato rango pari sono proiettivamente equivalenti, cioè che possiamo porre $c = 1$ in (26.3), e che tutte le forme quadratiche ellittiche di un dato rango sono proiettivamente equivalenti.[9] Si veda J. W. P. Hirschfeld (1979) per questi fatti e per ulteriori informazioni sulle forme canoniche. Dal teorema seguente discende che forme quadratiche iperboliche ed ellittiche non sono proiettivamente equivalenti.

Teorema 26.6. Una quadrica non degenere Q in $PG_n(q)$ ha cardinalità

$$\begin{cases} \dfrac{q^n - 1}{q - 1} & \text{se } n \text{ è pari, cioè } Q \text{ è parabolica,} \\ \dfrac{(q^{(n+1)/2} - 1)(q^{(n-1)/2} + 1)}{q - 1} & \text{se } n \text{ è dispari e } Q \text{ è iperbolica,} \\ \dfrac{(q^{(n+1)/2} + 1)(q^{(n-1)/2} - 1)}{q - 1} & \text{se } n \text{ è dispari e } Q \text{ è ellittica.} \end{cases}$$

Dimostrazione. In generale, se $f(x_1, \ldots, x_r) = x_1x_2 + g(x_3, \ldots, x_r)$ e vi sono N vettori $(x_3, \ldots, x_r)$ tali che $g(x_3, \ldots, x_r) = 0$, vi sono $(2q-1)N + (q-1)(q^{r-2} - N)$ vettori $(x_1, \ldots, x_r)$ tali che $f(x_1, \ldots, x_r) = 0$. Orig. 360
Ciò consente di verificare per induzione le seguenti formule per il numero di zeri in $\mathbb{F}_q^r$ di una forma quadratica f di rango r in r indeterminate:

$$\begin{cases} q^{r-1} & \text{se } r \text{ è dispari, cioè } f \text{ è parabolica,} \\ q^{r-1} + q^{r/2} - q^{r/2-1} & \text{se } r \text{ è pari e } f \text{ è iperbolica,} \\ q^{r-1} - q^{r/2} + q^{r/2-1} & \text{se } r \text{ è pari e } f \text{ è ellittica.} \end{cases}$$

[8] Nota di traduzione: il lemma richiamato è il 26.4.

[9] Nota di traduzione: "rango pari" è un refuso per "rango dispari". Inoltre, con la definizione stretta di equivalenza data sopra, per q dispari c può essere normalizzato a 1 soltanto se è un quadrato. La normalizzazione è sempre possibile per le *quadriche*, ammettendo anche un fattore scalare non nullo della forma, che non cambia il luogo degli zeri.

Naturalmente il numero di punti proiettivi delle quadriche corrispondenti in $PG_n(q)$ si ottiene sostituendo r con $n+1$, sottraendo 1, per il vettore nullo, e dividendo per $q-1$. □

Teorema 26.7. Sia Q una quadrica non degenere in $PG_n(q)$. La massima dimensione proiettiva di un sottospazio chiuso $F \subseteq Q$ è

$$\begin{cases} n/2-1 & \text{se } n \text{ è pari, cioè } Q \text{ è parabolica,} \\ (n-1)/2 & \text{se } n \text{ è dispari e } Q \text{ è iperbolica,} \\ (n-3)/2 & \text{se } n \text{ è dispari e } Q \text{ è ellittica.} \end{cases}$$

Dimostrazione. Sia f una forma quadratica non degenere in r indeterminate. L'enunciato equivale ad affermare che la massima dimensione di un sottospazio U di $\mathbb{F}_q^r$ su cui f si annulla è

$$\begin{cases} (r-1)/2 & \text{se } r \text{ è dispari, cioè } f \text{ è parabolica,} \\ r/2 & \text{se } r \text{ è pari e } f \text{ è iperbolica,} \\ r/2-1 & \text{se } r \text{ è pari e } f \text{ è ellittica.} \end{cases}$$

Osserviamo anzitutto che, se $f = f_0$ in (26.3), allora $f(x) = 0$ per ogni $x \in \operatorname{span}(e_2, e_4, \dots, e_{r-1})$, dove $e_1, \dots, e_r$ è la base canonica di $\mathbb{F}_q^r$. Se $f = f_1$ in (26.4), $f(x) = 0$ per ogni $x \in \operatorname{span}(e_2, e_4, \dots, e_r)$. Se $f = f_2$ in (26.5), $f(x) = 0$ per ogni $x \in \operatorname{span}(e_2, e_4, \dots, e_{r-2})$. Questi sottospazi hanno dimensioni rispettivamente $(r-1)/2$, $r/2$ e $r/2-1$.

Resta da mostrare che in nessuno dei casi f può annullarsi su un sottospazio di dimensione maggiore. Useremo il Teorema 26.5 e l'induzione. I casi $r = 1, 2$ sono banali. Supponiamo $f(x_1, \dots, x_r) = x_1x_2 + g(x_3, \dots, x_r)$ e $f(x) = 0$ per ogni x in un sottospazio $U \subseteq \mathbb{F}_q^r$ di dimensione k. Per completare la dimostrazione mostreremo che esiste un sottospazio $U' \subseteq \mathbb{F}_q^{r-2}$ di dimensione $\geq k-1$ tale che $g(y) = 0$ per ogni $y \in U'$. Orig. 361

Chiaramente $g(y) = 0$ per ogni y in

$$U_0 := \{(x_3, \dots, x_r) : (0, 0, x_3, \dots, x_r) \in U\}.$$

Se $\dim U_0 \geq k-1$, abbiamo finito; supponiamo dunque $\dim U_0 = k-2$. Allora in U esistono vettori

$$(1, 0, a_3, \dots, a_r) \quad \text{e} \quad (0, 1, b_3, \dots, b_r).$$

Quindi $(1, 1, a_3 + b_3, \dots, a_r + b_r) \in U$, per cui $g(a_3 + b_3, \dots, a_r + b_r) = -1$. La forma g si annulla evidentemente su tutti i vettori di

$$\operatorname{span}((a_3, \dots, a_r)) + U_0 \quad \text{e} \quad \operatorname{span}((b_3, \dots, b_r)) + U_0.$$

Uno di questi sottospazi deve avere dimensione $> k-2$, perché altrimenti $(a_3 + b_3, \dots, a_r + b_r) \in U_0$, in contraddizione con $g(a_3 + b_3, \dots, a_r + b_r) = -1$. □

Esempio 26.3. Sia f una forma quadratica in tre indeterminate e consideriamo la quadrica $Q(f)$ nel piano proiettivo $PG_2(q)$. Se f è non degenere, $Q(f)$ contiene $q+1$ punti proiettivi. Come osservato sopra, ogni retta L di $PG_2(q)$ incontra $Q(f)$ in una quadrica di L, che in questo caso consiste di 0, 1 o 2 punti, perché per il Teorema 26.7 $Q(f)$ non può contenere L. Quindi $Q(f)$ è un insieme di $q+1$ punti, nessun terzetto dei quali allineato, cioè un'ovale. Si veda il Problema 19I.

Se f ha rango 0, $Q(f)$ è tutto $PG_2(q)$. Se ha rango 1, $Q(f)$ consiste dei punti di una retta. Se ha rango 2, vi sono due casi. Se f è riducibile, per esempio proiettivamente equivalente a xy, $Q(f)$ consiste dei punti dell'unione di due rette di $PG_2(q)$; se f è irriducibile, $Q(f)$ è un singolo punto di $PG_2(q)$.

Esempio 26.4. I codici di Reed–Muller del primo ordine sono stati introdotti nel Capitolo 18. Ecco un modo per introdurre l'intera famiglia. Sia $V = \mathbb{F}_2^m$. Consideriamo vettori di lunghezza 2^m le cui coordinate sono indicizzate dagli elementi di V; concretamente, scriviamo $V = \{v_0, v_1, \dots, v_{2^m-1}\}$. Il codice di Reed–Muller di ordine k, $RM(k, m)$, è costituito da tutti i vettori di lunghezza 2^m Orig. 362

$$(f(v_0), f(v_1), \dots, f(v_{2^m-1})),$$

dove f percorre tutti i polinomi in $x_1, \dots, x_m$ di grado al più k.

Poiché su $\mathbb{F}_2$ una forma lineare $x_{i_1}+\cdots+x_{i_k}$ dà la stessa funzione della forma quadratica $x_{i_1}^2+\cdots+x_{i_k}^2$, le parole del codice del secondo ordine $RM(2,m)$ sono date dalle forme quadratiche binarie $f(x_1,\ldots,x_n)$ e dai loro "complementari" $f(x_1,\ldots,x_n)+1$. I Teoremi 26.4 e 26.5 sono utili per determinare i pesi delle parole di $RM(2,m)$.[10]

Bisogna considerare anche le forme degeneri: per esempio $x_1x_2+x_3x_4$ corrisponde a una parola di peso 24 in $RM(2,6)$. Si trova che i pesi delle parole di $RM(2,6)$ sono 0, 16, 24, 28, 32, 36, 40, 48 e 64.

Problema 26F. Sia $f(x) := x_1x_2+\cdots+x_{2m-1}x_{2m}$. Allora f determina una classe laterale C di $RM(1,2m)$ in $RM(2,2m)$, costituita dalle parole corrispondenti a $f(x)+a(x)$, dove $a(x)$ percorre le 2^{2m+1} funzioni affini, cioè lineari con un eventuale termine costante, in $2m$ variabili. Mostrare che in C metà delle parole ha peso $2^{2m-1}+2^{m-1}$ e metà peso $2^{2m-1}-2^{m-1}$.

Esempio 26.5. Sia Q_3 una quadrica ellittica non degenere nello spazio proiettivo tridimensionale $PG_3(q)$. Per il Teorema 26.6, $|Q_3|=q^2+1$. Per il Teorema 26.7, Q_3 non contiene rette. Ogni piano P incontra Q_3 in una quadrica di quel piano; per l'Esempio 26.3, deve incontrarla o in un'ovale oppure in un singolo punto. Ogni terna di punti di Q_3 è contenuta in un unico piano: dunque le intersezioni non banali dei piani con Q_3 forniscono i blocchi di un sistema di Steiner

$$S(3,q+1,q^2+1).$$

In generale, un insieme di q^2+1 punti di $PG_3(q)$, nessun terzetto dei quali allineato, si chiama *ovoide*; un $S(3,n+1,n^2+1)$ si chiama *piano di Möbius* o *piano inversivo*.

Esempio 26.6. Sia Q_4 una quadrica non degenere nello spazio proiettivo quadridimensionale $PG_4(q)$. Per il Teorema 26.6, $|Q_4|=q^3+q^2+q+1$. Sia $\mathcal{Q}$ la struttura d'incidenza i cui punti sono gli elementi di Q_4 e i cui blocchi sono le rette di $PG_4(q)$ interamente contenute in Q_4. Ogni punto di $\mathcal{Q}$ appartiene a esattamente $q+1$ blocchi di $\mathcal{Q}$ (si veda il Problema 26F).[11] Dati un punto x e un blocco L di $\mathcal{Q}$, l'intersezione del piano $P:=\{x\}\vee L$ con Q_4 è una quadrica Q_2 in P che contiene, ovviamente, una retta e un punto esterno a essa.[12] Per l'Esempio 26.3, Q_2 deve consistere nei punti di due rette incidenti. Ciò implica che $\mathcal{Q}$ è una geometria parziale $pg(r,k,t)$, nel senso del Capitolo 21, con

Orig. 363

$$r=q+1,\qquad k=q+1,\qquad t=1.$$

Esempio 26.7. Sia Q_5 una quadrica ellittica non degenere in $PG_5(q)$. Per il Teorema 26.6, $|Q_5|=(q+1)(q^3+1)$. Per il Teorema 26.7, Q_5 non contiene piani. Sia $\mathcal{Q}$ la struttura d'incidenza i cui punti sono gli elementi di Q_5 e i cui blocchi sono le rette di $PG_5(q)$ interamente contenute in Q_5. Per il Problema 26F, ogni punto di $\mathcal{Q}$ appartiene a q^2+1 rette di $\mathcal{Q}$. Un argomento analogo a quello dell'Esempio 26.6 mostra che $\mathcal{Q}$ è una geometria parziale $pg(r,k,t)$ con

$$r=q^2+1,\qquad k=q+1,\qquad t=1.$$

Le geometrie parziali con $t=1$ si chiamano *quadrangoli generalizzati*. Per ulteriori risultati e riferimenti si veda L. M. Batten (1986).

Problema 26G. Sia f una forma quadratica non degenere in n indeterminate, data da una matrice $C=(c_{ij})$ su $\mathbb{F}_q$ come in (26.1). Sia $Q=Q(f)$ la quadrica corrispondente in $PG_{n-1}(\mathbb{F}_q)$ e sia $p=\langle x\rangle$ uno dei suoi punti. Poniamo

$$T_p := \{\langle y\rangle : x(C+C^{\mathsf{T}})y^{\mathsf{T}}=0\}.$$

Per il Problema 26E, T_p è un iperpiano di $PG_{n-1}(\mathbb{F}_q)$. Mostrare che $T_p\cap Q$ consiste esattamente di p e dell'unione delle rette per p contenute in Q. Mostrare inoltre che, se W è un qualsiasi iperpiano di T_p non contenente p, allora $Q':=W\cap Q$ è una quadrica non degenere in $W=PG_{n-3}(\mathbb{F}_q)$ e che Q' è parabolica, iperbolica o ellittica secondo che lo sia Q. In particolare, il numero di rette per p interamente contenute in Q è $|Q'|$. Una *forma hermitiana* nelle indeterminate $x_1,\ldots,x_n$ su $\mathbb{F}_{q^2}$ è un'espressione

Orig. 364

$$h(x)=h(x_1,\ldots,x_n)=\sum_{i,j=1}^{n} c_{ij}x_ix_j^q, \tag{26.6}$$

[10] Nota di traduzione: qui le indeterminate sono m; il conteggio degli zeri necessario per i pesi è nel Teorema 26.6, oltre alla classificazione del 26.5. L'originale usa n e richiama 26.4 e 26.5.

[11] Nota di traduzione: il riferimento corretto è al Problema 26G, anche nel successivo Esempio 26.7.

[12] Nota di traduzione: qui si assume $x\notin L$, come richiede l'assioma della geometria parziale che si sta verificando.

dove $c_{ij} \in \mathbb{F}_{q^2}$ e $c_{ji} = c_{ij}^q$. In particolare, i coefficienti diagonali c_{ii}, fissati dall'automorfismo di Frobenius $x \mapsto x^q$, appartengono a $\mathbb{F}_q$.

Due forme hermitiane f, g su $\mathbb{F}_{q^2}$ sono proiettivamente equivalenti quando g si ottiene da f mediante una sostituzione lineare invertibile; in notazione matriciale, $g(x) = f(xA)$ per una matrice non singolare $n \times n$ A su $\mathbb{F}_{q^2}$. Se f è definita da C come in (26.6), cioè $f(x) = xCx^{\mathsf{T}}$, allora g è definita da ACA^*, dove A^* è la trasposta coniugata di A: se $A = (a_{ij})$, $A^* := (a_{ji}^q)$.[13]

Il *rango* di una forma hermitiana è il minimo numero di indeterminate che compaiono con coefficienti non nulli in una forma hermitiana proiettivamente equivalente.

Una *varietà hermitiana* in $PG_n(q^2)$ è un insieme di punti proiettivi

$$H = H(f) := \{\langle x \rangle : f(x) = 0\},$$

dove f è una forma hermitiana in $n+1$ indeterminate. Per dare questa definizione dobbiamo scegliere una base e identificare i vettori con $(n+1)$-uple su $\mathbb{F}_{q^2}$. Si può vedere che l'intersezione di una varietà hermitiana in $PG_n(q^2)$ con un sottospazio chiuso è una varietà hermitiana in quel sottospazio.

Teorema 26.8. Una forma hermitiana di rango n è proiettivamente equivalente a

$$x_1^{q+1} + x_2^{q+1} + \cdots + x_n^{q+1}. \tag{26.7}$$

DIMOSTRAZIONE. Non è difficile vedere che ogni forma hermitiana non nulla è proiettivamente equivalente a una h come in (26.6) con $c_{11} \neq 0$; lasciamo la verifica al lettore. Poniamo $y := c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n$. Allora $h = c_{11}^{-1} y y^q + g(x_2, \ldots, x_n)$, dove g è una forma hermitiana in $x_2, \ldots, x_n$.[14] Poiché $c_{11} \in \mathbb{F}_q$, esiste $a \in \mathbb{F}_{q^2}$ tale che $a^{q+1} = c_{11}^{-1}$; quindi $h = z^{q+1} + g(x_2, \ldots, x_n)$ con $z = ay$.

Il teorema segue da questo passo e dall'induzione. □

Orig. 365

Teorema 26.9. Il numero di punti di una varietà hermitiana non degenere H in $PG_n(q^2)$ è

$$\frac{(q^{n+1} + (-1)^n)(q^n - (-1)^n)}{q^2 - 1}.$$

DIMOSTRAZIONE. Per ogni $a \neq 0$ in $\mathbb{F}_q$ esistono $q+1$ valori di $x \in \mathbb{F}_{q^2}$ tali che $x^{q+1} = a$. Se

$$f(x_1, \ldots, x_n) = x_1^{q+1} + g(x_2, \ldots, x_n)$$

e vi sono N vettori $(x_2, \ldots, x_n)$ con $g(x_2, \ldots, x_n) = 0$, allora vi sono $N + (q+1)(q^{2(n-1)} - N)$ vettori $(x_1, \ldots, x_n)$ con $f(x_1, \ldots, x_n) = 0$. Per induzione, gli zeri di (26.7) in $\mathbb{F}_{q^2}^n$ sono $q^{2n-1} + (-1)^n(q^n - q^{n-1})$, e il teorema segue. □

Esempio 26.8. Consideriamo le varietà hermitiane nella retta proiettiva $PG_1(q^2)$. Se una forma hermitiana f in due indeterminate ha rango 0, la varietà $H(f)$ contiene tutti i q^2+1 punti; se ha rango 1, $H(f)$ consiste di un solo punto; se ha rango 2, $H(f)$ contiene $q+1$ punti. Ne segue che, per qualsiasi n, se H è una varietà hermitiana in $PG_n(q^2)$, le rette incontrano H in 1, $q+1$ oppure q^2+1 punti.

Consideriamo ora una varietà hermitiana non degenere H_2 nel piano proiettivo $PG_2(q^2)$. Per il Teorema 26.9 essa ha q^3+1 punti. Ogni retta L incontra H_2 in una varietà hermitiana $L \cap H_2$ di quella retta. Per esercizio, il lettore verifichi che H_2 non contiene rette; quindi $|L \cap H_2| = 1$ oppure $q+1$. Ne segue che le intersezioni non banali delle rette di $PG_2(q^2)$ con H_2 forniscono i blocchi di un sistema di Steiner

$$S(2, q+1, q^3+1)$$

sull'insieme di punti H_2.

I disegni con questi parametri si chiamano *unitali*. Un'analisi ulteriore mostra che i disegni costruiti sopra sono risolubili; si veda R. C. Bose (1959).

Concludiamo il capitolo con una costruzione di analoghi di dimensione superiore dei sistemi di Steiner $S(3, q+1, q^2+1)$ dell'Esempio 26.5; quelli costruiti qui sotto sono stati chiamati *geometrie di cerchi*.

Orig. 366

[13] Nota di traduzione: la formula matriciale di f nell'originale omette la coniugazione: va letta $f(x) = xCx^*$, dove $x^* = (x_i^q)^{\mathsf{T}}$.

[14] Nota di traduzione: con la convenzione di (26.6), per ottenere questa uguaglianza si deve porre $y = c_{11}x_1 + c_{21}x_2 + \cdots + c_{n1}x_n$, cioè usare la prima colonna di C anziché la prima riga.

Teorema 26.10. Se q è una potenza di un primo e n un intero positivo, esiste un sistema di Steiner $S(3, q+1, q^n+1)$.

DIMOSTRAZIONE. Sia V uno spazio vettoriale di dimensione 2 su $\mathbb{F}_{q^n}$ e sia $\mathcal{X}$ l'insieme dei suoi sottospazi di dimensione 1 su $\mathbb{F}_{q^n}$, cioè dei q^n+1 punti di $PG_1(q^n)$, la retta proiettiva di ordine q^n.

Pensiamo ora V come spazio vettoriale di dimensione $2n$ su $\mathbb{F}_q$. I blocchi del nostro sistema di Steiner proverranno dai sottospazi U di dimensione 2 su $\mathbb{F}_q$ di V che non sono contenuti in alcun elemento di $\mathcal{X}$. Per ciascuno poniamo

$$B_U := \{P \in \mathcal{X} : P \cap U \neq \{0\}\}.$$

Ogni $P \in B_U$ incontra U in un sottospazio di dimensione 1 su $\mathbb{F}_q$, contenente $q-1$ dei q^2-1 vettori non nulli di U, dunque $|B_U| = q+1$. Se $W = \lambda U$ per qualche scalare non nullo $\lambda \in \mathbb{F}_{q^n}$, allora $B_U = B_W$; prendiamo come blocchi soltanto gli insiemi B_U distinti.

Consideriamo tre punti distinti $P_i \in \mathcal{X}$, $i = 1, 2, 3$. Sia P_i generato su $\mathbb{F}_{q^n}$ da un vettore x_i. I tre vettori sono linearmente dipendenti su $\mathbb{F}_{q^n}$, diciamo

$$x_3 = \alpha x_1 + \beta x_2, \qquad \alpha, \beta \in \mathbb{F}_{q^n}.$$

È allora chiaro che $U := \mathrm{span}_{\mathbb{F}_q}\{\alpha x_1, \beta x_2\}$ incontra non banalmente tutti e tre i P_i. Supponiamo che un sottospazio W di dimensione 2 su $\mathbb{F}_q$ incontri non banalmente ciascun P_i, cioè contenga $\gamma_i x_i$ con $0 \neq \gamma_i \in \mathbb{F}_{q^n}$, $i = 1, 2, 3$. Questi vettori sono linearmente dipendenti su $\mathbb{F}_q$, diciamo

$$\gamma_3 x_3 = a\gamma_1 x_1 + b\gamma_2 x_2, \qquad a, b \in \mathbb{F}_q.$$

Poiché x_1, x_2 sono linearmente indipendenti su $\mathbb{F}_{q^n}$, abbiamo $\gamma_3\alpha = a\gamma_1$ e $\gamma_3\beta = b\gamma_2$. Ne segue $\gamma_3 U = W$: dunque tre punti distinti sono contenuti in un unico blocco. □

Problema 26H. Sia α una collineazione di un piano proiettivo $\mathcal{P}$.

(i) Mostrare che, se α fissa tutti i punti di una retta l e due punti esterni a l, allora fissa puntualmente $\mathcal{P}$. (ii) Se α fissa tutti i punti di una retta l, esiste un punto P tale che α fissi P e ogni retta per P. Orig. 367

(Un tale automorfismo di $\mathcal{P}$ si chiama *collineazione centrale*.)

Problema 26I. Nel Capitolo 23 abbiamo visto che $AG(3, q)$ è una sottogeometria di $PG(3, q)$, la cui parte mancante è un piano proiettivo P, talvolta chiamato piano all'infinito di $AG(3, q)$. Sia $q = 2^m$ e sia O un'iperovale in P. Definiamo una struttura d'incidenza I avente come punti quelli di $AG(3, q)$ e come rette quelle di $AG(3, q)$ che incontrano P in un punto di O. Mostrare che I è un quadrangolo generalizzato.

Problema 26J. Considerare un'iperovale O in $PG(2, 4)$. Definire un grafo G avente come vertici i punti del piano esterni a O e come spigoli le coppie (x, y) per le quali la retta per x, y incontra O. Dimostrare:

(i) Ogni spigolo appartiene a un unico triangolo.

(ii) Per ogni triangolo (x, y, z), tutti gli altri vertici sono adiacenti a esattamente uno fra x, y, z.

(iii) G è un quadrangolo generalizzato.

Problema 26K. Considerare un qualsiasi disegno simmetrico (v, k, λ). Definire un arco come un insieme S di punti, nessun terzetto dei quali appartenente a uno stesso blocco. Un blocco si chiama tangente a S se lo incontra in un punto. Trovare un limite superiore per $|S|$, distinguendo secondo che S abbia o no una tangente.

Problema 26L. Un'ovale in un disegno simmetrico è un arco che raggiunge il limite del Problema 26J.[15] Considerare un disegno simmetrico con parametri $(4\lambda - 1, 2\lambda, \lambda)$. Mostrare che le ovali di questo disegno sono le rette di cardinalità 3 del disegno complementare.

Note

Nella letteratura si usa spesso "(m, k)-arco massimale" per ciò che abbiamo chiamato "(m, k)-arco perfetto", ma per noi questo è un abuso intollerabile della parola "massimale".

[15] Nota di traduzione: il riferimento corretto è al Problema 26K.

Le proprietà combinatorie delle quadriche e delle varietà hermitiane sono discusse più dettagliatamente in D. K. Ray-Chaudhuri (1962) e in R. C. Bose e I. M. Chakravarti (1966).

Il metodo polinomiale illustrato nella dimostrazione del Teorema 26.3 ha altre applicazioni. Per esempio A. Blokhuis (1994) dimostrò che un insieme bloccante non banale in $PG(2,p)$ ha almeno $(3p+1)/2$ punti, una congettura di J. di Paola. L'idea è osservare che l'insieme bloccante S deve avere una tangente, che senza perdita di generalità è la retta all'infinito. Siano (a_i, b_i) gli altri punti nel piano affine, con $i = 1, \ldots, p+k$. Uno studio complicato, lungo una pagina, del polinomio Orig. 368

$$F(t,u) = \prod_{i=1}^{p+k} (t + a_i + ub_i)$$

mostra che $k \geq (p+1)/2$.

Riferimenti bibliografici

L. M. Batten (1986), *Combinatorics of Finite Geometries*, Cambridge University Press.

A. Blokhuis (1994), On the size of a blocking set in $PG(2,p)$, *Combinatorica* **14** (1994), 111–114.

R. C. Bose (1959), On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements, *Golden Jubilee Commemoration Volume (1958–59)*, Calcutta Math. Soc., pp. 341–354.

R. C. Bose and I. M. Chakravarti (1966), Hermitian varieties in a finite projective space $PG(N,q^2)$, *Canad. J. Math* **18**, 1161–1182.

A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combinatorial Theory (A)* **24** (1978), 251–253.

P. Dembowski (1968), *Finite Geometries*, Springer-Verlag.

R. H. F. Denniston (1969), Some maximal arcs in finite projective planes, *J. Combinatorial Theory* **6**, 317–319.

J. W. P. Hirschfeld (1979), *Projective Geometries over Finite Fields*, Clerendon Press.

D. K. Ray-Chaudhuri (1962), Some results on quadrics in finite projective geometry based on Galois fields, *Canad. J. Math.* **14**, 129–138.

Capitolo 27

Insiemi di differenze e automorfismi

Orig. 369

Una classe di disegni simmetrici nasce dagli insiemi di differenze, definiti sotto, nei gruppi abeliani. Un disegno di questo tipo è apparso nell'Esempio 19.6. Il gruppo ricompare nel gruppo degli automorfismi del disegno.

In una struttura d'incidenza semplice possiamo identificare i blocchi con insiemi di punti, cioè l'insieme dei blocchi $\mathcal{A}$ è una famiglia di sottoinsiemi dell'insieme dei punti X. Un *automorfismo* di un disegno simmetrico $(X, \mathcal{A})$, o di qualsiasi struttura d'incidenza semplice, è una permutazione α di X che porta $\mathcal{A}$ in $\mathcal{A}$: per $A \subseteq X$, $A \in \mathcal{A}$ se e solo se $\alpha(A) \in \mathcal{A}$. Cominciamo con un teorema generale sugli automorfismi dei disegni simmetrici.

Teorema 27.1. Sia $\mathcal{S} = (X, \mathcal{A})$ un disegno simmetrico (v, k, λ) e sia α un suo automorfismo. Allora il numero di punti fissati da α è uguale al numero di blocchi fissati da α.

DIMOSTRAZIONE. Sia N la matrice d'incidenza di $\mathcal{S}$. Definiamo una matrice di permutazione P, con righe e colonne indicizzate dai punti, ponendo

$$P(x, y) := \begin{cases} 1 & \text{se } \alpha(x) = y, \\ 0 & \text{altrimenti.} \end{cases}$$

Definiamo analogamente una matrice di permutazione Q, con righe e colonne indicizzate dai blocchi, ponendo

$$Q(A, B) := \begin{cases} 1 & \text{se } \alpha(A) = B, \\ 0 & \text{altrimenti.} \end{cases}$$

La traccia di P è il numero dei punti fissi, mentre la traccia di Q è il numero dei blocchi fissati da α. Ora

Orig. 370

$$\begin{aligned}(PNQ^{\mathsf{T}})(x, A) &= \sum_{y \in X,\ B \in \mathcal{A}} P(x, y) N(y, B) Q(A, B) \\ &= N(\alpha(x), \alpha(A)) = N(x, A).\end{aligned}$$

Cioè $PNQ^{\mathsf{T}} = N$, o equivalentemente $P = NQN^{-1}$. Le matrici P, Q sono dunque simili e hanno la stessa traccia; il teorema è dimostrato. □

Corollario. Il tipo della decomposizione in cicli di α sull'insieme dei punti X coincide con quello della decomposizione in cicli sull'insieme dei blocchi $\mathcal{A}$.

DIMOSTRAZIONE. Per il Teorema 27.1, α^i ha lo stesso numero di punti fissi e di blocchi fissi, per ogni $i = 1, 2, \ldots$.

Supponiamo che una permutazione β abbia c_i cicli di lunghezza i su un insieme S, $i = 1, 2, \ldots, |S|$. Sia f_j il numero di punti fissi di β^j. Allora

$$f_j = \sum_{i|j} i c_i,$$

e per inversione di Möbius, Teorema 10.4,

$$j c_j = \sum_{i|j} \mu(j/i) f_i.$$

Il punto è che i numeri di cicli di ogni lunghezza, cioè il tipo di β, sono completamente determinati dai numeri di punti fissi delle potenze di β. □

Corollario. Se Γ è un gruppo di automorfismi di un disegno simmetrico, il numero di orbite di Γ sull'insieme dei punti X coincide con quello delle orbite sull'insieme dei blocchi $\mathcal{A}$. In particolare, Γ è transitivo sui punti se e solo se è transitivo sui blocchi.

DIMOSTRAZIONE. Per il lemma di Burnside, Teorema 10.5, il numero di orbite di un gruppo Γ di permutazioni di un insieme S è determinato esattamente dal multiinsieme $(f(\alpha) : \alpha \in \Gamma)$, dove $f(\alpha)$ è il numero di elementi di S fissati da α. □ Prima di introdurre gli insiemi di differenze, facciamo una digressione per dare un teorema sulle orbite dei gruppi di automorfismi di 2-disegni arbitrari, noto come *lemma di Block*; si veda Block (1967). Esso fornisce un'altra dimostrazione del corollario precedente, perché per il Teorema 19.9 anche il duale di un disegno simmetrico è un 2-disegno. Orig. 371

Teorema 27.2. Se Γ è un gruppo di automorfismi di un disegno 2-(v, k, λ) con $v > k$, il numero di orbite di Γ sull'insieme dei punti X è minore o uguale al numero di orbite sull'insieme dei blocchi $\mathcal{A}$.

DIMOSTRAZIONE. Siano $X_1, \dots, X_s$ le orbite di Γ su X e $\mathcal{A}_1, \dots, \mathcal{A}_t$ quelle su $\mathcal{A}$. Definiamo due matrici $s \times t$, C, D, come segue. $C(i, j)$ è il numero di punti $x \in X_i$ incidenti con un blocco fissato $A \in \mathcal{A}_j$; questo numero è lo stesso per ogni blocco di $\mathcal{A}_j$. $D(i, j)$ è il numero di blocchi $A \in \mathcal{A}_j$ incidenti con un punto fissato $x \in X_i$; questo numero è lo stesso per ogni punto di X_i.

Consideriamo il prodotto $s \times s$ CD^{T}. L'elemento $(CD^{\mathsf{T}})(i, \ell)$ è la somma, su j, del numero di coppie ordinate $(x, A) \in X_i \times \mathcal{A}_j$ con x incidente con A e A incidente con un punto fissato $y \in X_\ell$. Quindi $(CD^{\mathsf{T}})(i, \ell) = \lambda|X_i|$ se $i \neq \ell$, mentre $(CD^{\mathsf{T}})(i, i) = (r - \lambda) + \lambda|X_i|$; cioè

$$CD^{\mathsf{T}} = (r - \lambda)I + \lambda \operatorname{diag}(|X_1|, \dots, |X_s|)J.$$

Questa relazione è simile all'equazione matriciale (19.7). Poiché $v > k$, abbiamo $r > \lambda$ e si può vedere in vari modi, per esempio calcolandone il determinante, che la matrice a destra è non singolare. Ne segue che C, e anche D, ha rango s, che non può superare il numero t delle colonne. □

* * *

Sia G un gruppo abeliano di ordine v. Un *insieme di differenze* (v, k, λ) in G è un sottoinsieme $D \subseteq G$ di k elementi tale che ogni $g \neq 0$ di G compaia esattamente λ volte nel multiinsieme $(x - y : x, y \in D)$ delle differenze di elementi di D. Più formalmente, richiediamo che il numero di coppie ordinate (x, y) con $x, y \in D$ e $x - y = g$ sia λ per $g \neq 0$ e sia k per $g = 0$. Evidentemente $\lambda(v - 1) = k(k - 1)$. Orig. 372

Esempio 27.1. Ecco alcuni insiemi di differenze:

$(7, 3, 1)$	$\{1, 2, 4\}$	in $\mathbb{Z}_7$
$(13, 4, 1)$	$\{0, 1, 3, 9\}$	in $\mathbb{Z}_{13}$
$(11, 5, 2)$	$\{1, 3, 9, 5, 4\}$	in $\mathbb{Z}_{11}$
$(16, 6, 2)$	$\{10, 20, 30, 01, 02, 03\}$	in $\mathbb{Z}_4 \times \mathbb{Z}_4$
$(16, 6, 2)$	$\{0000, 0001, 0010, 0100, 1000, 1111\}$	in $\mathbb{Z}_2^4$.

Un insieme di differenze è *non banale* quando $1 < k < v - 1$. Un insieme di differenze con $\lambda = 1$ si chiama talvolta *planare* o *semplice*.

Sia G un gruppo abeliano di ordine v. Per $S \subseteq G$ e $g \in G$, indichiamo con $S + g$ il traslato

$$S + g := \{x + g : x \in S\}$$

di S mediante g. Sia D un sottoinsieme di k elementi di G e siano $x, y \in G$. In generale, affermiamo che il numero di traslati $D + g$ contenenti sia x sia y è uguale al numero di volte in cui $d := x - y$ compare come differenza di elementi di D. Infatti $g \mapsto (x - g, y - g)$ è una corrispondenza biunivoca tra $\{g \in G : \{x, y\} \subseteq D + g\}$ e l'insieme delle coppie ordinate (a, b) di elementi di D con $a - b = x - y$. Il lettore può verificare che questo numero coincide anche con la cardinalità di $(D + x) \cap (D + y)$.

In particolare, $(G, \{D + g : g \in G\})$ è un disegno simmetrico (v, k, λ) se e solo se D è un insieme di differenze (v, k, λ).

Problema 27A. Un insieme di quozienti (v, k, λ) in un gruppo arbitrario G di ordine v, scritto moltiplicativamente, è un sottoinsieme $D \subseteq G$ di k elementi per cui vale una qualsiasi delle condizioni seguenti:

(1) Ogni elemento $g \neq 1$ di G compare esattamente λ volte nella lista $(xy^{-1} : x, y \in D)$ dei quozienti "destri" di elementi di D.

(2) Ogni elemento $g \neq 1$ compare esattamente λ volte nella lista $(x^{-1}y : x, y \in D)$ dei quozienti "sinistri".

(3) $|D \cap (Dg)| = \lambda$ per ogni $g \neq 1$.

(4) $|D \cap (gD)| = \lambda$ per ogni $g \neq 1$.

(5) $(G, \{Dg : g \in G\})$ è un disegno simmetrico (v, k, λ).

(6) $(G, \{gD : g \in G\})$ è un disegno simmetrico (v, k, λ).

Mostrare che le sei condizioni sono equivalenti.

Teorema 27.3. Sia G un gruppo di ordine v. L'esistenza di un insieme di quozienti (v, k, λ) in G equivale all'esistenza di un disegno simmetrico (v, k, λ) che ammetta un gruppo $\widehat{G}$ di automorfismi isomorfo a G e regolare, cioè strettamente transitivo, sui punti del disegno. Orig. 373

Dimostrazione. Sia D un insieme di quozienti (v, k, λ) in G. Allora $(G, \{gD : g \in G\})$ è un disegno simmetrico (v, k, λ). Per $g \in G$, definiamo la permutazione $\widehat{g}$ di G mediante $\widehat{g}(x) = gx$. Ciascuna $\widehat{g}$ è un automorfismo di $(G, \{gD : g \in G\})$ e il gruppo $\widehat{G} = \{\widehat{g} : g \in G\}$ è chiaramente isomorfo a G e regolare sui punti.

Viceversa, siano dati G e un disegno simmetrico (v, k, λ) $(X, \mathcal{A})$ con un gruppo regolare $\widehat{G}$ di automorfismi isomorfo a G. Basta esibire un insieme di quozienti (v, k, λ) in $\widehat{G}$.

Fissiamo un punto $x_0 \in X$ e un blocco $A_0 \in \mathcal{A}$. Poniamo

$$D := \{\sigma \in \widehat{G} : \sigma(x_0) \in A_0\}.$$

Affermiamo che D è un insieme di quozienti (v, k, λ) in $\widehat{G}$. Poiché $\widehat{G}$ è regolare e $|A_0| = k$, abbiamo $|D| = k$. Sia $\alpha \neq 1$ un elemento di $\widehat{G}$. Allora

$$\alpha D = \{\alpha\sigma : \sigma(x_0) \in A_0\} = \{\tau : \tau(x_0) \in \alpha(A_0)\},$$

perciò

$$D \cap (\alpha D) = \{\tau : \tau(x_0) \in A_0 \cap \alpha(A_0)\}.$$

Poiché $\widehat{G}$ è regolare, α non ha punti fissi e quindi, per il Teorema 27.1, non fissa blocchi. Il blocco $\alpha(A_0)$ è dunque distinto da A_0, per cui $|A_0 \cap \alpha(A_0)| = \lambda$ e, per regolarità, $|D \cap (\alpha D)| = \lambda$. Ciò vale per ogni $\alpha \neq 1$ e prova l'affermazione. □

In particolare, l'esistenza di un insieme di differenze ciclico (v, k, λ), cioè di un insieme di differenze in $\mathbb{Z}_v$, equivale all'esistenza di un disegno simmetrico (v, k, λ) che ammetta un automorfismo ciclico: un automorfismo la cui decomposizione in cicli sui punti, o sui blocchi, consiste di un solo ciclo di lunghezza v.

Ora restringiamo l'attenzione agli insiemi di differenze nei gruppi abeliani. Idealmente vorremmo descriverli e classificarli tutti: stabilire quali gruppi ne contengano, quanti ve ne siano e così via. Lo faremo per varie piccole terne di parametri, ma in generale già il solo problema dell'esistenza è estremamente difficile. Si osservi che $D \subseteq G$ è un insieme di differenze (v, k, λ) se e solo se $G \setminus D$ è un insieme di differenze $(v, v-k, v-2k+\lambda)$. Possiamo dunque limitarci al caso $k < \frac{1}{2}v$. Orig. 374

Si noti anche che D è un insieme di differenze se e solo se lo è ogni suo traslato.

Quando $(v, k) = 1$, possiamo scegliere un rappresentante naturale della classe di tutti i traslati; ciò può aiutare nella classificazione e sarà utile nel prossimo capitolo. Chiamiamo *normalizzato* un sottoinsieme di un gruppo abeliano G se la somma dei suoi elementi è zero.

Proposizione 27.4. Sia D un sottoinsieme di k elementi di un gruppo abeliano G di ordine v. Se $(v, k) = 1$, D ha un unico traslato normalizzato.

Dimostrazione. Sia h la somma degli elementi di D. La somma degli elementi di $D+g$ è $h+kg$. Poiché $(v, k) = 1$, esiste un unico elemento g del gruppo con $h + kg = 0$. □

Invitiamo il lettore a verificare che gli insiemi di differenze normalizzati con parametri $(v,k,\lambda) = (7,3,1),(13,4,1),(11,5,2),(21,5,1)$ sono rispettivamente:

$$\begin{aligned}
&\{1,2,4\},\ \{3,5,6\} && \text{in } \mathbb{Z}_7;\\
&\{0,1,3,9\},\ \{0,2,5,6\},\ \{0,4,10,12\},\ \{0,7,8,11\} && \text{in } \mathbb{Z}_{13};\\
&\{1,3,4,5,9\},\ \{2,6,7,8,10\} && \text{in } \mathbb{Z}_{11};\\
&\{7,14,3,6,12\},\ \{7,14,9,15,18\} && \text{in } \mathbb{Z}_{21}.
\end{aligned}$$

La verifica sarà facile dopo il Teorema 28.3: si veda l'Esempio 28.2. Naturalmente, se $(v,k) = 1$, il numero totale degli insiemi di differenze è v volte il numero di quelli normalizzati; per esempio in $\mathbb{Z}_{13}$ vi sono 52 insiemi di differenze $(13,4,1)$.

Un'ultima osservazione preliminare: se α è un automorfismo del gruppo G, un sottoinsieme $D \subseteq G$ è un insieme di differenze se e solo se lo è $\alpha(D)$. Da un insieme di differenze dato possiamo quindi ottenerne altri mediante traslazioni e simmetrie di G. Diciamo che D_1, D_2 in G sono *equivalenti* se esistono $\alpha \in \mathrm{Aut}(G)$ e $g \in G$ tali che $D_2 = \alpha(D_1) + g$. Verificare che si tratta di una relazione di equivalenza. Gli insiemi normalizzati elencati sopra sono equivalenti per ciascuna terna di parametri; anzi, ciascuno si può ottenere dagli altri moltiplicando per un intero primo con l'ordine del rispettivo gruppo. Orig. 375

Problema 27B. Mostrare che tutti gli insiemi di differenze $(16,6,2)$ in $\mathbb{Z}_2^4$ sono equivalenti.

Problema 27C. Ricordare dall'Esempio 19.4 che i disegni simmetrici con parametri $v = 4t^2$, $k = 2t^2 - t$, $\lambda = t^2 - t$ sono legati alle matrici di Hadamard regolari. Siano A, B rispettivamente insiemi di differenze $(4x^2, 2x^2 - x, x^2 - x)$ e $(4y^2, 2y^2 - y, y^2 - y)$ in gruppi G, H; si ammetta $x = 1$ o $y = 1$. Mostrare che

$$D := (A \times (H \setminus B)) \cup ((G \setminus A) \times B)$$

è un insieme di differenze $(4z^2, 2z^2 - z, z^2 - z)$ in $G \times H$, dove $z = 2xy$. Quindi, se G è il prodotto diretto di m gruppi di ordine 4, in G esiste un insieme di differenze $(4^m, 2 \cdot 4^{m-1} - 2^{m-1}, 4^{m-1} - 2^{m-1})$.

Descriviamo varie famiglie note di insiemi di differenze. Tutte le costruzioni note sembrano coinvolgere campi finiti e/o spazi vettoriali. Il primo esempio è essenzialmente contenuto nella discussione delle matrici di Paley nel Capitolo 18 sulle matrici di Hadamard, ma merita un enunciato esplicito. Gli insiemi di differenze con parametri

$$(v,k,\lambda) = (4n-1, 2n-1, n-1)$$

si chiamano spesso *insiemi di differenze di Hadamard*.

Teorema 27.5 (Paley, Todd). Sia $q = 4n - 1$ una potenza di un primo. Allora l'insieme D dei quadrati non nulli di $\mathbb{F}_q$ è un insieme di differenze $(4n-1, 2n-1, n-1)$ nel gruppo additivo di $\mathbb{F}_q$.

Dimostrazione. Chiaramente $|D| = 2n - 1$.

Poiché D è invariante per moltiplicazione per gli elementi dell'insieme S dei quadrati non nulli, anche il multiinsieme M delle differenze di elementi di D ha questa proprietà. Inoltre M è ovviamente invariante per moltiplicazione per -1. Poiché $q \equiv 3 \pmod 4$, $-1 \notin S$ e ogni elemento non nullo di $\mathbb{F}_q$ appartiene a S oppure è della forma $-s$ con $s \in S$. Dunque M è invariante per moltiplicazione per tutti gli elementi non nulli di $\mathbb{F}_q$, e D è un insieme di differenze $(4n-1, 2n-1, \lambda)$ per qualche λ. La relazione $\lambda(v-1) = k(k-1)$ impone $\lambda = n - 1$. □ Il Teorema 27.5 dà gli insiemi di differenze $\{1,2,4\}$ in $\mathbb{Z}_7$, $\{1,3,4,5,9\}$ in $\mathbb{Z}_{11}$ e $\{1,4,5,6,7,9,11,16,17\}$ in $\mathbb{Z}_{19}$. L'insieme di differenze $(27,13,6)$ che compare più avanti nella serie sarà nel gruppo abeliano elementare di ordine 27, non in $\mathbb{Z}_{27}$. Orig. 376

Problema 27D. Mostrare che gli insiemi di differenze di Paley–Todd sono normalizzati se $q > 3$.

Stanton e Sprott (1958) trovarono un'altra famiglia di insiemi di differenze di Hadamard.

Teorema 27.6. Se q e $q+2$ sono entrambe potenze dispari di primi, posto $4n - 1 := q(q+2)$ esiste un insieme di differenze $(4n-1, 2n-1, n-1)$ nel gruppo additivo dell'anello $R := \mathbb{F}_q \times \mathbb{F}_{q+2}$.

Dimostrazione. Sia $U := \{(a,b) \in R : a \neq 0, b \neq 0\}$ il gruppo degli elementi invertibili di R. Sia V il sottogruppo di U costituito dalle coppie (a,b) tali che a, b siano entrambi quadrati nei rispettivi campi $\mathbb{F}_q, \mathbb{F}_{q+2}$ oppure entrambi non quadrati. Verificare che V è un sottogruppo di indice 2 di U e che $(-1,-1) \notin V$. Poniamo $T := \mathbb{F}_q \times \{0\}$. Affermiamo che $D := T \cup V$ è l'insieme richiesto. In effetti $|D| = q + \frac{1}{2}(q-1)(q+1) = 2n - 1$.

Poiché D è invariante per moltiplicazione per gli elementi di V, anche il multiinsieme delle sue differenze lo è; inoltre esso è invariante per moltiplicazione per $(-1,-1)$. È dunque invariante per moltiplicazione per tutti gli elementi di U. Ogni elemento di U compare quindi come differenza lo stesso numero di volte, diciamo λ_1. Ogni elemento $(x,0)$ di R con $x \neq 0$ comparirà λ_2 volte, e ogni elemento $(0,y)$ con $y \neq 0$ comparirà λ_3 volte. Naturalmente,

$$k(k-1) = (q-1)(q+1)\lambda_1 + (q-1)\lambda_2 + (q+1)\lambda_3. \tag{27.1}$$

È facile valutare λ_2, λ_3. Le differenze della forma $(x,0)$, $x \neq 0$, di cui vi sono $q-1$ elementi, compaiono $q(q-1)$ volte da coppie di elementi di T, mai da una coppia con un elemento in T e uno in V, e $(q+1)\big(\frac{1}{2}(q-1)\big)\big(\frac{1}{2}(q-1)-1\big)$ volte da coppie di elementi di V; quindi

$$(q-1)\lambda_2 = q(q-1) + (q+1)\left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}-1\right),$$

da cui $\lambda_2 = \frac{1}{4}(q+3)(q-1)$. In modo analogo, Problema 27E, il lettore troverà $\lambda_3 = \frac{1}{4}(q+3)(q-1)$. Allora (27.1) implica anche $\lambda_1 = \frac{1}{4}(q+3)(q-1)$. □ Orig. 377

Problema 27E. Con la notazione della dimostrazione del Teorema 27.6, dimostrare che $\lambda_3 = \frac{1}{4}(q+3)(q-1)$.

Quando $q, q+2$ sono entrambi primi, cioè primi gemelli, il Teorema 27.6 dà insiemi di differenze ciclici. Infatti, se s,t sono interi coprimi, $\mathbb{Z}_s \times \mathbb{Z}_t$ e $\mathbb{Z}_{st}$ sono isomorfi come gruppi additivi, e anche come anelli. Un isomorfismo $\mathbb{Z}_{st} \to \mathbb{Z}_s \times \mathbb{Z}_t$ è dato da $x \pmod{st} \mapsto (x \pmod{s}, x \pmod{t})$. Otteniamo così l'insieme di differenze $(15,7,3)$ $\{0,5,10,1,2,4,8\}$ in $\mathbb{Z}_{15}$.

Problema 27F. Elencare gli elementi di un insieme di differenze ciclico $(35,17,8)$.

Come caso particolare del teorema di Singer, Teorema 27.7, otterremo un'altra famiglia di insiemi di differenze di Hadamard: insiemi ciclici con

$$v = 2^t - 1, \qquad k = 2^{t-1} - 1, \qquad \lambda = 2^{t-2} - 1.$$

Ricordiamo dal Capitolo 23 che i punti e gli iperpiani di $PG(n,q)$ formano un disegno simmetrico con

$$v = \frac{q^{n+1}-1}{q-1}, \qquad k = \frac{q^n - 1}{q-1}, \qquad \lambda = \frac{q^{n-1}-1}{q-1}. \tag{27.2}$$

Teorema 27.7. Per ogni potenza di primo q e intero positivo n, nel gruppo ciclico di ordine v esiste un insieme di differenze D con i parametri (27.2), tale che il disegno simmetrico risultante sia isomorfo a quello dei punti e degli iperpiani di $PG(n,q)$.

Dimostrazione. Per il Teorema 27.3 basta mostrare che esiste un automorfismo di $PG(n,q)$ che permuta i punti in un unico ciclo di lunghezza v, o equivalentemente le cui potenze agiscono transitivamente sui punti proiettivi. I punti di $PG(n,q)$ sono i sottospazi di dimensione 1 di uno spazio vettoriale V di dimensione $n+1$ su $\mathbb{F}_q$. Ogni trasformazione lineare non singolare T di V in sé porta sottospazi in sottospazi della stessa dimensione, e quindi induce un automorfismo di $PG(n,q)$. Orig. 378

Come spazio vettoriale di dimensione $n+1$ su $\mathbb{F}_q$ scegliamo $V := \mathbb{F}_{q^{n+1}}$, considerato sul suo sottocampo $\mathbb{F}_q$. Sia ω un elemento primitivo di $\mathbb{F}_{q^{n+1}}$ e consideriamo la trasformazione lineare su $\mathbb{F}_q$, $T : x \mapsto \omega x$. È chiaro che T è non singolare e che le sue potenze sono transitive sui punti proiettivi, e persino sui vettori non nulli! □

Gli insiemi costruiti nella dimostrazione si chiamano *insiemi di differenze di Singer*; si veda Singer (1938). Diamo una descrizione più concreta e un esempio. Sia ω primitivo in $\mathbb{F}_{q^{n+1}}$ e poniamo $v := (q^{n+1}-1)/(q-1)$. Il gruppo moltiplicativo ciclico $\langle\omega\rangle$ di $\mathbb{F}_{q^{n+1}}$ ha un unico sottogruppo di ordine $q-1$, cioè

$$\langle\omega^v\rangle = \{\omega^0 = 1, \omega^v, \omega^{2v}, \ldots, \omega^{(q-2)v}\}.$$

Ma il gruppo moltiplicativo del sottocampo $\mathbb{F}_q$ ha ordine $q-1$, quindi $\mathbb{F}_q = \{0, \omega^0, \omega^v, \omega^{2v}, \ldots, \omega^{(q-2)v}\}$.

Ora due "vettori" ω^i, ω^j di $\mathbb{F}_{q^{n+1}}$, pensato come spazio vettoriale su $\mathbb{F}_q$, rappresentano lo stesso sottospazio di dimensione 1 se e solo se $\omega^i = \alpha\omega^j$ per qualche $0 \neq \alpha \in \mathbb{F}_q$, cioè se e solo se $i \equiv j \pmod{v}$.

Abbiamo dunque una corrispondenza biunivoca tra l'insieme X dei sottospazi di dimensione 1, ossia dei punti proiettivi, e il gruppo $\mathbb{Z}_v$ delle classi residue modulo v:

$$\begin{aligned}
0 &\longleftrightarrow x_0 = \{0, \omega^0, \omega^v, \omega^{2v}, \dots, \omega^{(q-2)v}\},\\
1 &\longleftrightarrow x_1 = \{0, \omega^1, \omega^{v+1}, \omega^{2v+1}, \dots, \omega^{(q-2)v+1}\},\\
&\vdots\\
i &\longleftrightarrow x_i = \{0, \omega^i, \omega^{v+i}, \omega^{2v+i}, \dots, \omega^{(q-2)v+i}\},\\
&\vdots\\
v-1 &\longleftrightarrow x_{v-1} = \{0, \omega^{v-1}, \omega^{2v-1}, \omega^{3v-1}, \dots, \omega^{(q-1)v-1}\}.
\end{aligned}$$

L'applicazione $x_i \mapsto x_{i+1}$, con indici modulo v, è un automorfismo dello spazio proiettivo. Per ottenere un insieme di differenze, prendiamo un qualsiasi sottospazio U di dimensione n di $\mathbb{F}_{q^{n+1}}$ e poniamo $D := \{i \in \mathbb{Z}_v : x_i \subseteq U\}$.[1] Si ottiene un insieme di differenze normalizzato prendendo per U il sottospazio degli elementi di traccia zero, per la traccia da $\mathbb{F}_{q^{n+1}}$ a $\mathbb{F}_q$.

Orig. 379

Esempio 27.2. Consideriamo $n = 2, q = 5$. Costruiamo un insieme di differenze $(31, 6, 1)$. Uno zero ω del polinomio $y^3 + y^2 + 2$, con coefficienti in $\mathbb{F}_5$, è un elemento primitivo di $\mathbb{F}_{5^3}$ e $1, \omega, \omega^2$ ne formano una base su $\mathbb{F}_5$. I 124 elementi non nulli di $\mathbb{F}_{5^3}$ si dividono in 31 classi laterali modulo $\langle\omega^{31}\rangle = \{3, 4, 2, 1\} = \mathbb{F}_5 \setminus \{0\}$, ciascuna costituita dai vettori non nulli di un sottospazio di dimensione 1.

Prendiamo $U := \operatorname{span}\{1, \omega\}$ come sottospazio di dimensione 2. Rappresentanti dei punti proiettivi di U sono $1, \omega, \omega+1, \omega+2, \omega+3, \omega+4$ e, dopo qualche calcolo,

$$\begin{aligned}
1 &= \omega^0, & \omega &= \omega^1, & \omega+1 &= \omega^{29},\\
\omega+2 &= \omega^{99}, & \omega+3 &= \omega^{80}, & \omega+4 &= \omega^{84}.
\end{aligned}$$

L'insieme di differenze di Singer risultante è

$$\{0, 1, 29, 6, 18, 22\} \quad \text{in } \mathbb{Z}_{31}.$$

Problema 27G. Trovare un insieme di differenze $(57, 8, 1)$ in $\mathbb{Z}_{57}$. Probabilmente qualcuno non vorrà farlo a mano.

Consideriamo $n = 3, q = 2$. Qui i punti di $PG(3, 2)$ sono in corrispondenza biunivoca con gli elementi non nulli di $\mathbb{F}_{2^4}$, a loro volta in corrispondenza biunivoca con i residui modulo 15. Può essere istruttivo elencare tutte le rette e tutti i piani di questo minimo spazio proiettivo tridimensionale, rendendo evidente l'automorfismo ciclico.

Uno zero ω di $y^4 + y + 1$, con coefficienti in $\mathbb{F}_2$, è primitivo in $\mathbb{F}_{2^4}$, e $\omega^3, \omega^2, \omega, 1$ formano una base su $\mathbb{F}_2$. Ogni elemento si scrive univocamente $a_3\omega^3 + a_2\omega^2 + a_1\omega + a_0$, che sotto abbreviamo con $a_3a_2a_1a_0$. Abbiamo $\omega^4 + \omega + 1 = 0$, ossia $\omega^4 = 0011$. Costruiamo prima una tabella delle rappresentazioni vettoriali delle potenze di ω.

Orig. 380

$\mathbb{F}_{2^4}$

$$\begin{array}{lll}
\omega^0 = 0001 & \omega^5 = 0110 & \omega^{10} = 0111\\
\omega^1 = 0010 & \omega^6 = 1100 & \omega^{11} = 1110\\
\omega^2 = 0100 & \omega^7 = 1011 & \omega^{12} = 1111\\
\omega^3 = 1000 & \omega^8 = 0101 & \omega^{13} = 1101\\
\omega^4 = 0011 & \omega^9 = 1010 & \omega^{14} = 1001
\end{array}$$

$PG(3, 2)$

[1] Nota di traduzione: l'originale scrive $x_i \in U$, intendendo l'incidenza del punto proiettivo con il sottospazio; qui x_i è stato definito come sottospazio vettoriale, perciò si usa $\subseteq$.

Rette			Piani
$\{0,5,10\}$	$\{0,1,4\}$	$\{0,2,8\}$	$\{1,2,4,8,0,5,10\}$
$\{1,6,11\}$	$\{1,2,5\}$	$\{1,3,9\}$	$\{2,3,5,9,1,6,11\}$
$\{2,7,12\}$	$\{2,3,6\}$	$\{2,4,10\}$	$\{3,4,6,10,2,7,12\}$
$\{3,8,13\}$	$\{3,4,7\}$	$\{3,5,11\}$	$\{4,5,7,11,3,8,13\}$
$\{4,9,14\}$	$\{4,5,8\}$	$\{4,6,12\}$	$\{5,6,8,12,4,9,14\}$
	$\{5,6,9\}$	$\{5,7,13\}$	$\{6,7,9,13,5,10,0\}$
	$\{6,7,10\}$	$\{6,8,14\}$	$\{7,8,10,14,6,11,1\}$
	$\{7,8,11\}$	$\{7,9,0\}$	$\{8,9,11,0,7,12,2\}$
	$\{8,9,12\}$	$\{8,10,1\}$	$\{9,10,12,1,8,13,3\}$
	$\{9,10,13\}$	$\{9,11,2\}$	$\{10,11,13,2,9,14,4\}$
	$\{10,11,14\}$	$\{10,12,3\}$	$\{11,12,14,3,10,0,5\}$
	$\{11,12,0\}$	$\{11,13,4\}$	$\{12,13,0,4,11,1,6\}$
	$\{12,13,1\}$	$\{12,14,5\}$	$\{13,14,1,5,12,2,7\}$
	$\{13,14,2\}$	$\{13,0,6\}$	$\{14,0,2,6,13,3,8\}$
	$\{14,0,3\}$	$\{14,1,7\}$	$\{0,1,3,7,14,4,9\}$

Per $q = 2$ gli insiemi di differenze di Singer hanno parametri di Hadamard. Otteniamo insiemi $(31, 15, 7)$ tanto dal Teorema 27.5 quanto dal Teorema 27.7. I due insiemi non sono equivalenti, e neppure isomorfi. Due insiemi di differenze sono *isomorfi* se i corrispondenti disegni simmetrici lo sono. Insiemi equivalenti sono certamente isomorfi, ma il viceversa non vale. L'insieme D dei residui quadratici modulo 31 ha la proprietà

$$D \cap (D+1) \cap (D+3) = \{5, 8, 10, 19\}.$$

Il disegno $(\mathbb{Z}_{31}, \{D + g : g \in \mathbb{Z}_{31}\})$ non può essere isomorfo a quello dei punti e degli iperpiani di $PG(4,2)$, perché l'intersezione di sottospazi chiusi è ancora un sottospazio chiuso e $PG(4,2)$ non ne ha con esattamente quattro punti. Orig. 381

Gordon, Mills e Welch (1962) hanno mostrato che in alcuni casi la costruzione del teorema di Singer può essere modificata per produrre molti insiemi di differenze non equivalenti con gli stessi parametri.

Problema 27H. Sia D un insieme di differenze $(n^2+n+1, n+1, 1)$ in un gruppo abeliano G. Mostrare che $-D$ è un'ovale nel piano proiettivo associato.

Problema 27I. Sia $G = \{0, a_0, a_1, \ldots, a_q\}$ un qualsiasi gruppo di ordine $q+2$, dove q è una potenza di un primo. Sia V uno spazio vettoriale di dimensione 2 su $\mathbb{F}_q$ e siano $U_0, U_1, \ldots, U_q$ i suoi sottospazi di dimensione 1. Mostrare che

$$D := \bigcup_{i=0}^{q} \{a_i\} \times U_i$$

è un insieme di differenze in $G \times V$. Per esempio, otteniamo un insieme di differenze $(45, 12, 3)$.

Note

L'idea degli insiemi di differenze in un gruppo, come generalizzazione di quelli ciclici, è dovuta a R. H. Bruck (1955).

Il Problema 27I è un risultato di McFarland (1973).

Il Teorema 27.2 vale anche per 2-disegni arbitrari, semplici o no. Naturalmente bisogna definire un automorfismo di una struttura d'incidenza arbitraria $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$. Forse la definizione più precisa è una coppia ordinata (α, β), dove α è una permutazione di $\mathcal{P}$, β una permutazione di $\mathcal{B}$, tali che $(x, A) \in I$ se e solo se $(\alpha(x), \beta(A)) \in I$. Gli automorfismi formano un gruppo per composizione coordinata per coordinata. Le permutazioni α che compaiono come prime coordinate di un gruppo Γ di automorfismi formano un gruppo Γ_1 di permutazioni dei punti; le permutazioni β che compaiono come seconde coordinate formano un gruppo Γ_2 di permutazioni dei blocchi. Per orbite di Γ sui punti e sui blocchi intendiamo rispettivamente le orbite di Γ_1 e di Γ_2. Orig. 382

Riferimenti bibliografici

R. E. Block (1967), On the orbits of collineation groups, *Math Z.* **96**, 33–49.

R. H. Bruck (1955), Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78**, 464–481.

B. Gordon, W. H. Mills, and L. R. Welch (1962), Some new difference sets, *Canad. J. Math.* **14**, 614–625.

R. L. McFarland (1973), A family of difference sets in non-cyclic groups, *J. Combinatorial Theory (A)* **15**, 1–10.

J. Singer (1938), A theorem in finite projective geometry and some applications to number theorey, *Trans. Amer. Math. Soc.* **43**, 377–385.

R. G. Stanton and D. A. Sprott (1958), A family of difference sets, *Canad. J. Math.* **10**, 73–77.

Capitolo 28

Insiemi di differenze e anello di gruppo

Orig. 383

L'anello di gruppo offre un ambiente naturale e conveniente per studiare gli insiemi di differenze. Vedremo che l'esistenza di un insieme di differenze equivale all'esistenza di una soluzione di una certa equazione algebrica in un anello di gruppo. Lo useremo per ricavare il celebre teorema dei moltiplicatori di M. Hall, Jr., e criteri aritmetici sui parametri di un insieme di differenze più forti del teorema di Bruck–Ryser–Chowla.

Siano R un anello commutativo con unità e G un gruppo abeliano finito, scritto additivamente. Gli elementi dell'*anello di gruppo* $R[G]$ sono tutte le somme formali

$$A = \sum_{g \in G} a_g x^g,$$

dove $a_g \in R$ per ogni $g \in G$. Il simbolo x è soltanto un segnaposto: ciò che conta è avere un elemento a_g di R per ogni elemento g di G, cioè gli elementi dell'anello di gruppo sono in corrispondenza biunivoca con le applicazioni $G \to R$.

Definiamo addizione e moltiplicazione per scalari nel modo ovvio:

$$\sum_{g \in G} a_g x^g + \sum_{g \in G} b_g x^g := \sum_{g \in G} (a_g + b_g) x^g, \qquad c \sum_{g \in G} a_g x^g := \sum_{g \in G} (c a_g) x^g.$$

La moltiplicazione in $R[G]$ è definita da

$$\left(\sum_{g \in G} a_g x^g \right) \left(\sum_{g \in G} b_g x^g \right) := \sum_{g \in G} \left(\sum_{h + h' = g} a_h b_{h'} \right) x^g.$$

Orig. 384

Con queste definizioni $R[G]$ è un'algebra commutativa e associativa su R. La notazione scelta è adatta ai gruppi abeliani e sottolinea un'analogia con i polinomi. Quando G è il gruppo additivo dei residui modulo v, l'anello $R[\mathbb{Z}_v]$ consiste delle somme $\sum_{i=0}^{v-1} r_i x^i$, con esponenti modulo v, ed è isomorfo all'anello quoziente $R[x]/(x^v - 1)$ dell'anello di polinomi $R[x]$. In generale indicheremo anche gli elementi di anelli di gruppo arbitrari $R[G]$ con $A(x), B(x), \ldots$, quando conveniente. L'elemento $x^0 \in R[G]$ è l'identità moltiplicativa, e lo indichiamo con 1.

Ci occuperemo quasi esclusivamente degli anelli di gruppo $\mathbb{Z}[G]$ sugli interi. Per un sottoinsieme $A \subseteq G$ definiamo

$$A(x) := \sum_{g \in A} x^g \in \mathbb{Z}[G].$$

In particolare $G(x) = \sum_{g \in G} x^g$. Per $A, B \subseteq G$,

$$A(x) B(x) = \sum_{g \in G} c_g x^g,$$

dove c_g è il numero di volte in cui g compare nel multiinsieme $(h + h' : h \in A, h' \in B)$ delle somme di elementi di A, B.

Per $A(x) = \sum_{g\in G} a_g x^g \in \mathbb{Z}[G]$ scriviamo

$$A(x^{-1}) := \sum_{g\in G} a_g x^{-g}.$$

Dunque un sottoinsieme D di k elementi di un gruppo G di ordine v è un insieme di differenze (v, k, λ) se e solo se nell'anello $\mathbb{Z}[G]$ vale

$$D(x)D(x^{-1}) = n + \lambda G(x), \qquad n := k - \lambda.$$

Un importante omomorfismo da $\mathbb{Z}[G]$ a $\mathbb{Z}$ è dato da

$$A(x) \longmapsto A(1) := \sum_{g\in G} a_g \in \mathbb{Z}.$$

Orig. 385

Proposizione 28.1. Siano v, k, λ interi positivi con $\lambda(v-1) = k(k-1)$ e sia G un gruppo abeliano di ordine v. L'esistenza di un insieme di differenze (v, k, λ) in G equivale all'esistenza di un elemento $A(x) \in \mathbb{Z}[G]$ che soddisfi

$$A(x)A(x^{-1}) = n + \lambda G(x), \qquad n := k - \lambda. \tag{28.1}$$

Dimostrazione. Abbiamo già osservato che, per un sottoinsieme D di G, $D(x)$ soddisfa (28.1) se e solo se D è un insieme di differenze (v, k, λ). Resta da mostrare che, se esiste una soluzione $A(x)$ di (28.1), possiamo trovarne una $B(x) = \sum_{g\in G} b_g x^g$ con coefficienti b_g tutti uguali a 0 o 1.

Supponiamo che $A(x)$ soddisfi (28.1) e applichiamo l'omomorfismo "$x \mapsto 1$" da $\mathbb{Z}[G]$ a $\mathbb{Z}$. Troviamo

$$(A(1))^2 = n + \lambda v = k^2,$$

quindi $A(1) = k$ oppure $-k$. Se $A(x)$ soddisfa (28.1), anche $B(x) = -A(x)$ la soddisfa, perciò possiamo supporre $A(1) = \sum_g a_g = k$.

Il coefficiente di $1 = x^0$ in $A(x)A(x^{-1})$ è $k = \sum_{g\in G} a_g^2$. Quindi $\sum_{g\in G} a_g(a_g - 1) = 0$. Ma $a(a-1)$ è strettamente positivo a meno che l'intero a sia 0 o 1. □

Per ogni intero t, $g \mapsto tg$ è un omomorfismo di G in sé e induce l'omomorfismo di anelli $\mathbb{Z}[G] \to \mathbb{Z}[G]$ dato da

$$A(x) = \sum_{g\in G} a_g x^g \longmapsto A(x^t) := \sum_{g\in G} a_g x^{tg}.$$

Per $A, B \in \mathbb{Z}[G]$ e $n \in \mathbb{Z}$, scriviamo $A \equiv B \pmod n$ se $A - B = nC$ per qualche $C \in \mathbb{Z}[G]$. Ecco un semplice lemma che useremo spesso.

Lemma 28.2. Siano p un primo e $A \in \mathbb{Z}[G]$. Allora

$$(A(x))^p \equiv A(x^p) \pmod p.$$

Orig. 386

Dimostrazione. Procediamo per induzione sul numero di coefficienti non nulli di $A(x)$. Il lemma vale per $A(x) = 0$. Se $A(x) = cx^g + B(x)$, dove $B^p(x) \equiv B(x^p) \pmod p$, allora

$$\begin{aligned} A^p(x) &= (cx^g + B(x))^p \equiv (cx^g)^p + B^p(x) \\ &= c^p x^{pg} + B^p(x) \equiv cx^{pg} + B(x^p) = A(x^p), \end{aligned}$$

con congruenze modulo p. □

Siano G un gruppo abeliano e D un insieme di differenze in G. Un automorfismo α di G si chiama *moltiplicatore* di D se e solo se l'insieme di differenze $\alpha(D)$ è un traslato di D, cioè $\alpha(D) = D + g$ per qualche $g \in G$. Per esempio l'automorfismo $x \mapsto 3x$ di $\mathbb{Z}_{13}$ è un moltiplicatore dell'insieme $(13, 4, 1)$ $\{0, 2, 3, 7\}$, poiché $\{0, 6, 9, 8\} = \{0, 2, 3, 7\} + 6$.

Se t è un intero primo con l'ordine di G, $x \mapsto tx$ è un automorfismo di G; le applicazioni $x \mapsto t_1 x$ e $x \mapsto t_2 x$ coincidono se e solo se $t_1 \equiv t_2 \pmod{v^*}$, dove v^* è l'esponente di G, cioè il minimo comune multiplo degli ordini dei suoi elementi. Se $x \mapsto tx$ è un moltiplicatore di D, diciamo che t è un *moltiplicatore*

numerico, o *moltiplicatore di Hall*, di D. A prima vista sorprende che molti insiemi di differenze, per esempio tutti quelli ciclici noti, debbano necessariamente avere un moltiplicatore numerico non banale.

Problema 28A. Sia $q = p^t$ con p primo. Mostrare che p è un moltiplicatore degli insiemi di differenze di Singer descritti nel capitolo precedente.

Un automorfismo α di G è un moltiplicatore di D se e solo se nell'anello $\mathbb{Z}[G]$ vale $D(x^\alpha) = x^g D(x)$ per qualche $g \in G$.

Teorema 28.3 (Teorema dei moltiplicatori, prima versione). Sia D un insieme di differenze (v, k, λ) in un gruppo abeliano G di ordine v. Sia p un primo con $p \mid n$, $(p, v) = 1$ e $p > \lambda$. Allora p è un moltiplicatore numerico di D.

Conviene isolare parte della dimostrazione in un lemma.

Lemma 28.4. Siano α un automorfismo di G e D un insieme di differenze (v, k, λ) in G. Poniamo

$$S(x) := D(x^\alpha)D(x^{-1}) - \lambda G(x).$$

Allora α è un moltiplicatore di D se e solo se $S(x)$ ha coefficienti non negativi.

Orig. 387

DIMOSTRAZIONE. Se α è un moltiplicatore, $D(x^\alpha) = x^g D(x)$ per qualche $g \in G$, quindi

$$D(x^\alpha)D(x^{-1}) = x^g D(x)D(x^{-1}) = x^g(n + \lambda G(x)) = nx^g + \lambda G(x).$$

In questo caso $S(x) = nx^g$ per qualche g, e in particolare ha coefficienti non negativi. Viceversa, se $D(x^\alpha)D(x^{-1}) = nx^g + \lambda G(x)$, moltiplicando per $D(x)$ troviamo

$$\begin{aligned} D(x^\alpha)(n + \lambda G(x)) &= nx^g D(x) + \lambda D(x)G(x), \\ nD(x^\alpha) + \lambda k G(x) &= nx^g D(x) + \lambda k G(x). \end{aligned}$$

Quindi $D(x^\alpha) = x^g D(x)$ e α è un moltiplicatore.

Ora "$x \mapsto x^\alpha$" è un automorfismo di $\mathbb{Z}[G]$, perciò $D(x^\alpha)D(x^{-\alpha}) = n + \lambda G(x)$, cioè anche $\alpha(D)$ è un insieme di differenze, e

$$\begin{aligned} S(x)S(x^{-1}) &= \{D(x^\alpha)D(x^{-1}) - \lambda G(x)\}\{D(x^{-\alpha})D(x) - \lambda G(x)\} \\ &= \{n + \lambda G(x)\}^2 - 2\lambda k^2 G(x) + \lambda^2 v G(x) \\ &= n^2 + 2\lambda(n + \lambda v - k^2)G(x) = n^2. \end{aligned}$$

Supponiamo $S(x) = \sum_{g \in G} s_g x^g$ con $s_g \geq 0$. Se $s_g > 0$ e $s_h > 0$, il coefficiente di x^{g-h} in $S(x)S(x^{-1}) = n^2$ è almeno $s_g s_h > 0$, quindi $x^{g-h} = x^0$, cioè $g = h$. Dunque $S(x)$ può avere un solo coefficiente positivo, diciamo $S(x) = s_g x^g$. L'equazione $S(x)S(x^{-1}) = n^2$ impone $s_g = n$: abbiamo mostrato che $S(x) = nx^g$. Come osservato sopra, ne segue che α è un moltiplicatore. □

Dimostrazione del Teorema 28.3. Poniamo $S(x) := D(x^p)D(x^{-1}) - \lambda G(x)$. Per il Lemma 28.4 basta mostrare che $S(x)$ ha coefficienti non negativi. Per il Lemma 28.2,

$$\begin{aligned} D(x^p)D(x^{-1}) &\equiv D^p(x)D(x^{-1}) \equiv D^{p-1}(x)D(x)D(x^{-1}) \\ &\equiv D^{p-1}(x)(n + \lambda G(x)) \equiv nD^{p-1}(x) + \lambda k^{p-1} G(x) \\ &\equiv \lambda G(x) \pmod{p}, \end{aligned}$$

poiché p divide n e $\lambda k^{p-1} \equiv \lambda^p \equiv \lambda \pmod{p}$. Quindi i coefficienti di $D(x^p)D(x^{-1})$, chiaramente non negativi, sono tutti congrui a λ modulo p. Poiché $p > \lambda$, devono tutti essere maggiori o uguali a λ: $S(x)$ ha coefficienti non negativi. □

Orig. 388

Problema 28B. Trovare un elemento $S(x) \in \mathbb{Z}[\mathbb{Z}_7]$ tale che $S(x)S(x^{-1}) = 4$, ma $S(x) \neq \pm 2x^g$.

L'ipotesi $p > \lambda$ è stata essenziale per la dimostrazione. Eppure, per ogni insieme di differenze noto, ogni divisore primo di n che non divide v è un moltiplicatore. Può dunque darsi che l'ipotesi sia superflua; la questione ha ormai assunto lo status di classico problema aperto.[1] Vi sono state anche varie generalizzazioni del teorema originario, tutte banali se si potesse eliminare $p > \lambda$; ne enunceremo una dopo alcune applicazioni della versione attuale.

[1] Nota di traduzione: le affermazioni sullo stato delle conoscenze in questo capitolo si riferiscono all'edizione originale.

Corollario. Per $\lambda = 1$, ogni divisore primo di n, e quindi ogni divisore, è un moltiplicatore di ogni insieme di differenze $(n^2 + n + 1, n + 1, 1)$.

Esempio 28.1. Affermiamo che non esistono insiemi di differenze $(n^2 + n + 1, n + 1, 1)$ con $n \equiv 0 \pmod 6$. Sia D un ipotetico insieme del genere; senza perdita di generalità supponiamolo normalizzato, e quindi fissato da tutti i moltiplicatori. Tanto 2 quanto 3 sarebbero moltiplicatori. Per $x \in D$, anche $2x, 3x$ apparterrebbero a D. La differenza x comparirebbe due volte: come $2x - x$ e come $3x - 2x$. Sono occorrenze distinte purché $3x \neq 2x$, cioè $x \neq 0$, in contraddizione con $\lambda = 1$.

Problema 28C. Mostrare che non esistono insiemi di differenze $(n^2 + n + 1, n + 1, 1)$ con n divisibile per uno qualsiasi fra 10, 14, 15, 21, 22, 26, 34, 35.

Con il teorema dei moltiplicatori e altre tecniche è stato possibile dimostrare che per $n \leq 3600$ non esistono insiemi di differenze planari a meno che n sia una potenza di primo. Ma la congettura che n debba essere una potenza di primo rimane aperta.

Esempio 28.2. Consideriamo un insieme di differenze normalizzato $(21, 5, 1)$ D in $\mathbb{Z}_{21}$. Per il teorema dei moltiplicatori, 2 è un moltiplicatore e quindi $2D = D$. Dunque D deve essere unione di cicli di $x \mapsto 2x$ su $\mathbb{Z}_{21}$, che sono Orig. 389

$$\{0\}, \quad \{1, 2, 4, 8, 16, 11\}, \quad \{3, 6, 12\}, \quad \{5, 10, 20, 19, 17, 13\}, \quad \{7, 14\}, \quad \{9, 18, 15\}.$$

Poiché D ha 5 elementi, deve essere $\{7, 14, 3, 6, 12\}$ oppure $\{7, 14, 9, 18, 15\}$. Entrambi risultano essere insiemi di differenze. L'uno è costituito dagli opposti degli elementi dell'altro, perciò i 42 insiemi di differenze con questi parametri sono tutti equivalenti.

Problema 28D. Trovare tutti gli insiemi di differenze normalizzati con parametri $(7, 3, 1)$, $(11, 5, 2)$, $(13, 4, 1)$, $(19, 9, 4)$, $(31, 10, 3)$ e $(37, 9, 2)$. Per una delle terne non esistono insiemi di differenze.

Diamo ora altri due semplici lemmi sull'anello di gruppo.

Lemma 28.5. Siano G un gruppo abeliano di ordine v e p un primo con $p \nmid v$. Se $A \in \mathbb{Z}[G]$ e $A^m \equiv 0 \pmod p$ per qualche intero positivo m, allora $A \equiv 0 \pmod p$.

Dimostrazione. Scegliamo una potenza $q = p^e$ con $q \geq m$ e $q \equiv 1 \pmod v$. Certamente $A^q(x) \equiv 0 \pmod p$. Per il Lemma 28.2, però, $A^q(x) \equiv A(x^q) \pmod p$, quindi $A(x^q) \equiv 0 \pmod p$. Poiché $q \equiv 1 \pmod v$, $qg = g$ per ogni $g \in G$ e $A(x) = A(x^q)$. □

Si noti che $x^g G(x) = G(x)$ in $\mathbb{Z}[G]$. Ne segue

$$A(x)G(x) = A(1)G(x).$$

Per $n \in \mathbb{Z}$ e $A, B \in \mathbb{Z}[G]$ scriviamo $A \equiv B \pmod{n, G}$ quando $A - B$ appartiene all'ideale generato da n e $G = G(x)$, o equivalentemente quando

$$A - B = nC + mG$$

per qualche $C \in \mathbb{Z}[G]$ e intero m.

Lemma 28.6. Siano G un gruppo abeliano di ordine v e p un primo con $p \nmid v$. Se $A \in \mathbb{Z}[G]$ e $A^m \equiv 0 \pmod{p, G}$ per qualche intero positivo m, allora $A \equiv 0 \pmod{p, G}$.

Dimostrazione. Scegliamo $q = p^e$ con $q \equiv 1 \pmod v$ e $q \geq m$. Allora $A^q(x) \equiv 0 \pmod{p, G}$ e $A^q(x) \equiv A(x^q) = A(x) \pmod p$. □ Orig. 390

Teorema 28.7 (Teorema dei moltiplicatori, seconda versione). Sia D un insieme di differenze (v, k, λ) in un gruppo abeliano G di esponente v^*. Sia t un intero con $(t, v) = 1$. Supponiamo di poter trovare un divisore m di $n := k - \lambda$ tale che $m > \lambda$ e, per ogni divisore primo p di m, esista un intero f con $p^f \equiv t \pmod{v^*}$. Allora t è un moltiplicatore numerico di D.

Dimostrazione. Useremo i Lemmi 28.2, 28.4, 28.5 e l'osservazione seguente.

Siano D un insieme di differenze (v, k, λ) in G, α un automorfismo di G, e $S(x) := D(x^\alpha)D(x^{-1}) - \lambda G(x)$. Supponiamo che α abbia ordine e, così che α^e sia l'identità. Affermiamo che in $\mathbb{Z}[G]$

$$S(x)S(x^\alpha)S(x^{\alpha^2}) \cdots S(x^{\alpha^{e-1}}) = n^e.$$

Infatti, per ogni intero i,

$$D(x^{\alpha^i})D(x^{-\alpha^i}) = n + \lambda G(x) \equiv n \pmod{G}$$

e

$$S(x^{\alpha^i}) = D(x^{\alpha^{i+1}})D(x^{-\alpha^i}) - \lambda G(x) \equiv D(x^{\alpha^{i+1}})D(x^{-\alpha^i}) \pmod{G}.$$

Quindi

$$\begin{aligned} &S(x)S(x^\alpha)S(x^{\alpha^2})\cdots S(x^{\alpha^{e-1}}) \\ &\quad\equiv \{D(x^\alpha)D(x^{-1})\}\{D(x^{\alpha^2})D(x^{-\alpha})\}\cdots\{D(x)D(x^{-\alpha^{e-1}})\} \\ &\quad\equiv \{D(x)D(x^{-1})\}\{D(x^\alpha)D(x^{-\alpha})\}\cdots\{D(x^{\alpha^{e-1}})D(x^{-\alpha^{e-1}})\} \\ &\quad\equiv n^e \pmod{G}. \end{aligned}$$

Dunque il prodotto è $n^e + \ell G(x)$ per qualche intero ℓ. Ma $S(1) = (D(1))^2 - \lambda G(1) = k^2 - \lambda v = n$; applicando $x \mapsto 1$ troviamo $n^e = n^e + \ell v$, quindi $\ell = 0$.

Proseguiamo ponendo $S(x) := D(x^t)D(x^{-1}) - \lambda G(x)$. Per il Lemma 28.4 basta provare che $S(x)$ ha coefficienti non negativi. Ogni coefficiente di $S(x)$ è almeno $-\lambda$; poiché $m > \lambda$, la non negatività seguirà da $S(x) \equiv 0 \pmod{m}$. Per dimostrarla basta provare $S(x) \equiv 0 \pmod{p^i}$ ogni volta che p è primo e p^i divide m. Orig. 391

Sia e l'ordine di t modulo v^*, così che $t^e \equiv 1 \pmod{v^*}$. Come mostrato sopra,

$$S(x)S(x^t)S(x^{t^2})\cdots S(x^{t^{e-1}}) = n^e.$$

Sia p un divisore primo di m e sia f tale che $p^f \equiv t \pmod{v^*}$. Allora

$$S(x)S(x^{p^f})S(x^{p^{2f}})\cdots S(x^{p^{f(e-1)}}) = n^e.$$

Sia p^i la massima potenza di p che divide n e sia p^j la massima potenza che divide tutti i coefficienti di $S(x)$; scriviamo $S(x) = p^j T(x)$ con $T(x) \not\equiv 0 \pmod{p}$. Allora

$$p^j T(x)\, p^j T(x^{p^f})\cdots p^j T(x^{p^{f(e-1)}}) = n^e,$$

da cui $p^j \mid n$, quindi $j \le i$, e

$$T(x)T(x^{p^f})\cdots T(x^{p^{f(e-1)}}) = (n/p^j)^e.$$

Supponiamo $j < i$, così che $(n/p^j)^e$ sia divisibile per p. Allora

$$\begin{aligned} 0 &\equiv T(x)T(x^{p^f})\cdots T(x^{p^{f(e-1)}}) \\ &\equiv T(x)T(x)^{p^f}\cdots T(x)^{p^{f(e-1)}} \\ &\equiv T(x)^{1+p^f+\cdots+p^{f(e-1)}} \pmod{p}. \end{aligned}$$

[2] Per il Lemma 28.5, $T(x) \equiv 0 \pmod{p}$, in contraddizione con la scelta di j. Dunque $i = j$. □

Corollario. Se $n = p^e$, con p primo e $(p, v) = 1$, allora p è un moltiplicatore numerico di ogni insieme di differenze (v, k, λ).

Dimostrazione. Un insieme di differenze D e il suo complementare $G \setminus D$ hanno gli stessi moltiplicatori. Possiamo dunque supporre $k < \frac{1}{2}v$, da cui $n > \lambda$. Nel Teorema 28.7 prendiamo $m = n, t = p$. □ Orig. 392

Esempio 28.3. Consideriamo un ipotetico insieme di differenze $(25, 9, 3)$. Nel teorema precedente prendiamo $t = 2, m = 6$. Poiché $3^3 \equiv 2 \pmod{25}$, possiamo concludere che 2 è un moltiplicatore.

Problema 28E. Trovare tutti gli insiemi di differenze normalizzati con parametri $(15, 7, 3)$, $(25, 9, 3)$, $(39, 19, 9)$, $(43, 15, 5)$ e $(61, 16, 4)$. Per ciascuna terna, determinare se tali insiemi normalizzati siano equivalenti. Per la maggior parte delle terne non esistono insiemi di differenze.

Problema 28F. Sia D un insieme di differenze non banale (v, k, λ). Dimostrare che, se -1 è un moltiplicatore di D, allora v è pari.

Problema 28G. Trovare un insieme di differenze $(36, 15, 6)$ in $\mathbb{Z}_6 \times \mathbb{Z}_6$ avente -1 come moltiplicatore.

[2] Nota di traduzione: nella riga intermedia l'originale ripete un fattore $T(x)$ prima dell'ultima potenza; la riga è stata allineata al prodotto e all'esponente che la seguono.

* * *

Supponiamo che D sia un insieme di differenze (v,k,λ) in un gruppo abeliano G di ordine pari v. Per il Teorema 19.11(i) sappiamo che n è un quadrato. Nel caso degli insiemi di differenze possiamo però dire *di che cosa* sia il quadrato! Sia A un sottogruppo di indice 2 di G. Supponiamo che D contenga a elementi di A e b elementi di $B := G \setminus A$. Ogni elemento di B compare λ volte come differenza di elementi di D, e solo le differenze tra un elemento di A e uno di B appartengono a B; quindi $2ab = \frac{1}{2}\lambda v$. Da questo e da $a+b=k$ segue $(a-b)^2 = n$.

Supponiamo ora $3 \mid v$, sia A un sottogruppo di indice 3 e siano B, C le altre classi laterali di A in G. Supponiamo che D contenga a elementi di A, b di B e c di C. Il numero di differenze appartenenti, per esempio, a B è $ba + cb + ac$, che deve essere $\frac{1}{3}\lambda v$. Da questo e da $a+b+c=k$ si verifica

$$4n = (b+c-2a)^2 + 3(b-c)^2.$$

Non tutti gli interi si possono scrivere come un quadrato più tre volte un altro quadrato; questa condizione esclude dunque certi insiemi di differenze. Per esempio non esistono insiemi $(39,19,9)$, benché esistano disegni simmetrici con questi parametri, perché $4n = 40$ non ammette tale rappresentazione.

Generalizziamo queste condizioni necessarie sui parametri considerando omomorfismi dell'anello di gruppo. Un omomorfismo $\alpha : G \to H$ induce un omomorfismo di anelli $\mathbb{Z}[G] \to \mathbb{Z}[H]$: Orig. 393

$$A(x) = \sum_g a_g x^g \longmapsto A(x^\alpha) := \sum_g a_g x^{\alpha(g)} \in \mathbb{Z}[H].$$

Teorema 28.8. Sia D un insieme di differenze (v,k,λ) in un gruppo abeliano G. Sia $u > 1$ un divisore di v. Se p è un divisore primo di n e $p^f \equiv -1 \pmod{u}$ per qualche intero f, allora p non divide la parte libera da quadrati di n.

Dimostrazione. Dimostriamo qualcosa di più forte. Sia $\alpha : G \to H$ un omomorfismo suriettivo su un gruppo H di ordine u ed esponente u^*. Supponiamo p primo e $p^f \equiv -1 \pmod{u^*}$ per qualche f. Mostreremo che la massima potenza di p che divide n è una potenza pari p^{2j} e che, per questo j,

$$D(x^\alpha) \equiv 0 \pmod{p^j, H} \quad \text{in } \mathbb{Z}[H].$$

In altre parole, tutti i coefficienti di $D(x^\alpha)$, cioè i numeri di elementi di D nelle diverse classi laterali del nucleo di α, sono congrui tra loro modulo p^j.

Sia p^i la massima potenza di p che divide n. L'ipotesi significa che $D(x^{-\alpha}) = D(x^{p^f\alpha})$ in $\mathbb{Z}[H]$, dove svolgeremo i calcoli, perciò

$$\begin{aligned} D(x^\alpha)D(x^{p^f\alpha}) &= D(x^\alpha)D(x^{-\alpha}) \\ &= n + \lambda\frac{v}{u}H(x) \equiv 0 \pmod{p^i, H}. \end{aligned} \tag{28.2}$$

Sia p^j la massima potenza per cui $D(x^\alpha) \equiv 0 \pmod{p^j, H}$; scriviamo $D(x^\alpha) \equiv p^j A(x) \pmod{H}$. Il lettore può verificare che (28.2) implica $2j \le i$ e che, se $2j < i$, allora $A(x)A(x^{p^f}) \equiv 0 \pmod{p, H}$. I Lemmi 28.2 e 28.6 implicano successivamente $A(x)^{1+p^f} \equiv 0 \pmod{p, H}$ e $A(x) \equiv 0 \pmod{p, H}$, contro la scelta di j. Dunque $2j = i$. □

Dal Teorema 28.8 segue che, se $3 \mid v$, tutti i divisori primi della parte libera da quadrati di n sono congrui a 0 o 1 modulo 3; se $5 \mid v$, sono congrui a 0 o 1 modulo 5; se $7 \mid v$, sono congrui a 0, 1, 2 o 4 modulo 7. Orig. 394

Esempio 28.4. Diamo un'applicazione dell'affermazione più forte dimostrata nel Teorema 28.8. Consideriamo un ipotetico insieme di differenze $(154,18,2)$ D in G. Sia $\alpha : G \to H$ suriettivo con $|H| = u := 11$. Prendiamo $p := 2$. Poiché $2^5 \equiv -1 \pmod{11}$, concludiamo $D(x^\alpha) \equiv 0 \pmod{4, H}$. Ciò significa che gli 11 coefficienti di $D(x^\alpha)$ sono tutti congrui a un certo intero h modulo 4; poiché la loro somma è 18, $h = 2$. La somma sarebbe però almeno 22: questa contraddizione prova la non esistenza.

Problema 28H. Sia D un insieme di differenze $(q^4+q^2+1, q^2+1, 1)$ in un gruppo abeliano G. Sia $\alpha : G \to H$ un omomorfismo suriettivo con $|H| = u := q^2 - q + 1$. Mostrare che ogni classe laterale del nucleo di α è l'insieme dei punti di un sottopiano di Baer del piano proiettivo di ordine q^2 derivante da D. Per esempio, i 21 punti del piano proiettivo di ordine 4 sono partizionati in tre configurazioni di Fano.

Problema 28I. Sia D un insieme di differenze $(q^3+q^2+q+1, q^2+q+1, q+1)$ in un gruppo abeliano G. Sia $\alpha : G \to H$ suriettivo con $|H| = u := q+1$. Mostrare che i traslati di D incontrano le classi laterali del nucleo di α in $q+1$ punti oppure in un singolo punto. Mostrare inoltre che, se il disegno simmetrico derivante da D consiste dei punti e dei piani di $PG_3(q)$, tali classi sono ovoidi; si veda l'Esempio 26.5.

Note

Il celebre teorema dei moltiplicatori fu dimostrato per la prima volta per insiemi di differenze ciclici planari da Hall (1947). Hall e Ryser (1951) lo generalizzarono a $\lambda > 1$ e da allora è stato esteso in molti modi; si vedano, per esempio, Mann (1965), Baumert (1971), Lander (1983). La teoria algebrica dei numeri e i caratteri dei gruppi abeliani svolgono spesso un ruolo nelle dimostrazioni, ma qui abbiamo scelto di dimostrare i Teoremi 28.7 e 28.8 usando soltanto l'anello di gruppo.

Marshall Hall (1910–1990) svolse lavori fondamentali nella teoria dei gruppi, nella teoria dei codici e nei disegni combinatori. Esercitò un'enorme influenza su molti matematici, compresi gli autori. Il Teorema 28.8 è dovuto a K. Yamamoto (1963). Orig. 395

Riferimenti bibliografici

L. D. Baumert (1971), *Cyclic Difference Sets*, Lecture Notes in Math. **182**, Springer-Verlag.

M. Hall (1947), Cyclic projective planes, *Duke J. Math.* **14**, 1079–1090.

M. Hall and H. J. Ryser (1951), Cyclic incidence matrices, *Canad. J. Math.* **3**, 495–502.

E. S. Lander (1983), *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series **74**, Cambridge University Press.

H. B. Mann (1965), *Addition Theorems*, Wiley.

K. Yamamoto (1963), Decomposition fields of difference sets, *Pacific J. Math.* **13**, 337–352.

Capitolo 29

Codici e disegni simmetrici

In questo capitolo approfondiamo alcuni argomenti introdotti nel Capitolo 20. Là abbiamo visto che le righe della matrice d'incidenza di un piano proiettivo di ordine $n \equiv 2 \pmod 4$ generano un codice binario che, una volta esteso, è autoduale. H. A. Wilbrink (1985) e altri osservarono che questo risultato si può usare per mostrare che non esistono insiemi di differenze planari per $n > 2$ con $n \equiv 2 \pmod 4$; si veda il Teorema 29.7. Orig. 396

Si può considerare anche il codice generato dalle righe della matrice d'incidenza su altri campi primi $\mathbb{F}_p$. Con una dimostrazione essenzialmente uguale a quella del Teorema 20.6 si ottiene il seguente risultato.

Teorema 29.1. Se p divide $n := k - \lambda$, lo spazio C generato su $\mathbb{F}_p$ dalle righe della matrice d'incidenza N di un disegno simmetrico (v, k, λ) ha dimensione al più $(v+1)/2$. Se $(p, k) = 1$ e p^2 non divide n, la dimensione di questo codice p-ario è esattamente $(v+1)/2$.

Problema 29A. Dimostrare il Teorema 29.1.

In generale non è possibile estendere C a un codice di lunghezza $v+1$ auto-ortogonale rispetto al prodotto scalare standard su $\mathbb{F}_p^v$. Consideriamo però altri "prodotti scalari" per primi dispari p.

A una matrice non singolare $m \times m$ B su un campo $\mathbb{F}$ possiamo associare il prodotto scalare, o forma bilineare,

$$\langle x, y \rangle := xBy^{\mathsf{T}}, \qquad x, y \in \mathbb{F}^m.$$

Per un sottospazio C di $\mathbb{F}^m$ poniamo

$$C^B := \{x : \langle x, y \rangle = 0 \text{ per ogni } y \in C\}.$$

Allora C, C^B hanno dimensioni complementari e $(C^B)^B = C$.[1] Diciamo che C è *totalmente isotropo* quando $C \subseteq C^B$; è il termine appropriato per questa generalizzazione dell'auto-ortogonalità. Orig. 397

Useremo il seguente teorema di Witt; ne includiamo una dimostrazione perché è essenzialmente una riformulazione di parte del Teorema 26.6.

Teorema 29.2. Data una matrice simmetrica non singolare B su un campo $\mathbb{F}$ di caratteristica dispari, esiste in $\mathbb{F}^m$ un sottospazio totalmente isotropo di dimensione $m/2$ se e solo se $(-1)^{m/2} \det B$ è un quadrato in $\mathbb{F}$.[2]

Dimostrazione. Un sottospazio totalmente isotropo di dimensione $m/2$, considerato come insieme di punti proiettivi in $PG(m-1, 2)$,[3] è un sottospazio chiuso di dimensione proiettiva $m/2 - 1$ interamente contenuto nella quadrica Q definita dalla forma quadratica non degenere

$$f(x) = xBx^{\mathsf{T}}.$$

Per il Teorema 26.6, esso esiste se e solo se Q è iperbolica. Resta da verificare che ciò equivale a $(-1)^{m/2} \det B$ quadrato in $\mathbb{F}$.

[1] Nota di traduzione: per quest'ultima identità si assume la simmetria della forma, come nei teoremi successivi. Per una matrice non simmetrica arbitraria il doppio ortogonale sinistro non coincide necessariamente con C.

[2] Nota di traduzione: qui m è pari e il campo è *finito*, come nel contesto applicativo. La sola caratteristica dispari non basta per il criterio su un campo arbitrario; la dimostrazione usa la classificazione delle forme quadratiche sui campi finiti.

[3] Nota di traduzione: nell'originale compare $PG(m-1, 2)$; va letto $PG(m-1, \mathbb{F})$. Il risultato sulle dimensioni dei sottospazi contenuti nelle quadriche è il Teorema 26.7, richiamato qui come 26.6.

Se f_1 è proiettivamente equivalente a f, allora $f_1(x) = xB_1x^{\mathsf{T}}$, con $B_1 = UBU^{\mathsf{T}}$ per una matrice non singolare U. Naturalmente $(-1)^{m/2}\det B$ è un quadrato se e solo se lo è $(-1)^{m/2}\det B_1$.

Se Q è iperbolica, f è equivalente a $f_1 = x_1x_2 + \cdots + x_{m-1}x_m$ e B_1 è diagonale a blocchi, con $m/2$ matrici

$$W = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

sulla diagonale. Allora $(-1)^{m/2}\det B_1 = 1/2^m$, che è un quadrato.

Se Q è ellittica, f è equivalente a $f_1 = x_1x_2 + \cdots + x_{m-3}x_{m-2} + p(x_{m-1}, x_m)$, dove $p(x, y) = ax^2 + 2bxy + cy^2$ è irriducibile su $\mathbb{F}$. Qui B_1 è diagonale a blocchi, con $m/2-1$ matrici W e una matrice

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

sulla diagonale. Allora $(-1)^{m/2}\det B_1 = (b^2 - ac)/2^{m-2}$, che non è un quadrato in $\mathbb{F}$, perché p è irriducibile. □ Conviene mantenere il termine *autoduale* per un sottospazio totalmente isotropo di dimensione pari a metà della lunghezza. E. S. Lander (1983) ha mostrato come associare a un disegno simmetrico una famiglia di codici p-ari di lunghezza $v+1$ e un prodotto scalare, in modo che uno dei codici sia autoduale quando la massima potenza di p che divide n ha esponente dispari. Il Teorema 29.2 fornisce allora una condizione sui parametri del disegno. Risulta che tali condizioni sono già conseguenze del teorema di Bruck–Ryser–Chowla, Teorema 19.11. In un certo senso, questi codici autoduali forniscono quindi un'"interpretazione combinatoria" di parte del teorema BRC. In ogni caso contengono informazioni sul disegno e hanno ulteriori applicazioni nella teoria dei disegni simmetrici; si veda Lander (1983). Orig. 398

Teorema 29.3. Supponiamo che esista un disegno simmetrico (v, k, λ) per cui la massima potenza di un primo p che divide n abbia esponente dispari. Scriviamo $n = p^f n_0$, con f dispari, e $\lambda = p^b\lambda_0$, con $(n_0, p) = (\lambda_0, p) = 1$. Allora esiste un codice p-ario autoduale di lunghezza $v+1$ rispetto al prodotto scalare corrispondente a

$$B = \begin{cases} \operatorname{diag}(1, 1, \ldots, 1, -\lambda_0) & \text{se } b \text{ è pari,} \\ \operatorname{diag}(1, 1, \ldots, 1, n_0\lambda_0) & \text{se } b \text{ è dispari.} \end{cases}$$

Quindi, per il Teorema 29.2,

$$\begin{cases} -(-1)^{(v+1)/2}\lambda_0 \text{ è un quadrato modulo } p & \text{se } b \text{ è pari,} \\ (-1)^{(v+1)/2}n_0\lambda_0 \text{ è un quadrato modulo } p & \text{se } b \text{ è dispari.} \end{cases}$$

[4] Per dimostrare il teorema proviamo prima due proposizioni.

Data una matrice intera $m \times m$ A, consideriamo il $\mathbb{Z}$-modulo $M(A)$ di tutte le combinazioni lineari intere delle sue righe:

$$M(A) := \{yA : y \in \mathbb{Z}^m\}.$$

Fissiamo un primo p e per ogni intero non negativo i definiamo i moduli

$$M_i := \{x \in \mathbb{Z}^m : p^i x \in M(A)\}, \qquad N_i := \{y \in \mathbb{Z}^m : Ay^{\mathsf{T}} \equiv 0 \pmod{p^{i+1}}\}.$$

Abbiamo $M_0 = M(A)$, $M_i \subseteq M_{i+1}$ e $N_i \supseteq N_{i+1}$ per ogni i. Poniamo Orig. 399

$$C_i := M_i \pmod{p}, \qquad D_i := N_i \pmod{p}. \tag{29.1}$$

Cioè riduciamo modulo p tutti i vettori interi di M_i, N_i per ottenere C_i, D_i. Ciascuno è un sottospazio di $\mathbb{F}_p^m$, ossia un codice lineare p-ario. Chiaramente,

$$C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots, \qquad D_0 \supseteq D_1 \supseteq D_2 \supseteq \cdots.$$

Proposizione 29.4. Per ogni intero non negativo i vale $C_i^{\perp} = D_i$.

Dimostrazione. Siano x, y vettori interi tali che $x \pmod{p} \in C_i$ e $y \pmod{p} \in D_i$. Ciò significa

$$p^i(x + pa) = zA, \qquad A(y + pb)^{\mathsf{T}} \equiv 0 \pmod{p^{i+1}}$$

[4] Nota di traduzione: l'applicazione del Teorema 29.2 riguarda p dispari. Per $p = 2$ le espressioni non nulle modulo 2 sono comunque quadrati; la costruzione del codice resta valida.

per certi vettori interi a, b, z. Allora

$$p^i(x+pa)(y+pb)^{\mathsf{T}} = zA(y+pb)^{\mathsf{T}} \equiv 0 \pmod{p^{i+1}},$$

da cui $xy^{\mathsf{T}} = 0$ su $\mathbb{F}_p$.

Completiamo la dimostrazione mostrando che le dimensioni di C_i, D_i sommano a m. Esistono matrici unimodulari E, F, cioè matrici intere con inverse intere, tali che $S := EAF$ sia diagonale con elementi diagonali interi $d_1, \ldots, d_m$ che si dividono successivamente: $d_1 \mid d_2 \mid \cdots \mid d_m$. S è la forma normale di Smith di A e i d_i sono i fattori invarianti. Il lettore verifichi che i moduli M_i, N_i sono equivalenti rispettivamente a

$$M_i' := \{x : p^i x \in M(S)\}, \qquad N_i' := \{y : Sy^{\mathsf{T}} \equiv 0 \pmod{p^{i+1}}\},$$

nel senso che ciascuno si ottiene dall'altro mediante una trasformazione unimodulare. Quindi le dimensioni su $\mathbb{F}_p$ delle riduzioni modulo p di M_i, M_i' sono uguali, e lo stesso vale per N_i, N_i'. Supponiamo che p^{i+1} non divida $d_1, \ldots, d_t$ ma divida $d_{t+1}, \ldots, d_m$. Allora $y \in N_i'$ implica che le prime t coordinate di y siano divisibili per p; ogni vettore con le prime t coordinate nulle appartiene a N_i'. Dunque $N_i' \pmod p$ è generato dagli ultimi $m-t$ vettori della base canonica e ha dimensione $m-t$. Inoltre $x \in M_i'$ implica che le ultime $m-t$ coordinate di x siano divisibili per p;[5] riflettendo un poco si vede che $M_i' \pmod p$ è generato dai primi t vettori della base canonica e ha dimensione t. □ Orig. 400

Proposizione 29.5. Siano A, B, U matrici intere $m \times m$ tali che

$$ABA^{\mathsf{T}} = nU, \tag{29.2}$$

con U, B non singolari modulo un primo p. Scriviamo $n = p^e n_0$, $(p, n_0) = 1$. Definiamo da A la successione di codici p-ari C_i come in (29.1). Allora $C_e = \mathbb{F}_p^m$ e

$$C_i^B = C_{e-i-1} \qquad (i = 0, 1, \ldots, e-1).$$

In particolare, se e è dispari, $C_{(e-1)/2}$ è un codice p-ario autoduale rispetto al prodotto scalare dato da B su $\mathbb{F}_p^m$.

Dimostrazione. Siano x, y vettori interi tali che $x \pmod p \in C_i$ e $y \pmod p \in C_{e-i-1}$. Ciò significa

$$p^i(x+pa_1) = z_1 A, \qquad p^{e-i-1}(y+pa_2) = z_2 A$$

per certi vettori interi z_1, z_2, a_1, a_2. Allora, per (29.2),

$$p^{e-1}\langle x, y\rangle = p^{e-1} xBy^{\mathsf{T}} \equiv z_1 ABA^{\mathsf{T}} z_2^{\mathsf{T}} \equiv 0 \pmod{p^e}.$$

Dunque $\langle x, y\rangle = 0$ in $\mathbb{F}_p$ e vediamo che $C_{e-i-1} \subseteq C_i^B$.[6]

Sia ora $x \in C_i^B$. Ciò significa $xB \in C_i^{\perp}$, che per la Proposizione 29.4 è D_i. Esiste quindi un vettore intero x' che si riduce a x modulo p e tale che

$$x'BA^{\mathsf{T}} \equiv 0 \pmod{p^{i+1}}.$$

Da (29.2), $A \cdot BA^{\mathsf{T}}U^{-1} = nI$ e, poiché una matrice commuta con la propria inversa, Orig. 401

$$BA^{\mathsf{T}}U^{-1} \cdot A = nI. \tag{29.3}$$

Poiché U è non singolare modulo p, dU^{-1} è intera per qualche d primo con p, per esempio $d := \det U$. Moltiplicando (29.3) a sinistra per dx' otteniamo

$$x'BA^{\mathsf{T}}(dU^{-1})A = p^e dn_0 x',$$

quindi

$$zA = p^{e-i-1} dn_0 x', \qquad z := \frac{1}{p^{i+1}} x'BA^{\mathsf{T}}(dU^{-1}) \in \mathbb{Z}^m.$$

[5] Nota di traduzione: l'originale reca "$d-t$" invece di "$m-t$".

[6] Nota di traduzione: con la definizione di ortogonale sinistro data sopra, per questa inclusione si scambiano i ruoli di x, y nell'argomento; (29.2) annulla anche il prodotto nell'ordine inverso.

Ciò significa che $p^{e-i-1}dn_0x'$ appartiene a M_{e-i-1} e dunque $x \in C_{e-i-1}$.[7]

L'affermazione $C_e = \mathbb{F}_p^m$ è lasciata come semplice esercizio. □

Problema 29B. Dimostrare che $C_e = \mathbb{F}_p^m$.

Dimostrazione del Teorema 29.3. Sia N la matrice d'incidenza di un disegno simmetrico (v, k, λ) e sia p un primo. Supponiamo $\lambda = p^{2a}\lambda_0$ con $(\lambda_0, p) = 1$ e $a \geq 0$; spiegheremo poi come procedere quando la massima potenza di p che divide λ ha esponente dispari. Poniamo

$$A := \begin{pmatrix} N & p^a\mathbf{1} \\ p^a\lambda_0\mathbf{1}^\mathsf{T} & k \end{pmatrix}, \qquad B := \operatorname{diag}(1, \ldots, 1, -\lambda_0), \tag{29.4}$$

dove $\mathbf{1}$ è la colonna di v unità. Il lettore verifichi, usando le proprietà di N e $\lambda(v-1) = k(k-1)$, che $ABA^\mathsf{T} = nB$.

Se la massima potenza di p che divide λ ha esponente pari, applichiamo la Proposizione 29.5 con A, B date da (29.4) e $U := B$.

Se invece l'esponente è dispari, applichiamo il caso precedente al complementare del disegno, un disegno simmetrico $(v, v-k, \lambda')$ con $\lambda' = v - 2k + \lambda$. Scriviamo $\lambda' = p^c\lambda_0'$ con $(\lambda_0', p) = 1$. Da $\lambda\lambda' = n(n-1)$ segue che c è dispari e

$$\lambda_0\lambda_0' = n_0(n-1) \equiv -n_0 \pmod{p}.$$

[8] Nella conclusione abbiamo sostituito $-\lambda_0'$ con $\lambda_0 n_0$, il che è lecito perché differiscono per un fattore quadrato modulo p, così da esprimere il risultato mediante i parametri originali. □ Orig. 402

Il teorema seguente è conseguenza del Problema 19M, ma ne diamo una dimostrazione analoga a quella del Teorema 29.3.

Teorema 29.6. Se esiste una matrice di conferenza di ordine $n \equiv 2 \pmod 4$, nessun primo $p \equiv 3 \pmod 4$ può dividere la parte libera da quadrati di $n-1$.

Dimostrazione. Una matrice di conferenza di ordine n è, in particolare, una matrice intera A tale che $AA^\mathsf{T} = (n-1)I_n$. Per la Proposizione 29.5 con $A = U = I$,[9] esiste un codice p-ario autoduale rispetto al prodotto scalare standard, di lunghezza n, per ogni divisore primo p della parte libera da quadrati di $n-1$. Il Teorema 29.2 implica allora che ciascuno di questi primi è congruo a 1 modulo 4. □

* * *

Se p è un primo che non divide l'ordine v di un gruppo abeliano G, l'anello di gruppo $\mathbb{F}_p[G]$ è un'algebra *semisemplice* su $\mathbb{F}_p = \mathbb{Z}_p$. Ciò significa che non vi sono nilpotenti non nulli, cioè elementi $a \neq 0$ tali che $a^m = 0$ per qualche intero positivo m; la loro non esistenza è provata nel Lemma 28.5. Per il teorema di Wedderburn, ogni algebra commutativa semisemplice con unità $\mathcal{A}$ di dimensione finita su un campo $\mathbb{F}$ è isomorfa a un prodotto diretto di campi, ciascuno estensione di $\mathbb{F}$. Ne segue che ogni ideale I di $\mathcal{A}$ è principale e generato da un idempotente e, cioè da un elemento con $e^2 = e$. Per le dimostrazioni si veda un testo avanzato di algebra.

Non ci servono tutte queste informazioni, ma useremo alcuni fatti sugli ideali principali generati da idempotenti, che costituiscono buoni esercizi.

Anzitutto, se $I = \langle e_1 \rangle = \langle e_2 \rangle$ con e_1, e_2 idempotenti, allora $e_1 = e_2$. Se $I_1 = \langle e_1 \rangle$ e $I_2 = \langle e_2 \rangle$, con e_1, e_2 idempotenti, allora

$$I_1 \cap I_2 = \langle e_1e_2 \rangle, \qquad I_1 + I_2 = \langle e_1 + e_2 - e_1e_2 \rangle.$$

Si noti che e_1e_2 ed $e_1 + e_2 - e_1e_2$ sono ancora idempotenti. Orig. 403

Teorema 29.7. Sia D un insieme di differenze $(n^2+n+1, n+1, 1)$ in un gruppo abeliano G di ordine $v := n^2+n+1$. Se $n \equiv 0 \pmod 2$ ma $n \not\equiv 0 \pmod 4$, allora $n = 2$. Se $n \equiv 0 \pmod 3$ ma $n \not\equiv 0 \pmod 9$, allora $n = 3$.

[7] Nota di traduzione: più precisamente l'uguaglianza mostra che $p^{e-i-1}dn_0x' \in M(A)$, ossia $dn_0x' \in M_{e-i-1}$; poiché dn_0 è invertibile modulo p, segue la conclusione.

[8] Nota di traduzione: l'originale dice "c è dispari", ma $b + c = f$ con b, f dispari dà c *pari*; è proprio questo che consente di applicare il caso precedente.

[9] Nota di traduzione: va letto $B = U = I$; A rimane la matrice di conferenza.

DIMOSTRAZIONE. Sia D come nell'enunciato e sia p un divisore primo di n. Per il Teorema 28.3, p è un moltiplicatore di D; d'ora in poi supponiamo che D sia fissato da p. Lavoriamo nell'algebra $\mathbb{F}_p[G]$.

Siano I_1 l'ideale generato da $D(x)$ e I_2 quello generato da $D(x^{-1})$. Abbiamo $D(x^p) = D(x)$, ma per il Lemma 28.2 $D^p(x) = D(x^p)$, quindi $D^p(x) = D(x)$ in $\mathbb{F}_p[G]$. Allora $D^{p-1}(x)$ è idempotente e genera anch'esso I_1. Analogamente $D^{p-1}(x^{-1})$ è un generatore idempotente di I_2. Quindi il generatore idempotente di $I_1 \cap I_2$ è

$$D^{p-1}(x)D^{p-1}(x^{-1}) = (n + G(x))^{p-1} = G(x),$$

e quello di $I_1 + I_2$ è

$$D^{p-1}(x) + D^{p-1}(x^{-1}) - G(x).$$

Vogliamo ora considerare le dimensioni di I_1, I_2 su $\mathbb{F}_p$. In generale, la dimensione di un ideale principale generato da $A(x)$ è il rango della matrice $v \times v$ le cui righe sono i coefficienti di $x^g A(x)$, $g \in G$. Per $A(x) = D(x)$ o $D(x^{-1})$, questa è la matrice d'incidenza di un disegno simmetrico $(n^2+n+1, n+1, 1)$. Se supponiamo ora che p^2 non divida n, per il Teorema 29.1 I_1, I_2 hanno dimensione $(v+1)/2$. L'intersezione ha dimensione 1, perciò la somma deve avere dimensione v. Il generatore idempotente dell'intero anello di gruppo, considerato come ideale di sé stesso, è 1. Concludiamo dunque

$$D^{p-1}(x) + D^{p-1}(x^{-1}) - G(x) = 1 \quad \text{in } \mathbb{F}_p[G]. \tag{29.5}$$

Sappiamo sfruttare questa equazione soltanto per $p = 2$ o 3. Per $p = 2$, (29.5) afferma $D(x) + D(x^{-1}) \equiv 1 + G(x) \pmod 2$ in $\mathbb{Z}[G]$. Il numero di coefficienti dispari di $1 + G(x)$ è $v - 1 = n^2 + n$, mentre quello di $D(x) + D(x^{-1})$ non può superare $2(n + 1)$; segue $n \le 2$. Orig. 404

Per $p = 3$, (29.5) afferma $D^2(x) + D^2(x^{-1}) \equiv 1 + G(x) \pmod 3$ in $\mathbb{Z}[G]$. Affermiamo che i coefficienti non nulli di ciascuno fra $D^2(x)$ e $D^2(x^{-1})$ sono $n+1$ coefficienti uguali a 1 e $\binom{n+1}{2}$ coefficienti uguali a 2. Se C è un insieme di differenze planare, in $C^2(x)$ compare un termine x^{2g} per ogni $g \in C$ e un termine $2x^{g+h}$ per ogni coppia non ordinata $\{g, h\} \subseteq C$. Si noti che $\lambda = 1$ implica, per esempio, $g_1 + h_1 \ne g_2 + h_2$ a meno che $\{g_1, h_1\} = \{g_2, h_2\}$. La somma di due elementi di questo tipo dell'anello di gruppo non può avere più di $\binom{n+1}{2} + 2(n + 1)$ coefficienti congrui a 1 modulo 3, mentre $1 + G(x)$ ha $n^2 + n$ coefficienti uguali a 1. Segue $n \le 4$. □

Problema 29C. Supponiamo che D sia un insieme di differenze con $n \equiv 2 \pmod 4$ e che 2 sia un suo moltiplicatore. Quali sono i parametri di D, in funzione di n?

Note

Parte del materiale che precede la dimostrazione del Teorema 29.3 è più elegante introducendo i numeri p-adici, come in Lander (1983), ma abbiamo scelto di presentarlo senza di essi.

Riferimenti bibliografici

D. Jungnickel and K. Vedder (1984), On the geometry of planar difference sets, *European J. Combinatorics* **5**, 143–148.

E. S. Lander (1983), *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series **74**, Cambridge University Press.

V. Pless (1986), Cyclic projective planes and binary extended cyclic self-dual codes, *J. Combinatorial Theory (A)* **43**, 331–333.

H. A. Wilbrink (1985), A note on planar difference sets, *J. Combinatorial Theory (A)* **38**, 94–95.

Capitolo 30

Schemi di associazione

Orig. 405

Dati due sottoinsiemi A, B di k elementi di un insieme di n elementi, $n \geq 2k$, vi sono $k+1$ possibili relazioni tra essi: possono essere uguali, intersecarsi in $k-1$ elementi, intersecarsi in $k-2$ elementi, e così via, oppure essere disgiunti.

Date due parole, cioè k-uple, $a, b \in A^k$, dove A è un "alfabeto" di almeno due simboli, vi sono $k+1$ possibili relazioni tra esse: possono essere uguali, coincidere in $k-1$ coordinate, coincidere in $k-2$ coordinate, e così via, oppure differire in tutte le coordinate.

Questi esempi di un insieme dotato di una lista di relazioni binarie mutuamente esclusive ed esaustive sono *schemi di associazione*, che definiremo tra poco. Essi costituiscono uno dei fondamenti della combinatoria: includiamo perciò questo capitolo, benché la lettura sarà impegnativa. Sono stati impliciti in molti capitoli precedenti; abbiamo discusso esplicitamente gli schemi di associazione a due classi, equivalenti ai grafi fortemente regolari del Capitolo 21. Questo capitolo approfondisce parte del materiale di quel capitolo, ma con obiettivi diversi.

Gli schemi di associazione nacquero nella teoria statistica della progettazione degli esperimenti; il lavoro di Ph. Delsarte (1973) ha però mostrato come unifichino molti aspetti della nostra materia. In particolare, alcuni risultati della teoria dei codici e di quella dei t-disegni, scoperti originariamente in modo indipendente, si rivelano aspetti "formalmente duali" delle stesse idee negli schemi di associazione. Per esempio, la disuguaglianza di Fisher e la sua generalizzazione, Teorema 19.8, sono formalmente duali al limite dell'impacchettamento di sfere, Teorema 21.1.[1] Useremo questi strumenti per dimostrare il teorema di Lloyd sui codici perfetti e il suo duale formale per disegni stretti e schieramenti ortogonali. Le disuguaglianze di Delsarte, Teorema 30.3, sul vettore di distribuzione di un sottoinsieme di uno schema forniscono un "limite di programmazione lineare" alla cardinalità dei codici e interessano anche la teoria estremale degli insiemi.

Orig. 406

Per *relazione binaria* su un insieme X intendiamo un sottoinsieme di $X \times X$. Uno *schema di associazione a k classi*, o semplicemente *schema*, su un insieme X di punti consiste di $k+1$ relazioni binarie simmetriche non vuote $R_0, R_1, \ldots, R_k$ che partizionano $X \times X$, dove $R_0 = \{(x,x) : x \in X\}$ è la relazione identità, e per le quali esistono interi non negativi p_{ij}^{ℓ}, $0 \leq \ell, i, j \leq k$, tali che: data una coppia $(x,y) \in R_\ell$, esistono esattamente p_{ij}^{ℓ} elementi $z \in X$ con $(x,z) \in R_i$ e $(z,y) \in R_j$. Diciamo che x, y sono *i-esimi associati* quando $(x,y) \in R_i$.

I numeri p_{ij}^{ℓ} sono i *parametri* dello schema. L'esistenza di p_{ii}^0 significa che il numero degli i-esimi associati di un elemento di X è costante; lo si indica di solito con n_i. Abbiamo

$$p_{ii}^0 = n_i, \qquad p_{ij}^0 = 0 \quad \text{per } i \neq j, \tag{30.1}$$

e

$$n_0 = 1, \qquad n_0 + n_1 + \cdots + n_k = N, \qquad N := |X|.$$

I numeri $n_0, n_1, \ldots, n_k$ si chiamano *gradi* dello schema.

Esempio 30.1. Gli *schemi di Johnson* $J(v,k)$. I punti di $J(v,k)$ sono i $\binom{v}{k}$ sottoinsiemi di k elementi di un insieme S di v elementi. Due di essi A, B si dichiarano i-esimi associati quando $|A \cap B| = k - i$. Gli

[1] Nota di traduzione: i richiami al limite dell'impacchettamento di sfere come "Teorema 21.1" in questo capitolo vanno letti "Teorema 20.1".

associati di classe 0 sono dunque uguali. I parametri p_{ij}^{ℓ} esistono "per simmetria" e si possono esprimere come somme di prodotti di coefficienti binomiali, ma non li scriveremo esplicitamente in generale.

Per esempio, $J(6,3)$ è uno schema a tre classi con 20 punti. Il lettore verifichi $n_1 = n_2 = 9$, $n_3 = 1$. Alcuni degli altri parametri sono $p_{11}^1 = 4$, $p_{11}^2 = 4$, $p_{11}^3 = 0$.

Esempio 30.2. Gli *schemi di Hamming* $H(n,q)$. I punti sono le q^n parole di lunghezza n su un alfabeto di q simboli. Due n-uple x, y si dichiarano i-esimi associati quando differiscono in esattamente i coordinate. Gli associati di classe 0 sono dunque uguali. I parametri p_{ij}^{ℓ} esistono "per simmetria" e si possono esprimere come somme di prodotti di coefficienti binomiali e potenze di $q-1$, ma non li scriveremo in generale. Orig. 407

Per esempio, $H(5,3)$ è uno schema a cinque classi con 125 punti.[2] Il lettore verifichi $n_1 = 5 \cdot 2$, $n_2 = 10 \cdot 4$, eccetera.

Ogni relazione R_i può essere vista come la relazione di adiacenza di un grafo G_i sull'insieme dei vertici X. Uno schema è una particolare partizione, o colorazione, degli spigoli di un grafo completo. Partendo da uno schema a due classi, dovrebbe essere chiaro che G_1 è un grafo fortemente regolare di grado n_1, con $\lambda = p_{11}^1$ e $\mu = p_{11}^2$. Anzi, ogni grafo fortemente regolare dà uno schema a due classi dichiarando due vertici distinti primi associati se adiacenti in G, secondi associati altrimenti; gli altri parametri esistono, cioè sono costanti, e si calcolano da quelli del grafo. Per esempio $p_{12}^1 = k - \lambda - 1$.

Un *grafo regolare rispetto alla distanza* è un grafo G tale che il numero di vertici a distanza i da x e j da y dipenda soltanto dalla distanza ℓ fra x, y, non dai particolari vertici. Cioè, dichiarando due vertici i-esimi associati se e solo se la loro distanza in G è i, si ottiene uno schema di associazione, con numero di classi pari al diametro. Si veda Brouwer, Cohen e Neumaier (1989). Gli schemi che nascono in questo modo si dicono *metrici*. Lo sono quelli degli Esempi 30.1 e 30.2, e anche quelli degli Esempi 30.3 e 30.4 sotto.

È importante sapere che i parametri p_{ij}^{ℓ} esistono; non è altrettanto importante conoscerne i valori esatti. È una fortuna, perché spesso non vi è un'espressione comoda. In $J(v,k)$, per esempio, per il generico p_{ij}^{ℓ} sembra necessaria una somma tripla di coefficienti binomiali. Negli esempi dati sappiamo che esistono per "simmetria". Più precisamente, in ciascun caso esiste un gruppo G di permutazioni di X tale che due coppie ordinate $(x_1, y_1), (x_2, y_2)$ appartengano alla stessa relazione R_i se e solo se esiste $\sigma \in G$ con $\sigma(x_1) = x_2$ e $\sigma(y_1) = y_2$. Le relazioni $R_0, \ldots, R_k$ sono cioè le orbite di G su $X \times X$, con R_0 orbita banale di tutte le coppie (x,x). Nell'Esempio 30.1, G è il gruppo simmetrico S_v agente sui sottoinsiemi di k elementi; una permutazione porta una coppia ordinata in un'altra se e solo se le due intersezioni hanno la stessa cardinalità. Nell'Esempio 30.2, G è il prodotto intrecciato di S_q con S_n: ammettiamo ogni permutazione delle n coordinate, seguita da permutazioni indipendenti dei q simboli in ciascuna coordinata. Una trasformazione di questo tipo porta una coppia ordinata di n-uple in un'altra se e solo se le coppie coincidono nello stesso numero di coordinate. Orig. 408

In generale, se G è un gruppo transitivo di permutazioni di X le cui orbite su $X \times X$ sono simmetriche, esse possono essere prese come relazioni di uno schema su X. Anche i prossimi tre esempi nascono così.

Esempio 30.3. Il q-analogo dello schema di Johnson: prendiamo come punti i sottospazi di dimensione k di uno spazio V di dimensione v su $\mathbb{F}_q$. Due sottospazi A, B si dichiarano i-esimi associati quando $\dim(A \cap B) = k - i$.

Esempio 30.4. Prendiamo come punti le matrici $k \times m$ su $\mathbb{F}_q$, supponendo $k \leq m$. Due matrici A, B si dichiarano i-esimi associati quando il rango di $A - B$ è $k - i$.[3]

Per ricondurre l'esempio al quadro precedente, sia X l'insieme delle matrici $k \times m$ e prendiamo per G tutte le permutazioni $X \mapsto UXW + C$, dove U percorre le matrici non singolari $k \times k$, W quelle non singolari $m \times m$ e C le matrici $k \times m$. Se $(A, B), (A', B')$ sono coppie con $A - B, A' - B'$ dello stesso rango, allora $U(A - B)W = A' - B'$ per certe U, W non singolari, e $X \mapsto UXW + (B' - UBW)$ porta la prima coppia nella seconda.

Esempio 30.5. Gli *schemi ciclotomici* si ottengono così. Sia q una potenza di primo e sia $k \mid (q-1)$. Sia C_1 il sottogruppo di indice k del gruppo moltiplicativo di $\mathbb{F}_q$, e siano $C_1, C_2, \ldots, C_k$ le sue classi laterali. I punti sono gli elementi di $\mathbb{F}_q$; x, y si dichiarano i-esimi associati se $x - y \in C_i$, e associati di classe 0 se $x - y = 0$. Per ottenere uno schema nel senso della definizione richiediamo $-1 \in C_1$, così che

[2] Nota di traduzione: il numero corretto è $3^5 = 243$; 125 è un refuso dell'originale.

[3] Nota di traduzione: per avere R_0 uguale all'identità, il rango deve essere i, non $k - i$. Con tale correzione si ottiene lo schema metrico descritto.

le relazioni siano simmetriche; se q è dispari, $2k$ deve dunque dividere $q-1$. Si confronti l'Esempio 21.3, che è il caso $k=2$. Orig. 409

Introduciamo le *matrici di associazione* $A_0, A_1, \dots, A_k$, dette anche matrici di adiacenza, di uno schema. Sono matrici quadrate con righe e colonne indicizzate da X; definiamo

$$A_i(x,y) := \begin{cases} 1 & \text{se } (x,y) \in R_i, \\ 0 & \text{altrimenti.} \end{cases}$$

Sono matrici simmetriche a coefficienti 0 e 1, con

$$A_0 = I, \qquad A_0 + A_1 + \cdots + A_k = J,$$

dove J è la matrice $N \times N$ di tutti 1. Indichiamo con $\mathcal{A}$ lo spazio generato su $\mathbb{R}$ da $A_0, \dots, A_k$. Queste matrici sono linearmente indipendenti: ciascuna contiene almeno un 1, e una posizione in cui A_i ha un 1 contiene 0 in ogni altra matrice di associazione. Gli assiomi di uno schema sono esattamente ciò che serve per assicurare che $\mathcal{A}$ sia chiusa per moltiplicazione fra matrici. Basta mostrare che il prodotto di due matrici della base è in $\mathcal{A}$; infatti,

$$A_i A_j = \sum_{\ell=0}^{k} p_{ij}^{\ell} A_\ell, \tag{30.2}$$

perché $(A_iA_j)(x,y)$ è il numero degli z tali che $A_i(x,z)=1$ e $A_j(z,y)=1$, cioè p_{ij}^{ℓ} quando $A_\ell(x,y)=1$.

L'algebra $\mathcal{A}$ si chiama *algebra di Bose–Mesner* dello schema; per i grafi fortemente regolari è stata introdotta nel Capitolo 21. Osserviamo che essa è chiusa anche per la moltiplicazione di Hadamard, introdotta nel Problema 21E. Il prodotto di Hadamard $A \circ B$ è ottenuto moltiplicando elemento per elemento:

$$(A \circ B)(x,y) := A(x,y)B(x,y).$$

Come algebra rispetto al prodotto di Hadamard, $\mathcal{A}$ è quasi banale. Abbiamo Orig. 410

$$A_i \circ A_j = \begin{cases} A_i & \text{se } i = j, \\ O & \text{se } i \neq j, \end{cases}$$

cioè $A_0, \dots, A_k$ sono idempotenti ortogonali, e la loro somma è J, l'identità per questo prodotto. La moltiplicazione di Hadamard è dunque estremamente semplice quando le matrici sono espresse nella base $A_0, \dots, A_k$.

Un noto risultato della teoria delle matrici, estensione del teorema spettrale secondo cui una matrice reale simmetrica ha una base ortogonale di autovettori, afferma però che un'algebra commutativa di matrici reali simmetriche ha una base di idempotenti ortogonali per il prodotto ordinario, la cui somma è l'identità. Geometricamente esiste una decomposizione ortogonale

$$\mathbb{R}^X = V_0 \oplus V_1 \oplus \cdots \oplus V_k$$

dello spazio euclideo dei vettori con coordinate indicizzate da X, dotato del prodotto scalare standard, tale che le proiezioni ortogonali $E_0, \dots, E_k$ rispettivamente sui sottospazi $V_0, \dots, V_k$ costituiscano una base di $\mathcal{A}$. Abbiamo

$$E_iE_j = \begin{cases} E_i & \text{se } i = j, \\ O & \text{se } i \neq j, \end{cases} \qquad E_0 + E_1 + \cdots + E_k = I.$$

Naturalmente anche il prodotto ordinario è estremamente semplice nella base $E_0, \dots, E_k$.

I sottospazi $V_0, \dots, V_k$ si chiamano *autospazi* dello schema: per $M = \sum_{i=0}^{k} \lambda_i E_i$, ogni vettore di V_i è un autovettore di M di autovalore λ_i. In generale non c'è una numerazione naturale degli autospazi, con un'eccezione. Poiché $J \in \mathcal{A}$, il vettore j di tutti 1 è suo autovettore di autovalore N e tutti i vettori ortogonali a j hanno autovalore 0, uno degli autospazi deve consistere soltanto dei multipli scalari di j; supporremo sempre che sia V_0. La proiezione ortogonale su V_0, che ha j come autovettore di autovalore 1 e tutti i vettori ortogonali a j con autovalore 0, è Orig. 411

$$E_0 = \frac{1}{N} J.$$

Indichiamo con m_i la dimensione di V_i. Allora

$$m_0 = 1, \qquad m_0 + m_1 + \cdots + m_k = N.$$

Si noti che m_i è la traccia di E_i, perché gli autovalori di E_i sono 1, con molteplicità pari alla dimensione di V_i, e 0. I numeri $m_0, \dots, m_k$ si chiamano *molteplicità* dello schema.

Esempio 30.6. Possiamo descrivere esplicitamente gli autospazi di $H(n,2)$. I punti sono le n-uple binarie, o parole, di $\mathbb{F}_2^n$. Per ogni $a \in \mathbb{F}_2^n$ definiamo un vettore v_a, con coordinate indicizzate dai punti, ponendo

$$v_a(b) := (-1)^{\langle a,b\rangle}.$$

Questi vettori sono ortogonali e sono le righe di una matrice di Hadamard; si vedano la Figura 30.1 e il Capitolo 18. Affermiamo che si può prendere per V_i lo spazio generato dai v_a con a di peso i, per $i = 0, \dots, n$.

Verifichiamo che ogni v_a è autovettore di tutte le matrici A_j. Sia a di peso ℓ. Allora

$$\begin{aligned}(v_a A_j)(b) &= \sum_c v_a(c) A_j(c,b) \\ &= \sum_{c:d(b,c)=j} (-1)^{\langle a,c\rangle} = (-1)^{\langle a,b\rangle} \sum_{c:d(b,c)=j} (-1)^{\langle a,b+c\rangle} \\ &= v_a(b) \sum_{u:\mathrm{wt}(u)=j} (-1)^{\langle a,u\rangle} = v_a(b) \sum_{i=0}^{n} (-1)^i \binom{\ell}{i}\binom{n-\ell}{j-i}.\end{aligned}$$

Questo calcolo mostra, indicando con E_i la proiezione ortogonale su V_i, che

$$A_j = \sum_{\ell=0}^{n} \left(\sum_{i=0}^{n} (-1)^i \binom{\ell}{i}\binom{n-\ell}{j-i} \right) E_\ell,$$

perché i due membri danno lo stesso risultato se premoltiplicati per un qualsiasi v_a. Dunque $\mathcal{A} \subseteq \mathrm{span}\{E_0, \dots, E_n\}$; vale l'uguaglianza perché entrambi gli spazi hanno dimensione $n+1$. Orig. 412

Gli autovalori di $H(n,q)$ per q generale sono dati nel Teorema 30.1 sotto.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}$$

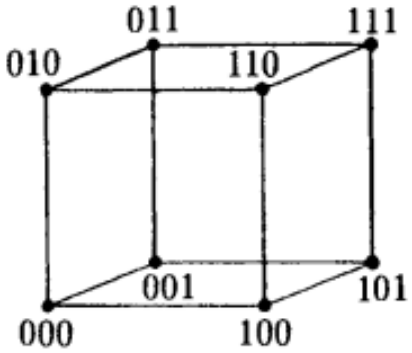


Figura 30.1

Per esempio, ordinando le parole di lunghezza $n = 3$ come

$$000,\ 100,\ 010,\ 001,\ 011,\ 101,\ 110,\ 111,$$

gli autospazi V_0, V_1, V_2, V_3 del cubo, cioè del grafo con matrice A_1 di $H(3,2)$, mostrato a destra nella Figura 30.1, sono generati rispettivamente dalla prima riga, dalle tre successive, dalle tre successive ancora e dall'ultima riga della matrice di Hadamard a sinistra.

Esempio 30.7. Descriviamo ora gli autospazi dello schema di Johnson $J(v,k)$, omettendo le dimostrazioni; si vedano Delsarte (1973) o Wilson (1984b).

L'insieme dei punti è l'insieme $\mathcal{X}$ dei sottoinsiemi S di k elementi di un insieme X di v elementi. Per ogni $T \subseteq X$ con $|T| \le k$, sia e_T il vettore di lunghezza $\binom{v}{k}$ in $\mathbb{R}^{\mathcal{X}}$ definito da

$$e_T(S) := \begin{cases} 1 & \text{se } T \subseteq S, \\ 0 & \text{altrimenti.} \end{cases}$$

Sia U_i lo spazio generato da $\{e_T : T \subseteq X, |T| = i\}$, $i = 0, \dots, k$. Affermiamo che $U_0 \subseteq U_1 \subseteq \cdots \subseteq U_k = \mathbb{R}^{\mathcal{X}}$ e che $\dim U_i = \binom{v}{i}$. Poniamo $V_0 := U_0$, i vettori costanti, e per $i > 0$ prendiamo il complemento ortogonale di U_{i-1} in U_i:

$$V_i := U_i \cap U_{i-1}^{\perp}.$$

È chiaro che i V_i sono ortogonali e la loro somma è $\mathbb{R}^{\mathcal{X}}$. Si può mostrare che ogni vettore di V_i è autovettore di A_j di autovalore $P_j(i)$, dato nel Teorema 30.1(i). Orig. 413

Avendo due basi di $\mathcal{A}$, possiamo considerare le matrici di cambiamento di base, chiamate *matrici degli autovalori* dello schema. Definiamo P, la prima matrice degli autovalori, e Q, la seconda, come matrici $(k+1) \times (k+1)$ con righe e colonne indicizzate da $0, 1, \dots, k$, tali che

$$(A_0, A_1, \dots, A_k) = (E_0, E_1, \dots, E_k)P,$$

$$N(E_0, E_1, \dots, E_k) = (A_0, A_1, \dots, A_k)Q.$$

Indichiamo con $P_\ell(i)$ l'elemento (i, ℓ) di P, e analogamente con $Q_\ell(i)$ quello di Q. Così

$$A_\ell = P_\ell(0)E_0 + P_\ell(1)E_1 + \cdots + P_\ell(k)E_k, \tag{30.3}$$

$$NE_\ell = Q_\ell(0)A_0 + Q_\ell(1)A_1 + \cdots + Q_\ell(k)A_k. \tag{30.4}$$

Naturalmente $Q = NP^{-1}$ e $P = NQ^{-1}$. La colonna ℓ di P consiste degli autovalori di A_ℓ.

Mentre non è così importante conoscere i parametri p_{ij}^ℓ, per le applicazioni è importante conoscere P, Q. Per le dimostrazioni del teorema seguente e la determinazione delle matrici di altri schemi si vedano Bannai e Ito (1984) o Delsarte (1973).

Teorema 30.1. (i) Per $J(v,k)$, i gradi sono $n_\ell = \binom{k}{\ell}\binom{v-k}{\ell}$ e le molteplicità $m_\ell = \binom{v}{\ell} - \binom{v}{\ell-1}$, $\ell = 0, 1, \dots, k$. Gli elementi della prima matrice degli autovalori sono $P_\ell(i)$, dove

$$P_\ell(x) = \sum_{\alpha=0}^{\ell} (-1)^{\ell-\alpha} \binom{k-\alpha}{\ell-\alpha}\binom{k-x}{\alpha}\binom{v-k+\alpha-x}{\alpha}.$$

(ii) Per $H(n,q)$, i gradi e le molteplicità sono $n_\ell = m_\ell = \binom{n}{\ell}(q-1)^\ell$, $\ell = 0, 1, \dots, n$. Gli elementi della prima matrice degli autovalori sono $P_\ell(i)$, dove Orig. 414

$$P_\ell(x) = \sum_{\alpha=0}^{\ell} (-q)^\alpha (q-1)^{\ell-\alpha} \binom{n-\alpha}{\ell-\alpha}\binom{x}{\alpha}.$$

Problema 30A. Calcolare la matrice P di $J(8,3)$ nel modo seguente. Calcolare prima A_1A_2 come combinazione lineare di A_0, A_1, A_2, A_3, poi completare la riga mancante:

$$\begin{aligned} A_1^0 &= A_0, \\ A_1^1 &= A_1, \\ A_1^2 &= 15A_0 + 6A_1 + 4A_2, \\ A_1^3 &= \dots, \\ A_1^4 &= 1245A_0 + 1036A_1 + 888A_2 + 720A_3. \end{aligned}$$

Da questa tabella si ricava, con calcoli solo moderatamente laboriosi, il polinomio minimo di A_1. Trovare gli autovalori di A_1. Esprimere poi A_2, A_3 come polinomi in A_1 e trovarne gli autovalori. Trovare le molteplicità. Controllare verificando le relazioni di ortogonalità del Teorema 30.2 oppure calcolando direttamente dal Teorema 30.1(i).

Problema 30B. Mostrare come calcolare tutti i parametri p_{ij}^ℓ di uno schema a partire dalla matrice P, cioè provare che sono univocamente determinati da essa.

Problema 30C. I grafi di quadrati latini sono grafi $srg(v, k, \lambda, \mu)$ con, per certi interi n, r,

$$v = n^2, \quad k = r(n-1), \quad \lambda = (n-2) + (r-1)(r-2), \quad \mu = r(r-1).$$

Sono stati introdotti nell'Esempio 21.7 per $r = 3$. Trovare P, Q per gli schemi a due classi corrispondenti.

I cosiddetti grafi di quadrati latini negativi sono grafi fortemente regolari i cui parametri si ottengono sostituendo sopra n con $-n$ e r con $-r$. Quindi $v = (-n)^2$, $k = (-r)(-n-1)$, eccetera. È strano che ciò dia parametri che soddisfano (21.4), ma accade. Trovare P, Q per i corrispondenti schemi a due classi. Orig. 415

Teorema 30.2. Le matrici degli autovalori soddisfano le relazioni di ortogonalità

$$P^{\mathsf{T}} \operatorname{diag}(1, m_1, \dots, m_k) P = N \operatorname{diag}(1, n_1, \dots, n_k),$$

$$Q^{\mathsf{T}} \operatorname{diag}(1, n_1, \dots, n_k) Q = N \operatorname{diag}(1, m_1, \dots, m_k).$$

Dimostrazione. Dotiamo $\mathcal{A}$ di un prodotto scalare in modo abbastanza naturale: definiamo $\langle A, B\rangle$ come la somma degli elementi del prodotto di Hadamard $A \circ B$. Verificare che coincide con la traccia di AB^{T}, e quindi con $\operatorname{tr}(AB)$ se B è simmetrica.

La base $A_0, \dots, A_k$ è ortogonale, ma non ortonormale, e $\langle A_i, A_i\rangle = Nn_i$. Anche $E_0, \dots, E_k$ è ortogonale, perché $E_iE_j = 0$ per $i \neq j$; abbiamo $\langle E_i, E_i\rangle = \operatorname{tr}(E_i) = m_i$. Il teorema segue ora dall'algebra lineare elementare.

Consideriamo la prima relazione. L'elemento di posto (α, β) a destra è

$$\begin{aligned}\langle A_\alpha, A_\beta\rangle &= \left\langle \sum_i P_\alpha(i) E_i, \sum_j P_\beta(j) E_j \right\rangle \\ &= \sum_{i,j} P_\alpha(i) P_\beta(j) \langle E_i, E_j\rangle = \sum_i m_i P_\alpha(i) P_\beta(i),\end{aligned}$$

che è l'elemento (α, β) a sinistra. La seconda relazione si ottiene analogamente. □ Un altro modo di esprimere il teorema è Orig. 416

$$Q = \operatorname{diag}(1, n_1, \dots, n_k)^{-1} P^{\mathsf{T}} \operatorname{diag}(1, m_1, \dots, m_k).$$

Equivalentemente,

$$m_j P_i(j) = n_i Q_j(i) \tag{30.5}$$

per $i, j = 0, 1, \dots, k$.

Con i Teoremi 30.1 e 30.2 possiamo trovare Q per $J(v, k)$ e $H(n, q)$. È un po' sorprendente che $P = Q$ per $H(n, q)$; il lettore lo verifichi.

Problema 30D. Spiegare perché la riga e la colonna di indice 0 di P, Q sono quelle indicate:

$$P = \begin{pmatrix} 1 & n_1 & \cdots & n_k \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & m_1 & \cdots & m_k \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix}. \tag{30.6}$$

Delsarte (1973) osservò che le colonne di Q forniscono un sistema di vincoli lineari, che chiameremo *disuguaglianze di Delsarte*, su ciò che egli chiama "vettore di distribuzione interna" di un sottoinsieme non vuoto Y dell'insieme dei punti X di uno schema. Definiamo il *vettore di distribuzione* di Y come $a = (a_0, a_1, \dots, a_k)$, dove

$$a_i := \frac{1}{|Y|} |(Y \times Y) \cap R_i|.$$

Cioè a_i è il numero medio di i-esimi associati $y \in Y$ di un elemento $x \in Y$. Abbiamo

$$a_0 = 1, \qquad a_0 + a_1 + \cdots + a_k = |Y|.$$

Per molti sottoinsiemi interessanti, il numero degli i-esimi associati $y \in Y$ di $x \in Y$ è costante, indipendente da x. È così, per esempio, se C è un codice lineare in $H(n, q)$: il vettore di distribuzione coincide allora con ciò che nel Capitolo 21 abbiamo chiamato enumeratore dei pesi di C.[4] Ciò vale anche per altre belle configurazioni discusse nei capitoli precedenti, i cui vettori sono elencati sotto. Hamming(7) indica il codice di Hamming di lunghezza 7, "Golay" abbrevia "codice di Golay", "X" significa esteso e "$*$" indica il codice duale. Orig. 417

[4] Nota di traduzione: la trattazione dell'enumeratore dei pesi è nel Capitolo 20; qui il vettore ne elenca i coefficienti.

Oggetto	Schema	Vettore di distribuzione
$S(2,3,7)$	$J(7,3)$	$(1,0,6,0)$
$S_2(2,5,11)$	$J(11,5)$	$(1,0,0,10,0,0)$
$S_2(3,6,12)$	$J(12,6)$	$(1,0,0,20,0,0,1)$
$S(5,6,12)$	$J(12,6)$	$(1,0,45,40,45,0,1)$
$S(4,7,23)$	$J(23,7)$	$(1,0,0,0,140,0,112,0)$
$S(5,8,24)$	$J(24,8)$	$(1,0,0,0,280,0,448,0,30)$
Hamming(7)	$H(7,2)$	$(1,0,0,7,7,0,0,1)$
X-Hamming(7)	$H(8,2)$	$(1,0,0,0,14,0,0,0,1)$
Golay binario	$H(23,2)$	$(1,0,0,0,0,0,0,253,506,0,0,1288,\ldots)$
X-Golay binario	$H(24,2)$	$(1,0,0,0,0,0,0,0,759,0,0,0,2576,0,\ldots)$
Golay ternario	$H(11,3)$	$(1,0,0,0,0,132,132,0,330,110,0,24)$
$*$-Golay ternario	$H(11,3)$	$(1,0,0,0,0,0,132,0,0,110,0,0)$

Teorema 30.3. Il vettore di distribuzione a di un sottoinsieme non vuoto di uno schema soddisfa

$$aQ \geq 0,$$

dove 0 è il vettore riga di $k+1$ zeri.

Dimostrazione. Sia $\varphi \in \mathbb{R}^X$ il vettore caratteristico di Y, cioè $\varphi(x) = 1$ se $x \in Y$ e 0 altrimenti. Allora

$$a_i = \frac{1}{|Y|}\varphi A_i \varphi^{\mathsf{T}}.$$

Poiché E_ℓ è idempotente e simmetrica,

$$\begin{aligned} 0 \leq \|\varphi E_\ell\|^2 &= (\varphi E_\ell)(\varphi E_\ell)^{\mathsf{T}} = \varphi E_\ell \varphi^{\mathsf{T}} \\ &= \frac{1}{N}\varphi \left(\sum_{i=0}^{k} Q_\ell(i) A_i \right) \varphi^{\mathsf{T}} = \frac{|Y|}{N} \sum_{i=0}^{k} Q_\ell(i) a_i. \end{aligned}$$

□ Per uso successivo osserviamo che nella disuguaglianza di indice ℓ vale l'uguaglianza se e solo se la proiezione φE_ℓ è il vettore nullo. La disuguaglianza di indice 0 è banale, perché la coordinata 0 di aQ è $a_0 + a_1 + \cdots + a_k$, naturalmente non negativa. Orig. 418

Esempio 30.8. Per $J(8,3)$, eliminate le frazioni, le disuguaglianze di Delsarte sono

$$\begin{aligned} 15 + 7a_1 - a_2 - 9a_3 &\geq 0, \\ 30 + 2a_1 - 5a_2 + 9a_3 &\geq 0, \\ 10 - 2a_1 + a_2 - a_3 &\geq 0. \end{aligned}$$

Sono condizioni necessarie per l'esistenza di una famiglia $\mathcal{F}$ di sottoinsiemi di tre elementi di un insieme di otto elementi con vettore di distribuzione $(1, a_1, a_2, a_3)$.

Possiamo chiederci cosa implichino su $|\mathcal{F}|$ supponendo nulli alcuni a_i. Per esempio, poniamo $a_3 = 0$, cioè nessuna coppia di membri di $\mathcal{F}$ è disgiunta. Il massimo di $1 + a_1 + a_2 = |\mathcal{F}|$ soggetto a queste disuguaglianze è 21; è un problema di programmazione lineare. Sapevamo già $|\mathcal{F}| \leq 21$ per il teorema di Erdős–Ko–Rado, Teorema 6.4. Il Teorema 30.3 implica il Teorema 6.4; si vedano le note.

Il Teorema 30.3 conduce a un limite di programmazione lineare per la cardinalità dei codici. Per lo schema $H(n,q)$, dato un intero d, consideriamo il problema:

massimizzare $1 + a_d + a_{d+1} + \cdots + a_n$ soggetto a $a_i \geq 0$ e

$$(1, 0, \ldots, 0, a_d, a_{d+1}, \ldots, a_n)Q \geq 0,$$

dove Q è la seconda matrice degli autovalori dello schema, di ordine $n+1$. Se lpb è questo massimo e C è un qualsiasi codice q-ario di lunghezza n con distanza minima almeno d, allora $|C| \leq$ lpb: il vettore di distribuzione di C soddisfa infatti i vincoli e le sue coordinate sommano a $|C|$.

Per gli schemi di Hamming, se a è il vettore di distribuzione di un codice lineare C, allora $\frac{1}{|C|}aQ$ è il vettore di distribuzione del duale $C^\perp$. Basta confrontare le formule del teorema di MacWilliams, Teorema 20.3, con quelle del Teorema 30.1(ii). Ciò spiega certamente perché $aQ \geq 0$ per un codice lineare, ma abbiamo provato che vale anche quando C non è lineare. Orig. 419

n	d	SPB	LPB	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
11	3	170.7	170.7	1	0	0	18.3	36.7	29.3	29.3	36.7	18.3	0	0	1				
11	5	30.6	24	1	0	0	0	0	11	11	0	0	0	0	1				
11	7	8.8	4	1	0	0	0	0	0	0	2	1	0	0	0				
12	3	315.1	292.6	1	0	0	20	45	48	56	65.1	40.7	11.4	3.4	1.7	0.1			
12	5	51.9	40	1	0	0	0	0	15	17.5	0	0	5	1.5	0	0			
12	7	13.7	5.3	1	0	0	0	0	0	0	2.7	1.7	0	0	0	0			
13	3	585.1	512	1	0	0	22	55	72	96	116	87	40	16	6	1	0		
13	5	89.0	64	1	0	0	0	0	18	24	4	3	10	4	0	0	0		
13	7	21.7	8	1	0	0	0	0	0	0	4	3	0	0	0	0	0		
14	3	1092.3	1024	1	0	0	28	77	112	168	232	203	112	56	28	7	0	0	
14	5	154.6	128	1	0	0	0	0	28	42	8	7	28	14	0	0	0	0	
14	7	34.9	16	1	0	0	0	0	0	0	8	7	0	0	0	0	0	0	
15	3	2048	2048	1	0	0	35	105	168	280	435	435	280	168	105	35	0	0	1
15	5	270.8	256	1	0	0	0	0	42	70	15	15	70	42	0	0	0	0	1
15	7	56.9	32	1	0	0	0	0	0	0	15	15	0	0	0	0	0	0	1

Figura 30.2

In generale è difficile estrarre informazioni utili dal limite di programmazione lineare, LPB; si può però mostrare che è sempre almeno altrettanto buono del limite dell'impacchettamento di sfere, SPB, Teorema 21.1; si veda Delsarte (1973). Per piccoli parametri si può usare l'algoritmo del simplesso e valutare esplicitamente il limite. Lo abbiamo fatto per alcuni n, d nel caso binario, riportando i risultati nella Figura 30.2. La tabella dà un vettore non negativo $(1, 0, \dots, 0, a_d, \dots, a_n)$ la cui somma è massima sotto il vincolo $aQ \geq 0$. È un buon esercizio cercare di stabilire se esistano davvero codici che raggiungono il limite della tabella. Vari esempi si possono ottenere da un interessante codice binario di lunghezza 16, il *codice di Nordstrom–Robinson*, con 256 parole e distanza minima 6. Non è lineare. Si vedano i Problemi 30I e 30J.

Sembra esserci una sorta di "dualità" fra le due basi dell'algebra di Bose–Mesner e fra i suoi prodotti ordinario e di Hadamard. Talvolta esiste un secondo schema in cui gli E_i, rispetto al prodotto di Hadamard, si comportano come gli A_i del primo rispetto al prodotto ordinario, a meno di un fattore scalare, e viceversa. Due schemi si dicono *formalmente duali* quando la prima matrice P dell'uno è uguale alla seconda matrice Q dell'altro; cfr. Problema 30E. Sono note molte coppie di grafi fortemente regolari formalmente duali. Lo schema di Hamming è formalmente duale a sé stesso. Lo schema di Johnson di solito non ha un duale formale, perché in generale i parametri di Krein definiti sotto non sono interi. Orig. 420

I *parametri di Krein* di uno schema sono i $(k+1)^3$ numeri q_{ij}^ℓ definiti da

$$NE_i \circ E_j = \sum_{\ell=0}^{k} q_{ij}^\ell E_\ell. \tag{30.7}$$

Se lo schema ha un duale formale, sono i parametri p_{ij}^ℓ del duale e quindi interi non negativi. Vale sempre

$$q_{ij}^\ell \geq 0 \qquad (0 \leq i, j, \ell \leq k),$$

perché sono, a meno di un fattore positivo, autovalori del prodotto di Hadamard di due matrici semidefinite positive, e dunque non negativi; cfr. Problema 21E. In linea di principio i parametri di Krein sono

funzioni dei parametri originali p_{ij}^{ℓ}, si veda il Problema 30E, e la loro non negatività è una condizione necessaria per l'esistenza di uno schema con parametri assegnati; lo abbiamo fatto per i grafi fortemente regolari nel Teorema 21.3.

Problema 30E. Mostrare come calcolare tutti i parametri q_{ij}^{ℓ} di uno schema a partire dalla matrice Q, cioè provare che sono univocamente determinati da essa.

Ci servirà sapere che

$$q_{ii}^{0} = m_i, \qquad q_{ij}^{0} = 0 \quad \text{per } i \neq j. \tag{30.8}$$

Segue da (30.7), considerando la somma di tutti gli elementi delle matrici nei due membri; la somma degli elementi a sinistra è N volte

Orig. 421

$$\langle E_i, E_j \rangle = \begin{cases} m_i & \text{se } i = j, \\ 0 & \text{altrimenti.} \end{cases}$$

Per certe applicazioni a codici e disegni dobbiamo conoscere più dettagli dello schema. Prima di specializzarci, ecco però un risultato interessante valido in generale.

Dato uno schema a k classi e un sottoinsieme $K \subseteq \{1, \dots, k\}$, un sottoinsieme Y dei punti si chiama *K-cricca* se ogni coppia di elementi distinti $x, y \in Y$ è costituita da j-esimi associati per qualche $j \in K$. Si chiama *K-cocricca* se nessuna coppia distinta è costituita da j-esimi associati con $j \in K$. Se G ha matrice di adiacenza $\sum_{j \in K} A_j$, le cricche di G sono esattamente le K-cricche dello schema e le cocricche, cioè gli insiemi indipendenti di vertici, sono le K-cocricche.

Teorema 30.4. Siano $A \subseteq X$ una K-cocricca e $B \subseteq X$ una K-cricca in uno schema a k classi su X, con $K \subseteq \{1, \dots, k\}$. Allora

$$|A|\,|B| \leq N.$$

Dimostrazione. Siano $a = (a_0, \dots, a_k)$ e $b = (b_0, \dots, b_k)$ i vettori di distribuzione di A, B. Invertiamo la prima equazione del Teorema 30.2, premoltiplichiamo per a e postmoltiplichiamo per b^{T}, ottenendo

$$aQ\,\mathrm{diag}(1, m_1, \dots, m_k)^{-1}(bQ)^{\mathsf{T}} = Na\,\mathrm{diag}(1, n_1, \dots, n_k)^{-1}b^{\mathsf{T}}. \tag{30.9}$$

Per il Teorema 30.3, aQ, bQ sono non negativi. Le loro coordinate di indice 0 sono rispettivamente $|A|, |B|$, quindi lo scalare a sinistra è almeno $|A|\,|B|$. L'ipotesi implica $a_i b_i = 0$ per $i > 0$, per cui lo scalare a destra è N. □

Un esempio di uguaglianza in $J(v, k)$ si ha quando esiste un $S(t, k, v)$. Prendiamo $K = \{1, 2, \dots, k-t\}$. I blocchi del sistema formano una K-cocricca; tutti i sottoinsiemi di k elementi contenenti un sottoinsieme fissato di t elementi formano una K-cricca. Un esempio di uguaglianza in $H(n, q)$ si ha quando esiste un codice perfetto C che corregge e errori. Prendiamo $K = \{1, \dots, 2e\}$. Allora C è una K-cocricca e una sfera di raggio e centrata in una parola fissata è una K-cricca.

Orig. 422

Problema 30F. Trovare un grafo regolare G, una cricca A e una cocricca B tali che $|A|\,|B| > |G|$.

Problema 30G. Dimostrare che, se A è una cricca e B una cocricca in un grafo G che ammette un gruppo transitivo di automorfismi, allora $|A|\,|B| \leq |G|$.

Definiamo ora gli *schemi polinomiali*, di due tipi. Uno schema, con una particolare numerazione $A_1, \dots, A_k$ delle matrici di associazione, si dice *P-polinomiale* se A_i è un polinomio di grado i in A_1 per $i = 0, 1, \dots, k$. Uno schema, con una particolare numerazione $E_1, \dots, E_k$ degli idempotenti, si dice *Q-polinomiale* se E_i è un polinomio di Hadamard di grado i in E_1: esiste cioè un polinomio di grado i che, applicato elemento per elemento a E_1, produce E_i.

Problema 30H. Dimostrare che uno schema di associazione è P-polinomiale se e solo se è metrico.

Gli schemi Q-polinomiali si chiamano anche *cometrici*, ma non sembra esserci una semplice interpretazione geometrica di questa parola. Useremo i termini metrico e cometrico invece di P-polinomiale e Q-polinomiale. Si può vedere che gli schemi di Hamming e Johnson sono cometrici; si veda Delsarte (1973).

Definiamo un *d-codice* in uno schema metrico come un sottoinsieme $S \subseteq X$ il cui vettore caratteristico φ soddisfa

$$\varphi A_i \varphi^{\mathsf{T}} = 0 \qquad (i = 1, 2, \dots, d-1).$$

Definiamo un *t-disegno* in uno schema cometrico come un sottoinsieme $S \subseteq X$ il cui vettore caratteristico soddisfa

$$\varphi E_i \varphi^{\mathsf{T}} = 0 \qquad (i = 1, 2, \ldots, t).$$

Il significato combinatorio di d-codice è immediato: nessuna coppia distinta di S è costituita da i-esimi associati con $i < d$. Nello schema di Hamming, quindi, S è un $(2e+1)$-codice se e solo se corregge e errori, cioè ha distanza minima almeno $2e+1$. Il significato combinatorio di t-disegno è meno chiaro e richiede una conoscenza più approfondita dello schema particolare. Si noti che S è un t-disegno se e solo se le prime t disuguaglianze non banali del Teorema 30.3 per il suo vettore di distribuzione sono uguaglianze, cioè $\varphi E_i = 0$ per $i = 1, \ldots, t$. Orig. 423

Il teorema seguente spiega che i disegni negli schemi di Johnson e Hamming corrispondono rispettivamente ai concetti classici di t-disegno e schieramento ortogonale. Uno *schieramento ortogonale* di indice λ e forza t su un insieme A di q simboli è un sottoinsieme $C \subseteq A^n$ di λq^t parole tale che, per ogni scelta di t delle n coordinate, ogni possibile t-upla di simboli di A compaia esattamente λ volte in quelle coordinate fra i membri di C.

Teorema 30.5. (i) Una famiglia S di sottoinsiemi di k elementi di un insieme di v elementi è un t-disegno come sottoinsieme di $J(v,k)$ se e solo se è l'insieme dei blocchi di un t-disegno classico.

(ii) Una famiglia S di n-uple su un alfabeto A di q elementi è un t-disegno come sottoinsieme di $H(n,q)$ se e solo se è l'insieme delle colonne di uno schieramento ortogonale di forza t.

Dimostrazione parziale. Mostreremo che la definizione negli schemi implica che S sia un t-disegno classico o uno schieramento ortogonale, lasciando al lettore le implicazioni inverse di entrambe le parti.

Sia S un t-disegno in $J(v,k)$ e sia φ il suo vettore caratteristico. Nell'Esempio 30.7 abbiamo visto che $E_0 + E_1 + \cdots + E_t$ è la proiezione ortogonale sullo spazio generato dai e_T con T sottoinsieme di t elementi. Il numero dei membri di S contenenti T è

$$\varphi e_T^{\mathsf{T}} = \varphi(E_0 + E_1 + \cdots + E_t) e_T^{\mathsf{T}} = \varphi E_0 e_T^{\mathsf{T}}.$$

Poiché E_0 è un multiplo scalare di J, questo numero è indipendente da T.

Sia ora S un t-disegno in $H(n,q)$ e φ il suo vettore caratteristico. Nell'Esempio 30.6 abbiamo descritto gli autospazi per $q = 2$, e proveremo il teorema soltanto in questo caso. Una dimostrazione completa è in Delsarte (1973). Orig. 424

Con la notazione dell'Esempio 30.6,

$$\langle \varphi, v_a \rangle = \sum_{b \in S} (-1)^{\langle a,b \rangle},$$

quindi S è un t-disegno se e solo se

$$\sum_{b \in S} (-1)^{\langle a,b \rangle} = 0 \quad \text{per ogni } a \neq 0 \text{ di peso } \leq t.$$

Per esempio, prendendo a di peso 1, l'equazione implica che in ogni coordinata metà dei membri di S ha 0 e metà 1. Prendendo a di peso 2, per esempio $(1,1,0,\ldots,0)$, implica che il numero dei membri che iniziano con 00 o 11 è uguale al numero di quelli che iniziano con 10 o 01. Insieme all'osservazione precedente, ciò dà che esattamente un quarto delle n-uple in S inizia con ciascuna fra 00,10,01,11.

In generale, fissiamo un insieme $T \subseteq \{1, \ldots, n\}$ di t coordinate. Per $I \subseteq T$, sia λ_I il numero di $a \in S$ con 1 nelle coordinate di I e 0 in quelle di $T \setminus I$. Per $J \subseteq T$, sia a_J l'n-upla binaria con 1 nelle coordinate di J e 0 nelle rimanenti $n - |J|$. Abbiamo 2^t equazioni lineari, una per ogni $J \subseteq T$:

$$\sum_{|I \cap J| \equiv 0 \pmod 2} \lambda_I - \sum_{|I \cap J| \equiv 1 \pmod 2} \lambda_I = \begin{cases} |S| & \text{se } J = \varnothing, \\ 0 & \text{altrimenti.} \end{cases}$$

Chiaramente $\lambda_I = |S|/2^t$ per ogni $I \subseteq T$ è una soluzione. Ma la matrice dei coefficienti è una matrice di Hadamard di ordine 2^t, si veda il Capitolo 18, ed è dunque non singolare: la soluzione è unica. Quindi S è uno schieramento ortogonale di forza t. □

I due prossimi teoremi sono "duali formali": le dimostrazioni sono simili, ma scambiano i ruoli delle basi A_i, E_i e dei prodotti ordinario e di Hadamard. Per gli schemi di Hamming il Teorema 30.6(i) si

riduce al limite dell'impacchettamento di sfere, Teorema 21.1, e la parte (iii) dà una condizione molto forte, dovuta a S. P. Lloyd (1957), perché valga l'uguaglianza: i codici perfetti del Capitolo 20. Per gli schemi di Johnson, il Teorema 30.7(i) si riduce al Teorema 19.8 e la parte (iii) dà una condizione molto forte, dovuta a Ray-Chaudhuri e Wilson (1975), per l'uguaglianza: i disegni stretti del Capitolo 19. Orig. 425

Teorema 30.6. Sia C un $(2e+1)$-codice in uno schema metrico a k classi su X, e sia $\varphi \in \mathbb{R}^X$ il suo vettore caratteristico.

(i) $|C| \le N/(1+n_1+\cdots+n_e)$.

(ii) Esistono almeno e indici $i \in \{1,\dots,k\}$ tali che $\varphi E_i \varphi^{\mathsf{T}} \neq 0$.

(iii) Vale l'uguaglianza in (i) se e solo se vale in (ii); in tal caso gli e indici i con $\varphi E_i \varphi^{\mathsf{T}} \neq 0$ sono esattamente gli interi per cui

$$\sum_{\ell=0}^{e} P_\ell(i) = 0.$$

Dimostrazione. Sia φ il vettore caratteristico di C e consideriamo

$$\alpha := \varphi(c_0A_0 + c_1A_1 + \cdots + c_eA_e)^2\varphi^{\mathsf{T}},$$

dove $c_0,\dots,c_e$ sono scalari. Valuteremo α in due modi. Introduciamo

$$f(i) := c_0P_0(i) + c_1P_1(i) + \cdots + c_eP_e(i)$$

come funzione dei c_j. Per (30.3), $\sum_{j=0}^{e} c_jA_j = \sum_{i=0}^{k} f(i)E_i$, quindi

$$\alpha = \left(\sum_{i=0}^{k} f(i)\varphi E_i\right)\left(\sum_{i=0}^{k} f(i)\varphi E_i\right)^{\mathsf{T}} = \sum_{i=0}^{k} f(i)^2 \varphi E_i \varphi^{\mathsf{T}}.$$

D'altra parte A_i è un polinomio di grado i in A_1, perciò $(A_0+A_1+\cdots+A_e)^2$ è un polinomio di grado $2e$ in A_1, e dunque combinazione lineare di $A_0,\dots,A_{2e}$. Per ipotesi $\varphi A_i \varphi^{\mathsf{T}} = 0$ per $i = 1,\dots,2e$. Per valutare α ci serve quindi soltanto il coefficiente di A_0 nel quadrato della combinazione lineare; da (30.2) e (30.1), Orig. 426

$$\alpha = \left(\sum_{i,j=0}^{e} c_ic_jp_{ij}^0\right)\varphi A_0\varphi^{\mathsf{T}} = \left(\sum_{i=0}^{e} c_i^2 n_i\right)|C|.$$

Per (30.6), $f(0) = c_0n_0 + c_1n_1 + \cdots + c_en_e$. Combinando i due valori e ricordando $E_0 = J/N$, da cui $\varphi E_0 \varphi^{\mathsf{T}} = |C|^2/N$, otteniamo

$$\begin{aligned}(c_0^2 + c_1^2n_1 + \cdots + c_e^2n_e)|C| &= \sum_{i=0}^{k} f(i)^2 \varphi E_i \varphi^{\mathsf{T}} \\ &\ge \frac{1}{N}(c_0 + c_1n_1 + \cdots + c_en_e)^2|C|^2.\end{aligned} \tag{30.10}$$

Tutto seguirà da (30.10). La parte (i) si ottiene ponendo tutti i $c_i = 1$.

Per (ii), supponiamo per assurdo che vi siano meno di e indici $i \ge 1$ con $\varphi E_i \varphi^{\mathsf{T}} \neq 0$. Per algebra lineare elementare esistono scalari $c_0,\dots,c_e$, non tutti nulli, tali che $f(i) = 0$ per $i = 0$ e per tutti gli indici con $\varphi E_i \varphi^{\mathsf{T}} \neq 0$. Ma (30.10) dà allora $|C|\sum_{i=0}^{e} n_ic_i^2 = 0$, assurdo.

Supponiamo l'uguaglianza in (i). Allora (30.10), con tutti i $c_i = 1$, mostra $f(i) = \sum_{\ell=0}^{e} P_\ell(i) = 0$ per gli almeno e valori di i con $\varphi E_i \varphi^{\mathsf{T}} \neq 0$. Affermiamo che $f(i) = 0$ non può valere per più di e indici. Infatti $f(0),\dots,f(k)$ sono gli autovalori di $A_0 + \cdots + A_e$, un polinomio di grado e in A_1: si ottengono valutando tale polinomio sugli autovalori $P_1(0),\dots,P_1(k)$ di A_1. La matrice A_1 ha $k+1$ autovalori distinti, perché genera un'algebra di dimensione $k+1$. L'affermazione segue dal fatto che un polinomio di grado e ha al più e zeri. Quindi vale l'uguaglianza in (ii) e (iii) è provato in questo caso. Infine, supponiamo l'uguaglianza in (ii). Scegliamo $c_0,\dots,c_e$ in modo che $f(i) = 0$ per tutti gli indici non banali con $\varphi E_i \varphi^{\mathsf{T}} \neq 0$ e $f(0) = 1$. Allora (30.10) dà $|C| = N(c_0^2 + c_1^2n_1 + \cdots + c_e^2n_e)$. La disuguaglianza di Cauchy–Schwarz dà Orig. 427

$$1 = \left(\sum_{i=0}^{e} c_in_i\right)^2 \le \left(\sum_{i=0}^{e} c_i^2n_i\right)\left(\sum_{i=0}^{e} n_i\right),$$

quindi $|C| \geq N/(1 + n_1 + \cdots + n_e)$. Vale dunque l'uguaglianza in (i). □

Corollario (Teorema di Lloyd). Se esiste un codice perfetto che corregge e errori, di lunghezza n su un alfabeto di q simboli, allora

$$L_e(x) := \sum_{i=0}^{e} (-1)^i (q-1)^{e-i} \binom{n-x}{e-i} \binom{x-1}{i}$$

ha e zeri interi distinti.

DIMOSTRAZIONE. È il Teorema 30.6(iii) per lo schema di Hamming. La somma $\sum_{\ell=0}^{e} P_\ell(x)$, con P_ℓ come nel Teorema 30.1(ii), si semplifica nel polinomio $L_e(x)$ scritto sopra. □

Esempio 30.9. Mostriamo che non vi sono codici binari perfetti non banali che correggono due errori. Se un tale codice ha lunghezza $n > 2$, la sua cardinalità è $2^n/(1 + n + \binom{n}{2})$, quindi $1 + n + \binom{n}{2} = 2^r$ per qualche intero r. È insolito che n abbia questa proprietà, ma può accadere, per esempio per $n = 90$. Dal Teorema 30.1(ii), per $H(n, 2)$,

$$P_0(x) + P_1(x) + P_2(x) = 2x^2 - 2(n+1)x + 1 + n + \binom{n}{2},$$

e il Teorema 30.6(iii) afferma che

$$x^2 - (n+1)x + 2^{r-1} = 0$$

ha due radici intere x_1, x_2. Devono essere $x_1 = 2^a$, $x_2 = 2^b$ per interi positivi a, b con $a + b = r - 1$ e $2^a + 2^b = n + 1$. Si verifica allora facilmente

$$(2^{a+1} + 2^{b+1} - 1)^2 = 2^{a+b+4} - 7.$$

Se $a, b \geq 2$, il primo membro è congruo a 1 modulo 16, il secondo a 9: assurdo. Il lettore può esaminare gli altri casi e troverà come unica possibilità $\{a, b\} = \{1, 2\}$, che dà $n = 5$. Orig. 428

Teorema 30.7. Sia D un $2s$-disegno in uno schema cometrico a k classi su X e sia $\varphi \in \mathbb{R}^X$ il suo vettore caratteristico.

(i) $|D| \geq 1 + m_1 + m_2 + \cdots + m_s$.

(ii) Vi sono almeno s indici $i \in \{1, \ldots, k\}$ con $\varphi A_i \varphi^{\mathsf{T}} \neq 0$.

(iii) Vale l'uguaglianza in (i) se e solo se vale in (ii); in tal caso gli s indici i con $\varphi A_i \varphi^{\mathsf{T}} \neq 0$ sono esattamente gli interi per cui

$$\sum_{\ell=0}^{s} Q_\ell(i) = 0.$$

DIMOSTRAZIONE. Sia φ il vettore caratteristico di D e consideriamo

$$\beta := \varphi\big[(c_0 E_0 + \cdots + c_s E_s) \circ (c_0 E_0 + \cdots + c_s E_s)\big]\varphi^{\mathsf{T}},$$

dove $c_0, \ldots, c_s$ sono scalari. Valuteremo β in due modi. Introduciamo

$$g(i) := \frac{1}{N}\big(c_0 Q_0(i) + c_1 Q_1(i) + \cdots + c_s Q_s(i)\big)$$

come funzione dei c_i. Per (30.4), $\sum_{j=0}^{s} c_j E_j = \sum_{i=0}^{k} g(i) A_i$, perciò

$$\beta = \varphi \left[\left(\sum_{i=0}^{k} g(i) A_i \right) \circ \left(\sum_{i=0}^{k} g(i) A_i \right) \right] \varphi^{\mathsf{T}} = \sum_{i=0}^{k} g(i)^2 \varphi A_i \varphi^{\mathsf{T}}.$$

[5] D'altra parte E_i è un polinomio di Hadamard di grado i in E_1, quindi il quadrato di Hadamard di $E_0 + \cdots + E_s$ è un polinomio di Hadamard di grado $2s$ in E_1, e dunque combinazione lineare di Orig. 429

[5] Nota di traduzione: nell'originale i fattori φ sono collocati dentro il prodotto di Hadamard di due vettori, dando un'espressione non conforme. Qui si esplicita il prodotto delle matrici, come richiede la definizione di β.

$E_0, \dots, E_{2s}$. L'ipotesi implica $\varphi E_i \varphi^{\mathsf{T}} = 0$ per $i = 1, \dots, 2s$. Per valutare β ci serve quindi soltanto il coefficiente di E_0 nel quadrato di Hadamard della combinazione lineare; per (30.7) e (30.8),

$$\beta = \left(\frac{1}{N} \sum_{i,j=0}^{s} c_i c_j q_{ij}^0 \right) \varphi E_0 \varphi^{\mathsf{T}} = \frac{1}{N^2} \left(\sum_{i=0}^{s} c_i^2 m_i \right) |D|^2.$$

Per (30.6), $g(0) = \frac{1}{N}(c_0 m_0 + c_1 m_1 + \cdots + c_s m_s)$. Combinando i due valori otteniamo

$$\begin{aligned} \frac{1}{N^2}(c_0^2 + c_1^2 m_1 + \cdots + c_s^2 m_s)|D|^2 &= \sum_{i=0}^{k} g(i)^2 \varphi A_i \varphi^{\mathsf{T}} \\ &\geq \frac{1}{N^2}(c_0 + c_1 m_1 + \cdots + c_s m_s)^2 |D|. \end{aligned} \tag{30.11}$$

[6] Tutto segue da (30.11) in modo analogo alla dimostrazione del Teorema 30.6. □

Problema 30I. Considerare il codice di Golay esteso G_{24}. Per comodità, ordinare le coordinate in modo che $c = (1, \dots, 1, 0, \dots, 0)$, con 1 nelle prime otto posizioni e 0 altrove, sia una parola del codice.

(i) Con argomenti di conteggio, mostrare che G_{24} contiene 30 parole di peso 8 senza 1 nelle prime otto posizioni, dunque a distanza 16 da c. Mostrare poi che tutte le parole senza 1 nelle prime otto posizioni formano un sottocodice essenzialmente uguale a $R(1, 4)$.

(ii) Sia A l'insieme delle 16-uple $(a_9, a_{10}, \dots, a_{24})$ ottenute eliminando le prime otto coordinate delle parole $a = (a_1, \dots, a_{24})$ di G_{24} per le quali il peso di $(a_1, \dots, a_7)$ è ≤ 1. Mostrare che A è un codice di lunghezza 16 con 256 parole e distanza minima 6.

(iii) Usare A per costruire esempi di codici che raggiungono il limite della Figura 30.2.

Orig. 430

Problema 30J. Mostrare che non esiste un codice lineare binario con parametri $[13, 6, 5]$. Quindi non esistono neppure codici lineari binari $[16, 8, 6]$.

Problema 30K. Il *grafo dispari* ha come vertici i sottoinsiemi di k elementi di un insieme di $2k + 1$ elementi, adiacenti se disgiunti. Per $k = 2$ è il grafo di Petersen.

(i) Mostrare che il grafo è regolare rispetto alla distanza.

(ii) Per $k = 3$, mostrare che i vertici "corrispondenti" al piano di Fano formano un codice perfetto nel grafo.

Problema 30L. Trovare tutti gli esempi di 3-codici perfetti nello schema di Johnson $J(v, 3)$. Tutti gli esempi sono banali.

Note

Gli schemi di associazione furono introdotti dagli statistici insieme ai disegni parzialmente bilanciati. Una struttura d'incidenza è parzialmente bilanciata rispetto a uno schema sui suoi punti quando ogni coppia di i-esimi associati compare in un numero costante λ_i di blocchi. Ne sono esempi le geometrie parziali del Capitolo 21. I disegni parzialmente bilanciati furono introdotti per aggirare la disuguaglianza di Fisher $b \geq v$, o equivalentemente $r \geq k$, che per essi non è necessariamente valida. Le replicazioni costano denaro o richiedono tempo, e r è il "numero di replicazioni": per ragioni pratiche lo si vuole piccolo.

Per analizzare un esperimento nel quale sia stato usato un certo disegno, cioè una struttura d'incidenza, occorre fare calcoli con NN^{T}, dove N è la matrice d'incidenza. Per i disegni parzialmente bilanciati questi calcoli si semplificano enormemente, perché in uno schema a m classi

$$NN^{\mathsf{T}} = \lambda_0 A_0 + \lambda_1 A_1 + \cdots + \lambda_m A_m$$

appartiene all'algebra di Bose–Mesner di piccola dimensione, anche se l'ordine delle matrici può essere molto maggiore di $m + 1$.

Le disuguaglianze di Delsarte implicano il teorema generale di Erdős–Ko–Rado: se $n \geq (t+1)(k-t+1)$ e $\mathcal{F}$ è una famiglia di sottoinsiemi di k elementi di un insieme di n elementi tali che ogni coppia si incontri in almeno t punti, allora $|\mathcal{F}| \leq \binom{n-t}{k-t}$. Si veda Wilson (1984a). Per ulteriori informazioni sulla non esistenza di codici perfetti si veda Van Lint (1999).

Orig. 431

[6] Nota di traduzione: l'originale usa $|C|$ al posto di $|D|$ in questo passaggio e, nell'ultimo membro di (30.11), scrive $1/N$ anziché $1/N^2$. Le correzioni seguono da $g(0)^2 \varphi A_0 \varphi^{\mathsf{T}} = g(0)^2 |D|$ e sono necessarie per ottenere (i).

Riferimenti bibliografici

E. Bannai and T. Ito (1984), *Association Schemes*, Benjamin/Cummings.

A. E. Brouwer, A. M. Cohen, and A. Neumaier (1989), *Distance Regular Graphs*, Springer-Verlag.

Ph. Delsarte (1973), *An Algebraic Approach to the Association Schemes of Coding Theory*, Philips Res. Rep. Suppl. **10**.

Ph. Delsarte (1975), The association schemes of coding theory, in: *Combinatorics (Proc. Nijenrode Conf.)*, M. Hall, Jr. and J. H. van Lint, eds., D. Reidel.

J. H. van Lint (1999), *Introduction to Coding Theory*, Third edition, Springer-Verlag.

S. P. Lloyd (1957), Binary block coding, *Bell System Tech. J.* **36**, 517–535.

D. K. Ray-Chaudhuri and R. M. Wilson (1975), On t-designs, *Osaka J. Math.* **12**, 737–744.

R. M. Wilson (1984a), The exact bound in the Erdős–Ko–Rado theorem, *Combinatorica* **4**, 247–257.

R. M. Wilson (1984b), On the theory of t-designs, pp. 19–50 in: *Enumeration and Design (Proceedings of the Waterloo Silver Jubilee Conference)*, D. M. Jackson and S. A. Vanstone, eds., Academic Press.

Capitolo 31

(Altre) tecniche algebriche nella teoria dei grafi

Nel capitolo 9 abbiamo applicato tecniche di algebra lineare alle matrici di adiacenza dei grafi, e nel capitolo 21 ne abbiamo fatto un uso esteso. Raccogliamo qui diverse altre eleganti applicazioni. Si veda anche il capitolo 36. Orig. 432

Un *torneo* è un orientamento di un grafo completo, cioè un grafo orientato tale che, per ogni coppia di vertici distinti x e y, vi sia uno spigolo da x a y, oppure uno spigolo da y a x, ma non entrambi. I tornei sono stati brevemente introdotti nel problema 3D. La matrice di adiacenza di un grafo orientato ha un 1 nella posizione (x, y) quando vi è uno spigolo da x a y, e 0 altrimenti.

Lemma 31.1. Il rango della matrice di adiacenza A di un torneo su n vertici è n oppure $n-1$.

Dimostrazione. La definizione di torneo assicura che $A + A^{\mathsf{T}} = J - I$, dove tutte le matrici sono $n \times n$. Supponiamo che il rango di A sia al più $n-2$. Esiste allora un vettore riga non nullo x tale che $xA = 0$ e $xJ = 0$. Calcoliamo quindi

$$0 = x(A + A^{\mathsf{T}})x^{\mathsf{T}} = x(J - I)x^{\mathsf{T}} = -xx^{\mathsf{T}} < 0,$$

in contraddizione con l'esistenza di x. □

Il teorema seguente è dovuto a R. L. Graham e H. O. Pollak. La loro dimostrazione originale applicava la legge di Sylvester, che avevano già utilizzato per dimostrare il teorema 9.1.

Teorema 31.2. Supponiamo che il grafo completo K_n possa essere espresso come unione di k sottografi $H_1, H_2, \ldots, H_k$, a spigoli disgiunti, ciascuno dei quali è un grafo bipartito completo. Allora $k \geq n-1$. Orig. 433

Dimostrazione. Orientiamo ciascun sottografo bipartito completo H_i dirigendone tutti gli spigoli da una delle due classi di colore all'altra. Si ottiene così un torneo su n vertici, la cui matrice di adiacenza A è la somma delle k matrici di adiacenza A_i dei grafi orientati H_i (ampliate a matrici $n \times n$ includendo tutti i vertici). Dopo un'opportuna rinumerazione dei vertici, la matrice di adiacenza di un tale sottografo bipartito completo orientato ha la forma a blocchi

$$\begin{pmatrix} O & J & O \\ O & O & O \\ O & O & O \end{pmatrix}$$

e, in particolare, ha rango 1. Ne segue che il rango di A è al più k; il lemma 31.1 completa la dimostrazione. □

Questo richiama il teorema di De Bruijn–Erdős, teorema 19.1, il quale afferma, in una terminologia del tutto diversa e con una dimostrazione del tutto diversa, che se K_n è unione di k sottografi completi a spigoli disgiunti, allora $k \geq n$. Non si conosce però alcuna dimostrazione del teorema 31.2 che non utilizzi l'algebra lineare.

Essendo una matrice simmetrica reale, la matrice di adiacenza $A = A(G)$ di un grafo finito G possiede una base ortogonale di autovettori. (Autovettori corrispondenti ad autovalori distinti sono necessariamente ortogonali.) Per "autovalori di G" intendiamo gli autovalori di $A(G)$. Ecco una breve tabella degli spettri, cioè degli elenchi completi degli autovalori, di alcuni grafi:

Grafo	Spettro
K_5	$4, -1, -1, -1, -1$
$K_{3,3}$	$3, 0, 0, 0, 0, -3$
Cubo	$3, 1, 1, 1, -1, -1, -1, -3$
Pentagono	$2, \frac{-1+\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}$
Grafo di Petersen	$3, 1, 1, 1, 1, 1, -2, -2, -2, -2$
$L_2(3)$	$4, 1, 1, 1, 1, -2, -2, -2, -2$
Grafo di Heawood	$3, \sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2},$ $-\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -3$

Orig. 434

(Il grafo di Heawood è il "grafo bipartito di incidenza" della configurazione di Fano: sette vertici rappresentano i punti e altri sette le rette. Lo incontreremo nuovamente nel capitolo 35.)

Grafi non isomorfi possono avere lo stesso spettro. Per esempio, nel capitolo 21 abbiamo ricordato che esistono quattro grafi fortemente regolari non isomorfi con i parametri di $T(8)$; cfr. il teorema 21.5.

Problema 31A. Mostrare che non è possibile trovare in K_{10} tre copie del grafo di Petersen a spigoli disgiunti. Suggerimento: se A_1, A_2, A_3 sono le matrici di adiacenza di tre sottografi di Petersen a spigoli disgiunti di K_{10}, tutte e tre hanno lo stesso spettro, tutte hanno come autovettore il vettore j con tutte le componenti uguali a 1, e $A_1 + A_2 + A_3 = J - I$.

Sia S una matrice simmetrica. L'espressione $xSx^{\mathsf{T}}/xx^{\mathsf{T}}$, per $x \neq 0$, si chiama *quoziente di Rayleigh*.[1] Sia $e_1, e_2, \ldots, e_n$ una base ortonormale di autovettori, con corrispondenti autovalori

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n.$$

Se scriviamo x in questa base, ponendo $x = a_1e_1 + \cdots + a_ne_n$, allora

$$\frac{xSx^{\mathsf{T}}}{xx^{\mathsf{T}}} = \frac{\lambda_1a_1^2 + \lambda_2a_2^2 + \cdots + \lambda_na_n^2}{a_1^2 + a_2^2 + \cdots + a_n^2}. \tag{31.1}$$

In particolare, per ogni x non nullo,

$$\lambda_1 \geq \frac{xSx^{\mathsf{T}}}{xx^{\mathsf{T}}} \geq \lambda_n.$$

Benché la maggior parte dei grafi che considereremo sia semplice, osserviamo che nulla impedisce di considerare nel seguito matrici di adiacenza di multigrafi (nelle quali l'elemento di riga x e colonna y è il numero di spigoli che congiungono x e y), oppure matrici di adiacenza di grafi "pesati" (nelle quali quell'elemento è un "peso" associato allo spigolo che congiunge x e y).

A prima vista sorprende che lo spettro di un grafo abbia qualche relazione con le sue proprietà più geometriche o combinatorie. Uno dei primi collegamenti osservati è il seguente teorema di A. J. Hoffman. Una *cocricca*, o *insieme indipendente di vertici*, di un grafo G è un insieme di vertici nessuno dei quali è adiacente a un altro dell'insieme.

Orig. 435

Teorema 31.3. Sia G un grafo su n vertici, regolare di grado d, e sia $\lambda_{\min}$ il suo minimo autovalore, che è dunque negativo. Allora, per ogni cocricca S di G,

$$|S| \leq \frac{-n\lambda_{\min}}{d - \lambda_{\min}}.$$

Dimostrazione. Siano A la matrice di adiacenza di G e $\lambda := \lambda_{\min}$. Allora $A - \lambda I$ è semidefinita positiva, cioè tutti i suoi autovalori sono non negativi; si osservi che i suoi autovettori coincidono con quelli di A. Uno di essi è $j := (1, 1, \ldots, 1)$ e si ha

$$j(A - \lambda I) = (d - \lambda)j.$$

Posto quindi

$$M := A - \lambda I - \frac{d - \lambda}{n}J,$$

avremo $jM = 0$. Ogni altro autovettore e di A può essere scelto ortogonale a j, cosicché $eJ = 0$, ed è allora anche un autovettore di M con autovalore non negativo. Anche M, dunque, è semidefinita positiva.

[1] Nota redazionale: nell'originale il cognome è scritto "Raleigh".

Sia ora ϕ il vettore caratteristico di una cocricca S costituita da m vertici di G: $\phi(x) = 1$ se $x \in S$ e 0 altrimenti. Allora $\phi A \phi^{\mathsf{T}} = 0$ e abbiamo

$$0 \le \phi M \phi^{\mathsf{T}} = -\lambda \phi \phi^{\mathsf{T}} - \frac{d-\lambda}{n} \phi J \phi^{\mathsf{T}} = -\lambda m - \frac{d-\lambda}{n} m^2.$$

Segue la disuguaglianza enunciata. □

Esistono estensioni e varianti del teorema 31.3 per grafi non regolari: si veda Haemers (1979).

Problema 31B. Applicare il teorema 31.3 al complementare di un grafo semplice regolare G per ottenere una maggiorazione della cardinalità di una cricca di G in funzione dello spettro. Trovare diversi esempi nei quali la maggiorazione sia raggiunta.

Problema 31C. Il *grafo degli spigoli* $L = L(G)$ di un grafo semplice G è stato introdotto nel capitolo 17. Per esempio, $L_2(m)$, definito nel capitolo 21, è il grafo degli spigoli di $K_{m,m}$; $T(m)$ è quello di K_m, e il grafo degli spigoli di un pentagono è un pentagono. (i) Mostrare che il grafo di Petersen non è il grafo degli spigoli di alcun grafo. (ii) Dimostrare che, se G ha più spigoli che vertici, il minimo autovalore del grafo degli spigoli $L(G)$ è -2. (Suggerimento: sia N la matrice di incidenza di G e si consideri $N^{\mathsf{T}}N$.) Orig. 436

L. Lovász (1979) osservò che la maggiorazione della cardinalità di una cocricca nel teorema 31.3 è anche una maggiorazione della cosiddetta *capacità di Shannon* di un grafo. Questo concetto nasce nella teoria dell'informazione. Supponiamo di voler utilizzare un insieme di "lettere" per trasmettere messaggi. Si assume che alcune coppie di lettere siano "confondibili". Diciamo che due possibili messaggi (parole, o stringhe di n di queste lettere) sono confondibili quando, in ciascuna posizione, le lettere sono identiche oppure confondibili. Cerchiamo un insieme di parole nessuna coppia delle quali sia confondibile.

Per formulare la questione nel linguaggio della teoria dei grafi, introduciamo il grafo G i cui vertici sono le lettere e nel quale due vertici sono adiacenti se e solo se le lettere sono confondibili. Un insieme di lettere a due a due non confondibili è dunque esattamente una cocricca di questo grafo. Il *prodotto forte* $G \otimes H$ di due grafi semplici G e H è il grafo semplice definito da $V(G \otimes H) := V(G) \times V(H)$, nel quale due vertici distinti (x_1, y_1) e (x_2, y_2) sono adiacenti quando x_1, x_2 sono uguali oppure adiacenti e y_1, y_2 sono uguali oppure adiacenti. I vertici di $G^n := G \otimes G \otimes \cdots \otimes G$ (n fattori) corrispondono alle parole di lunghezza n, e due di essi sono adiacenti in G^n precisamente quando le parole sono confondibili. Ci interessa quindi la cardinalità di una cocricca massima di G^n.

Il *numero di indipendenza* $\alpha(G)$ di un grafo G è la massima cardinalità di una sua cocricca. La capacità di Shannon di G è

$$\Theta(G) := \lim_{n\to\infty} (\alpha(G^n))^{1/n} = \sup_n (\alpha(G^n))^{1/n}.$$

L'esistenza del limite e la sua uguaglianza con l'estremo superiore seguono dall'osservazione che il prodotto di cocricche di G e H è una cocricca di $G \otimes H$, e dunque $\alpha(G^{k+m}) \ge \alpha(G^k)\alpha(G^m)$. (Si veda il lemma di Fekete nel capitolo 11.)

Esempio 31.1. Il problema di determinare la capacità di Shannon di grafi semplici quanto il pentagono P_5 rimase aperto per molti anni prima che Lovász riconoscesse l'utilità delle tecniche algebriche. È facile trovare 2^n parole di lunghezza n a due a due non confondibili, per esempio tutte le parole formate da 1 e 3. Ne segue $\Theta(P_5) \ge 2$. Non è un risultato particolarmente buono: in questo modo otteniamo soltanto quattro parole di lunghezza 2, mentre è facile trovarne cinque: Orig. 437

$$(1,1), \quad (2,3), \quad (3,5), \quad (4,2), \quad (5,4).$$

Per n pari possiamo prendere il prodotto di $n/2$ copie dell'insieme delle cinque parole precedenti, ottenendo $(\sqrt{5})^n$ parole di lunghezza n a due a due non confondibili; questo mostra che $\Theta(P_5) \ge \sqrt{5}$. Possiamo fare di meglio, magari per valori molto grandi di n? No: come vedremo dopo il teorema 31.6, $\Theta(P_5) \le \sqrt{5}$.

Ecco l'approccio di Lovász (1979). Osserviamo anzitutto che, con la definizione di prodotto di Kronecker del capitolo 18, per vettori $x, y \in \mathbb{R}^n$, $v, w \in \mathbb{R}^n$ si ha

$$(x \circ v)(y \circ w)^{\mathsf{T}} = \langle x, y \rangle \langle v, w \rangle. \tag{31.2}$$

Sia G un grafo. Per semplicità supporremo sempre che i suoi vertici siano $1, 2, \ldots, n$. Una *rappresentazione ortonormale* di G è un sistema $(v_1, \ldots, v_n)$ di vettori unitari di uno spazio euclideo tale che, se i e j

sono vertici non adiacenti, v_i e v_j siano ortogonali. Ogni grafo ha evidentemente una rappresentazione ortonormale, per esempio mediante vettori a due a due ortogonali.

Lemma 31.4. Siano $(u_1, \dots, u_n)$ e $(v_1, \dots, v_m)$ rappresentazioni ortonormali di G e H, rispettivamente. Allora i vettori $u_i \circ v_j$ formano una rappresentazione ortonormale di $G \otimes H$.

DIMOSTRAZIONE. È una conseguenza di (31.2). □

Definiamo il *valore* di una rappresentazione ortonormale $(u_1, \dots, u_n)$ come

$$\min_c \max_{1 \le i \le n} \frac{1}{\langle c, u_i \rangle^2},$$

dove c varia tra tutti i vettori unitari. Il vettore c che realizza il minimo si chiama *manico* della rappresentazione. Denotiamo con $\theta(G)$ il minimo dei valori di tutte le rappresentazioni di G. È facile vedere che tale minimo viene raggiunto. Una rappresentazione di valore $\theta(G)$ si dice *ottimale*.

Orig. 438

Lemma 31.5. $\theta(G \otimes H) \le \theta(G)\theta(H)$.

DIMOSTRAZIONE. Siano $(u_1, \dots, u_n)$ e $(v_1, \dots, v_m)$ rappresentazioni ortonormali ottimali di G e H, con manici c e d, rispettivamente. Per (31.2), $c \circ d$ è un vettore unitario e, ancora per (31.2),

$$\begin{aligned} \theta(G \otimes H) &\le \max_{i,j} \frac{1}{\langle c \circ d, u_i \circ v_j \rangle^2} \\ &= \max_{i,j} \frac{1}{\langle c, u_i \rangle^2} \cdot \frac{1}{\langle d, v_j \rangle^2} = \theta(G)\theta(H). \end{aligned}$$

(Si può dimostrare che in questo lemma vale l'uguaglianza.) □

Teorema 31.6. $\Theta(G) \le \theta(G)$.

DIMOSTRAZIONE. Mostriamo dapprima che $\alpha(G) \le \theta(G)$. Sia $(u_1, \dots, u_n)$ una rappresentazione ortonormale ottimale di G, con manico c. Supponiamo che $\{1, 2, \dots, k\}$ sia un insieme indipendente massimo di G: allora $u_1, \dots, u_k$ sono a due a due ortogonali. Pertanto

$$1 = \|c\|^2 \ge \sum_{i=1}^{k} \langle c, u_i \rangle^2 \ge \alpha(G)/\theta(G).$$

Da questo e dal lemma 31.5 ricaviamo $\alpha(G^n) \le \theta(G^n) \le \theta(G)^n$. □

Esempio 31.1, continuazione. Possiamo ora mostrare che $\Theta(C_5) = \sqrt{5}$ grazie a un'elegante idea di Lovász (1979). Consideriamo un ombrello il cui manico e le cui cinque stecche abbiano lunghezza unitaria. Aprendolo, passeremo per una posizione nella quale gli angoli tra stecche non adiacenti sono tutti $\pi/2$. Se chiamiamo c il manico e $u_1, \dots, u_5$ le stecche, orientandoli tutti a partire dal punto comune, allora $u_1, \dots, u_5$ è una rappresentazione ortonormale di C_5 in $\mathbb{R}^3$. Un semplice calcolo mostra che $\langle c, u_i \rangle = 5^{-1/4}$. Il teorema 31.6 e la definizione di $\theta(C_5)$ danno quindi il risultato.

Il risultato segue anche dal corollario seguente.

Corollario. Sia G un grafo su n vertici, regolare di grado d, e sia $\lambda_{\min}$ il suo minimo autovalore. Allora

$$\Theta(G) \le \frac{-n\lambda_{\min}}{d - \lambda_{\min}}.$$

Orig. 439

DIMOSTRAZIONE. Sia A la matrice di adiacenza di G. Nella dimostrazione del teorema 31.3 abbiamo visto che, posto $\lambda := \lambda_{\min}$, la matrice $M := A - \lambda I - \frac{d-\lambda}{n} J$ è semidefinita positiva (e singolare). Dunque $M = BB^{\mathsf{T}}$ per qualche matrice reale B di rango minore di n. Siano $x_1, \dots, x_n$ le righe di B; si ha

$$\langle x_i, x_i \rangle = -\lambda - \frac{d-\lambda}{n}, \qquad \langle x_i, x_j \rangle = -\frac{d-\lambda}{n},$$

la seconda uguaglianza quando i, j non sono adiacenti. Sia c un qualsiasi vettore unitario ortogonale alle righe x_i di B e definiamo

$$v_i := \frac{1}{\sqrt{-\lambda}} x_i + \frac{1}{\sqrt{-\lambda n/(d-\lambda)}} c.$$

Si verifichi che $v_1, \ldots, v_n$ è una rappresentazione ortogonale di G.[2] Infine, per ogni i,

$$\frac{1}{\langle c, v_i\rangle^2} = \frac{-\lambda n}{d-\lambda}.$$

Il risultato segue dal teorema 31.6. □

Presentiamo ora due applicazioni dell'*interlacciamento* degli autovalori.

Lemma 31.8. Sia A una matrice simmetrica di ordine n con autovalori

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n.$$

Supponiamo che N sia una matrice reale $m \times n$ tale che $NN^{\mathsf{T}} = I_m$, sicché $m \leq n$. Poniamo $B := NAN^{\mathsf{T}}$ e siano $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$ i suoi autovalori. Allora gli autovalori di B si interlacciano con quelli di A, nel senso che

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}, \qquad i = 1, 2, \ldots, m.$$

DIMOSTRAZIONE. Sia $e_1, \ldots, e_n$ una base ortonormale di autovettori di A corrispondenti a $\lambda_1, \ldots, \lambda_n$, e sia $f_1, \ldots, f_m$ una base ortonormale di autovettori di B corrispondenti a $\mu_1, \ldots, \mu_m$. Fissiamo i e consideriamo $U := \operatorname{span}\{f_1, \ldots, f_i\}$. Per (31.1), Orig. 440

$$\frac{xBx^{\mathsf{T}}}{xx^{\mathsf{T}}} \geq \mu_i$$

per ogni $x \in U$ non nullo. Poniamo $W := \{xN : x \in U\}$. Allora W è un sottospazio di dimensione i e

$$\frac{yAy^{\mathsf{T}}}{yy^{\mathsf{T}}} \geq \mu_i \tag{31.3}$$

per ogni $y \in W$. Scegliamo $y \neq 0$ in $W \cap \operatorname{span}\{e_i, e_{i+1}, \ldots, e_n\}$. Oltre a (31.3), abbiamo allora, per (31.1),

$$\frac{yAy^{\mathsf{T}}}{yy^{\mathsf{T}}} \leq \lambda_i,$$

e ciò dimostra $\lambda_i \geq \mu_i$.

Un ragionamento analogo, con $U := \operatorname{span}\{f_i, \ldots, f_m\}$, dimostra $\mu_i \geq \lambda_{n-m+i}$. □

Il termine interlacciamento risulta particolarmente naturale nel caso $m = n-1$, nel quale

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \lambda_3 \geq \cdots \geq \lambda_{n-1} \geq \mu_{n-1} \geq \lambda_n.$$

Un importante caso particolare del lemma 31.8 si ha quando le righe di N sono m vettori distinti della "base canonica" di lunghezza n, cioè con un solo 1 in ciascuna riga. La matrice B è allora semplicemente una sottomatrice principale $m \times m$ di A. L'osservazione seguente è dovuta a D. M. Cvetković.

Teorema 31.9. La cardinalità di una cocricca di un grafo G non può superare né il numero degli autovalori non negativi né quello degli autovalori non positivi di G.

DIMOSTRAZIONE. Se G possiede una cocricca di cardinalità m, la matrice di adiacenza A ha una sottomatrice principale $m \times m$ tutta nulla. Se gli autovalori di A sono $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, per l'interlacciamento $\lambda_m \geq 0$ e $0 \geq \lambda_{n-m+1}$; pertanto A ha almeno m autovalori maggiori o uguali a 0 e almeno m minori o uguali a 0. □

Il teorema seguente è un risultato di A. J. Hoffman sul numero cromatico di un grafo. Osserviamo che, per grafi regolari, esso seguirebbe dal teorema 31.3. Orig. 441

Teorema 31.10. Siano $\lambda_1 \geq \cdots \geq \lambda_n$ gli autovalori di un grafo G. Allora

$$\chi(G) \geq 1 + \lambda_1/(-\lambda_n).$$

[2] Nota redazionale: per la definizione e per il calcolo delle norme, la rappresentazione qui costruita è ortonormale nel senso del testo.

DIMOSTRAZIONE. Supponiamo che G ammetta una colorazione propria con m colori. Le classi di colore inducono una partizione della matrice di adiacenza

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mm} \end{pmatrix},$$

dove A_{ij} è la sottomatrice costituita dalle righe indicizzate dai vertici di colore i e dalle colonne indicizzate dai vertici di colore j. Ciascun blocco diagonale A_{ii} è una matrice quadrata nulla.

Sia e un autovettore di A corrispondente all'autovalore massimo λ_1, e scriviamo $e = (e_1, \dots, e_m)$, dove e_i ha le coordinate indicizzate dai vertici di colore i. Poniamo

$$N := \begin{pmatrix} e_1/\|e_1\| & 0 & 0 & \cdots \\ 0 & e_2/\|e_2\| & 0 & \cdots \\ 0 & 0 & e_3/\|e_3\| & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

(matrice $m \times n$) e $B := NAN^{\mathsf{T}}$. Per il lemma 31.8, gli autovalori $\mu_1, \dots, \mu_m$ di B si interlacciano con quelli di A e sono quindi compresi tra λ_1 e λ_n. D'altra parte, abbiamo costruito B in modo che λ_1 ne sia un autovalore, poiché

$$(\|e_1\|, \dots, \|e_m\|)B = eAN^{\mathsf{T}} = \lambda_1 eN^{\mathsf{T}} = \lambda_1(\|e_1\|, \dots, \|e_m\|).$$

Infine gli elementi diagonali di B sono nulli, perciò

$$0 = \operatorname{tr}(B) = \mu_1 + \cdots + \mu_m \geq \lambda_1 + (m-1)\lambda_n.$$

Questo dimostra il teorema. (Avremmo però dovuto forse precisare che, se alcuni e_i sono nulli, le corrispondenti righe non vanno incluse in N.) □

Orig. 442

Problema 31D. Mostrare che, per ogni grafo finito G, $\chi(G) \leq 1 + \lambda_1$, dove λ_1 è il massimo autovalore di G. Suggerimento: considerare i gradi di un sottografo indotto di G minimale tra quelli aventi lo stesso numero cromatico di G.

Oltre a essere simmetrica, la matrice di adiacenza di un grafo è anche una matrice non negativa. Esiste un'utile teoria di queste matrici, al cui centro si trova il teorema di Perron–Frobenius, teorema 31.11 qui sotto. Una dimostrazione completa si trova in Gantmacher (1959).

Una matrice quadrata A, le cui righe e colonne siano indicizzate da un insieme X, si dice *irriducibile* quando non è possibile trovare un sottoinsieme proprio S di X tale che $A(x, y) = 0$ per ogni $x \in S$ e $y \in X \setminus S$.[3] Equivalentemente, A non è irriducibile se e solo se è possibile applicare una stessa permutazione a righe e colonne ottenendo una matrice della forma

$$\begin{pmatrix} B & O \\ C & D \end{pmatrix},$$

dove B e D sono quadrate e hanno ordine almeno 1. Dovrebbe essere chiaro che, se A è la matrice di incidenza di un grafo, essa è irriducibile se e solo se il grafo è connesso.[4]

Problema 31E. Sia D un grafo orientato finito. Sia A la matrice di adiacenza di D, oppure una qualsiasi matrice le cui righe e colonne siano indicizzate dai vertici di D, con $A(x, y) = 0$ se non vi sono spigoli orientati da x a y e $A(x, y) > 0$ se ve ne sono. (i) Mostrare che $A^k(x, y) > 0$ se e solo se in D esiste una passeggiata orientata di lunghezza k da x a y. (ii) Mostrare che A è irriducibile se e solo se D è fortemente connesso, cioè se e solo se, per ogni coppia di vertici x, y di D, esiste un cammino orientato da x a y.

Teorema 31.11 (Perron–Frobenius). Sia A una matrice non negativa irriducibile $n \times n$. A meno di multipli scalari, esiste un unico autovettore $a = (a_1, \dots, a_n)$ le cui coordinate a_i siano tutte non negative. Le coordinate di questo vettore sono, in realtà, strettamente positive. L'autovalore corrispondente λ, detto *autovalore dominante* di A, ha molteplicità algebrica 1 e soddisfa $\lambda \geq |\mu|$ per ogni autovalore μ di

A. Dimostrazione parziale. Omettiamo la dimostrazione dell'esistenza di un autovettore non negativo, ma mostriamo come interviene l'irriducibilità e diamo gran parte del resto della dimostrazione. Orig. 443

Mostreremo che ogni autovettore non negativo a di A, corrispondente a un autovalore λ, è positivo in tutte le coordinate. Consideriamo A come matrice di un grafo orientato fortemente connesso, come nel problema 31E. Poiché da ogni vertice a ogni altro esiste un cammino orientato di lunghezza al più $n-1$,

$$I + A + A^2 + \cdots + A^{n-1} > O.$$

Qui e nel seguito una disuguaglianza tra matrici o vettori si intende valida in ogni coordinata. Poiché $a \geq 0$ ma $a \neq 0$,

$$0 < a(I + A + A^2 + \cdots + A^{n-1}) = (1 + \lambda + \cdots + \lambda^{n-1})a,$$

e quindi $0 < a$.

Mostriamo poi che l'autovalore λ ha molteplicità geometrica 1, ossia che il suo autospazio ha dimensione 1. Sia a' un qualsiasi autovettore corrispondente a λ, con coordinate positive, negative o nulle. Sommando o sottraendo ad a piccoli multipli scalari di a', otteniamo altri autovettori positivi o non negativi $a - ca'$ corrispondenti a λ. Possiamo scegliere c in modo che $a + ca' \geq 0$, ma almeno una coordinata sia nulla. Ciò contraddice il risultato del paragrafo precedente, a meno che $a - ca' = 0$.[5] Omettiamo la dimostrazione che λ ha molteplicità algebrica 1, cioè è uno zero semplice del polinomio caratteristico.

Sia a l'autovettore positivo di A, con autovalore λ, e sia b quello positivo di A^T; poniamo $Ab^\mathsf{T} = \nu b^\mathsf{T}$. Allora

$$\lambda ab^\mathsf{T} = (aA)b^\mathsf{T} = a(Ab^\mathsf{T}) = \nu ab^\mathsf{T}.$$

Ciò è impossibile a meno che $\nu = \lambda$, dunque $Ab^\mathsf{T} = \lambda b^\mathsf{T}$. Supponiamo che u sia un autovettore di A non proporzionale ad a, con $uA = \mu u$ e $\mu \neq \lambda$. Allora

$$\lambda ub^\mathsf{T} = u(Ab^\mathsf{T}) = (uA)b^\mathsf{T} = \mu ub^\mathsf{T},$$

il che implica $ub^\mathsf{T} = 0$. Nessun altro autovettore u può dunque avere coordinate non negative. Poniamo ora $\widehat{u} := (|u_1|, \ldots, |u_n|)$ e verifichiamo che da $A \geq O$ segue facilmente $\widehat{u}A \geq |\mu|\widehat{u}$. Quindi Orig. 444

$$\lambda \widehat{u}b^\mathsf{T} = \widehat{u}(Ab^\mathsf{T}) = (\widehat{u}A)b^\mathsf{T} \geq |\mu|\widehat{u}b^\mathsf{T},$$

da cui $\lambda \geq |\mu|$. □

Teorema 31.12. Sia λ l'autovalore dominante di un grafo connesso G. Allora G è bipartito se e solo se anche $-\lambda$ è un autovalore di G.

Dimostrazione. Supponiamo dapprima G bipartito. Rinumerando, se necessario, i vertici in modo che le classi di colore siano costituite dai primi k e dagli ultimi $n-k$ vertici, la matrice di adiacenza ha la forma

$$A = \begin{pmatrix} O & B \\ B^\mathsf{T} & O \end{pmatrix},$$

dove B è $k \times (n-k)$. Sia e un autovettore corrispondente all'autovalore μ, e scriviamo $e = (e_1, e_2)$, con e_1 formato dalle prime k coordinate. Si verifica che $(e_1, -e_2)$ è allora un autovettore di autovalore $-\mu$. Quindi, se G è bipartito, connesso o meno, il suo spettro è simmetrico rispetto a 0.

Supponiamo ora che λ sia l'autovalore dominante di un grafo connesso G e che anche $-\lambda$ sia un autovalore. Sia $e = (e_1, -e_2)$ un autovettore unitario corrispondente a $-\lambda$, avendo numerato i vertici in modo che e_1 ed e_2 abbiano entrambi tutte le coordinate non negative. Partizioniamo conformemente la matrice di adiacenza:

$$A = \begin{pmatrix} B & C \\ D & E \end{pmatrix}.$$

Allora

$$-\lambda = eAe^\mathsf{T} = e_1 Be_1^\mathsf{T} + e_2 Ee_2^\mathsf{T} - e_1 Ce_2^\mathsf{T} - e_2 De_1^\mathsf{T},$$

e dunque

$$(e_1, e_2)A(e_1, e_2)^\mathsf{T} \geq \lambda \tag{31.4}$$

con uguaglianza se e solo se Orig. 445

[3] Nota redazionale: si intende un sottoinsieme proprio non vuoto, come chiarisce subito la formulazione equivalente a blocchi.

[4] Nota redazionale: l'originale scrive "incidence matrix"; qui deve intendersi la matrice di adiacenza, che è quadrata e ha righe e colonne indicizzate dai vertici.

[5] Nota redazionale: l'originale alterna qui $a - ca'$ e $a + ca'$. Il ragionamento usa un unico segno: si sceglie il multiplo in modo da raggiungere il bordo del cono dei vettori non negativi.

$$e_1 B e_1^{\mathsf{T}} = e_2 E e_2^{\mathsf{T}} = 0. \tag{31.5}$$

L'equazione (31.1) e il fatto che λ sia l'autovalore dominante implicano che in (31.4) debba valere l'uguaglianza e che (e_1, e_2) sia un autovettore corrispondente a λ. Il teorema 31.11 implica allora che tutte le sue coordinate siano positive. Infine (31.5) dà $B = E = O$, e questo significa che G è bipartito. □

Teorema 31.13. Sia G un grafo finito e sia A la sua matrice di adiacenza. Esiste un polinomio $f(x)$ tale che $f(A) = J$ se e solo se G è connesso e regolare.

DIMOSTRAZIONE. Supponiamo che $f(A) = J$ per qualche polinomio $f(x)$. Poiché polinomi in una stessa matrice commutano, $AJ = JA$. L'elemento di riga x e colonna y di AJ è $\deg_G(x)$; quello nella stessa posizione di JA è $\deg_G(y)$. Quindi G è regolare.

Se $f(A) = J$, per ogni x, y deve in particolare esistere un k tale che $A^k(x, y) \neq 0$. L'elemento di riga x e colonna y di A^k è il numero delle passeggiate di lunghezza k da x a y in G. Quindi G è connesso.

Supponiamo ora che G sia connesso e regolare di grado d. Allora j è un autovettore di A corrispondente a d. Per il teorema 31.11, tale autovalore ha molteplicità uno. Per ogni matrice simmetrica M, la matrice della proiezione ortogonale su uno qualsiasi dei suoi autospazi è un polinomio in M; esplicitamente, se $(x - \mu_1)(x - \mu_2) \cdots (x - \mu_k)$ è il polinomio minimo di M, si lascia per esercizio mostrare che

$$\frac{(M - \mu_2 I) \cdots (M - \mu_k I)}{(\mu_1 - \mu_2) \cdots (\mu_1 - \mu_k)}$$

è la proiezione ortogonale sull'autospazio $\{a : aM = \mu_1 a\}$. Poiché la proiezione ortogonale sul sottospazio generato da j è $\frac{1}{v} J$, questa matrice è un polinomio in A.[6] □

Grafi isomorfi hanno gli stessi autovalori ma, come già ricordato, il viceversa non è vero: grafi non isomorfi possono avere lo stesso spettro (multinsieme di autovalori). Si veda il problema 21O. Possiamo però avere un viceversa parziale, in particolare per i "grafi circolanti" con un numero primo di vertici. Sia G un gruppo abeliano, scritto additivamente. Per $S \subseteq G$, il *grafo di Cayley* $\Gamma(G, S)$ ha insieme dei vertici G, e vi è uno spigolo orientato da x a y se e solo se $y - x \in S$. I grafi di Cayley sono comparsi numerose volte nei capitoli precedenti. Un grafo di Cayley può essere considerato non orientato quando $-S = S$, e non ha cappi quando $0 \notin S$. Un *grafo circolante* è un grafo di Cayley $\Gamma(G, S)$ con G ciclico. Orig. 446

(I grafi di Cayley possono essere definiti anche per gruppi non abeliani, ma nel seguito consideriamo soltanto il caso abeliano.)

Una *G-matrice* è una matrice quadrata A le cui righe e colonne sono indicizzate dagli elementi di G e tale che, per un certo vettore di oggetti $(a_g : g \in G)$, si abbia $A(i, j) = a_{j-i}$. Una *matrice circolante*, o semplicemente *circolante*, è una G-matrice con G ciclico. In generale, la matrice di adiacenza di un grafo di Cayley basato su G è una G-matrice.

Osserviamo che le G-matrici su un anello R sono chiuse rispetto alla moltiplicazione e che l'algebra di tali matrici è isomorfa all'anello di gruppo $R[G]$ del capitolo 28.

Proposizione 31.14. Sia ω una radice primitiva n-esima dell'unità in un campo F, e sia U la matrice con righe e colonne indicizzate da $\mathbb{Z}_n$, con $U(i, j) = \omega^{ij}$. Sia A la circolante basata sugli elementi $(a_i : i \in \mathbb{Z}_n)$ di F. Allora UAU^{-1} è la matrice diagonale con elementi diagonali

$$\lambda_j := \sum_{i=0}^{n-1} a_i \omega^{ji}, \qquad j = 0, 1, \ldots, n-1.$$

Gli autovalori di A sono dunque $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ e gli autovettori corrispondenti sono le righe di U.[7]

Problema 31F. (i) Dimostrare la proposizione 31.14. (ii) Per chi conosce i caratteri di un gruppo abeliano: mostrare che gli autovalori di una G-matrice razionale A sono $\lambda_\chi = \sum_{g \in G} a_g \chi(g)$, al variare di χ tra i caratteri di G. Cfr. l'esempio 30.6.

Il risultato seguente proviene da Elspas e Turner (1970).

Teorema 31.15. Siano A e B matrici circolanti razionali di ordine primo $p > 2$, basate rispettivamente sui vettori $(a_i : i \in \mathbb{Z}_p)$ e $(b_i : i \in \mathbb{Z}_p)$. Se A e B hanno lo stesso spettro, allora esiste $t \neq 0$ in $\mathbb{Z}_p$ tale che Orig. 447

[6] Nota redazionale: qui v è il numero dei vertici, indicato con n in altri passi del capitolo.

[7] Nota redazionale: con la convenzione $A(i, j) = a_{j-i}$ e autovettori riga, il calcolo diretto dà $\sum_i a_i \omega^{-ji}$ sulla diagonale di UAU^{-1}. Il multinsieme degli autovalori enunciato resta invariato, sostituendo j con $-j$; si conserva qui la formulazione originale.

$a_i = b_{ti}$ per ogni $i \in \mathbb{Z}_p$, leggendo gli indici modulo p.

DIMOSTRAZIONE. Sia ω una radice complessa primitiva p-esima dell'unità. Per la proposizione 31.14, $\alpha := \sum_{i=0}^{p-1} a_i\omega^i$ è un autovalore di A, quindi è uno degli autovalori di B, e dunque

$$\sum_{i=0}^{p-1} a_i\omega^i = \sum_{i=0}^{p-1} b_i\omega^{si}$$

per qualche s.[8]

Supponiamo dapprima $s \neq 0$ e scegliamo t tale che $st \equiv 1 \pmod{p}$. Allora

$$\sum_{i=0}^{p-1}(a_i - b_{ti})\omega^i = 0.$$

Poiché il polinomio minimo di ω sui razionali è $1 + x + x^2 + \cdots + x^{p-1}$, possiamo concludere che esiste una costante c tale che $a_i - b_{ti} = c$ per ogni i. Le tracce di A e B, che devono essere uguali, sono rispettivamente pa_0 e pb_0. Quindi $a_0 = b_0$, e allora $c = 0$.

Se $s = 0$, α è razionale e

$$(a_0 - \alpha) + a_1\omega + \cdots + a_{p-1}\omega^{p-1} = 0.$$

Concludiamo che tutti i coefficienti precedenti sono uguali a una costante c; ciò significa $A = \alpha I + cJ$.

Ripetiamo il ragionamento scambiando i ruoli di A e B, e troviamo che vale l'enunciato del teorema oppure $B = \beta I + dJ$ per certi numeri razionali β, d.

Gli autovalori di $aI + bJ$ sono $a + pb$, di molteplicità 1, e $a + b$, di molteplicità $p - 1$.[9] Se $A = \alpha I + cJ$ e $B = \beta I + dJ$ hanno lo stesso spettro e $p > 2$, segue $A = B$ e il teorema vale per ogni t. □

Osserviamo che per $p = 2$ l'enunciato non è valido, poiché, per esempio, le circolanti

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \text{e} \qquad \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

hanno lo stesso spettro $\{2, 0\}$. È però valido se A e B sono entrambe non negative.

Orig. 448

Corollario. Grafi circolanti di ordine primo sono isomorfi se e solo se essi, cioè le loro matrici di adiacenza, hanno gli stessi autovalori.

DIMOSTRAZIONE. Abbiamo già affermato che grafi isomorfi hanno lo stesso spettro.

Supponiamo che i grafi circolanti $\Gamma(\mathbb{Z}_p, S)$ e $\Gamma(\mathbb{Z}_p, T)$, con $S, T \subseteq \mathbb{Z}_p$ e p primo, abbiano matrici di adiacenza A, B con lo stesso spettro. Qui A è la circolante basata su $(a_i : i \in \mathbb{Z}_p)$, dove $a_i = 1$ se $i \in S$ e $a_i = 0$ altrimenti; analogamente B è basata su $(b_i : i \in \mathbb{Z}_p)$, con $b_i = 1$ se $i \in T$ e 0 altrimenti. Il teorema 31.15 (per $p = 2$ occorre l'osservazione) dice che $a_i = b_{ti}$ per qualche $t \neq 0$. La permutazione $\phi : i \mapsto ti$ di $\mathbb{Z}_p$ è allora un isomorfismo di $\Gamma(\mathbb{Z}_p, S)$ su $\Gamma(\mathbb{Z}_p, T)$ perché

$$\begin{aligned} i \to j \text{ in } \Gamma(\mathbb{Z}_p, S) &\iff i - j \in S \\ &\iff t(i - j) \in T \iff ti \to tj \text{ in } \Gamma(\mathbb{Z}_p, T), \end{aligned}$$

dove $x \to y$ significa che esiste uno spigolo orientato da x a y.[10] □

Corollario. Dati $S, T \subseteq \mathbb{Z}_p$, i grafi circolanti $\Gamma(\mathbb{Z}_p, S)$ e $\Gamma(\mathbb{Z}_p, T)$ sono isomorfi se e solo se $T = tS$ per un "moltiplicatore" $t \neq 0$ in $\mathbb{Z}_p$.

DIMOSTRAZIONE. Se i due grafi sono isomorfi, hanno lo stesso spettro; come nella dimostrazione del corollario precedente, $a_i = b_{ti}$ per un $t \neq 0$, il che significa $T = tS$.

Viceversa, se $T = tS$, abbiamo già visto che $\phi : i \mapsto ti$ è un isomorfismo. □

[8] Nota redazionale: nelle prime somme di questa dimostrazione l'originale scrive $n - 1$ invece di $p - 1$; si rende esplicito l'ordine p fissato nell'enunciato.

[9] Nota redazionale: il secondo autovalore è a, non $a + b$; sui vettori ortogonali a j la matrice J agisce infatti come zero. Questo refuso non altera la conclusione della dimostrazione.

[10] Nota redazionale: secondo la definizione a p. 446, la differenza nelle equivalenze deve essere $j - i$, non $i - j$. La dimostrazione dell'isomorfismo resta valida sostituendo coerentemente questa differenza.

Si era congetturato che il corollario precedente restasse valido sostituendo p con un intero qualsiasi n e la condizione $t \neq 0$ con $(t, n) = 1$, ma esistono controesempi per $n = 8, 9$ e altri valori. In realtà, il corollario con n al posto di p vale esattamente quando n è privo di fattori quadrati oppure è quattro volte un numero dispari privo di fattori quadrati. Si veda M. Muzychuk (1997).

Problema 31G. Dimostrare che i vertici di ogni grafo semplice finito possono essere colorati di rosso e di blu in modo che ogni vertice rosso sia adiacente a un numero pari di vertici rossi e ogni vertice blu a un numero dispari di vertici rossi. Dimostrare prima il lemma: se $S = (a_{ij})$ è una matrice simmetrica a elementi $0, 1$, la sua diagonale $a = (a_{11}, a_{22}, \ldots, a_{nn})$, considerata come vettore colonna, appartiene allo spazio generato dalle colonne di S sul campo $\mathbb{F}_2$. Orig. 449

Problema 31H. Sia G un grafo connesso regolare con esattamente tre autovalori distinti. Mostrare che G è fortemente regolare.

Problema 31I. Sia G un grafo fortemente regolare non banale e, per $x \in V(G)$, sia $\Delta(x)$ il sottografo indotto dai vertici non adiacenti a x. Dimostrare che $\Delta(x)$ è connesso: (1) spiegando perché $k-\mu$ sarebbe un autovalore di G se $\Delta(x)$ non fosse connesso; (2) verificando mediante un calcolo che $k - \mu$ non è un autovalore di G.

Problema 31J. Supponiamo che il grafo di Petersen P sia l'unione di sottografi ricoprenti H, K, regolari di grado rispettivamente 1 e 2. Siano A la matrice di adiacenza di P e B, C quelle di H, K, cosicché $A = B + C$.

Mostrare che esiste un vettore u che è autovettore di A per l'autovalore 1 e contemporaneamente autovettore di B per l'autovalore -1 (quindi autovettore di C per l'autovalore 2). Spiegare poi perché K non possa essere connesso. (Questo mostra che P non è hamiltoniano.)

Problema 31K. Sia G un grafo orientato su n vertici, senza spigoli multipli. Consentiamo che compaiano simultaneamente gli spigoli $a \to b$ e $b \to a$, nel qual caso chiamiamo $\{a, b\}$ uno spigolo non orientato. Supponiamo che, per ogni coppia di vertici a, b, vi sia esattamente una passeggiata di lunghezza 3 da a a b quando $a \neq b$, e nessuna quando $a = b$. Se A è la matrice di adiacenza di G, la proprietà si esprime mediante

$$A^3 = J - I. \tag{31.6}$$

(i) Dimostrare che G è regolare; (ii) se c è la valenza di G, mostrare che $n = c^3 + 1$; (iii) dimostrare che G ha esattamente $\frac{1}{2}(c^2 + c)$ spigoli non orientati; (iv) costruire un esempio per $n = 9$.

Note

Il teorema 31.3 non fu mai pubblicato da Hoffman, uno dei primi "teorici algebrici dei grafi", ma colpì l'immaginazione di molti di coloro che ne vennero a conoscenza ed è divenuto un classico. Il problema 31D è un risultato di H. Wilf. Il problema 31A è un risultato inedito di A. J. Schwenk. Orig. 450

Riferimenti bibliografici

- N. Biggs (1974), *Algebraic Graph Theory*, Cambridge University Press.
- D. M. Cvetković, M. Doob e H. Sachs (1979), *Spectra of Graphs, a Monograph*, V. E. B. Deutscher Verlag der Wissenschaften.
- B. Elspas e J. Turner (1970), Graphs with circulant adjacency matrices, *J. Combinatorial Theory* **9**, 297–307.
- F. R. Gantmacher (1959), *The Theory of Matrices*, Chelsea.
- W. Haemers (1979), *Eigenvalue Techniques in Design and Graph Theory*, Mathematisch Centrum, Amsterdam.
- L. Lovász (1979), On the Shannon capacity of a graph, *IEEE Trans. Information Theory* **25**, 1–7.
- M. Muzychuk (1997), On Adam's conjecture for circulant graphs, *Discrete Math.* **176**, 285–298.

Capitolo 32

Connessione dei grafi

Orig. 451

Per $k \geq 2$, un grafo G si dice *k-connesso rispetto ai vertici*, o semplicemente *k-connesso*, quando $|V(G)| \geq k+1$ e la rimozione da G di $k-1$ vertici qualsiasi (e degli spigoli incidenti) non produce un grafo sconnesso. Usiamo "1-connesso" come sinonimo di connesso.

Se un grafo G con almeno $k+1$ vertici non è k-connesso e la cancellazione di un insieme S di $k-1$ vertici lo sconnette, esiste una partizione di $V(G)\setminus S$ in insiemi non vuoti X, Y tra i quali non passa alcuno spigolo (con un estremo in X e l'altro in Y). Siano H, K i sottografi indotti da $X \cup S$ e $Y \cup S$, con l'eccezione che gli spigoli con entrambi gli estremi in S vanno assegnati a uno e uno solo tra H e K. Otteniamo così sottografi H, K a spigoli disgiunti, la cui unione è G, tali che $|V(H) \cap V(K)| = k-1$. Viceversa, se esistono tali sottografi e ciascuno contiene almeno un vertice oltre a quelli della loro intersezione, G non è k-connesso.

Un grafo si dice *non separabile* quando è 2-connesso e privo di cappi, oppure quando è un *grafo a fascio* (due vertici e un numero positivo qualsiasi di spigoli che li congiungono, compreso il *grafo-spigolo* con un unico spigolo), un *grafo-cappio* (uno spigolo che congiunge un unico vertice a se stesso), o un *grafo-vertice*. Tutti i poligoni, per esempio, sono non separabili; i grafi-cammino e gli altri alberi con almeno due spigoli non lo sono.

(Non vogliamo cappi, se vi sono altri spigoli, perché, anche se la cancellazione del vertice incidente può non sconnettere il grafo in senso combinatorio, lo sconnette in senso topologico. Con un altro tipo di 2-connessione, quello di Tutte, non occorrerebbe proibire esplicitamente i cappi o ammettere esplicitamente i piccoli grafi; si veda il problema 32D.)

Ecco una piccola osservazione sulla "struttura" dei grafi non separabili.

Orig. 452

Lemma 32.1. Sia G un grafo finito non separabile con almeno due spigoli e sia H un suo sottografo proprio non separabile massimale. Allora G è l'unione di H e di un grafo-cammino P che congiunge due vertici distinti di H e non ha vertici interni in H.

Il cammino dell'enunciato può essere chiamato un'"ansa". La figura 32.1 suggerisce la situazione.

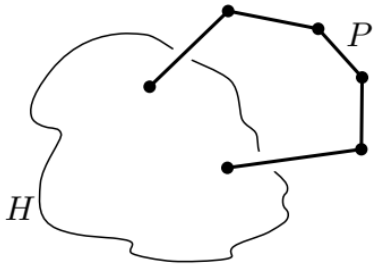


Figura 32.1

Dimostrazione. Può accadere che $V(H) = V(G)$. In questo caso, sia e uno spigolo di G non appartenente a H e sia P il grafo-spigolo costituito da e e dai suoi estremi. Aggiungere e a H produce un grafo non separabile; poiché H è massimale tra i sottografi propri non separabili, l'unione di H e P è G.

Se $V(H) \neq V(G)$, la connessione di G implica che esista uno spigolo e con un estremo $x \in V(H)$ e l'altro $y \notin V(H)$. Per la connessione di $G - x$, esiste un cammino semplice che, senza passare per x,

congiunge y a un altro vertice w di H. Se z è il primo vertice di H su tale cammino, procedendo da y a w, lo spigolo e e il tratto iniziale del cammino formano un grafo-cammino P che congiunge x a z, senza spigoli in H e senza vertici in H oltre ai suoi estremi. Allora $H \cup P$ è un grafo non separabile più grande di H, quindi coincide con G. □

Come conseguenza del lemma, dato un grafo finito non separabile G con almeno due spigoli, esiste una successione di sottografi non separabili

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_k = G,$$

dove H_0 è un grafo-spigolo e ogni H_{i+1} è l'unione di H_i e di un'ansa.

Una *suddivisione* di un grafo G è, informalmente, un grafo H ottenuto inserendo ulteriori vertici in alcuni spigoli. Più precisamente, possiamo sostituire gli spigoli di G con grafi-cammino finiti i cui vertici interni siano "nuovi", cioè non siano vertici del grafo originale G; consentiamo inoltre di sostituire i cappi con poligoni. Due grafi si dicono *omeomorfi* se sono isomorfi a suddivisioni di uno stesso grafo. La suddivisione di un grafo non separabile, diverso dal grafo-spigolo, conserva la non separabilità. Orig. 453

Problema 32A. Definiamo il *rango* di un grafo connesso G come $|E(G)| - |V(G)| + 1$. (Nel capitolo 34 vedremo che è la dimensione di quello che lì viene chiamato spazio dei cicli di G.) Aggiungendo un'ansa a un grafo non separabile, il rango aumenta di uno. I grafi connessi di rango 0 sono gli alberi. I grafi non separabili di rango 1 sono i poligoni. Quelli di rango 2 sono i *grafi-θ*, omeomorfi alla lettera θ, cioè suddivisioni del grafo a fascio con tre spigoli, poiché questo è tutto ciò che può risultare dall'aggiunta di un'ansa a un poligono. Descrivere tutti i grafi non separabili di rango 3 come suddivisioni di quattro grafi.

È chiaro che, se G non è non separabile e H, K sono sottografi a spigoli disgiunti, con al più un vertice in comune, la cui unione è G, uno spigolo di H e uno di K non possono appartenere insieme ad alcun poligono di G.

Teorema 32.2. Ogni coppia di spigoli di un grafo non separabile G è contenuta nell'insieme degli spigoli di un sottografo poligonale.

Dimostrazione. Affermiamo che, dati due vertici distinti x, y e uno spigolo e di un grafo non separabile G, esiste un cammino da x a y che percorre e. Se x, y sono gli estremi di un altro spigolo e', otteniamo quindi un poligono contenente e ed e'. Dimostriamo l'affermazione per induzione sul numero totale di spigoli (oppure sul rango).

Il grafo-spigolo con spigolo e è un sottografo non separabile. Sia H un sottografo proprio non separabile massimale contenente e. Se x, y appartengono entrambi a H, basta l'ipotesi induttiva. Altrimenti G è l'unione di H e di un grafo-cammino P che congiunge due vertici, diciamo a, b, di H, e almeno uno tra x, y è un vertice interno di P. Se entrambi sono vertici di P, un cammino da a a b in H che percorra e, insieme a tratti di P, fornisce il cammino richiesto. Infine supponiamo x interno a P e $y \in V(H)$, per esempio con $y \neq a$. Un cammino in H da y ad a che percorra e, insieme al tratto di P da x ad a, fornisce il cammino richiesto. □ Orig. 454

Corollario. Ogni coppia di vertici di un grafo non separabile G, diverso dal grafo-spigolo, è contenuta in un poligono di G.

Dimostrazione. Scegliamo uno spigolo incidente a ciascuno dei due vertici e, se gli spigoli sono distinti, applichiamo il teorema. Se coincidono, esiste un poligono contenente tale spigolo, purché il grafo possieda un secondo spigolo da qualche parte. □

Il corollario è in realtà equivalente al teorema 32.2: per ricavare quest'ultimo, basta inserire nuovi vertici a metà degli spigoli dati e applicare il corollario ai nuovi vertici.

Il corollario è il caso particolare $k = 2$ del seguente teorema di H. Whitney (1932).

Teorema 32.3. Un grafo G con almeno $k + 1$ vertici è k-connesso rispetto ai vertici se e solo se, per ogni coppia di vertici distinti x, y, esistono k cammini internamente disgiunti che li congiungono, cioè cammini che non hanno vertici in comune oltre agli estremi x, y.

Questo sarà una conseguenza immediata del teorema di Menger qui sotto, che enunciamo nella versione per grafi orientati. Come al solito, un grafo non orientato può essere considerato orientato sostituendo ogni spigolo con una coppia di spigoli orientati, uno per verso.

Applicheremo il teorema 7.2 sui flussi interi e ci servirà l'osservazione seguente, quasi identica al problema 7B.

Problema 32B. Sia f un flusso non negativo da s a t in un grafo orientato D; non sono richieste capacità. (i) Mostrare che, se f ha valore positivo, esiste un cammino orientato da s a t su tutti i cui spigoli e si ha $f(e) > 0$. (ii) Concludere che, se f è intero e ha valore k, esistono k cammini orientati $p_1, p_2, \ldots, p_k$ da s a t in D tali che, per ogni $e \in E(D)$, il numero dei cammini p_i che percorrono e sia al più $f(e)$.

Problema 32C. Siano s, t vertici distinti di un grafo orientato D. Mostrare che il massimo numero di cammini orientati a spigoli disgiunti da s a t è uguale al minimo numero di spigoli in un insieme E la cui cancellazione separi s e t in tale direzione, cioè tale che ogni cammino orientato da s a t contenga almeno uno spigolo di E. Orig. 455

Siano s, t vertici distinti di un grafo orientato D. Un *insieme* (s,t)*-separante* è un sottoinsieme $S \subseteq V(D) \setminus \{s,t\}$ tale che ogni cammino orientato da s a t contenga almeno un vertice di S.

Teorema 32.4 (Teorema di Menger). Siano s, t vertici distinti di un grafo orientato D e supponiamo che non vi sia uno spigolo orientato da s a t. Se nessun insieme (s,t)-separante ha cardinalità minore di k, in D esistono k cammini orientati internamente disgiunti da s a t.

Dimostrazione. Costruiamo una rete di trasporto N i cui vertici siano s, t e una coppia di nuovi vertici x_1, x_2 per ciascun vertice x di D diverso da s, t. A ogni spigolo di D da s a un vertice x corrisponde uno spigolo di N da s a x_1 di capacità infinita (o di qualunque capacità intera almeno k). A ogni spigolo di D da un vertice x a t corrisponde uno spigolo di N da x_2 a t di capacità infinita. A ogni spigolo e di D da x a y, con x, y diversi da s, t, corrisponde uno spigolo da x_2 a y_1 di capacità infinita. Infine, per ogni vertice x diverso da s, t, vi è uno spigolo da x_1 a x_2 di capacità 1.

Per costruzione, i vertici di un cammino orientato da s a t in N devono presentarsi nella forma

$$s, a_1, a_2, b_1, b_2, \ldots, z_1, z_2, t,$$

dove $s, a, b, \ldots, z, t$ sono i vertici di un cammino orientato da s a t in D.

Supponiamo di avere in N un flusso intero f da s a t di valore k. I valori di f possono essere soltanto 0 e 1, poiché ogni spigolo di N o entra in un vertice x_1 il cui unico spigolo uscente ha capacità 1, o esce da un vertice x_2 il cui unico spigolo entrante ha capacità 1, oppure è uno spigolo $x_1 \to x_2$ di capacità 1. Per il problema 32B esistono k cammini orientati da s a t in N che, complessivamente, percorrono ogni spigolo e al più una volta. Questi cammini sono a spigoli disgiunti, quindi anche internamente disgiunti: due cammini orientati che condividano un vertice x_1 o x_2 devono condividere l'unico spigolo $x_1 \to x_2$. I corrispondenti k cammini in D sono dunque internamente disgiunti. Per assicurare l'esistenza di tale flusso, consideriamo un taglio (S, T) di N che separi s e t e supponiamo, per assurdo, che la sua capacità sia minore di k. Gli unici spigoli di N con capacità eventualmente minore di k sono quelli da x_1 a x_2 per qualche $x \in V(D)$. Se V è l'insieme dei vertici x di D tali che $x_1 \in S$ e $x_2 \in T$, la capacità del taglio è $|V|$. Ogni cammino orientato da s a t in N deve attraversare uno di questi spigoli $x_1 \to x_2$. Equivalentemente, ogni cammino orientato da s a t in D deve attraversare un vertice x di V, che è quindi (s,t)-separante. Questo contraddice l'ipotesi del teorema. □ Orig. 456

* * *

Un *politopo convesso* P in $\mathbb{R}^n$ è l'inviluppo convesso di un numero finito di punti, cioè

$$P = \{\lambda_1 x_1 + \cdots + \lambda_k x_k : \lambda_i \geq 0,\ \lambda_1 + \cdots + \lambda_k = 1\}.$$

La dimensione di un politopo è la dimensione del suo inviluppo affine. Un *iperpiano di appoggio* di P è un iperpiano

$$H = \{x : \ell(x) = c\},$$

dove $\ell : \mathbb{R}^n \to \mathbb{R}$ è un funzionale lineare non nullo e c uno scalare, tale che $H \cap P \neq \varnothing$ e P giaccia interamente in uno dei semispazi chiusi delimitati da H, per esempio

$$P \subseteq \{x : \ell(x) \geq c\}.$$

Una *faccia* di P è l'intersezione di un suo iperpiano di appoggio con P (benché spesso si includa tra le facce anche l'insieme vuoto). Un *vertice* di P è una faccia di dimensione 0; uno *spigolo* è una faccia di dimensione 1. Il grafo G di un politopo P, detto anche 1-*scheletro* di P, ha come $V(G)$ ed $E(G)$ rispettivamente i vertici e gli spigoli di P, con l'incidenza determinata dall'inclusione.

Una faccia F è a sua volta un politopo convesso: precisamente, è l'inviluppo convesso dei vertici di P che contiene (si veda Grünbaum, 1967). Il grafo di F è un sottografo del grafo di P. Il risultato seguente è dovuto a M. Balinski (1961). Per dimostrarlo occorre il seguente fatto della teoria della programmazione lineare; si veda Grünbaum (1967). Se s è un vertice di un politopo P in $\mathbb{R}^m$ e ℓ un funzionale lineare, allora $\ell(s) \geq \ell(x)$ per ogni $x \in P$, oppure esiste un vertice t di P adiacente a s tale che $\ell(t) > \ell(s)$. Orig. 457

Teorema 32.5. Il grafo G di un politopo convesso di dimensione n è n-connesso.

Dimostrazione. Procediamo per induzione su n. Un politopo di dimensione 0 consiste di un unico punto. Il grafo di un politopo di dimensione 1 consiste di due vertici e di uno spigolo che li congiunge.

Siano $x_1, x_2, \ldots, x_{n-1}, a, b$ vertici distinti del grafo G di un politopo convesso P di dimensione n. Possiamo supporre $P \subseteq \mathbb{R}^n$. Vogliamo trovare in G una passeggiata da a a b che eviti $x_1, \ldots, x_{n-1}$. Scegliamo uno spazio affine S di dimensione $n-2$ contenente tali vertici. Esiste un iperpiano H, cioè un sottospazio affine di dimensione $n-1$, passante per S, rispetto al quale a, b si trovano nello stesso semispazio: $H = \{z : \ell(z) = \alpha\}$ e $\ell(a) \geq \alpha$, $\ell(b) \geq \alpha$, per un funzionale lineare ℓ e uno scalare α. (Consentiamo che uno o entrambi i punti appartengano a H.)

Poiché $P \not\subseteq H$, possiamo supporre che P contenga punti z con $\ell(z) > \alpha$; altrimenti a, b sono in H e possiamo sostituire ℓ, α con i loro opposti, considerando l'altro semispazio.

Per il fatto di programmazione lineare citato sopra, esistono cammini p, q in G da a, b a vertici a', b', rispettivamente, nei quali ℓ raggiunge il suo massimo α', e tali che nessun vertice di p, q, eccetto quelli iniziali, appartenga a H. L'intersezione $P \cap H'$, dove $H' := \{z : \ell(z) = \alpha'\}$, è una faccia di P di dimensione al più $n-1$ e, in particolare, ha un grafo connesso. Esiste quindi un cammino r in G da a' a b' con vertici in H'. Concatenando p, r e il cammino q percorso a ritroso, troviamo una passeggiata da a a b. □

Problema 32D. Un grafo G si dice *k-connesso secondo Tutte* quando, per ogni $\ell < k$, non è possibile trovare una coppia (H, K) di sottografi non vuoti a spigoli disgiunti di G, ciascuno contenente almeno ℓ spigoli, tali che $H \cup K = G$ e $|V(H) \cap V(K)| = \ell$. Una tale coppia può essere chiamata una *ℓ-separazione* di G. I concetti di connessione rispetto ai vertici e di connessione secondo Tutte sono diversi. È però facile vedere, per un grafo non nullo, che la 1-connessione secondo Tutte coincide con la connessione ordinaria e la 2-connessione secondo Tutte coincide con la non separabilità. Un grafo 2-connesso secondo Tutte con almeno due spigoli non può avere cappi: altrimenti avremmo due sottografi a spigoli disgiunti, uno costituito da un cappio e l'altro da tutti gli spigoli rimanenti, ciascuno con almeno uno spigolo ma con un solo vertice in comune. Dimostrare che, per un grafo G con $|V(G)| \geq k+1$, la k-connessione secondo Tutte equivale alla k-connessione rispetto ai vertici e all'assenza di poligoni con meno di k spigoli. Orig. 458

Note

Si vedano le note al capitolo 34 per alcune osservazioni su H. Whitney.

Karl Menger (1902–1985) fu un matematico austriaco che nel 1937 lasciò l'Austria per gli Stati Uniti, dove trascorse il resto della vita. Lavorò in molti campi, tra cui logica, didattica ed economia, ma è noto soprattutto per i suoi studi sulla teoria della dimensione e sulla teoria delle curve. Dopo il dottorato lavorò con L. E. J. Brouwer ad Amsterdam, per poi tornare a Vienna come professore nel 1927. Qui fondò il Colloquio matematico di Vienna, che annoverava membri celebri quali K. Gödel e A. Wald e un gran numero di visitatori. I risultati furono pubblicati in otto volumi prima che il seminario fosse costretto a interrompersi per la presenza di numerosi collaboratori ebrei.

Riferimenti bibliografici

- M. Balinski (1961), On the graph structure of convex polyhedra in n-space, *Pacific J. Math.* **11**, 431–434.
- L. R. Ford, Jr. e D. R. Fulkerson (1962), *Flows in Networks*, Princeton University Press.
- B. Grünbaum (1967), *Convex Polytopes*, J. Wiley (Interscience).
- H. Whitney (1932), Nonseparable and planar graphs, *Trans. Amer. Math. Soc.* **34**, 339–362.

Capitolo 33

Planarità e colorazione

Orig. 459

Cominciamo con alcune considerazioni sulla cancellazione e sulla contrazione. Nel prossimo capitolo vedremo che si tratta di concetti "duali"; cfr. il problema 34C.

Siano G un grafo ed $e \in E(G)$. Definiamo due grafi G'_e e G''_e con lo stesso insieme di spigoli $E(G)\setminus\{e\}$. Il primo, G'_e, si ottiene da G cancellando lo spigolo e. (Talvolta conviene eliminare successivamente gli eventuali vertici isolati, ma qui li lasceremo.) Il secondo, G''_e, si ottiene identificando gli estremi di e e rimuovendo e stesso. Possiamo immaginare di "riavvolgere" o "accorciare" uno spigolo in un disegno del grafo, come nella figura 33.1.

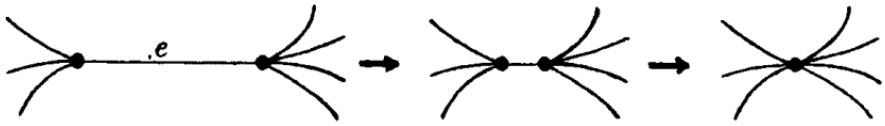


Figura 33.1

Il *polinomio cromatico* χ_G di un grafo finito G è stato introdotto nel capitolo 25: $\chi_G(\lambda)$ è il numero delle colorazioni proprie di G con λ colori. Per esempio,

$$\chi_{K_n}(\lambda) = \lambda(\lambda-1)(\lambda-2)\cdots(\lambda-n+1).$$

Nel capitolo 25 abbiamo mostrato che χ_G è un polinomio in λ; si veda anche l'osservazione successiva a (33.1).

Esempio 33.1. Affermiamo che, per un albero T su n vertici,

$$\chi_T(\lambda) = \lambda(\lambda-1)^{n-1}.$$

Orig. 460

Per verificarlo, osserviamo che, se x è un vertice monovalente di T, dopo aver colorato propriamente l'albero su $n-1$ vertici ottenuto eliminando x, rimangono $\lambda-1$ colori disponibili per x. L'affermazione segue per induzione sul numero dei vertici.

Se e è uno spigolo di G che non sia un cappio, possiamo dividere le colorazioni proprie di G'_e in due classi: quelle nelle quali gli estremi di e hanno colori diversi (sono le colorazioni proprie di G), e quelle nelle quali hanno lo stesso colore (in corrispondenza biunivoca con le colorazioni proprie di G''_e). Questo dimostra

$$\chi_G(\lambda) = \chi_{G'_e}(\lambda) - \chi_{G''_e}(\lambda). \tag{33.1}$$

L'equazione (33.1) fornisce un altro modo per vedere che $\chi_G(\lambda)$ è un polinomio. Un grafo H con cappi non ammette colorazioni proprie, cioè $\chi_H(\lambda) = 0$. Per un grafo H privo di spigoli e con n vertici, $\chi_H(\lambda) = \lambda^n$. In entrambi i casi abbiamo polinomi. Basta ora usare (33.1) e l'induzione sul numero di spigoli.

Anche il polinomio cromatico di un albero T si potrebbe ottenere per induzione mediante (33.1): T''_e è un albero, mentre T'_e ha due componenti che sono alberi.

Problema 33A. Sia $\tau(G)$ il numero degli alberi ricoprenti di un grafo G, talvolta detto *complessità* di G. Mostrare che, per ogni spigolo $e \in E(G)$ che non sia un cappio, $\tau(G) = \tau(G'_e) + \tau(G''_e)$.

Problema 33B. Trovare il polinomio cromatico dell'n-gono C_n. Trovare il polinomio cromatico della *ruota* W_n, ottenuta da C_n aggiungendo un nuovo vertice e congiungendolo a tutti i vertici di C_n.

Non ha senso chiedere il numero delle colorazioni proprie di un grafo con -1 colori, ma, essendo $\chi_G(\lambda)$ un polinomio, possiamo calcolare $\chi_G(-1)$. R. P. Stanley (1973) scoprì la seguente interpretazione combinatoria di $|\chi_G(-1)|$. Un *orientamento* di un grafo è uno dei grafi orientati ottenuti scegliendo, per ogni spigolo, uno degli estremi come testa e l'altro come coda. Il numero di orientamenti è dunque 2^m, dove m è il numero degli spigoli che non sono cappi, benché, per ragioni topologiche, sia opportuno considerare anche un cappio come dotato di due possibili versi.

Orig. 461

Teorema 33.1. Il numero degli orientamenti aciclici di un grafo G, cioè privi di circuiti orientati, è $(-1)^{|V(G)|}\chi_G(-1)$.

Dimostrazione. Se G ha cappi, $\chi_G(\lambda) = 0$ e G non ha orientamenti aciclici; il teorema vale quindi in questo caso.

Consideriamo un orientamento aciclico di G'_e, con e non cappio. Vi sono due modi di orientare e ottenendo un orientamento di G. Affermiamo che uno o entrambi sono aciclici e che i casi nei quali entrambi sono aciclici sono in corrispondenza biunivoca con gli orientamenti aciclici di G''_e. Infatti orientare e dall'estremo x all'estremo y produce un orientamento non aciclico se e solo se in G'_e esiste un cammino orientato da y a x; in G'_e non possono esistere contemporaneamente cammini orientati da x a y e da y a x, avendo supposto l'orientamento aciclico; inoltre, non vi è un cammino orientato da y a x in G'_e se e solo se identificare x e y produce un orientamento aciclico di G''_e.[1]

Pertanto

$$\omega(G) = \omega(G'_e) + \omega(G''_e),$$

se $\omega(H)$ denota il numero degli orientamenti aciclici di H. Per (33.1) la stessa ricorrenza è soddisfatta ponendo $\omega(H) = (-1)^{|V(H)|}\chi_H(-1)$. Il teorema segue per induzione sul numero degli spigoli, verificatolo per i grafi privi di spigoli. □

Per *immersione*, o *disegno proprio*, di un grafo G su una superficie S intendiamo un disegno nel quale gli spigoli non si incrociano, ma si incontrano soltanto nei vertici. Più precisamente, i vertici sono rappresentati da punti di S, gli spigoli da archi di Jordan (immagini continue e iniettive dell'intervallo unitario) che congiungono i punti corrispondenti agli estremi dello spigolo, e nessun punto interno di un arco di Jordan appartiene a un altro arco o coincide con un punto rappresentante un vertice di G. Consideriamo soltanto immersioni di grafi finiti. Sebbene il piano non sia compatto, si immerge naturalmente nella sfera, sua compattificazione a un punto; un grafo è planare se e solo se ammette un'immersione nella sfera.

Esempi di grafi non planari sono $K_{3,3}$ e K_5; più avanti menzioneremo diversi modi per verificarlo. Neppure le suddivisioni di questi grafi, né i grafi contenenti una di tali suddivisioni, sono planari. Un importante teorema che qui non dimostreremo è il seguente. Se ne trovano dimostrazioni in Chartrand e Lesniak (1986), Tutte (1984) e Diestel (1997).

Orig. 462

Teorema 33.2 (Kuratowski). Un grafo G è planare se e solo se non possiede sottografi isomorfi a suddivisioni di K_5 o di $K_{3,3}$.

Problema 33C. Trovare una suddivisione di $K_{3,3}$ come sottografo del grafo di Petersen.

Un *minore* di un grafo G è un grafo H ottenuto da G cancellando e contraendo spigoli ed eventualmente cancellando poi alcuni o tutti i vertici isolati.

L'ordine in cui si cancellano o si contraggono gli spigoli non ha importanza. Per esempio, contraendo in un ordine qualsiasi gli spigoli di un sottoinsieme $S \subseteq E(G)$, si ottiene un grafo isomorfo al grafo G''_S, detto una *contrazione* di G, così definito. I vertici di G''_S sono, formalmente, le componenti del sottografo ricoprente di G con insieme di spigoli S, denotato $G : S$. L'insieme degli spigoli di G''_S è $E(G) \setminus S$. Gli estremi in G''_S di uno spigolo $e \in E(G) \setminus S$ sono le componenti di $G : S$ che contengono gli estremi di e considerato come spigolo di G. Informalmente, le componenti di $G : S$ vengono ridotte a singoli vertici.

Usiamo G'_S per il grafo ottenuto cancellando gli spigoli di S, cioè $G : (E(G) \setminus S)$; con questa notazione conviene però richiedere che vengano cancellati anche tutti i vertici isolati.

Esempio 33.2. Sia A l'insieme dei cinque "raggi" del consueto disegno del grafo di Petersen P, a sinistra nella figura 1.4. Il sottografo $P : A$ ha cinque componenti, quindi P''_A ha cinque vertici. La

[1] Nota redazionale: nell'ultima equivalenza occorre escludere cammini orientati in entrambi i versi tra x e y; questo è precisamente il caso in cui entrambe le scelte del verso di e sono acicliche. L'originale nomina qui soltanto uno dei versi.

contrazione G''_S in questo caso è K_5.[2] Se B è l'insieme dei cinque spigoli del pentagramma interno, $P : B$ ha sei componenti e P''_B è la ruota W_5. Se C è l'insieme degli spigoli di un albero ricoprente di P, P''_C consiste di un unico vertice con sei cappi. (Un grafo con un unico vertice può essere chiamato *coalbero*.)

È del tutto possibile che G''_S abbia cappi e/o spigoli paralleli anche se G è semplice. (Le contrazioni senza cappi di un grafo semplice G sono in corrispondenza biunivoca con gli elementi dei reticoli $\Pi(G)$, sottoreticoli dei reticoli delle partizioni, introdotti nell'esempio 23.6.) Orig. 463

Un grafo G è una contrazione di ogni sua suddivisione H, poiché contrarre $k-1$ spigoli qualsiasi di un grafo-cammino con k spigoli produce un grafo-spigolo.

Dato un disegno di G su una superficie S ed $e \in E(G)$, esiste evidentemente un disegno naturale di G'_e su S. Se e non è un cappio, esiste anche un disegno indotto naturale di G''_e: gli estremi dello spigolo possono essere avvicinati continuamente sulla superficie (figura 33.1). Secondo la nostra definizione combinatoria, contrarre un cappio equivale a cancellarlo. In particolare, se G ammette un'immersione su una superficie S, lo stesso vale per ogni suo minore.

Problema 33D. Mostrare che un grafo G avente un minore isomorfo a K_5 o $K_{3,3}$ contiene anche una suddivisione di K_5 o $K_{3,3}$. Più in generale, dimostrare: (i) se un grafo trivalente H compare come minore di G, allora G contiene come sottografo una suddivisione di H; quindi, se $K_{3,3}$ è un minore, una sua suddivisione è un sottografo; (ii) se K_5 è un minore di G, allora G contiene una suddivisione di K_5 oppure di $K_{3,3}$.

Un teorema profondo ed estremamente importante di N. Robertson e P. Seymour afferma che ogni insieme infinito di grafi ne contiene due tali che uno sia minore dell'altro. Si veda il capitolo 12 di Diestel (1997) per una discussione di parte di questo lavoro. Ne segue che l'insieme dei grafi che non si immergono in una superficie assegnata e sono minimali rispetto a questa proprietà, nel senso che ogni minore proprio si può immergere, è finito. Per il piano, essi sono due.

Data un'immersione di G su S, definiamo le *facce*, o *regioni*, relative all'immersione come le componenti topologicamente connesse che rimangono eliminando da S vertici e spigoli, più precisamente i punti corrispondenti ai vertici e gli insiemi di punti degli archi di Jordan corrispondenti agli spigoli. Indichiamo l'insieme delle facce con $F(G)$. Sappiamo che è una notazione terribile, poiché le facce dipendono dall'immersione, e in particolare dalla superficie, e non sono in generale determinate da G. La useremo comunque. In generale queste facce possono essere o non essere 2-celle, cioè omeomorfe al disco unitario aperto, senza "buchi". Per un'immersione di un grafo connesso nella sfera, però, le regioni sono 2-celle. Questo fatto è legato al teorema della curva di Jordan: eliminando dalla sfera i punti dell'immagine continua e iniettiva della circonferenza unitaria, lo spazio topologico risultante ha esattamente due componenti semplicemente connesse, entrambe 2-celle. Orig. 464

Teorema 33.3 (Formula di Eulero). Per un disegno di un grafo planare connesso G sulla sfera o sul piano,

$$f - e + v = 2,$$

dove f, e, v sono rispettivamente i numeri di facce, spigoli e vertici. Più in generale, per ogni grafo G immerso nella sfera,

$$1 - |F(G)| + |E(G)| - |V(G)| + |C(G)| = 0, \tag{33.2}$$

dove $C(G)$ è l'insieme delle componenti di G.

Dimostrazione. Dimostriamo la seconda affermazione per induzione sul numero degli spigoli. Per un grafo privo di spigoli, $|C(G)| = |V(G)|$ e $|F(G)| = 1$, dunque vale (33.2).

Supponiamo che G abbia uno spigolo a non cappio. Consideriamo un'immersione di G e osserviamo che la contrazione di uno spigolo non cambia il numero di facce. Applicando l'ipotesi induttiva a G''_a otteniamo

$$1 - |F(G''_a)| + |E(G''_a)| - |V(G''_a)| + |C(G''_a)| = 0.$$

Abbiamo $|E(G)| = |E(G''_a)| + 1$, $|V(G)| = |V(G''_a)| + 1$, $|C(G)| = |C(G''_a)|$ e $|F(G)| = |F(G''_a)|$. Quindi (33.2) vale per G.

Supponiamo che G abbia cappi; scegliamone uno, a, e applichiamo l'ipotesi induttiva a G'_a:

$$1 - |F(G'_a)| + |E(G'_a)| - |V(G'_a)| + |C(G'_a)| = 0.$$

[2] Nota redazionale: l'originale scrive qui G''_S; nel contesto si tratta di P''_A.

Naturalmente $|E(G)| = |E(G'_a)| + 1$, $|V(G)| = |V(G'_a)|$ e $|C(G)| = |C(G'_a)|$. Sulla sfera, il teorema della curva di Jordan implica che le due facce incidenti al cappio siano distinte; perciò $|F(G)| = |F(G'_a)| + 1$ e otteniamo (33.2). □

Orig. 465

Esempio 33.3. Mostriamo che K_5 e $K_{3,3}$ non sono planari. L'insieme degli spigoli incidenti a una faccia in un'immersione planare di un grafo non separabile G, diverso dal grafo-spigolo, contiene un sottografo poligonale; si veda il capitolo 34. Il *grado* di una faccia è il numero degli spigoli incidenti, cioè il suo grado come vertice del grafo duale del capitolo 34. La somma dei gradi delle facce è il doppio del numero degli spigoli, poiché ciascuno spigolo è incidente a due facce.

Consideriamo un'ipotetica immersione di K_5 nel piano. Per la formula di Eulero, vi sono sette facce. Ciascuna ha però grado almeno 3, perciò la somma dei gradi è almeno 21, in contraddizione con $|E(K_5)| = 10$.

Analogamente, in un'ipotetica immersione di $K_{3,3}$ nel piano vi sarebbero cinque facce, ciascuna di grado almeno 4, poiché $K_{3,3}$ ha maglia 4. La somma dei gradi sarebbe quindi almeno 20, in contraddizione con $|E(K_{3,3})| = 9$.

(Un ragionamento analogo mostra che il grafo di Petersen non è planare. Lo sapevamo già, poiché esso ha come minori sia K_5 sia $K_{3,3}$, che non sono planari.)

Problema 33E. Determinare tutte le coppie di interi (d_1, d_2), con $d_i \geq 2$, per le quali esiste un grafo planare, non necessariamente semplice, regolare di grado d_1 e avente tutte le facce di grado d_2. Le coppie comprenderanno i gradi dei vertici e delle facce dei cinque solidi platonici.

E. Steinitz (1922) caratterizzò i grafi dei politopi convessi tridimensionali.

Teorema 33.4. Un grafo G è il grafo di un politopo convesso tridimensionale se e solo se è semplice, planare e 3-connesso.

Che il grafo di un politopo tridimensionale sia 3-connesso è un caso particolare del teorema 32.5. Non dimostriamo il resto del teorema.

La domanda "Si possono colorare i paesi di una carta sulla sfera con quattro colori o meno, in modo che paesi adiacenti abbiano colori diversi?" compare in una lettera del 23 ottobre 1852 di Augustus de Morgan a Sir William Rowan Hamilton. È probabile che l'ideatore fosse Francis Guthrie, fratello di Frederick Guthrie, allievo di de Morgan. Colorare i paesi, cioè le regioni, di una carta planare equivale a colorare i vertici del grafo duale che introdurremo nel prossimo capitolo. Per noi, dunque, il "problema dei quattro colori" chiede se ogni grafo planare sia 4-colorabile.

Orig. 466

Quattro colori sono evidentemente necessari, poiché K_4 è planare, ma è facile trovare molti altri grafi planari non 3-colorabili. Il problema ha motivato una grande parte della teoria dei grafi. Altre notizie sulla sua storia si trovano in Biggs, Lloyd e Wilson (1976).

Nel 1890 P. J. Heawood dimostrò il teorema dei cinque colori, teorema 33.6 qui sotto: un grafo planare senza cappi G ha numero cromatico $\chi(G) \leq 5$. Heawood utilizzò idee di A. B. Kempe, in particolare il procedimento di ricolorazione che richiameremo. Nel 1976 K. Appel e W. Haken risolsero finalmente il problema annunciando una dimostrazione del teorema dei quattro colori: $\chi(G) \leq 4$. Forse sorprendentemente, la dimostrazione non utilizzava la grande quantità di risultati e teorie sviluppati nel Novecento, ma tornava alle idee di Kempe e Heawood. Altra possibile sorpresa: richiedeva oltre 1000 ore di calcolo al computer. All'inizio non era chiaro se il calcolo sarebbe mai terminato. Semplificando molto, vi erano numerosi casi da esaminare, ma non era certo che fossero in numero finito; il programma generava esso stesso nuovi casi e avrebbe potuto continuare indefinitamente a scomporli in sottocasi. Si vedano Appel, Haken e Koch (1977), e Appel e Haken (1977). Non abbiamo spazio per discutere il lavoro nei dettagli, ma dimostreremo il teorema dei cinque colori.

Proposizione 33.5. Ogni grafo planare semplice non nullo G ha un vertice di grado al più 5.

Dimostrazione. Segue rapidamente dalla formula di Eulero. Basta dimostrare che una componente ha un tale vertice, quindi supponiamo G connesso. Un suo disegno abbia f regioni, e spigoli e v vertici. Se nessun vertice ha grado minore di sei, la somma dei gradi, uguale a $2e$, è almeno $6v$, cioè

$$v \leq e/3.$$

Poiché G è semplice e possiamo supporre che non sia il grafo-spigolo, ogni regione è incidente ad almeno

Orig. 467

tre spigoli; quindi la somma degli f gradi dei vertici di G^*, uguale a $2e$, è almeno $3v$,[3] cioè

$$f \leq 2e/3.$$

Otteniamo allora la contraddizione

$$2 = f - e + v \leq \frac{e}{3} - e + \frac{2e}{3} = 0. \qquad \square$$

Naturalmente colorare un grafo senza cappi equivale a colorare un grafo semplice: basta sopprimere gli spigoli multipli. Una conseguenza immediata è il teorema dei sei colori: per un grafo planare senza cappi G, $\chi(G) \leq 6$. Eliminato un vertice x di grado al più cinque da un grafo planare semplice e colorato il grafo rimanente con sei colori per induzione, vi è sempre un colore disponibile per x.

Richiamiamo l'idea di ricolorazione introdotta nel capitolo 3. Supponiamo che G sia colorato propriamente e siano α, β due dei colori. Possiamo scambiarli su una qualsiasi componente del sottografo indotto dai vertici di questi due colori, ottenendo un'altra colorazione propria. Dati dunque vertici x, y di colore rispettivamente α, β, o esiste un cammino, di lunghezza dispari, con vertici $a_0 = x, a_1, \ldots, a_n = y$ alternatamente colorati α, β (una cosiddetta *catena di Kempe*), oppure esiste una colorazione propria nella quale x, y hanno entrambi, per esempio, colore α, mentre i vertici di colori diversi da α, β conservano il loro colore.

Teorema 33.6. Se G è un grafo planare senza cappi, $\chi(G) \leq 5$.

Dimostrazione. Procediamo per induzione sul numero dei vertici. L'affermazione è certamente vera con al più cinque vertici. Consideriamo un disegno planare di un grafo senza cappi G e supponiamo il teorema vero per tutti i grafi con un vertice in meno. Possiamo supporre G semplice.

Per la proposizione 33.5 esiste $x \in V(G)$ di grado al più 5. Sia G_x il grafo ottenuto cancellando x e gli spigoli incidenti. Il disegno di G induce un disegno planare naturale di G_x. Per ipotesi induttiva, G_x ha una colorazione propria con cinque colori. Vi è un colore disponibile per x, e abbiamo concluso, a meno che x abbia grado esattamente cinque e i vertici adiacenti $y_1, y_2, \ldots, y_5$, elencati nell'ordine ciclico del disegno, abbiano ricevuto cinque colori distinti. Supponiamo quindi che y_i abbia ricevuto il colore i, per $i = 1, \ldots, 5$. Si veda la figura 33.2. Orig. 468

Consideriamo i colori 1 e 3. O esiste una colorazione propria di G_x nella quale y_1, y_3 hanno entrambi colore 1, mentre y_2, y_4, y_5 conservano il colore originale, oppure esiste in G_x un cammino semplice con sequenza di vertici, diciamo,

$$y_1, a_1, b_1, a_2, b_2, \ldots, a_s, b_s, y_3, \tag{33.3}$$

alternatamente colorati 1 e 3. Nel primo caso assegniamo a x il colore 3 e abbiamo concluso. Analogamente, o esiste una colorazione propria di G_x nella quale y_2, y_4 hanno entrambi colore 2, lasciando invariati i colori di y_1, y_3, y_5, oppure esiste un cammino semplice con sequenza

$$y_2, c_1, d_1, c_2, d_2, \ldots, c_t, d_t, y_4, \tag{33.4}$$

alternatamente colorato 2 e 4. Nel primo caso assegniamo a x il colore 4 e abbiamo concluso.

Per completare la dimostrazione osserviamo che i due cammini non possono esistere entrambi. Se esiste quello in (33.3), allora

$$x, y_1, a_1, b_1, a_2, b_2, \ldots, a_s, b_s, y_3, x \tag{33.5}$$

è la sequenza dei vertici di un cammino semplice chiuso, che divide il piano in due regioni. Il vertice y_2 si trova in una, y_4 nell'altra. Ogni cammino da y_2 a y_4 in G_x deve necessariamente avere un vertice in comune con il cammino in (33.4), e in particolare un vertice di colore 1 o 3; perciò un cammino come in (33.5) non può esistere.[4] $\square$ Orig. 469

[3] Nota redazionale: l'originale scrive $3v$; per ottenere la disuguaglianza seguente si deve leggere $3f$.

[4] Nota redazionale: gli ultimi due riferimenti dell'originale sono scambiati. Il cammino da y_2 a y_4 deve incontrare il circuito (33.5), e quindi il tratto (33.3); ciò esclude il cammino bicolore (33.4).

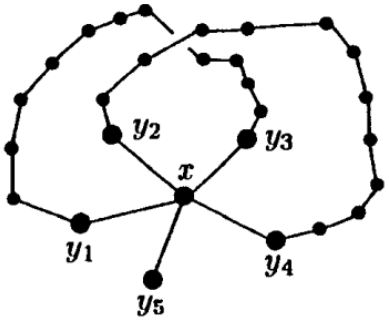


Figura 33.2

Nel capitolo 17 abbiamo trattato le colorazioni da liste per spiegare la dimostrazione di Galvin della congettura di Dinitz. Consideriamo ora un risultato di C. Thomassen (1994), che fornisce una seconda dimostrazione del teorema dei cinque colori assegnando prima a ogni vertice una lista di cinque colori distinti, non necessariamente la stessa per tutti i vertici. Un'idea della dimostrazione merita particolare attenzione, poiché spesso rende più agevoli le prove: si rafforza l'ipotesi induttiva e così il passo induttivo diventa più semplice.

Teorema 33.7. Sia G un grafo planare con N vertici $v_1, v_2, \ldots, v_N$. Per $i = 1, \ldots, N$, sia S_i un insieme di cinque elementi, chiamati colori. Esiste un'applicazione f sui vertici tale che $f(v_i) \in S_i$ e $f(v_i) \neq f(v_j)$ per ogni coppia di vertici adiacenti: una colorazione da liste di cinque colori di G.

Dimostrazione. Rendiamo anzitutto il problema più difficile aggiungendo spigoli che trasformino G in un poligono triangolato. Numeriamo i vertici in modo che $v_1, v_2, \ldots, v_k$ siano, nell'ordine, quelli del poligono (figura 33.3). Dalla lista di ciascuno di essi eliminiamo due colori, lasciando ai vertici sul perimetro soltanto tre colori disponibili. Di nuovo, il problema è più difficile. Infine restringiamo ulteriormente le scelte, selezionando due vertici adiacenti sul perimetro e assegnando a ciascuno un colore della sua lista. Affermiamo che, con queste condizioni iniziali, si può completare la colorazione.[5] La dimostrazione è per induzione sul numero dei vertici; i casi piccoli sono banali.

Orig. 470

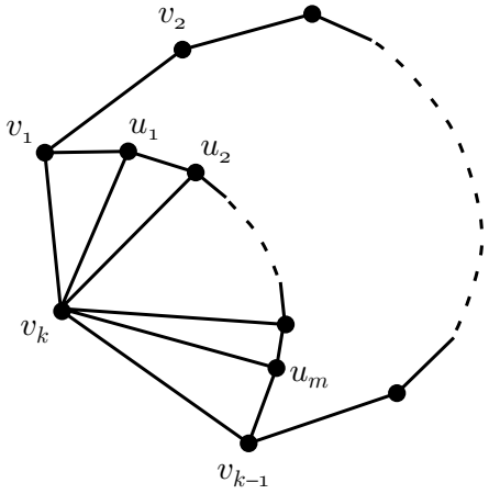


Figura 33.3

Distinguiamo due casi. Nel primo supponiamo che il poligono abbia uno spigolo tra due vertici del perimetro non consecutivi sul perimetro, cioè una corda. La corda divide il poligono in due parti, una delle quali contiene entrambi i vertici precolorati, eventualmente con uno di essi come estremo della corda. Per ipotesi induttiva possiamo completare la colorazione di questa parte. L'altra eredita così una precolorazione di due vertici adiacenti sul perimetro; una seconda applicazione dell'induzione conclude.

Supponiamo ora che non vi siano corde. Siano v_1, v_2 i vertici precolorati sul perimetro, e siano $v_1, u_1, u_2, \ldots, u_m, v_{k-1}$, in quest'ordine in senso orario (figura 33.3), i vertici adiacenti a v_k. Gli u_i sono

[5] Nota redazionale: i due vertici adiacenti precolorati devono ricevere colori distinti, come richiesto da una colorazione propria.

interni e, per la triangolazione, esistono gli spigoli $(v_1, u_1), (u_1, u_2), \ldots, (u_{m-1}, u_m), (u_m, v_{k-1})$. La lista di v_k contiene almeno due colori diversi dal colore di v_1. Ne scegliamo due e li eliminiamo dalle liste di $u_1, \ldots, u_m$, accorciando ulteriormente tali liste, se necessario, fino a tre colori. Per induzione possiamo completare la colorazione di $G \setminus \{v_k\}$. È possibile che v_{k-1} abbia ricevuto uno dei due colori della lista di v_k, ma ne resta almeno uno per completare la colorazione di G. □

Note

A. B. Kempe (1849–1922) conseguì nel 1872 una laurea con particolare distinzione in matematica al Trinity College di Cambridge, dove divenne noto anche per la sua bella voce da controtenore. Scelse la professione legale senza abbandonare gli studi matematici. Orig. 471

Il matematico polacco Kazimierz, o Casimir, Kuratowski (1896–1980) insegnò all'Università di Varsavia per quasi quarant'anni e al Politecnico di Leopoli, prima di andare in pensione nel 1966. Il suo celebre teorema che caratterizza i grafi planari fu dimostrato nel 1930.

Ernst Steinitz (1871–1928) fu professore di matematica a Breslavia, oggi Wrocław, e a Kiel. Diede importanti contributi, insieme a Hilbert, alla teoria dei campi.

Nel 1993 M. Voigt trovò un esempio di grafo planare con 238 vertici che non ammette una colorazione da liste di quattro colori.

Riferimenti bibliografici

- K. Appel e W. Haken (1977), The solution of the four-color map problem, *Scientific American* **237**, 108–121.
- K. Appel, W. Haken e J. Koch (1977), Every planar map is four colorable, *Illinois J. Math.* **21**, 429–567.
- N. L. Biggs, E. K. Lloyd e R. J. Wilson (1976), *Graph Theory 1736–1936*, Oxford University Press.
- G. Chartrand e L. Lesniak (1986), *Graphs and Digraphs*, 2a ed., Wadsworth.
- R. Diestel (1997), *Graph Theory*, Springer-Verlag, Graduate Texts in Mathematics **173**.
- R. P. Stanley (1973), Acyclic orientations of graphs, *Discrete Math.* **5**, 171–178.
- E. Steinitz (1922), Polyeder und Raumeinteilungen, *Enzykl. Math. Wiss.* **3**, 1–139.
- C. Thomassen (1994), Every planar graph is 5-choosable, *J. Combin. Theory Ser. B* **62**, 180–181.
- W. T. Tutte (1984), *Graph Theory*, Encyclopedia of Math. and its Appl. **21**, Addison-Wesley. Ripubblicato da Cambridge University Press.

Capitolo 34

Dualità di Whitney

Un arco di Jordan divide un piccolo intorno di un suo punto interno in due "metà". Oltre a essere incidente a due vertici, che possono coincidere, uno spigolo di una carta è dunque incidente a due regioni, che possono anch'esse coincidere. Si veda la figura 34.1. Orig. 472

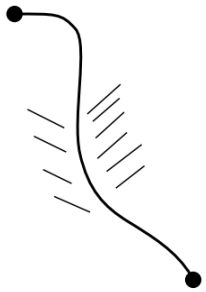
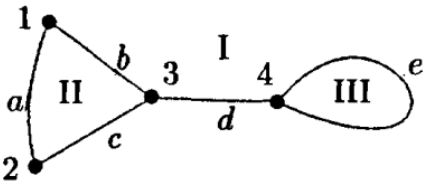


Figura 34.1

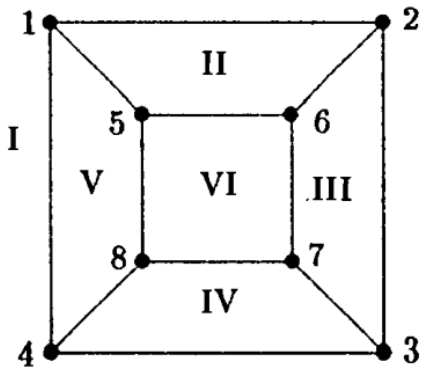
Questo permette di definire il *grafo duale* G^* di un grafo G rispetto a un'immersione a 2-celle su una superficie S. I vertici $V(G^*)$ sono le regioni dell'immersione; gli spigoli $E(G^*)$ sono gli stessi di G; gli estremi in G^* di uno spigolo e sono le regioni alle quali e è incidente. La figura 34.2 mostra due esempi.

Abbiamo definito G^* astrattamente, ma è importante osservare che esso ammette un'immersione sulla stessa superficie S: rappresentiamo ogni regione mediante un punto interno; i punti interni di due regioni che condividono uno spigolo e possono essere congiunti da un arco di Jordan che attraversa soltanto l'arco rappresentante e in G. Il disegno del duale del cubo della figura 34.2 è mostrato nella figura 34.3.

Gli esempi convinceranno il lettore che $(G^*)^*$ è isomorfo a G. Altri due fatti sui quali invitiamo a riflettere, senza tentare una dimostrazione formale, sono: un grafo non connesso non può avere un'immersione a 2-celle; il grafo duale rispetto a un'immersione a 2-celle è sempre connesso. Orig. 473



Estremi in G	Spigolo	Estremi in G^*
$1, 2$	a	I,II
$1, 3$	b	I,II
$2, 3$	c	I,II
$3, 4$	d	I,I
$4, 4$	e	I,III



Estremi in G	Spigolo	Estremi in G^*
$1,2$	a	I,II
$2,3$	b	I,III
$3,4$	c	I,IV
$4,1$	d	I,V
$5,6$	e	II,VI
$6,7$	f	III,VI
$7,8$	g	IV,VI
$8,5$	h	V,VI
$1,5$	i	II,V
$2,6$	j	II,III
$3,7$	k	III,IV
$4,8$	l	IV,V

Figura 34.2

I duali planari della successione dei poligoni sono i grafi a fascio, cioè grafi con due vertici e un numero positivo qualsiasi di spigoli che li congiungono. In particolare, il grafo-cappio e il grafo-spigolo sono duali. Il duale planare di un albero è un coalbero e un duale planare di un coalbero è un albero.

Orig. 474

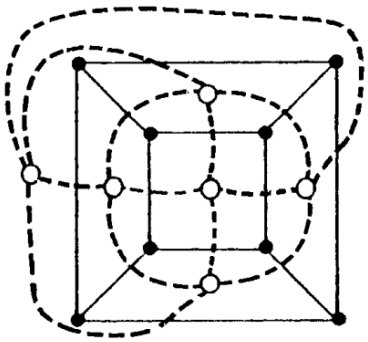


Figura 34.3

In generale un grafo può avere diversi grafi duali planari. La figura 34.4 mostra due coalberi isomorfi e i loro duali planari non isomorfi rispetto alle due immersioni. La figura 34.5 mostra due immersioni di un grafo non separabile G e i corrispondenti duali, non isomorfi.

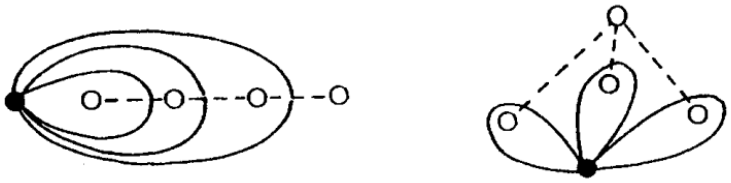


Figura 34.4

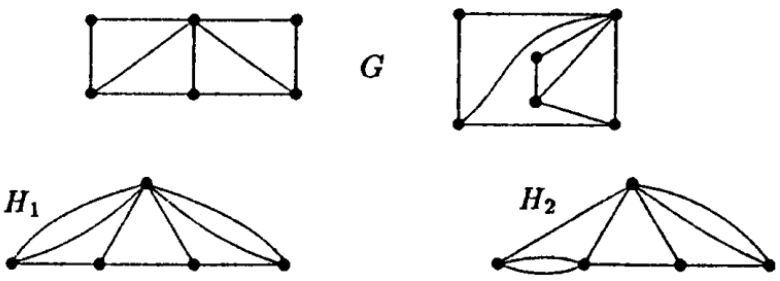


Figura 34.5

Lo scopo del capitolo è comprendere "combinatoriamente" la relazione tra un grafo planare e il suo grafo duale, o i suoi grafi duali. Useremo questa comprensione, la dualità di Whitney, per dimostrare alcuni teoremi sui grafi planari e sui loro duali senza riferimenti a disegni planari o alla topologia.

Orig. 475

Ricordiamo che la matrice di incidenza $N = N(G)$ di un grafo G ha righe indicizzate da $V(G)$, colonne indicizzate da $E(G)$, e

$$N(x,e) = \begin{cases} 1 & \text{se } x \text{ è incidente allo spigolo non cappio } e, \\ 2 & \text{se } e \text{ è un cappio incidente a } x, \\ 0 & \text{se } x \text{ non è incidente a } e. \end{cases}$$

Lavoreremo sul campo $\mathbb{F}_2$ di due elementi, perciò i cappi corrispondono essenzialmente a colonne nulle. Ogni altra colonna contiene due 1 e, in particolare, la somma modulo 2 di tutte le righe di N è il vettore nullo.

Possiamo considerare il *codice* $C(G)$ di un grafo G, cioè il codice binario generato dalla matrice di incidenza $N(G)$. Un grafo H è un *duale di Whitney* di G quando $E(G) = E(H)$ e il codice $C(G)$ coincide con il codice duale $C(H)^\perp$ di H. Evidentemente H è duale di Whitney di G se e solo se G lo è di H. La definizione richiede che G, H abbiano lo stesso insieme di spigoli, per comodità di notazione; informalmente basta che i loro spigoli siano etichettati dallo stesso insieme, o posti in corrispondenza biunivoca.

Il codice di un poligono con n spigoli consiste di tutte le parole di lunghezza n e peso pari; il codice di un grafo a fascio con n spigoli consiste delle due parole costanti. Il codice di un albero consiste di tutte le parole; quello di un coalbero della sola parola nulla.

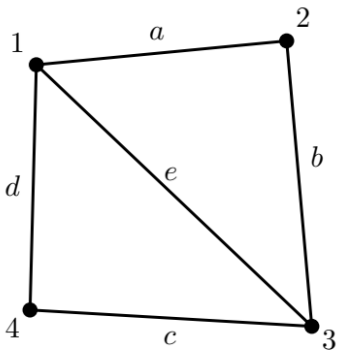
Alcuni termini della teoria dei grafi vengono usati in contesti diversi con significati variabili. In questo capitolo usiamo "ciclo", "circuito", "taglio" e "legame" per indicare certi sottoinsiemi, descritti sotto, di $E(G)$. Gli altri usi di questi termini eventualmente noti al lettore vanno temporaneamente dimenticati.

Come nel capitolo 20, il *supporto* di una parola x è il sottoinsieme degli indici delle sue coordinate non nulle. Per codici binari possiamo identificare le parole con i loro supporti. I supporti delle parole di $C(G)$ si chiamano *tagli* di G; quelli delle parole di $C(G)^\perp$ si chiamano *cicli* di G. I termini *circuito* e *legame* indicano rispettivamente cicli e tagli non vuoti minimali. Usiamo *spazio dei cicli* e *spazio dei tagli* per gli insiemi di tutti i cicli e di tutti i tagli, rispettivamente. Sono naturalmente spazi vettoriali su $\mathbb{F}_2$, dove la somma di due insiemi è la loro differenza simmetrica. Orig. 476

È abbastanza facile capire quando un sottoinsieme $S \subseteq E(G)$ è un ciclo o un taglio. La somma binaria delle righe della matrice di incidenza indicizzate dai vertici di X ha come supporto l'insieme $\times(X,Y)$ degli spigoli che "attraversano" da X a $Y := V(G) \setminus X$, cioè hanno un estremo in ciascuno dei due insiemi. Dunque S è un taglio se e solo se $S = \times(X,Y)$ per opportuni X, Y. Usiamo questa notazione soltanto quando X, Y partizionano l'insieme dei vertici; consentiamo che uno dei due sia vuoto, nel qual caso S è vuoto.

Un vettore di supporto S è ortogonale su $\mathbb{F}_2$ alla riga di N indicizzata dal vertice x se e solo se x è incidente a un numero pari di spigoli di S, contando due volte i cappi. I cicli sono dunque i sottoinsiemi di $E(G)$ per i quali ogni vertice ha grado pari in $G : S$, il sottografo ricoprente con insieme degli spigoli S.

Esempio 34.1. Sia G il grafo seguente.



La matrice di incidenza di G è

	a	b	c	d	e
1	1	0	0	1	1
2	1	1	0	0	0
3	0	1	1	0	1
4	0	0	1	1	0

.

Vi sono quattro cicli: $\varnothing$, $\{a,b,e\}$, $\{c,d,e\}$ e $\{a,b,c,d\}$. Gli ultimi tre sono in realtà circuiti. Vi sono otto tagli. L'insieme $\{a,b,c,d\}$ è sia un ciclo sia un taglio, essendo il supporto della somma delle righe 2 e 4. Non è però un legame: contiene un taglio più piccolo, per esempio il supporto $\{a,b\}$ della riga 2. L'insieme $\{a,b\}$ è un legame. Un altro esempio è $\{b,d,e\}$, supporto della somma delle righe $1,2$, oppure $3,4$. Orig. 477

Problema 34A. (i) Sia G connesso. Dimostrare una delle affermazioni equivalenti: il numero dei tagli è esattamente $2^{|V(G)|-1}$; la dimensione dello spazio dei tagli è $|V(G)|-1$. (ii) Dimostrare in generale che la dimensione dello spazio dei tagli è $|V(G)|-|C(G)|$, dove $C(G)$ è l'insieme delle componenti. Come corollario, la dimensione dello spazio dei cicli è $|E(G)|-|V(G)|+|C(G)|$.[1]

Esempio 34.2. Gli spazi dei cicli di K_6 e del grafo di Petersen sono codici binari di lunghezza 15 e dimensioni rispettivamente 10 e 6. (La figura 35.1 del prossimo capitolo mostra che K_6 è duale del grafo di Petersen rispetto a un'immersione nel piano proiettivo reale; non sono però duali di Whitney, poiché la somma delle dimensioni dei loro codici supera il numero degli spigoli.) Le distanze minime sono rispettivamente 3 e 5. Osserviamo che si può aggiungere il vettore con tutte le componenti uguali a 1 a un insieme di generatori di questi due codici: le distanze minime rimangono 3 e 5, mentre in entrambi i casi la dimensione aumenta di 1.

Teorema 34.1. Sia G un grafo. (i) Un insieme $S \subseteq E(G)$ è un circuito se e solo se è l'insieme degli spigoli di un sottografo poligonale di G. (ii) Supponiamo G connesso. Un taglio $\times(X,Y)$ è un legame se e solo se i sottografi indotti da X e da Y sono entrambi connessi.

Dimostrazione. È evidente che gli spigoli di un poligono formano un ciclo non vuoto minimale. Un ciclo non vuoto non può essere l'insieme degli spigoli di una foresta, poiché ogni albero ha vertici monovalenti, e contiene quindi gli spigoli di un poligono. Un ciclo non vuoto minimale è dunque l'insieme degli spigoli di un poligono.

Sia $S = \times(X,Y)$. Se i sottografi indotti da X, Y sono connessi, S non può contenere propriamente un taglio non vuoto, poiché cancellare un sottoinsieme proprio dei suoi spigoli non produce un grafo sconnesso. Se invece, per esempio, il sottografo indotto da Y non è connesso, esiste una partizione di Y in insiemi non vuoti Y_1, Y_2 senza spigoli tra loro. Allora $S' := \times(X \cup Y_1, Y_2)$ è contenuto in S. La connessione assicura che vi siano spigoli sia tra X, Y_1 sia tra X, Y_2, perciò S' è non vuoto ed è un sottoinsieme proprio di S. □ Orig. 478

Il lettore può verificare che un insieme di spigoli di un grafo arbitrario è un legame se e solo se è un legame in una delle sue componenti. Inoltre S è un legame se e solo se la cancellazione dei suoi spigoli produce un grafo con più componenti di G, per esempio un grafo sconnesso se G era connesso, ed S è minimale rispetto a questa proprietà.

Dato un insieme S di spigoli, esso è un circuito se e solo se cancellare gli spigoli non in S e gli eventuali vertici isolati produce un poligono; è un legame se e solo se contrarre gli spigoli non in S e cancellare gli eventuali vertici isolati produce un grafo a fascio.

L'insieme $S(x)$ degli spigoli incidenti a un vertice x, esclusi i cappi, è sempre un taglio. Questi insiemi generano lo spazio dei tagli, essendo i supporti delle righe della matrice di incidenza. Per il teorema 34.1(ii), $S(x)$ è un legame per ogni $x \in V(G)$ se e solo se G è 2-connesso, oppure è un grafo connesso con due vertici.

Problema 34B. Mostrare che i circuiti generano lo spazio dei cicli e i legami generano lo spazio dei tagli. Basta verificare che le parole non nulle di un codice lineare binario C i cui supporti siano minimali tra i supporti di tutte le parole non nulle generano il codice. Questo vale per codici lineari su qualunque campo.

Quindi G, H sono duali di Whitney quando i circuiti di G sono esattamente i legami di H, oppure quando i legami di G sono esattamente i circuiti di H.

[1] Nota redazionale: qui $C(G)$ indica l'insieme delle componenti, mentre sopra indicava il codice del grafo; si conserva la notazione dell'originale.

Esempio 34.3. I due grafi descritti da ciascuna tabella della figura 34.2 sono duali di Whitney, poiché ogni coppia è formata da duali planari: si veda il teorema 34.2 qui sotto. Per esempio, $\{a, e, g, c\}$ e $\{a, j, b\}$ sono legami nel cubo G e circuiti in G^*; l'insieme $\{a, b, c, d\}$ è un circuito in G e un legame in G^*. Orig. 479

Problema 34C. Siano G, H duali di Whitney con $E(G) = E(H) = E$. Spiegare perché G'_e e H''_e sono duali di Whitney per ogni $e \in E$.

Problema 34D. Siano G, H duali di Whitney con $E(G) = E(H) = E$, entrambi connessi. Mostrare che S è l'insieme degli spigoli di un albero ricoprente in G se e solo se $E \setminus S$ lo è in H.

Teorema 34.2. Un grafo G è planare se e solo se ha un duale di Whitney. Un duale G^* rispetto a un qualsiasi disegno planare di G è un duale di Whitney.

Per ora dimostriamo soltanto la seconda frase, che implica la necessità nella prima, rinviando l'altra parte alla fine del capitolo.

Dimostrazione. Sia G^* un duale planare di G relativo a un suo disegno planare.

Sia S un circuito di G. Esso è l'insieme degli spigoli di un sottografo poligonale P che, per il teorema della curva di Jordan, divide la sfera o il piano in due parti. Siano F_1 le facce interne a P e F_2 quelle esterne: esse partizionano i vertici di G^*. Ogni spigolo di P è incidente a una faccia di F_1 e una di F_2. Ogni altro spigolo giace, tranne eventualmente gli estremi, in una delle due parti ed è quindi incidente soltanto a elementi di F_1 oppure di F_2. In conclusione $S = \times(F_1, F_2)$ è un taglio di G^*. Poiché i circuiti generano lo spazio dei cicli di G, abbiamo mostrato che questo è contenuto nello spazio dei tagli di G^*.

Osserviamo ora che, per un'immersione in una superficie qualsiasi, lo spazio dei tagli di G^* è contenuto nello spazio dei cicli di G. Gli spigoli incidenti a un vertice hanno un ordine ciclico, nel quale i cappi compaiono due volte. Partizioniamo i vertici di G^*, cioè le regioni o facce, colorandoli per esempio di rosso e blu, e consideriamo il taglio C formato dagli spigoli incidenti a una regione rossa e una blu. Il numero degli spigoli di C incidenti a un vertice di G è certamente pari: si veda la figura 34.6. È come dire che, se i vertici di un poligono sono rossi o blu, il numero degli spigoli con estremi di colore diverso è pari. Quindi C è un ciclo di G. Pertanto lo spazio dei cicli di G coincide con lo spazio dei tagli di G^*. □ Orig. 480

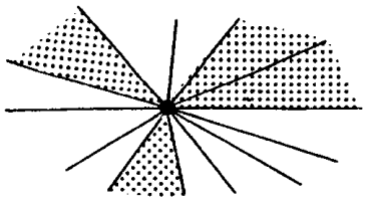


Figura 34.6

La formula di Eulero è un corollario di quanto abbiamo dimostrato. Per il problema 34A, lo spazio dei cicli di G ha dimensione $|E(G)| - (|V(G)| - |C(G)|)$, mentre lo spazio dei tagli di G^* ha dimensione $|F(G)| - 1$, avendo osservato che G^* è sempre connesso. Uguagliandole otteniamo (33.2).

Il teorema di Whitney permette una rapida dimostrazione del seguente teorema di S. MacLane (1937).

Teorema 34.3. Un grafo G è planare se e solo se il suo spazio dei cicli possiede una base $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ tale che ciascuno spigolo compaia in al più due suoi elementi.

Dimostrazione. Se G è planare, i bordi di tutte le facce tranne una forniscono una base del genere. Infatti, se G^* è il duale rispetto a un'immersione nel piano, poiché G^* è connesso, gli insiemi di tutti gli spigoli non cappi incidenti a ciascuno dei suoi vertici tranne uno, cioè alle facce di G tranne una, formano una base dello spazio dei tagli di G^*, che è lo spazio dei cicli di G. Ogni spigolo appartiene ad al più due di questi insiemi.

Supponiamo viceversa che esista una base come nell'enunciato. Poniamo $B_0 = B_1 + B_2 + \cdots + B_k$. Ogni spigolo appartiene a 0 oppure 2 degli insiemi B_i, $0 \le i \le k$. Definiamo un grafo H con vertici $0, 1, \ldots, k$ e insieme di spigoli $E(G)$: se e appartiene a due degli insiemi, B_j, B_ℓ, esso è incidente in H ai vertici j, ℓ; se non appartiene ad alcun B_i, è un cappio in H presso un vertice qualsiasi. Affermiamo che H è duale di Whitney di G.

L'insieme degli spigoli non cappi incidenti al vertice i di H è precisamente B_i, che è un taglio di H. Poiché i B_i generano i cicli di G, lo spazio dei cicli di G è contenuto nello spazio dei tagli di H. Il Orig. 481

primo ha dimensione k, mentre il secondo ha dimensione al più k, poiché H ha $k+1$ vertici. I due spazi coincidono: i grafi sono duali di Whitney. Per il teorema 34.2, G è quindi planare. □

Come promesso, ricaviamo ora risultati sui grafi planari e sui loro duali mediante la dualità di Whitney, senza fare alcun riferimento al piano o alla sfera.

Teorema 34.4. Se G, H sono duali di Whitney e H è connesso, G è bipartito se e solo se H è euleriano, cioè ammette un circuito euleriano.

DIMOSTRAZIONE. G è bipartito se e solo se l'intero insieme $E(G)$ è un taglio. Poiché G^* è connesso, è euleriano se e solo se $E(G)$ è un ciclo di G^*: si veda il teorema 1.2. Le due condizioni sono equivalenti poiché G^* è duale di Whitney di G.[2] □

Una *colorazione di Tait*, dal nome del matematico inglese P. G. Tait, di un grafo trivalente è una colorazione degli spigoli con tre colori, per esempio α, β, γ, tale che presso ogni vertice compaiano tutti e tre. La figura 34.7 ne mostra un esempio. L'esistenza di una colorazione di Tait equivale alla possibilità di partizionare gli spigoli in tre accoppiamenti perfetti (cfr. capitolo 5); dunque un grafo bipartito trivalente ammette una colorazione di Tait per il problema 5A.

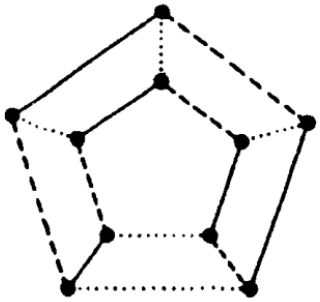


Figura 34.7

Teorema 34.5. Se G, H sono duali di Whitney e G è trivalente, G ammette una colorazione di Tait se e solo se H è 4-colorabile.

Orig. 482

DIMOSTRAZIONE. Affermiamo che un grafo trivalente G ammette una colorazione di Tait se e solo se esistono due cicli S_1, S_2 tali che $E(G) = S_1 \cup S_2$. Data la colorazione, prendiamo come S_1 l'unione degli spigoli di colore α, γ, e come S_2 quelli di colore β, γ. Sono entrambi cicli, poiché ogni vertice è incidente a due spigoli di ciascuno. Viceversa, se $E(G) = S_1 \cup S_2$, assegniamo a e il colore

$$\begin{cases} \alpha & \text{se } e \in S_1,\ e \notin S_2, \\ \beta & \text{se } e \notin S_1,\ e \in S_2, \\ \gamma & \text{se } e \in S_1 \cap S_2. \end{cases}$$

Ogni vertice x ha grado pari, compreso tra 0 e 3, nei sottografi ricoprenti con spigoli S_1, S_2; poiché la loro unione è $E(G)$, entrambi i gradi sono 2 e vi è uno spigolo di ogni colore incidente a x.

La seconda affermazione è che H ammette una colorazione propria con quattro colori se e solo se $E(H)$ è unione di due tagli. Se $E(H) = \times(X_1, X_2) \cup \times(Y_1, Y_2)$, allora $X_1 \cap Y_1, X_1 \cap Y_2, X_2 \cap Y_1, X_2 \cap Y_2$ sono le classi di una colorazione propria con quattro colori. Se invece A, B, C, D sono tali classi, $E(H)$ è l'unione di $\times(A \cup B, C \cup D)$ e $\times(A \cup C, B \cup D)$.

Le due osservazioni, con la definizione di dualità di Whitney, concludono la dimostrazione. □

Un *istmo* è uno spigolo la cui cancellazione aumenta il numero delle componenti, cioè sconnette il grafo se questo era connesso. È il concetto duale di cappio. Un istmo è uno spigolo e per il quale il singoletto $\{e\}$ è un taglio; un cappio è uno spigolo e per il quale $\{e\}$ è un ciclo. Alcuni autori chiamano l'istmo *spigolo aciclico*, non essendo contenuto in alcun circuito; si usa anche il termine *ponte*.

Problema 34E. Mostrare che un grafo trivalente con un istmo non ammette una colorazione di Tait.

Per il teorema dei quattro colori, ogni grafo planare trivalente senza istmi ammette una colorazione di Tait. Un istmo di G corrisponderebbe a un cappio nel duale, che non potrebbe essere colorato propriamente. La planarità è necessaria: il grafo di Petersen è trivalente e senza istmi, ma non ammette una

Orig. 483

[2]Nota redazionale: nella dimostrazione l'originale denota il duale H con G^*.

colorazione di Tait.

Viceversa, per dimostrare il teorema dei quattro colori basterebbe stabilire che ogni grafo planare trivalente senza istmi ammette una colorazione di Tait. Supponiamo infatti che le regioni di ogni grafo planare trivalente senza istmi possano essere colorate propriamente con quattro colori. Dato un grafo planare G, sostituiamo ciascun vertice x di grado diverso da 3 con la configurazione indicata nella figura 34.8 per il caso di grado 5. Questo si può fare anche per gradi 1 e 2. Si creano altre regioni, cioè altri vertici nel duale G^*, ma si conserva l'adiacenza delle regioni originali. Una colorazione con quattro colori delle regioni del grafo ampliato, ormai trivalente, fornisce quindi una colorazione di quelle del grafo originale. Per il teorema 34.5, le regioni del grafo ampliato sono 4-colorabili se e solo se esso ammette una colorazione di Tait.

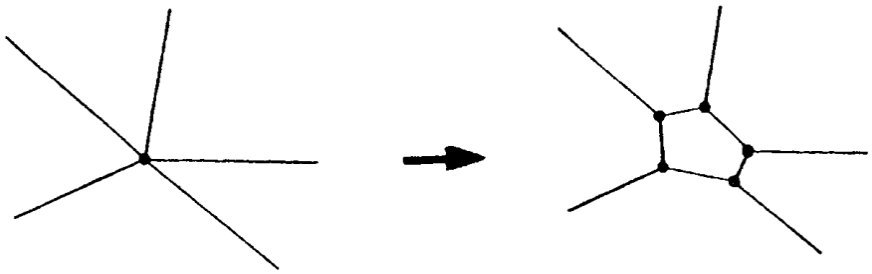


Figura 34.8

Nel 1880 Tait congetturò che ogni grafo planare trivalente 3-connesso abbia un circuito hamiltoniano; ciò avrebbe implicato l'esistenza di una colorazione di Tait. W. T. Tutte (1956) trovò un controesempio, ma dimostrò che ogni grafo planare trivalente 4-connesso è hamiltoniano.[3]

Teorema 34.6. Se G, H sono duali di Whitney senza vertici isolati e G è non separabile, anche H è non separabile.

Dimostrazione. Il teorema 32.2 mostra che ogni coppia di spigoli di G è contenuta in un suo circuito. Quindi ogni coppia di spigoli di H è contenuta in un suo legame. Se due spigoli a, b appartengono a un legame $\times(X, Y)$, possiamo trovare un cammino semplice nel sottografo indotto da X che congiunga un estremo di a a uno di b, e uno nel sottografo indotto da Y che congiunga gli altri estremi: otteniamo così un poligono contenente a, b. Ogni coppia di spigoli di H è dunque contenuta in un circuito di H, e questo implica la non separabilità. □ Orig. 484

Corollario. L'insieme degli spigoli incidenti a una faccia in un'immersione planare di un grafo non separabile G, diverso dal grafo-spigolo, è un circuito di G.

Dimostrazione. L'insieme S degli spigoli incidenti a una faccia è l'insieme degli spigoli incidenti a un vertice di G^*. Ma G^* è non separabile per il teorema 34.5,[4] quindi S è un legame di G^* e dunque un circuito di G. □

Problema 34F. Due spigoli a, b di un grafo connesso G contenuti insieme in un circuito appartengono anche a uno stesso legame.

Teorema 34.7. Siano G, H grafi semplici senza vertici isolati, duali di Whitney. Se G è 3-connesso, anche H lo è.

Dimostrazione. Supponiamo G 3-connesso. Per $x \in V(G)$, sia $S(x)$ l'insieme degli spigoli incidenti a x. Ciascun $S(x)$ è un legame tale che $G'_{S(x)}$ sia non separabile; questi legami generano, per definizione, lo spazio dei tagli di G.

In H esiste quindi una famiglia $\mathcal{F}$ di circuiti che genera lo spazio dei cicli, ciascun elemento S della quale ha la proprietà che H''_S sia non separabile.

Sappiamo che H è non separabile; supponiamo per assurdo che non sia 3-connesso. Allora H è l'unione a spigoli disgiunti di due sottografi A, B, ciascuno con almeno due spigoli, la cui intersezione consiste di due vertici isolati, diciamo x, y. Un poligono di H che contenga spigoli sia di A sia di B deve avere tra

[3] Nota redazionale: un grafo trivalente non può essere 4-connesso rispetto ai vertici. Il risultato di Tutte riguarda ogni grafo planare 4-connesso, senza l'aggettivo "trivalente", presente nell'originale.

[4] Nota redazionale: il riferimento corretto è al teorema 34.6.

i suoi vertici x, y. Contraendone gli spigoli otterremmo un grafo separabile: esso sarebbe l'unione dei grafi ottenuti da A, B contraendo gli spigoli del poligono in ciascuno, e identificando così x, y. Questi sottografi contratti avrebbero in comune soltanto il vertice risultante dall'identificazione dei vertici del poligono; il lettore può verificare che in ciascuno rimane almeno uno spigolo. Quindi i circuiti di $\mathcal{F}$ sono contenuti interamente in $E(A)$ oppure in $E(B)$. Sia C un circuito qualsiasi di H. Poiché $\mathcal{F}$ genera lo spazio dei cicli, $C \cap E(A)$ e $C \cap E(B)$ sono rispettivamente somme modulo 2 di elementi di $\mathcal{F}$ contenuti in $E(A)$ e in $E(B)$. Entrambe le intersezioni sarebbero quindi cicli, e la minimalità di C imporrebbe che una fosse vuota. Ogni circuito di H sarebbe dunque contenuto in $E(A)$ o in $E(B)$, in contraddizione con la non separabilità di H. □ Orig. 485

Problema 34G. (i) Sia G un grafo semplice 3-connesso e S un suo legame. Mostrare che G'_S è non separabile se e solo se $S = S(x)$, insieme degli spigoli incidenti a un vertice x di G. (ii) Dimostrare: se G, H sono grafi semplici 3-connessi con codici equivalenti, allora sono isomorfi.

Teorema 34.8. Sia G un grafo semplice 3-connesso immerso nella sfera. Un circuito C è l'insieme degli spigoli incidenti a una faccia di questa immersione se e solo se G''_C è non separabile.

Dimostrazione. C è l'insieme degli spigoli incidenti a una faccia se e solo se è quello degli spigoli incidenti a un vertice del duale $H := G^*$. Per il problema 34G(i), ciò accade se e solo se H'_C è non separabile. Quest'ultimo grafo è duale di Whitney di G''_C. □

I poligoni che delimitano le facce di un'immersione di un grafo planare semplice 3-connesso sono dunque univocamente determinati. Non è così per i grafi non separabili in generale: si veda la figura 34.5. Se conosciamo le facce, cioè i circuiti che le delimitano, l'immersione è determinata (questo sarà in parte spiegato nel prossimo capitolo), e otteniamo il risultato seguente.

Corollario. Un grafo planare semplice 3-connesso ha un'unica immersione nella sfera.

Esempio 34.4. Se K_5 fosse planare, nessun quadrilatero potrebbe essere una faccia: contraendone i quattro spigoli si ottiene infatti un grafo con due vertici, quattro spigoli di collegamento e due cappi presso uno dei vertici, che non è non separabile. Viceversa, un triangolo sarebbe necessariamente una faccia. Otteniamo un'altra dimostrazione della non planarità dei grafi semplici 3-connessi $K_5, K_{3,3}$ e del grafo di Petersen: contraendo gli spigoli di un triangolo di K_5, di un quadrilatero di $K_{3,3}$ o di un pentagono del grafo di Petersen, si ottiene sempre un grafo non separabile. Se fossero planari, per il teorema 34.8 ogni triangolo, quadrilatero e pentagono, rispettivamente, delimiterebbe una faccia. Ma ogni spigolo appartiene a tre triangoli, quattro quadrilateri e quattro pentagoni nei rispettivi grafi: una contraddizione con la planarità. Orig. 486

E. Steinitz (1922) caratterizzò i grafi dei politopi convessi tridimensionali.

Teorema 34.9. Un grafo G è il grafo di un politopo convesso tridimensionale se e solo se è semplice, planare e 3-connesso.

Che il grafo di un politopo tridimensionale sia 3-connesso è un caso particolare del teorema 32.5. Non dimostriamo qui il resto del teorema.

Per la sufficienza nel teorema 34.2 serve un lemma.

Lemma 34.10. Siano G, H grafi con lo stesso insieme di spigoli E. Supponiamo che G sia l'unione di sottografi G_1, G_2 a spigoli disgiunti, con $|V(G_1) \cap V(G_2)| \leq 1$. Siano H_1, H_2 i sottografi di H con insiemi di spigoli $E(G_1), E(G_2)$, rispettivamente, eliminati i vertici isolati. (i) Se G, H sono duali di Whitney, lo sono G_i, H_i per $i = 1, 2$. (ii) Se G_i, H_i sono duali di Whitney per entrambi gli indici e $|V(H_1) \cap V(H_2)| \leq 1$, allora G, H sono duali di Whitney.

Dimostrazione. Dal teorema 34.1 si vede facilmente che ogni legame di G è contenuto interamente in $E(G_1)$ oppure in $E(G_2)$. Inoltre $S \subseteq E(G_i)$ è un legame di G_i se e solo se è un legame di G.

Supponiamo G, H duali di Whitney. Se S è un legame di G_i, è un circuito di H contenuto in $E(H_i)$ e dunque un circuito di H_i. Se S è un circuito di H_i, lo è anche di H, quindi è un legame di G contenuto in $E(G_i)$, ossia un legame di G_i.

Supponiamo che G_i, H_i siano duali di Whitney per $i = 1, 2$ e che $|V(H_1) \cap V(H_2)| \leq 1$. Un legame S di G è un legame di G_1 o G_2, dunque un circuito di H_1 o H_2 e certamente di H. Se S è un circuito di H, lo è di H_1 oppure di H_2; quindi è un legame di G_1 oppure di G_2, e dunque di G. □ Orig. 487

Dimostrazione del teorema 34.2, continuazione. Per il viceversa, stabiliamo dapprima l'affermazione seguente. Data una coppia G, H di duali di Whitney senza vertici isolati, con lo stesso insieme di spigoli

E, esiste un duale di Whitney eventualmente diverso $\widetilde{H}$ che ammette quello che chiameremo un *sistema di passeggiate* per G. Si tratta di una famiglia $\{w_x : x \in V(G)\}$ di passeggiate in $\widetilde{H}$, una per ciascun vertice x di G, tale che w_x percorra in $\widetilde{H}$ esattamente gli spigoli incidenti a x in G, due volte i cappi e una volta gli altri spigoli. Procediamo per induzione sul numero degli spigoli. Possiamo supporre G privo di vertici isolati.

L'affermazione è facile se G è non separabile. Vale naturalmente per un grafo-cappio. Altrimenti non vi sono cappi e, per ogni vertice x, l'insieme $S(x)$ degli spigoli incidenti a x è un legame di G, dunque un circuito di H. Basta prendere come w_x un cammino semplice chiuso in H che percorra gli spigoli di $S(x)$.

Se G non è non separabile, esistono sottografi G_1, G_2 a spigoli disgiunti, ciascuno con almeno uno spigolo, senza vertici in comune oppure con uno solo, la cui unione è G. Con H_1, H_2 come nel lemma 34.10, H_i è duale di Whitney di G_i, per $i = 1, 2$. Per ipotesi induttiva esistono duali di Whitney $\widetilde{H}_i$ di G_i che ammettono sistemi $\{w_x^{(i)} : x \in V(G_i)\}$ per G_i. Possiamo supporre $\widetilde{H}_1, \widetilde{H}_2$ a vertici disgiunti. Se G_1, G_2 sono disgiunti, prendiamo come $\widetilde{H}$ l'unione disgiunta dei due duali: l'unione dei sistemi di passeggiate fornisce il sistema per G. Se G_1, G_2 condividono un vertice z, esistono passeggiate $w_z^{(1)}, w_z^{(2)}$ nei due duali che percorrono gli spigoli incidenti a z in G_1, G_2, rispettivamente. Otteniamo $\widetilde{H}$ unendo i duali e identificando un vertice della prima passeggiata con un vertice della seconda. Combiniamo queste due passeggiate in una sola, che percorre gli spigoli incidenti a z in G; insieme alle altre passeggiate, essa dà il sistema richiesto. In entrambi i casi $\widetilde{H}$ è un duale di Whitney di G per il lemma 34.10.

Orig. 488

Dimostriamo infine quanto segue. Sia G un grafo con un duale di Whitney H che ammette un sistema di passeggiate $\{w_x : x \in V(G)\}$ per G. Affermiamo che G ammette un'immersione nella sfera tale che gli spigoli incidenti a x in G si presentino nello stesso ordine ciclico in cui compaiono in w_x. Procediamo per induzione sul numero degli spigoli.

Se G ha soltanto cappi, H è una foresta. Sia e un cappio di G che sia incidente a un vertice monovalente in H, e sia z il vertice incidente a e in G. La passeggiata w_z in H percorre evidentemente e due volte consecutive, per esempio

$$w_z = (s_0, e, s_1, e, s_2 = s_0, a_3, s_3, a_4, s_4, \ldots, a_k, s_0),$$

dove gli s_i sono vertici di H. I grafi G'_e, H''_e sono duali di Whitney; sopprimendo e in w_z si ottiene un sistema di passeggiate in H''_e per G'_e. Per ipotesi induttiva, G'_e ammette un disegno planare nel quale gli spigoli incidenti a z hanno lo stesso ordine ciclico della passeggiata w_z privata di e. In un piccolo intorno del punto rappresentante z possiamo inserire il cappio e e ottenere l'immersione richiesta di G (figura 34.9).

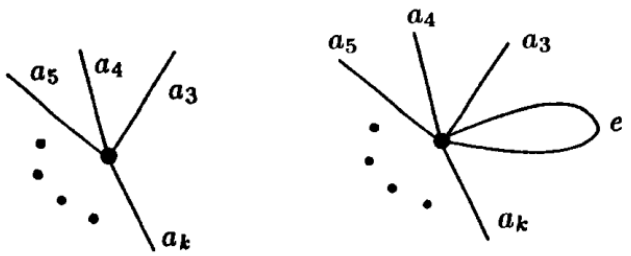


Figura 34.9

Sia ora e uno spigolo non cappio di G, con estremi y, z. Allora G''_e, H'_e sono duali di Whitney e affermiamo che esiste un sistema naturale di passeggiate $\{u_x : x \in V(G''_e)\}$ in H'_e per G''_e. Per $x \neq y, z$ poniamo $u_x := w_x$. Per il nuovo vertice x_0, ottenuto identificando y, z, combiniamo w_y, w_z omettendo e nel modo seguente. Siano

$$w_y = (s_0, e, s_1, a_2, s_2, \ldots, s_{k-1}, a_k, s_0)$$

e

Orig. 489

$$w_z = (t_0, e, t_1, b_2, t_2, \ldots, t_{m-1}, b_m, t_0),$$

dove $e, a_2, a_3, \ldots, a_k$ ed $e, b_2, b_3, \ldots, b_m$ sono gli spigoli incidenti in G a y e z, rispettivamente, con i cappi ripetuti due volte, e gli s_i, t_j sono vertici di H. Invertendo una passeggiata se necessario, possiamo supporre $s_0 = t_0$ e $s_1 = t_1$. Poniamo quindi

$$u_{x_0} := (s_1, a_2, s_2, \ldots, s_{k-1}, a_k, s_0, b_m, t_{m-1}, b_{m-1}, \ldots, b_3, t_2, b_2, s_1).$$

Per ipotesi induttiva, G''_e ammette un'immersione nel piano nella quale gli spigoli incidenti a x hanno lo stesso ordine ciclico della passeggiata u_x. In un piccolo intorno del punto che rappresenta x_0 possiamo "annullare la contrazione" di e, ottenendo l'immersione richiesta di G (figura 34.10). □

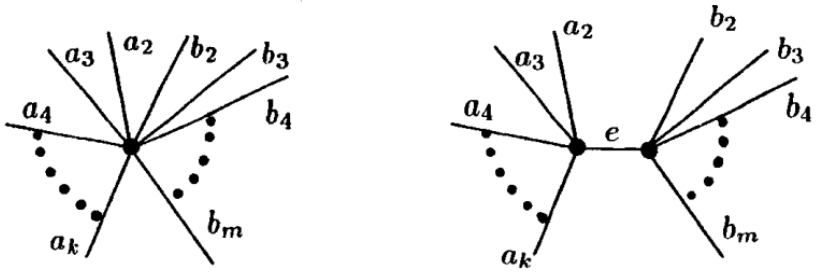


Figura 34.10

Problema 34H. In un grafo k-connesso secondo Tutte, definito nel problema 32D, con almeno $2k-2$ spigoli, ogni circuito e ogni legame contiene almeno k spigoli.

Problema 34I. Un *matroide* consiste di un insieme X, qui supposto finito, e di una famiglia $\mathcal{C}$ di sottoinsiemi non vuoti, detti circuiti, tali che nessun circuito sia un sottoinsieme proprio di un altro e, se $A, B \in \mathcal{C}$, $x \in A \cap B$, $y \in A \setminus B$, esista $C \in \mathcal{C}$ con $C \subseteq A \cup B$, $y \in C$, $x \notin C$. Quest'ultima proprietà si chiama "assioma di eliminazione".

(i) Dimostrare che l'insieme degli spigoli di un grafo finito, insieme alla famiglia di tutti i suoi circuiti, cioè insiemi degli spigoli di poligoni, è un matroide.

(ii) Dimostrare che i supporti non vuoti minimali delle parole di un codice lineare su un campo qualsiasi formano i circuiti di un matroide. (iii) Sia $(X, \mathcal{F})$ una geometria combinatoria come definita nel capitolo 23, e sia $\mathcal{C}$ la famiglia dei sottoinsiemi dipendenti minimali di X. Mostrare che $(X, \mathcal{C})$ è un matroide. Orig. 490

(Per risolvere tutte le parti può convenire dimostrare prima (iii) e dedurne le altre.)

Note

Hassler Whitney (1907–1989), pioniere della topologia, negli ultimi vent'anni della sua vita si occupò intensamente anche di educazione matematica. Fu professore a Harvard e poi all'Institute for Advanced Study di Princeton. Ricevette il premio Wolf nel 1982. Aveva una laurea in musica a Yale, suonava violino, viola e pianoforte, ed era primo violino della Princeton Community Orchestra.

I matroidi furono introdotti da Hassler Whitney nel 1935 per astrarre certe proprietà dell'indipendenza lineare, dei circuiti e dei legami nei grafi, e della dualità. La loro teoria è "criptomorfa" a quella dei reticoli geometrici. Si vedano Welsh (1976) e Crapo e Rota (1971).

Riferimenti bibliografici

- H. Crapo e G.-C. Rota (1971), *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, M. I. T. Press.
- S. MacLane (1937), A structural characterization of planar combinatorial graphs, *Duke Math. J.* **3**, 460–472.
- P. G. Tait (1880), Remarks on the colouring of maps, *Proc. Roy. Soc. Edinburgh* **10**, 501–503.
- W. T. Tutte (1956), A theorem on planar graphs, *Trans. Amer. Math. Soc.* **82**, 99–116.
- W. T. Tutte (1984), *Graph Theory*, Encyclopedia of Math. and its Appl. **21**, Addison-Wesley.
- D. J. A. Welsh (1976), *Matroid Theory*, Academic Press.
- H. Whitney (1932), Nonseparable and planar graphs, *Trans. Amer. Math. Soc.* **34**, 339–362.
- H. Whitney (1935), On the abstract properties of linear dependence, *Amer. J. Math.* **57**, 509–533.

Capitolo 35

Immersioni di grafi sulle superfici

Orig. 491

Consideriamo immersioni di grafi su superfici diverse dalla sfera. La classificazione delle superfici (si veda Fréchet e Fan, 1967) mostra che, a meno di omeomorfismo, vi sono due famiglie infinite di superfici. Indichiamo con T_g, $g \geq 0$, la superficie orientabile di genere g, il *g-toro*. Essa si realizza come una sfera con g "manici" o g "buchi"; T_0 è la sfera. Indichiamo con N_n, $n \geq 1$, la superficie non orientabile ottenuta inserendo n "calotte incrociate" (*cross-cap*) sulla sfera; queste superfici non si possono immergere senza autointersezioni in $\mathbb{R}^3$. Enunciamo l'estensione della formula di Eulero. Una dimostrazione si trova in Fréchet e Fan (1967), oppure, per il caso orientabile, in Chartrand e Lesniak (1986).

Teorema 35.1. Per un'immersione a 2-celle di un grafo G su T_g,

$$|F(G)| - |E(G)| + |V(G)| = 2 - 2g.$$

Per un'immersione a 2-celle di un grafo connesso G su N_n,

$$|F(G)| - |E(G)| + |V(G)| = 2 - n.$$

Per un'immersione qualsiasi, non necessariamente a 2-celle, valgono le disuguaglianze ottenute sostituendo "=" con "≥" nelle formule precedenti.

Esempio 35.1. La figura 35.1 mostra un'immersione del grafo di Petersen P nel piano proiettivo reale N_1. Nel disegno si devono identificare i punti diametralmente opposti del bordo. Vi sono sei facce, tutte pentagonali. Più precisamente, il grafo duale rispetto a questa immersione è il grafo completo K_6.

Orig. 492

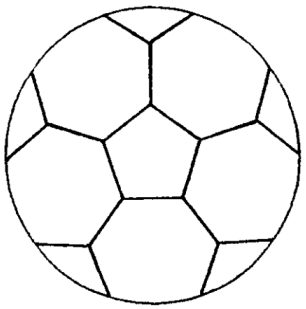


Figura 35.1

Questo stabilisce una curiosa corrispondenza biunivoca tra i 15 spigoli di P e quelli di K_6. Abbiamo già visto una corrispondenza biunivoca tra i 10 vertici di P e i 10 spigoli di K_5.

Il piano proiettivo reale può essere pensato come la superficie della sfera con i punti diametralmente opposti identificati. Il grafo di Petersen può essere pensato come il grafo di un dodecaedro regolare con i punti diametralmente opposti identificati.

Esempio 35.2. La figura 35.2 mostra un'immersione di K_7 nel toro T_1. Usiamo la rappresentazione consueta del toro: i lati orizzontali e quelli verticali del bordo vanno identificati. Vi sono 14 facce triangolari. Il duale ha 14 vertici di grado 3 e sette facce esagonali, a due a due adiacenti. È il grafo di

Heawood, definito nel capitolo 31, che fornisce un esempio di carta sul toro le cui facce richiedono sette colori.

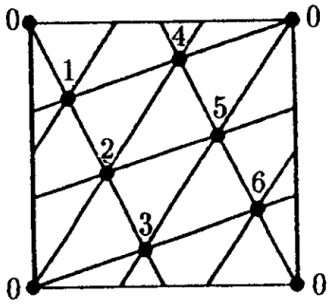


Figura 35.2

Orig. 493

Teorema 35.2. Se un grafo senza cappi G ammette un'immersione in T_g, con $g > 0$, allora

$$\chi(G) \leq \frac{7 + \sqrt{1 + 48g}}{2}.$$

DIMOSTRAZIONE. Supponiamo che G si immerga in T_g. Possiamo assumerlo semplice, connesso e con almeno tre vertici. Affermiamo che esiste un vertice x di grado al più $N-1$, dove $N := (7+\sqrt{1+48g})/2$. Una volta stabilito questo, il teorema segue per induzione sul numero dei vertici: eliminato x e colorato propriamente il grafo rimanente con $\lfloor N \rfloor$ colori, resta un colore libero per x.

Per il teorema 35.1,

$$2 - 2g \leq f - e + v,$$

dove $f := |F(G)|$, $e := |E(G)|$, $v := |V(G)|$. Ogni faccia è incidente ad almeno tre spigoli, quindi $3f \leq 2e$. Sia d il grado medio dei vertici. Supponiamo per assurdo $d > N-1$, da cui $v > N$. Inoltre $d > 6$, poiché $N \geq 7$ per $g \geq 1$, e

$$\begin{aligned} 2 - 2g &\leq \tfrac{2}{3}e - e + v = -\tfrac{1}{3}e + v = -\tfrac{1}{6}vd + v = \tfrac{1}{6}v(6-d), \\ 12g - 12 &\geq v(d-6) > N(N-7) = 12g - 12. \end{aligned}$$

Ecco la contraddizione promessa. □

Segue una breve tabella delle maggiorazioni del teorema 35.2:

Genere g	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\chi \leq$	7	8	9	10	11	12	12	13	13	14	15	15	16	16	16

L'affermazione che il teorema 35.2 fosse ottimale, cioè che qualche grafo immerso in T_g richiedesse $\lfloor (7+\sqrt{1+48g})/2 \rfloor$ colori, fu nota come *congettura di Heawood* fino alla dimostrazione di Ringel e Youngs nel 1968. Si veda Ringel (1974). Essi dimostrarono in realtà il risultato più forte seguente.

Orig. 494

Teorema 35.3 (Ringel–Youngs). Dato $g \geq 0$, poniamo

$$n := \left\lfloor \frac{7 + \sqrt{1 + 48g}}{2} \right\rfloor.$$

Allora il grafo completo K_n si può immergere in T_g.

Qui dimostreremo soltanto una piccola parte del risultato (si veda il teorema 35.4 qui sotto).[1] Per esempio, il teorema 35.3 dà $\chi(G) \leq 19$ per grafi immersi in T_{20}, T_{21}, T_{22}. Il teorema 35.4 mostra che K_{19} si immerge in T_{20}, e quindi anche in T_{21}, T_{22}, verificando la congettura di Heawood per $g = 20, 21, 22$.

Dobbiamo comprendere combinatoriamente le immersioni a 2-celle, in termini del grafo stesso. Ecco il punto essenziale.

Data un'immersione a 2-celle di G su una superficie S, possiamo percorrere il bordo di ogni faccia F ottenendo una passeggiata chiusa w_F in G. Non sono importanti il vertice iniziale né il verso. Spesso

[1] Nota redazionale: il risultato annunciato compare nell'originale con il numero 35.8, mantenuto in questa traduzione; i riferimenti a 35.4 in questo paragrafo rinviano ad esso.

si tratta di un cammino semplice chiuso; ma, per esempio, se G è un albero immerso nella sfera, vi è una sola faccia e la passeggiata percorre ogni spigolo due volte (figura 2.4). In generale ogni spigolo appartiene a esattamente due passeggiate di $\{w_F : F \in F(G)\}$ oppure compare due volte in una di esse. Un sistema $\mathcal{M}$ di passeggiate chiuse con questa proprietà, cioè nel quale ogni spigolo di G compare due volte complessivamente, si chiamerà una *maglia* di G.

Esempio 35.3. Ecco due maglie in K_5, descritte mediante le sequenze dei vertici:

$$\begin{aligned}\mathcal{M}_1 = \{&(1,2,3,4,5,1),\\ &(1,2,4,1),(2,3,5,2),(3,4,1,3),(4,5,2,4),(5,1,3,5)\},\\ \mathcal{M}_2 = \{&(1,2,4,5,1),(1,3,2,5,3,4,2,3,5,4,1),(1,4,3,1,5,2,1)\}.\end{aligned}$$

La maglia $\mathcal{M}_1$ consiste di cammini semplici, un pentagono e cinque triangoli; la seconda passeggiata di $\mathcal{M}_2$ percorre invece due spigoli due volte.

Una *maglia triangolare* è costituita da cammini semplici chiusi di lunghezza 3. Una maglia triangolare di K_n equivale quindi a un 2-disegno $S_2(2,3,n)$ con blocchi di cardinalità 3 e indice 2. Questi disegni corrispondono però raramente a immersioni di K_n su superfici, perché occorre un'importante condizione aggiuntiva. Data una maglia $\mathcal{M}$ in un grafo connesso G, possiamo tentare di costruire un'immersione a 2-celle nella quale le passeggiate delimitino le facce. Non abbiamo in realtà scelta e dobbiamo procedere così. A ogni passeggiata $w \in \mathcal{M}$ di lunghezza ℓ facciamo corrispondere un disco chiuso F_w, per esempio un ℓ-gono convesso con il suo interno nel piano, anche per $\ell = 1, 2$, benché in questi casi gli spigoli non possano essere segmenti rettilinei. Etichettiamo i vertici e gli spigoli di F_w con i vertici e gli spigoli della passeggiata, nel loro ordine. Se essa non è un cammino semplice chiuso, alcuni vertici ed eventualmente spigoli del disco ricevono la stessa etichetta. "Incolleremo" o "cuciremo" questi dischi lungo i bordi. Orig. 495

Consideriamo l'unione disgiunta dei dischi F_w. Per ogni vertice x di G identifichiamo tutti i punti etichettati x. Per ogni spigolo e identifichiamo i punti interni degli spigoli dei dischi etichettati e mediante una corrispondenza continua biunivoca, nel verso indicato dagli estremi. Occorre convenire che i cappi abbiano due versi.

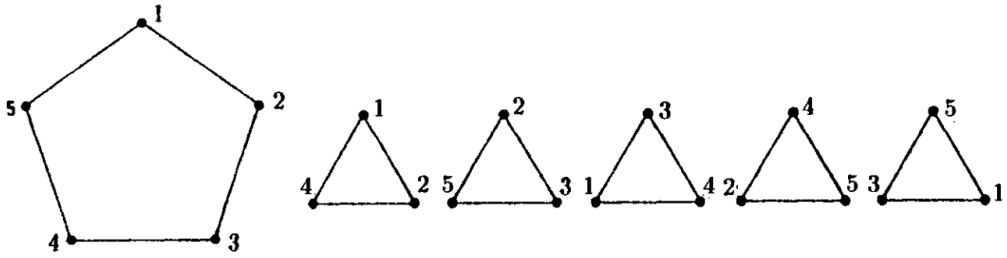


Figura 35.3

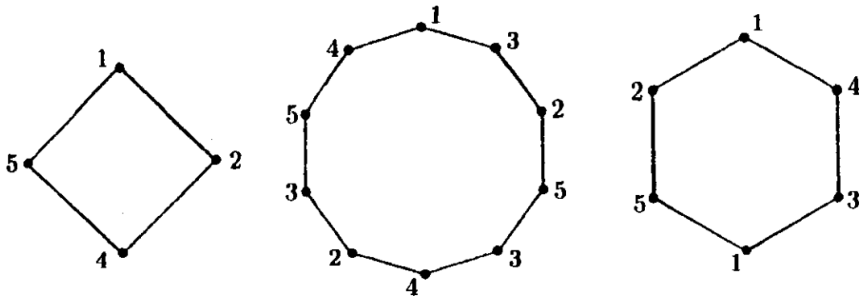


Figura 35.4

Le figure 35.3 e 35.4 mostrano regioni poligonali del piano, cioè dischi, etichettate rispettivamente dai vertici delle passeggiate nelle maglie dell'esempio 35.3. Nella figura 35.5 abbiamo iniziato l'incollamento dei dischi della figura 35.3; resta da identificare i punti diametralmente opposti del bordo, ottenendo il piano proiettivo reale con K_5 disegnato su di esso. Orig. 496

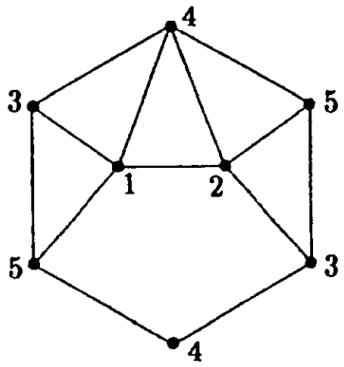


Figura 35.5

In generale, nello spazio topologico costruito mediante l'incollamento i punti interni ai dischi hanno intorni omeomorfi al disco aperto, cioè 2-celle; lo stesso vale per i punti interni agli spigoli dei bordi, poiché ogni spigolo appartiene a due passeggiate della maglia. Possono però sorgere difficoltà nei vertici, dove si incontrano molti dischi. Per esempio, supponiamo che le passeggiate passanti per un vertice x abbiano sequenze

$$(\ldots,1,x,2,\ldots),\quad (\ldots,2,x,3,\ldots),\quad (\ldots,3,x,1,\ldots),$$
$$(\ldots,4,x,5,\ldots),\quad (\ldots,5,x,6,\ldots),\quad (\ldots,6,x,4,\ldots).$$

I dischi corrispondenti alle prime tre formano attorno a x un intorno che è una 2-cella; aggiungendo gli altri tre, un intorno di x assomiglia a due coni che si toccano nei vertici. Il grafo $\mathcal{M}_x$ definito sotto sarebbe in questo caso l'unione di due triangoli disgiunti.

Per $x \in V(G)$, consideriamo il grafo $\mathcal{M}_x$ il cui insieme dei vertici è l'insieme degli spigoli di G incidenti a x, e nel quale a, b sono adiacenti quando compaiono come spigoli consecutivi in una passeggiata di $\mathcal{M}$, con x tra loro. Se compaiono consecutivamente due volte, congiungiamo a, b con due spigoli, anche se ciò probabilmente non accadrà spesso. Evidentemente $\mathcal{M}_x$ è regolare di grado 2. La *condizione ai vertici* richiede che $\mathcal{M}_x$ sia connesso, cioè un unico poligono, per ogni x. Orig. 497

Lo spazio costruito incollando una maglia in un grafo connesso è una superficie se e solo se la maglia soddisfa la condizione ai vertici. Esiste un'immersione naturale di G in questa superficie. Le maglie dell'esempio 35.3 soddisfano tale condizione. Si vedano l'esempio 35.4 e la figura 35.6.

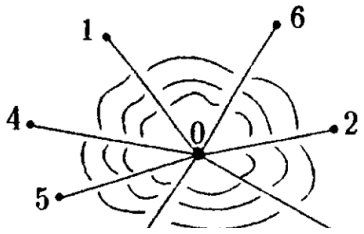


Figura 35.6

Per scoprire quale superficie S è stata costruita dalla maglia $\mathcal{M}$, calcoliamo prima la *caratteristica di Eulero* $h := |\mathcal{M}| - |E(G)| + |V(G)|$. Per il teorema 35.1, se h è dispari deve essere $S = N_{2-h}$. Se h è pari occorre decidere se la superficie è orientabile, salvo $h = 2$, quando la sfera è l'unica possibilità: $S = T_{1-h/2}$ nel caso orientabile, $S = N_{2-h}$ altrimenti. Affermiamo senza dimostrazione che S è orientabile se e solo se si possono orientare le passeggiate, scegliendo uno dei due versi per ciascuna, in modo che ogni spigolo venga percorso esattamente una volta in ciascun verso. In questo caso anche la maglia si dice *orientabile*.

È facile controllare l'orientabilità di una maglia che soddisfi la condizione ai vertici. Orientiamo una passeggiata: questo determina il verso di tutte quelle che condividono uno spigolo con essa, e quindi di altre ancora. La condizione ai vertici implica che sia determinato il verso di ogni passeggiata della maglia (perché?). Controlliamo poi, spigolo per spigolo, i versi in cui viene percorso.

Esempio 35.3, continuazione. La maglia $\mathcal{M}_1$ fornisce un'immersione di K_5 nel piano proiettivo reale N_1. La maglia $\mathcal{M}_2$ è orientabile: basta orientare le passeggiate come sono state scritte. Otteniamo

un'immersione a 2-celle di K_5 nel doppio toro T_2. Negli esempi seguenti, descrivendo passeggiate di grafi semplici elencheremo le sequenze di vertici tra parentesi quadre, omettendo il vertice finale perché coincide con quello iniziale. Conviene inoltre chiamare triangoli, quadrilateri, ecc. i cammini di lunghezza $3, 4, \ldots$, ignorando la differenza tra passeggiate nel grafo e sottografi poligonali. Orig. 498

Esempio 35.4. Mostriamo che K_8 si può immergere nel doppio toro T_2. Sono quindi necessari almeno otto colori per T_2, e la congettura di Heawood è provata per $g = 2$.

Devono esserci 18 facce, perché $f - e + v = -2$, e la somma dei loro gradi deve essere 56. Esibiamo una soluzione con due quadrilateri e 16 triangoli come facce, usando i "metodi delle differenze" (cfr. capitolo 19).

Prendiamo come vertici di K_8 gli elementi di $\mathbb{Z}_8$. I quadrilateri hanno sequenze $[0, 2, 4, 6]$ e $[1, 3, 5, 7]$. I triangoli sono i traslati modulo 8 dei due triangoli iniziali $[0, 1, 4]$ e $[0, 3, 2]$. Il lettore controlli che ogni spigolo compaia in esattamente due passeggiate. Verifichiamo la condizione ai vertici. Poiché le traslazioni modulo 8 conservano i poligoni, basta controllare il vertice 0. Le passeggiate che lo attraversano sono $[0, 2, 4, 6]$, $[0, 1, 4]$, $[7, 0, 3]$, $[4, 5, 0]$, $[0, 3, 2]$, $[5, 0, 7]$ e $[6, 1, 0]$. Si raccordano in un unico poligono come nella figura 35.6.

Resta da controllare l'orientabilità. Orientando i quadrilateri come $[0, 2, 4, 6]$ e $[7, 5, 3, 1]$, e invertendo anche un triangolo ogni due, cioè ogni volta che si trasla un triangolo iniziale mediante un elemento dispari di $\mathbb{Z}_8$, si ottiene una maglia orientata.

Problema 35A. Trovare una maglia di cinque quadrilateri in K_5, una di sei pentagoni in K_6 e una di sette esagoni in K_7, tutte soddisfacenti la condizione ai vertici. Quali superfici si sono costruite?

Problema 35B. Trovare una maglia di 16 pentagoni nel grafo di Clebsch (esempio 21.4). Controllare la condizione ai vertici e l'orientabilità. Quale superficie, se esiste, si è costruita? Qual è il duale rispetto a questa immersione? Cfr. il problema 35G.

Problema 35C. (i) Mostrare che, se un grafo semplice G è immerso nella superficie non orientabile N_g, $g \geq 1$, allora Orig. 499

$$\chi(G) \leq \frac{7 + \sqrt{1 + 24g}}{2}.$$

(ii) Mostrare che, se un grafo semplice è immerso nella bottiglia di Klein N_2, allora ha un vertice di grado al più 5 oppure è regolare di grado 6. Mostrare che esiste un'unica maglia di 14 triangoli in K_7 che soddisfa la condizione ai vertici e che essa è orientabile; dunque K_7 non si immerge nella bottiglia di Klein. Concludere che $\chi(G) \leq 6$ per i grafi immersi in N_2.

(Dunque, dopo tutto, K_7 non si immerge nella bottiglia di Klein. Concludiamo che $\chi(G) \leq 6$ per i grafi immersi in N_2.)

Problema 35D. Prima di proseguire con superfici diverse dalla sfera, osserviamo che la comprensione delle maglie permette una rapida dimostrazione del fatto seguente: se G, H sono duali di Whitney non separabili, esiste un'immersione di G nella sfera rispetto alla quale G^* sia isomorfo a H. Come nella dimostrazione del teorema 34.2, gli spigoli incidenti a un vertice di H formano un circuito di G. Il sistema di passeggiate così ottenuto in G è una maglia $\mathcal{M}$. Mostrare che soddisfa la condizione ai vertici. Spiegare perché la superficie costruita sia la sfera e perché G^* sia isomorfo a H.

Problema 35E. Considerare un grafo connesso G e una maglia $\mathcal{M}$ che soddisfi la condizione ai vertici, cioè una carta. Per semplicità, supporre G semplice e le passeggiate di $\mathcal{M}$ cammini semplici chiusi, che identifichiamo con poligoni e chiamiamo facce. Un *automorfismo* della carta è una permutazione di $V(G)$ che manda spigoli in spigoli e facce in facce, cioè un automorfismo di G che conserva $\mathcal{M}$. Mostrare che, se un automorfismo α fissa un vertice x, uno spigolo e incidente a x e una faccia F incidente a e, allora è l'identità.

(Ne segue, per esempio, che una carta semplice come sopra ha al più $4|E(G)|$ automorfismi. L'uguaglianza vale per i solidi platonici e per le carte degli esempi 35.1 e 35.2.)

Teorema 35.8. Se $n \equiv 7 \pmod{12}$, il grafo completo K_n ammette un'immersione triangolare su una superficie orientabile di genere $g := (n-3)(n-4)/12$. Orig. 500

Dimostrazione. Costruiamo una maglia triangolare orientabile in K_n che soddisfi la condizione ai vertici. Scriviamo $n = 12s + 7$ e usiamo $\mathbb{Z}_n$ come insieme dei vertici.

La costruzione è codificata nei diagrammi della figura 35.7, relativi a $n = 7, 19, 31$ e a $n = 12s + 7$ in generale. Nel caso generale gli spigoli verticali sono orientati alternativamente ed etichettati consecutivamente $1, 2, \ldots, 2s$. Potremmo descrivere la costruzione semplicemente come un'applicazione del metodo delle differenze, senza figure, ma sarebbe un peccato: i diagrammi sono stati molto utili concettualmente per trovare questa e altre immersioni.

Gli spigoli sono etichettati con gli interi da 1 a $6s + 3$. Vale la legge di "conservazione", o "legge delle correnti di Kirchhoff": in ogni vertice la somma dei valori sugli spigoli entranti è uguale a quella sugli spigoli uscenti. A parte l'assenza di sorgente e pozzo, si tratta di un flusso di valore zero come nel capitolo 7.

Conviene pensare presenti anche gli spigoli orientati opposti a quelli indicati: l'opposto di uno spigolo della figura porta l'etichetta negativa di quella mostrata. Tutti i valori non nulli modulo $n = 12s + 7$ compaiono allora sugli spigoli orientati, ciascuno esattamente una volta. I vertici sono di due tipi: pieni, che rappresentano il senso orario, e vuoti, che rappresentano il senso antiorario.

Ogni vertice dei diagrammi fornisce una famiglia di n triangoli orientati di K_n, traslati l'uno dell'altro modulo n. Per ogni vertice pieno dal quale escano spigoli di valori a, b, c in ordine orario, prendiamo i triangoli

$$[x, x + a, x + a + b], \qquad x \in \mathbb{Z}_n.$$

Poiché $a + b + c = 0$ in $\mathbb{Z}_n$, otteniamo gli stessi triangoli, ma con vertici iniziali diversi, prendendo $[y, y + b, y + b + c]$ oppure $[z, z + c, z + c + a]$, al variare di y, z in $\mathbb{Z}_n$. Per ogni vertice vuoto dal quale escano spigoli di valori a, b, c in ordine antiorario, prendiamo analogamente Orig. 501

$$[x, x + a, x + a + b], \qquad x \in \mathbb{Z}_n.$$

Per esempio, nel terzo diagramma, con $n = 31$, vi è un vertice vuoto con spigoli entranti etichettati $7, 2$ e uno uscente etichettato 9. Li consideriamo come spigoli uscenti etichettati $-7, -2, 9$, in senso antiorario, e prendiamo i 31 triangoli orientati traslati di $[0, -7, -9]$ modulo 31, oppure di $[0, 9, 2]$ o $[0, -2, 7]$. Un altro vertice del diagramma dà i 31 traslati di $[0, 14, 13]$.

Non è difficile vedere che i triangoli orientati ottenuti formano una maglia triangolare orientata. Per esempio, con $n = 31$, per trovare un triangolo che percorra lo spigolo da 4 a 23 in quel verso, osserviamo che $23 - 4 = -12$ in $\mathbb{Z}_n$. Lo spigolo etichettato -12 esce da un vertice pieno con altri spigoli uscenti etichettati $15, -3$, e troviamo il triangolo $[4, 4+(-12), 4+(-12)+15] = [4, 23, 7]$. Il triangolo che percorre lo spigolo da 23 a 4 è $[23, 4, 6]$.

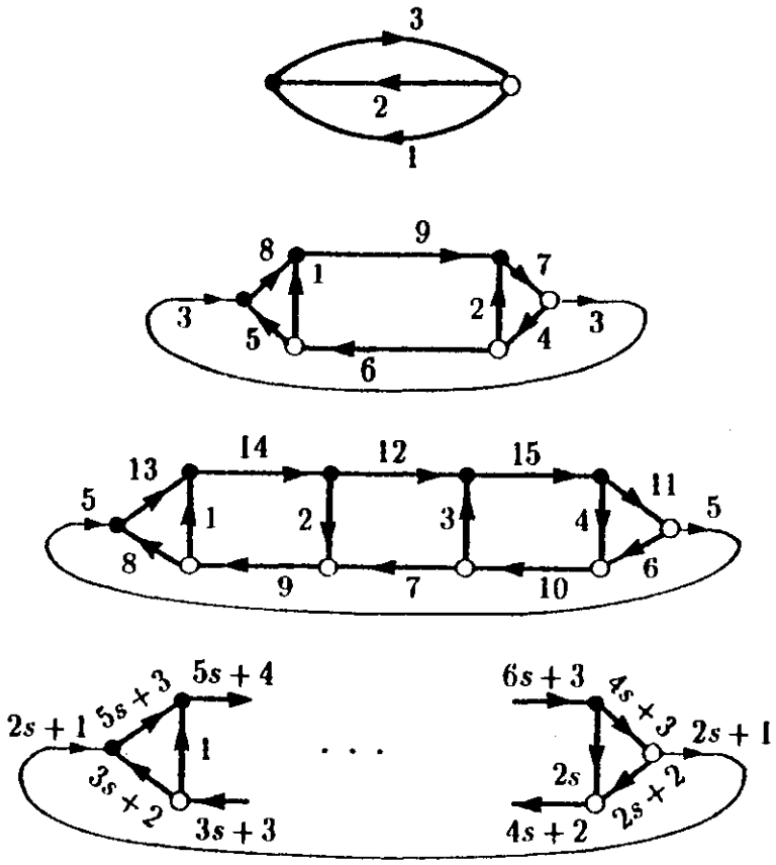


Figura 35.7

Orig. 502

Basta verificare la condizione ai vertici in 0. Indichiamo con e_i lo spigolo $\{0, i\}$ di K_n. Consideriamo il triangolo della maglia che attraversa 0 entrando sullo spigolo e_a. Nel diagramma, lo spigolo etichettato a entra in un vertice dal quale escono spigoli etichettati, diciamo, $-a, p, q$, in ordine orario o antiorario secondo che il vertice sia pieno o vuoto. Il triangolo è cioè $[a, 0, p]$ ed esce da 0 lungo e_p. Riassumendo, se un triangolo entra in 0 lungo e_i, il valore j tale che ne esca lungo e_j si trova così: si cerca nel diagramma lo spigolo etichettato i; giunti alla testa si svolta nel senso prescritto e si esce lungo lo spigolo successivo; la sua etichetta è j.

Per $n = 31$, per esempio, la successione degli spigoli e_{i_ℓ}, tale che il triangolo entrante in 0 lungo e_{i_ℓ} ne esca lungo $e_{i_{\ell+1}}$, è

$$e_1, e_{-13}, e_{-8}, e_{-9}, e_{-7}, e_{-10}, e_{-6}, e_5,$$
$$e_{13}, e_{14}, e_{12}, e_{15}, e_{11}, e_6, e_{-4}, e_{-15}, e_{-3}, e_7, e_{-2}, e_{-14},$$
$$e_{-1}, e_8, e_{-5}, e_{-11}, e_4, e_{10}, e_3, e_{-12}, e_2, e_9, e_1, \dots.$$

Le coppie consecutive sono adiacenti in $\mathcal{M}_0$, che risulta quindi un unico poligono. Il lettore controlli che tutti i diagrammi della figura 35.7 producano analogamente una successione che percorre ogni spigolo del diagramma una volta in ciascun verso. È davvero sorprendente. □

Problema 35F. (i) Se K_n ammette un'immersione nella superficie orientabile T_g con tutte le facce delimitate da triangoli, allora $g = (n-3)(n-4)/12$. (ii) Se $K_{n,n}$ ammette un'immersione in T_g con tutte le facce delimitate da quadrilateri, qual è g in funzione di n? Qual è il minimo $n > 2$ per cui esiste tale immersione?

Per presentare la dimostrazione del teorema 35.8 nel modo più rapido e semplice possibile, abbiamo estratto la costruzione dal suo contesto originale. Chiudiamo il capitolo discutendo brevemente alcune idee che permisero a Ringel e Youngs di trovare costruzioni per ogni valore di n. Una tecnica per immergere grafi in superfici orientabili fu descritta da J. Edmonds (1960). La si può pensare come derivante dalla maglia nel grafo duale dell'immersione. Se un grafo connesso semplice G è immerso in una superficie orientabile S, la scelta di un'orientazione di S induce presso ogni vertice una permutazione

Orig. 503

ciclica degli spigoli incidenti. Edmonds osservò che qualunque scelta di tali "permutazioni cicliche locali" determina un'immersione. Sia G semplice e, per ogni vertice x, sia assegnata una permutazione ciclica σ_x dell'insieme $S(x)$ degli spigoli incidenti. È allora determinata una maglia orientata naturale $\mathcal{M}$: nella passeggiata orientata che percorre uno spigolo e da un estremo y all'altro x, lo spigolo successivo deve essere $\sigma_x(e)$.

Gli esempi seguenti riguardano grafi semplici, perciò possiamo abbreviare le permutazioni locali come permutazioni dei vertici adiacenti e descrivere le passeggiate mediante le sequenze dei vertici.

Esempio 35.5. Consideriamo K_5 con vertici $\{1,2,3,4,5\}$ e permutazioni locali

$$\begin{array}{c|l} 1 & (2435) \\ 2 & (1435) \\ 3 & (4125) \\ 4 & (1325) \\ 5 & (1234) \end{array} .$$

Conviene forse pensare alle passeggiate risultanti come a una decomposizione degli spigoli del grafo orientato completo su cinque vertici. Se e_{ij} è lo spigolo da i a j, le sequenze degli spigoli sono

$$(e_{12}, e_{24}, e_{45}, e_{51}),$$
$$(e_{13}, e_{32}, e_{25}, e_{53}, e_{34}, e_{42}, e_{23}, e_{35}, e_{54}, e_{41}),$$
$$(e_{14}, e_{43}, e_{31}, e_{15}, e_{52}, e_{21}).$$

Le sequenze dei vertici sono esattamente quelle di $\mathcal{M}_2$ nell'esempio 35.3.

Nella famiglia di grafi con $4s+2$ vertici della figura 35.7 abbiamo prescritto un ordine ciclico presso ogni vertice usando un vertice pieno per indicare una permutazione locale oraria e un vertice vuoto per indicarne una antioraria. Nella dimostrazione del teorema 35.8 dovevamo verificare che le immersioni risultanti avessero esattamente una faccia. Orig. 504

Dato un gruppo finito Γ e un sottoinsieme S di elementi diversi dall'identità tale che $\alpha \in S$ implichi $\alpha^{-1} \in S$, il grafo di Cayley $G(\Gamma, S)$ è il grafo semplice con vertici Γ, nel quale α, β sono adiacenti se e solo se $\beta\alpha^{-1} \in S$. Il grafo completo K_n è un grafo di Cayley rispetto a ogni gruppo di ordine n, prendendo come S tutti gli elementi diversi dall'identità. Spesso si richiede che S generi il gruppo, assicurando così la connessione del grafo.

W. Gustin (1963) introdusse la teoria delle "varietà quoziente" e sviluppò metodi per immergere grafi di Cayley in superfici orientabili. Non abbiamo spazio per una descrizione precisa, ma diamo qualche esempio. Consideriamo il caso in cui le permutazioni locali ai vertici di un grafo di Cayley siano tutte traslate di una permutazione ciclica iniziale $(s_1\ s_2\ \ldots\ s_k)$ dell'insieme S dei vertici adiacenti a 0; la permutazione locale in α è cioè

$$(s_1+\alpha \quad s_2+\alpha \quad \cdots \quad s_k+\alpha),$$

in notazione additiva.

Esempio 35.6. Consideriamo K_7 con vertici $\{0,1,2,3,4,5,6\}$ e permutazione locale $(1+i\ 3+i\ 2+i\ 6+i\ 4+i\ 5+i)$ modulo 7 in i:

$$\begin{array}{c|l} 0 & (132645) \\ 1 & (243056) \\ 2 & (354160) \\ 3 & (465201) \\ 4 & (506312) \\ 5 & (610423) \\ 6 & (021534) \end{array} .$$

Le passeggiate sono:

$$[1,2,4] \quad [2,3,5] \quad [3,4,6] \quad [4,5,0] \quad [5,6,1] \quad [6,0,2] \quad [0,1,3],$$
$$[3,5,6] \quad [4,6,0] \quad [5,0,1] \quad [6,1,2] \quad [0,2,3] \quad [1,3,4] \quad [2,4,5].$$

È l'immersione triangolare di K_7 nel toro già vista nell'esempio 35.2. Se proviamo questo metodo su K_{31}, Orig. 505

per esempio, con vertici $\mathbb{Z}_{31}$ e permutazione locale iniziale

$$(1, -13, -8, -9, -7, -10, -6, 5, 13, 14, 12, 15, 11, 6, -4,$$
$$-15, -3, 7, -2, -14, -1, 8, -5, -11, 4, 10, 3, -12, 2, 9),$$

ritroviamo la maglia triangolare della dimostrazione del teorema 35.8. I diagrammi della figura 35.7 rappresentano in realtà le "varietà quoziente" dei grafi duali di K_n rispetto alle immersioni prescritte. Per $n = 12s + 7$, il grafo immerso rappresentato dal diagramma ha $4s + 2$ vertici, $6s + 3$ spigoli e una faccia; l'immersione risultante di K_n ha $(4s + 2)n$ facce, $(6s + 3)n$ spigoli e n vertici.

Problema 35G. Sia ω un elemento non nullo di $\mathbb{F}_q$, con q potenza di un primo. Supponiamo che ω abbia ordine m nel gruppo moltiplicativo e che -1 sia una potenza di ω. Consideriamo il grafo di Cayley $G(\mathbb{F}_q, \langle\omega\rangle)$, dove $\langle\omega\rangle = \{1, \omega, \omega^2, \ldots\}$. Per il grafo usiamo il gruppo additivo del campo: a, b sono adiacenti se e solo se $a - b \in \langle\omega\rangle$. Si tratta di un grafo completo quando ω è primitivo in $\mathbb{F}_q$; del grafo di Clebsch quando $q = 16, m = 5$. Prendiamo come permutazione locale in 0 il ciclo $(1, \omega, \omega^2, \ldots, \omega^{m-1})$ e otteniamo le altre per traslazione. Quali sono la grandezza e il numero delle facce nella maglia risultante?

Note

P. J. Heawood (1861–1955) trascorse gran parte della carriera a Durham, in Inghilterra, come professore di matematica, divenendo infine vicerettore.

Riferimenti bibliografici

- G. Chartrand e L. Lesniak (1986), *Graphs and Digraphs*, 2a ed., Wadsworth.
- J. Edmonds (1960), A combinatorial representation for polyhedral surfaces, *Notices Amer. Math. Soc.* **7**, 646.
- M. Fréchet e K. Fan (1967), *Initiation to Combinatorial Topology*, Prindle, Weber and Schmidt.

Orig. 506

- W. Gustin (1963), Orientable embedding of Cayley graphs, *Bull. Amer. Math. Soc.* **69**, 272–275.
- G. Ringel (1974), *Map Color Theorem*, Springer-Verlag.
- G. Ringel e J. W. T. Youngs (1968), Solution of the Heawood map coloring problem, *Proc. Nat. Acad. Sci. U.S.A.* **60**, 438–445.
- A. T. White (1973), *Graphs, Groups, and Surfaces*, Mathematical Studies **8**, North-Holland.

Capitolo 36

Reti elettriche e quadrati suddivisi in quadrati

Orig. 507

Cominciamo con il *teorema matrice-albero*, che esprime il numero degli alberi ricoprenti di un grafo come determinante di un'opportuna matrice.

Teorema 36.1. Il numero degli alberi ricoprenti di un grafo connesso G su n vertici e senza cappi è il determinante di una qualsiasi sottomatrice principale $(n-1)\times(n-1)$ della matrice $D-A$, dove A è la matrice di adiacenza di G e D è diagonale, con sulla diagonale i gradi dei corrispondenti vertici.

Per un multigrafo senza cappi conveniamo che $A(x,y)$ sia il numero degli spigoli che congiungono i vertici distinti x, y. Rinviamo la dimostrazione a quando avremo sviluppato alcuni strumenti, ma diamo subito degli esempi.

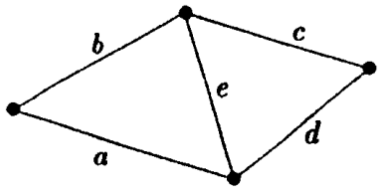


Figura 36.1

Esempio 36.1. Sia G il grafo della figura 36.1. Allora

$$D-A=\begin{pmatrix} 2 & -1 & 0 & -1 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}$$

e G ha 8 alberi ricoprenti.

Orig. 508

Esempio 36.2. Nel teorema 36.1 prendiamo $G=K_n$. In questo caso $D-A=nI-J$, dove I è la matrice identità di ordine n e J la matrice $n\times n$ con tutti gli elementi uguali a 1. Il determinante di una sottomatrice principale $(n-1)\times(n-1)$ si può calcolare in vari modi, mediante operazioni sulle righe o considerando gli autovalori, e viene lasciato per esercizio. Si ottiene così un'altra dimostrazione del teorema di Cayley, cfr. capitolo 2: K_n ha n^{n-2} alberi ricoprenti.

Problema 36A. Sia M una matrice $n\times n$ con tutte le somme di riga e di colonna nulle. Uno dei suoi autovalori è quindi $\lambda_1=0$; siano $\lambda_2,\lambda_3,\ldots,\lambda_n$ gli altri. Mostrare che tutte le sottomatrici principali $(n-1)\times(n-1)$ hanno lo stesso determinante, uguale a $\frac{1}{n}\lambda_2\lambda_3\cdots\lambda_n$.

Esempio 36.3. Il problema precedente permette di calcolare il numero degli alberi ricoprenti di grafi regolari di spettro noto. Per esempio, la matrice di adiacenza A del grafo di Petersen ha autovalori

$$3,1,1,1,1,1,-2,-2,-2,-2$$

(si veda il capitolo 21). La matrice $M = 3I - A$ ha dunque autovalori

$$0, 2, 2, 2, 2, 2, 5, 5, 5, 5.$$

Concludiamo che il grafo di Petersen ha 2000 alberi ricoprenti.

Il lemma seguente è noto come teorema di Cauchy–Binet. Più spesso viene enunciato e applicato prendendo come matrice diagonale Δ la matrice identità.

Lemma 36.2. Siano A, B matrici rispettivamente $r \times m$ e $m \times r$, e sia Δ la matrice diagonale $m \times m$ con elemento e_i nella posizione (i, i). Per un sottoinsieme $S \subseteq \{1, 2, \dots, m\}$ di cardinalità r, siano A_S, B^S le sottomatrici $r \times r$ formate rispettivamente dalle colonne di A e dalle righe di B indicizzate da S. Allora

$$\det(A\Delta B) = \sum_S \det(A_S) \det(B^S) \prod_{i \in S} e_i,$$

dove la somma è estesa a tutti i sottoinsiemi S di cardinalità r.

Orig. 509

DIMOSTRAZIONE. Dimostriamo l'identità supponendo $e_1, \dots, e_m$ indeterminate indipendenti; essa varrà quindi per ogni loro scelta di valori.

Gli elementi di $A\Delta B$ sono forme lineari nelle indeterminate: se $A = (a_{ij})$ e $B = (b_{ij})$, l'elemento (i, k) è $\sum_{j=1}^{m} a_{ij} b_{jk} e_j$. Quindi $\det(A\Delta B)$ è un polinomio omogeneo di grado r in $e_1, \dots, e_m$.

Consideriamo un monomio $e_1^{t_1} e_2^{t_2} \cdots$ nel quale compaiano meno di r indeterminate distinte, cioè vi siano meno di r esponenti positivi. Sostituiamo con 0 le indeterminate che non vi compaiono. Il monomio e il suo coefficiente rimangono invariati, ma dopo la sostituzione Δ ha rango minore di r, perciò $\det(A\Delta B)$ diventa il polinomio nullo.

Il coefficiente di un monomio è dunque nullo, salvo che il monomio sia il prodotto di r indeterminate distinte, cioè $\prod_{i \in S} e_i$ per un sottoinsieme S di cardinalità r. Per ottenere il coefficiente di tale monomio poniamo $e_i = 1$ per $i \in S$ ed $e_j = 0$ per $j \notin S$. Con questa sostituzione $A\Delta B$ diventa $A_S B^S$, quindi il coefficiente è $\det(A_S) \det(B^S)$. □

In questo capitolo useremo ampiamente grafi orientati H. Tutti i termini della teoria dei grafi, come alberi, componenti, circuiti, saranno applicati a un grafo orientato con lo stesso significato che hanno per il grafo non orientato sottostante, ottenuto ignorando i versi. Un cammino in un grafo orientato percorre quindi alcuni spigoli "in avanti" e altri "all'indietro". Ci interessano in realtà grafi non orientati, ma per la teoria conviene scegliere un orientamento: qualunque scelta produce essenzialmente la stessa teoria.

Come spesso nei capitoli precedenti, usiamo $M(i, j)$ per l'elemento di riga i e colonna j di M, e $f(i)$ per la coordinata i del vettore f.

La *matrice di incidenza* N di un grafo orientato H ha righe indicizzate da $V(H)$, colonne indicizzate da $E(H)$ e

Orig. 510

$$N(x, e) = \begin{cases} 0 & \text{se } x \text{ non è incidente a } e \text{ oppure } e \text{ è un cappio,} \\ 1 & \text{se } x \text{ è la testa di } e, \\ -1 & \text{se } x \text{ è la coda di } e. \end{cases}$$

Osserviamo che

$$\operatorname{rank}(N) = |V(H)| - |C(H)|, \tag{36.1}$$

dove $C(H)$ è l'insieme delle componenti. Infatti, se g è un vettore riga indicizzato da $V(H)$, la condizione $gN = 0$ significa che, per ogni spigolo e diretto da x a y, $g(y) - g(x) = 0$. Ciò accade se e solo se g è costante sui vertici di ogni componente; lo spazio dei tali g ha quindi dimensione $|C(H)|$.

Osserviamo inoltre che una matrice quadrata con al più un 1 e al più un -1 per colonna, e tutti gli altri elementi nulli, ha determinante 0 oppure ± 1. Si dimostra per induzione: se ogni colonna ha un $+1$ e un -1, la somma delle righe è nulla e la matrice è singolare. Altrimenti si sviluppa il determinante lungo una colonna con un solo elemento non nullo, ottenendo ± 1 volte il determinante di una matrice più piccola con la stessa proprietà. Ogni sottomatrice quadrata della matrice di incidenza di un grafo orientato ha dunque determinante 0 o ± 1. Le matrici con questa proprietà si chiamano *totalmente unimodulari*.

Dimostrazione del teorema 36.1. Sia H un grafo orientato connesso su n vertici, con matrice di incidenza N. Sia S un insieme di $n - 1$ spigoli e consideriamo, nella notazione di Cauchy–Binet, la sottomatrice N_S di dimensioni $n \times (n - 1)$, le cui colonne sono indicizzate da S. Per (36.1), N_S ha rango $n - 1$ se e solo se il sottografo ricoprente con spigoli S è connesso, cioè se e solo se S è l'insieme degli spigoli di un

albero ricoprente. Sia N' ottenuta eliminando una riga qualsiasi da N. Poiché la somma delle righe di N, o di N_S, è nulla, N'_S ha lo stesso rango di N_S. Le osservazioni precedenti mostrano che

$$\det(N'_S) = \begin{cases} \pm 1 & \text{se } S \text{ è l'insieme degli spigoli di un albero ricoprente,} \\ 0 & \text{altrimenti.} \end{cases} \tag{36.2}$$

Dato un grafo connesso senza cappi G su n vertici, siano H un suo orientamento e N la relativa matrice di incidenza. Allora $NN^{\mathsf{T}} = D - A$, poiché Orig. 511

$$(NN^{\mathsf{T}})(x,y) = \sum_{e \in E(G)} N(x,e)N(y,e) = \begin{cases} \deg(x) & x = y, \\ -t & x, y \text{ congiunti da } t \text{ spigoli.} \end{cases}$$

Una sottomatrice principale $(n-1)\times(n-1)$ di $D-A$ ha la forma $N'N'^{\mathsf{T}}$, dove N' si ottiene eliminando una riga. Per Cauchy–Binet,

$$\det(N'N'^{\mathsf{T}}) = \sum_S \det(N'_S)\det(N'^{\mathsf{T}}_S) = \sum_S (\det(N'_S))^2,$$

con somma su tutti i sottoinsiemi S di $n-1$ spigoli. Per (36.2) questo è il numero degli alberi ricoprenti di G. □

Osservazione. Se consideriamo $E(G)$ come insieme di indeterminate e applichiamo il lemma 36.2 alle sottomatrici principali $(n-1)\times(n-1)$ di $N\Delta N^{\mathsf{T}}$, dove Δ è diagonale, indicizzata dagli spigoli e con $\Delta(e,e) := e$, troviamo che $\det(N\Delta N^{\mathsf{T}})$ è la somma dei monomi corrispondenti agli insiemi di spigoli degli alberi di G.[1] Per il grafo della figura 36.1,

$$N\Delta N^{\mathsf{T}} = \begin{pmatrix} a+b & -b & 0 & -a \\ -b & b+c+e & -c & -e \\ 0 & -c & c+d & -d \\ -a & -e & -d & a+d+e \end{pmatrix}.$$

Naturalmente la matrice è singolare, avendo nulle tutte le somme di riga e colonna, ma il determinante della matrice 3×3 ottenuta eliminando l'ultima riga e colonna è

$$\begin{aligned} &(a+b)(b+c+e)(c+d) - b^2(c+d) - c^2(a+b) \\ &\qquad = abc + abd + acd + ace + ade + bcd + bce + bde, \end{aligned}$$

che rappresenta gli otto alberi ricoprenti. Orig. 512

Diamo ora una generalizzazione del teorema 36.1 dovuta a W. T. Tutte (1948), con una dimostrazione più breve di quella del primo teorema! L'enunciato più generale consente un'induzione non disponibile nel caso originale. Si recupera il teorema 36.1 applicando il teorema 36.3 al grafo orientato ottenuto sostituendo ogni spigolo non orientato con due spigoli, uno per verso.

Teorema 36.3. Sia G un grafo orientato con vertici $x_1, \dots, x_n$. Definiamo $M = M(G) = (m_{ij})$ ponendo m_{ii} uguale al numero degli spigoli uscenti da x_i, esclusi i cappi, e, per $i \neq j$, m_{ij} uguale all'opposto del numero degli spigoli da x_i a x_j. Il numero $A_\ell = A_\ell(G)$ delle arborescenze ricoprenti radicate in x_ℓ è il minore della posizione (ℓ,ℓ) di M, cioè il determinante della sottomatrice principale ottenuta eliminando la riga e la colonna ℓ.

Dimostrazione. Per comodità poniamo $\ell = 1$. Se per un $i > 1$ non vi sono spigoli uscenti da x_i, l'enunciato è vero: la riga i di $M(G)$ è nulla, e sia il minore $(1,1)$ sia il numero delle arborescenze sono zero.

Se invece da un x_i, $i > 1$, esce più di uno spigolo, siano G_1, G_2 uguali a G salvo che alcuni, almeno uno, di tali spigoli sono assegnati a G_1, e gli altri, almeno uno, a G_2. Ogni arborescenza ricoprente radicata in x_1 deve contenere esattamente uno spigolo uscente da x_i, quindi $A_1(G) = A_1(G_1) + A_1(G_2)$. Le matrici $M(G), M(G_1), M(G_2)$ differiscono soltanto nella riga i, e la riga i della prima è la somma delle corrispondenti righe delle altre. Il minore $(1,1)$ della prima matrice è quindi la somma dei due minori corrispondenti.

[1] Nota redazionale: il determinante va riferito alla sottomatrice principale con una riga e una colonna eliminate, non all'intera matrice $N\Delta N^{\mathsf{T}}$, che è singolare, come osserva subito l'originale.

Basta pertanto verificare l'enunciato per grafi orientati con $m_{ii} = 1$ per ogni $i > 1$, cioè con un unico spigolo uscente da ciascun vertice diverso da x_1.

Se un tale grafo ha un cammino orientato chiuso che non passa per x_1, per esempio $x_2 \to x_3, x_3 \to x_4, \ldots, x_k \to x_2$, la somma delle righe da 2 a k è nulla e il minore $(1,1)$ è zero. Da nessuno di questi vertici parte un cammino orientato verso x_1, quindi non vi sono arborescenze ricoprenti. Orig. 513

Se invece non vi sono cammini orientati chiusi che evitino x_1, il cammino che parte da un vertice x_j e segue l'unico spigolo uscente da ogni vertice incontrato deve raggiungere x_1. Eliminati gli spigoli uscenti da x_1, che non possono comparire in alcuna arborescenza radicata in esso, il grafo è esso stesso un'arborescenza ricoprente: $A_1(G) = 1$. Anche il minore $(1,1)$ vale 1, come si vede per induzione sviluppando il determinante lungo una colonna j corrispondente a un vertice x_j di grado entrante zero nell'arborescenza: essa ha un 1 nella posizione (j,j) e zeri nelle posizioni (i,j) con $i > 1$, $i \neq j$. □

Se gli spigoli di G sono considerati indeterminate indipendenti e formiamo una matrice analoga a $M(G)$ i cui elementi siano somme formali di spigoli invece di interi, i minori diventano le somme formali delle arborescenze, ciascuna rappresentata dal prodotto dei suoi spigoli. Il lettore può facilmente adattare la dimostrazione. Per esempio, per il grafo su $1,2,3$ con spigolo a da 2 a 1, b da 3 a 1 e c da 3 a 2, consideriamo

$$M = \begin{pmatrix} 0 & 0 & 0 \\ -a & a & 0 \\ -b & -c & b+c \end{pmatrix}.$$

Il minore $(1,1)$ è $ab + ac$, che rappresenta le due arborescenze radicate in 1.

Problema 36B. (Facile.) Sia T_n il "torneo transitivo" su $1, 2, \ldots, n$, con spigoli da j a i quando $i < j$. Qual è $M(T_n)$? Quante sono le arborescenze ricoprenti radicate in 1? Descriverle tutte.

Possiamo ora dare una seconda dimostrazione del teorema 8.2 sul numero delle successioni di De Bruijn. Sia G_n il grafo orientato definito nel capitolo 8; tutti i suoi gradi entranti e uscenti valgono 2. La soluzione suggerita nell'appendice 1 al problema 2B mostra che il numero dei cicli euleriani orientati di G_n coincide con quello delle arborescenze ricoprenti radicate in un vertice qualsiasi. Per il teorema 36.3 e il problema 36A, tale numero si ottiene dagli autovalori di $M(G_n)$. Orig. 514

Numeriamo righe e colonne di una matrice B_n di ordine 2^{n-1} con gli interi da 0 a $2^{n-1} - 1$. Poniamo $b_{ij} = 1$ se $j = 2i$ o $2i + 1$ modulo 2^{n-1}. La metà superiore e quella inferiore di B_n sono uguali. Allora $M(G_n) = 2I - B_n$. Calcoliamo il determinante $D_n(x)$ di $xI - M(G_n)$. Con le ovvie operazioni su righe e colonne nella metà inferiore del determinante si ottiene

$$D_n(x) = (x-2)^{2^{n-2}} D_{n-1}(x).$$

Poiché $D_2(x) = x(x-2)$, tutti gli autovalori non nulli di M_n valgono 2; per il problema 36A, il numero dei cicli di De Bruijn di lunghezza 2^n è

$$\frac{1}{2^{n-1}} 2^{2^{n-1}-1} = 2^{2^{n-1}-n}.$$

* * *

Sia N la matrice di incidenza di un grafo orientato H. Lo spazio delle righe di N si chiama *spazio dei cobordi*; il nucleo di N^{T}, cioè lo spazio dei vettori riga f tali che $fN^{\mathsf{T}} = 0$, si chiama *spazio dei cicli*. Questi spazi hanno importanza nella teoria delle reti elettriche e nella topologia algebrica. Per (36.1), il primo ha dimensione $|V(H)| - |C(H)|$, quindi il secondo ha dimensione $|E(H)| - |V(H)| + |C(H)|$.

Per definizione, f è un ciclo se e solo se, presso ogni vertice x, la somma dei valori $f(e)$ sugli spigoli uscenti coincide con quella sugli entranti. Un esempio, detto *ciclo elementare*, si ottiene da un cammino semplice chiuso p ponendo $f(e) = +1$ sugli spigoli percorsi in avanti, -1 su quelli percorsi all'indietro, e 0 sugli altri. Un vettore è un cobordo se e solo se è ortogonale a tutti i cicli; in particolare la somma dei valori di un cobordo sugli spigoli in avanti di un cammino semplice chiuso coincide con quella sugli spigoli all'indietro. Orig. 515

Problema 36C. Un vettore g con coordinate indicizzate da $E(H)$ è un cobordo su un grafo orientato H se e solo se, per ogni passeggiata chiusa w, la somma con segno dei valori di g sugli spigoli, cioè la somma sugli spigoli in avanti meno quella sugli spigoli all'indietro, è zero.

Conveniamo che una *rete elettrica* consista di un grafo orientato H, di una funzione r che associa a ogni spigolo e una "resistenza" $r(e) \geq 0$ e di una funzione s che vi associa una "forza elettromotrice

impressa", o "sorgente di tensione", $s(e)$. Ogni spigolo va dunque pensato come un resistore, una batteria o entrambi. Collegando batterie e resistori, ogni spigolo sarà percorso da una "corrente" $f(e)$ e ai suoi capi sarà misurabile una "differenza di potenziale", o "tensione", $g(e)$. Qui basta sapere che f, g sono determinati da r, s mediante le leggi di Kirchhoff e la legge di Ohm. La legge di Kirchhoff delle correnti e quella delle tensioni affermano rispettivamente che f è un ciclo e g un cobordo. La legge di Ohm dice $g(e) = -s(e) + r(e)f(e)$, oppure, in notazione matriciale, $g = -s + fR$, dove R è diagonale con gli $r(e)$ sulla diagonale e s, g, f sono vettori riga.

Problema 36D. Supponiamo che $\{e : r(e) = 0\}$ non contenga circuiti, cioè sia l'insieme degli spigoli di una foresta. Mostrare che la rete elettrica ha un'unica soluzione: per ogni s esistono unici vettori f, g che soddisfano le leggi precedenti.

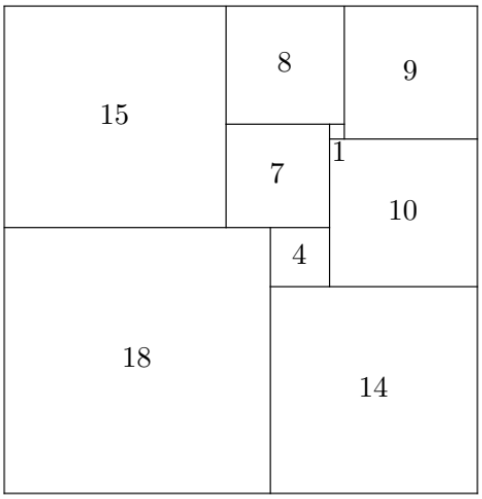


Figura 36.2

Orig. 516

Per *rettangolo suddiviso in quadrati* intendiamo un rettangolo partizionato in un numero finito di quadrati. Le figure 36.2 e 36.3 danno due esempi, di dimensioni rispettivamente 33×32 e 177×176. Tali rettangoli sono considerati eleganti quando tutti i quadrati interni hanno dimensioni diverse e non contengono un rettangolo più piccolo già suddiviso in quadrati.

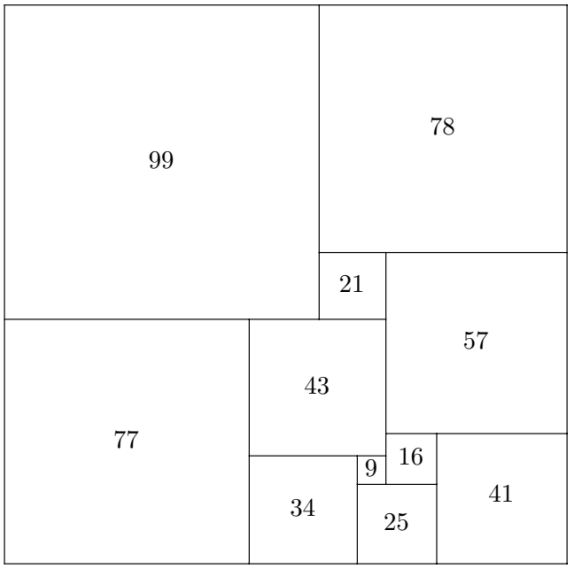


Figura 36.3

Problema 36E. Trovare dimensioni intere per i piccoli quadrati della figura 36.4, in modo che il disegno rappresenti un rettangolo suddiviso in quadrati.

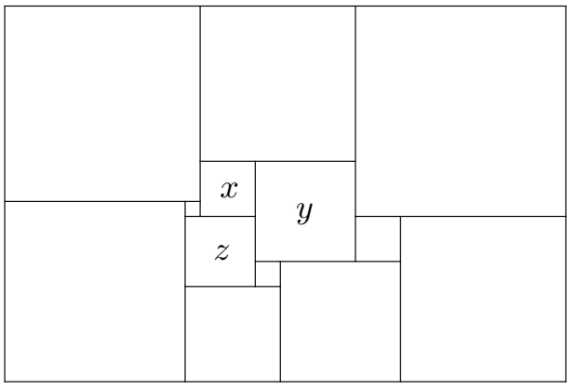


Figura 36.4

Orig. 517

Per molti anni non si seppe se un quadrato potesse essere partizionato in un numero finito di quadrati più piccoli, tutti di dimensioni diverse. Alla fine degli anni Trenta furono finalmente scoperte tali suddivisioni. Un esempio apparve sulla copertina del *Journal of Combinatorial Theory* finché A. J. W. Duijvestijn (1978) ne trovò uno più piccolo; l'illustrazione fu aggiornata nel gennaio 1979. È una partizione nel minimo numero possibile di quadrati: 21. Questi risultati impiegano il computer, ma uno strumento importante nello studio dei rettangoli suddivisi è il collegamento con le reti elettriche, scoperto da quattro studenti di Cambridge tra il 1936 e il 1938. Un resoconto divulgativo di parte del loro lavoro è dato da W. T. Tutte (1961, 1965), che era uno di loro.

Descriviamo informalmente il collegamento. Chiamiamo *rete speciale* una rete elettrica con uno spigolo distinto e_0, tale che $s(e) = 0$ per $e \neq e_0$ e

$$r(e) = \begin{cases} 1 & e \neq e_0, \\ 0 & e = e_0. \end{cases}$$

Abbiamo cioè un sistema di resistori unitari e un'unica batteria.

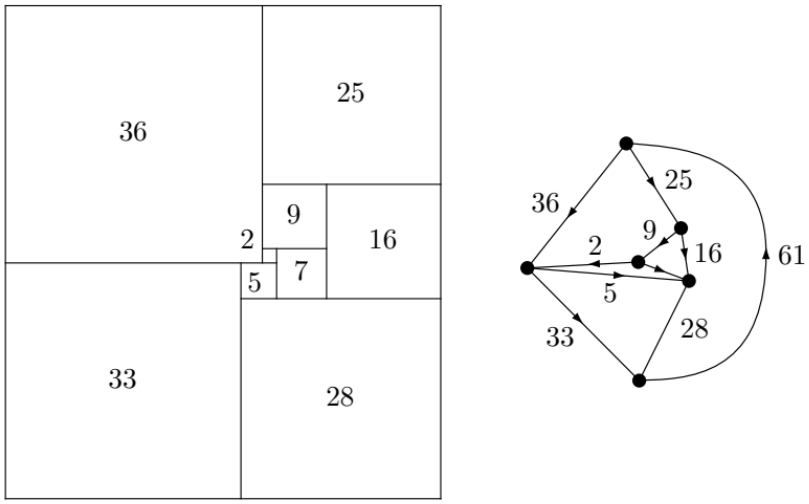


Figura 36.5

Da un rettangolo suddiviso in quadrati nasce una rete speciale nel modo seguente. Definiamo un grafo orientato H i cui vertici sono i segmenti orizzontali massimali del disegno. Gli spigoli sono i piccoli quadrati, ai quali aggiungiamo uno spigolo speciale e_0 per l'intero rettangolo. Orientiamo ogni spigolo, tranne e_0, verso il basso, cioè verso il segmento inferiore. La figura 36.5 mostra un esempio. H è evidentemente planare. A ogni spigolo è naturalmente associato il numero reale $f(e)$ uguale al lato del corrispondente quadratino; poniamo $f(e_0)$ uguale alla larghezza del rettangolo. È facile vedere che f è un ciclo: per ogni segmento orizzontale massimale, la somma dei lati dei quadrati "appoggiati sopra" coincide con quella dei quadrati "appesi sotto". Se non fosse per lo spigolo speciale, f sarebbe anche un cobordo: per ogni vertice, cioè segmento orizzontale, x, poniamo $h(x)$ uguale alla distanza dal lato

Orig. 518

superiore del rettangolo; allora, per $e \neq e_0$, $f(e) = h(\text{testa di } e) - h(\text{coda di } e)$. Ponendo $s(e_0)$ uguale all'altezza del rettangolo e prendendo g come cobordo di h, f, g sono i vettori delle correnti e delle tensioni che risolvono la rete: $g = -s + Rf$.[2]

Viceversa, una rete speciale con grafo planare conduce alla costruzione di un rettangolo suddiviso in quadrati. Non ne diamo la dimostrazione. Il rapporto larghezza/altezza è il rapporto tra la corrente $f(e_0)$ e la tensione $-g(e_0)$ nella soluzione. Alcuni spigoli possono avere corrente negativa, ma basta invertirne il verso per renderla positiva; quelli con corrente nulla possono essere cancellati o contratti e non danno origine a quadrati. Un quadrato suddiviso in quadrati corrisponde dunque a una rete planare di resistori la cui resistenza equivalente sia un ohm.

Problema 36F. Risolvere con il metodo preferito le reti speciali della figura 36.6 e disegnare i corrispondenti rettangoli suddivisi. Anche i duali possono essere considerati reti speciali: quali rettangoli si ottengono dalle reti duali?

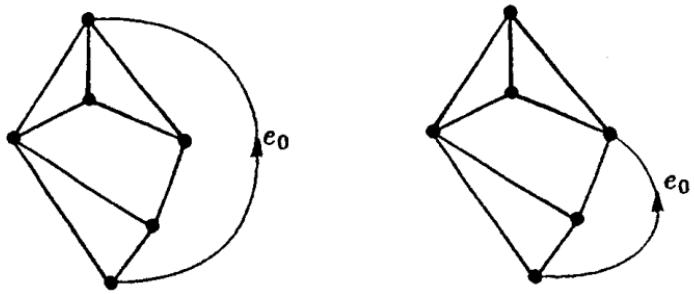


Figura 36.6

Orig. 519

Sia N la matrice di incidenza di un grafo orientato D e sia Δ diagonale, indicizzata da $E(D)$, con $\Delta(e,e) = r(e) > 0$, resistenza dello spigolo. Poniamo $C := N\Delta^{-1}N^{\mathsf{T}}$. Se si aggiunge uno spigolo e_0 diretto da un vertice y a un altro x, e su esso solo si imprime una tensione sufficiente a farvi scorrere una corrente $f(e_0)$, le leggi di Kirchhoff implicano che la differenza di potenziale $g(e)$ ai capi di uno spigolo e da a a b è data da

$$g(e) = \frac{f(e_0)}{\tau(D)}(xy.ab), \tag{36.3}$$

dove $(xy.ab)$ denota il cofattore dell'elemento c_{yb} nel cofattore dell'elemento c_{xa} di $C = (c_{ij})$, e $\tau(D)$ è il numero degli alberi ricoprenti di D, la sua complessità. Si veda Jeans (1908).[3]

Ne consegue il teorema seguente.

Teorema 36.4. Se la tensione $s(e_0)$ sullo spigolo distinto di una rete speciale con grafo G è scelta uguale al numero degli alberi ricoprenti contenenti e_0, tutti i valori $f(a)$ delle correnti risultanti sono interi e la corrente $f(e_0)$ è uguale al numero degli alberi ricoprenti che non contengono e_0.

Dimostrazione. Nella discussione precedente prendiamo D come orientamento di G'_{e_0} e Δ come identità. Se $f(e_0) = \tau(D) = \tau(G'_{e_0})$, da (36.3) è chiaro che tutti i valori $f(a) = g(a)$ sono interi. Resta da mostrare che $-g(e_0)$ è il numero degli alberi ricoprenti contenenti e_0.

Per (36.3), $g(e_0) = (xy.yx) = -(xy.xy)$. Per definizione $(xy.xy)$ è il determinante di $N''N''^{\mathsf{T}}$, dove N'' è N privata delle righe x, y. Per Cauchy–Binet, esso è

$$\sum_S (\det(N''_S))^2,$$

con somma su tutti i sottoinsiemi S di $n-2$ spigoli, e dove N''_S è la sottomatrice quadrata di N'' le cui righe sono indicizzate da S.[4] La dimostrazione si completa osservando che $\det(N''_S) = 0$ salvo che $S \cup \{e_0\}$ sia l'insieme degli spigoli di un albero ricoprente di G, nel qual caso vale ± 1. La verifica è simile a quella di (36.2) e viene lasciata per esercizio. □

Orig. 520

[2] Nota redazionale: con i vettori riga adottati a p. 515 la scrittura coerente è $g = -s + fR$; l'originale scrive qui Rf.

[3] Nota redazionale: per resistenze arbitrarie il denominatore appropriato è il cofattore pesato di C, ossia la somma sugli alberi dei prodotti delle conduttanze $1/r(e)$. Esso coincide con il numero non pesato $\tau(D)$ quando tutte le resistenze sono unitarie, come nell'applicazione seguente.

[4] Nota redazionale: si tratta delle colonne, indicizzate dagli spigoli, non delle righe; l'originale scrive "rows".

In sintesi, il teorema 36.4 dice che la resistenza tra gli estremi di uno spigolo e_0 di G, quando tutti gli altri spigoli sono resistori unitari, è $\tau(G''_{e_0})/\tau(G'_{e_0})$. Il lettore può verificare che questo concorda con ciò che sa sulle reti elettriche quando G è un poligono o un grafo a fascio. Un quadrato suddiviso in quadrati si ottiene trovando un grafo planare e uno spigolo e_0 tali che $\tau(G''_{e_0}) = \tau(G'_{e_0})$. Da sola, questa affermazione non necessariamente aiuta la ricerca, e gli ingegneri elettrici penseranno comunque che si tratti di uno spreco di resistori. Grafi del genere sembrano piuttosto rari.

Note

La prima apparizione in letteratura del problema di costruire un rettangolo con quadrati non congruenti sembra essere M. Dehn (1903). Le prime tavole estese di quadrati suddivisi furono pubblicate da C. J. Bouwkamp, A. J. W. Duijvestijn e P. Medema (1960).

W. T. Tutte (1918–) ha dato numerosi contributi importanti alla teoria dei grafi. È professore emerito nel Dipartimento di Combinatoria e Ottimizzazione dell'Università di Waterloo, uno dei pochi dipartimenti universitari al mondo il cui nome contiene la parola "combinatoria".[5]

Per la dimostrazione del teorema 36.3 abbiamo seguito De Bruijn e Van Aardenne-Ehrenfest (1951).

Uno degli studenti di Cambridge ricordati sopra, C. A. B. Smith, scrisse un bellissimo resoconto della loro collaborazione, intitolato "Did Erdős save Western Civilization?" (si veda Graham e Nešetřil, 1997). Pare che Erdős avesse congetturato che ogni dissezione di un quadrato in quadrati minori dovesse contenerne almeno due della stessa grandezza. Una cosa portò all'altra e Tutte finì a Bletchley Park invece che nell'esercito. Si racconta che lì abbia fornito l'indizio decisivo per decifrare Enigma, il che spiega il titolo dell'articolo.

Riferimenti bibliografici

- N. G. de Bruijn e T. van Aardenne-Ehrenfest (1951), Circuits and trees in oriented linear graphs, *Simon Stevin* **28**, 203–217. Orig. 521
- C. J. Bouwkamp, A. J. W. Duijvestijn, P. Medema (1960), Tables relating to simple squared rectangles of order nine through fifteen, T. H. Eindhoven.
- A. J. W. Duijvestijn (1978), Simple perfect squared square of lowest order, *J. Combinatorial Theory (B)* **25**, 555–558.
- M. Dehn (1903), Zerlegung von Rechtecke in Rechtecken, *Math. Ann.* **57**.
- R. L. Graham e J. Nešetřil (a cura di) (1997), *The Mathematics of P. Erdős*, Springer.
- J. H. Jeans (1908), *The Mathematical Theory of Electricity and Magnetism*, Cambridge University Press.
- W. T. Tutte (1948), The dissection of equilateral triangles into equilateral triangles, *Proc. Cambr. Phil. Soc.* **44**, 463–482.
- W. T. Tutte (1961), Squaring the square, in M. Gardner, *The 2nd Scientific American Book of Mathematical Puzzles and Diversions*, Simon and Schuster.
- W. T. Tutte (1965), The quest of the perfect square, *Amer. Math. Monthly* **72**, n. 2, 29–35.

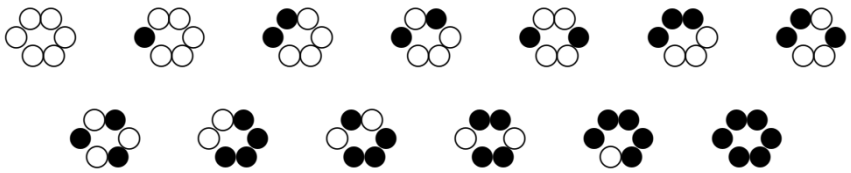
[5] Nota redazionale: si conservano i dati biografici e il tempo verbale dell'edizione originale.

Capitolo 37

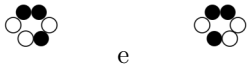
La teoria enumerativa di Pólya

In questo capitolo torniamo ai problemi di enumerazione. Vi sono molti casi in cui non ci interessa il numero degli oggetti elementari, bensì il numero delle loro classi di equivalenza rispetto a un'opportuna relazione. Inoltre, queste relazioni di equivalenza sono spesso indotte in modo naturale da determinati gruppi di permutazioni. Orig. 522

Questione 1. Quante collane «essenzialmente diverse» si possono costruire con n perline di due colori? Per $n = 6$, si vede per ispezione che questo numero è 13.



Si osservi che scegliamo di considerare le collane



(37.1)

essenzialmente uguali, poiché riflettendo l'una rispetto a un asse verticale (o capovolgendola) si ottiene l'altra. È evidente che alla base del nostro concetto di «essenzialmente diverse» vi è il gruppo diedrale D_n degli automorfismi dell'n-gono.

Questione 2. Quanti sono i grafi semplici non isomorfi su n vertici? Per $n = 4$ sono 11.

Questione 3. In quanti modi essenzialmente diversi si possono colorare con n colori le facce (oppure gli spigoli, oppure i vertici) del cubo? Orig. 523

Questione 4. Date tre palline bianche e una nera, in quanti modi si possono distribuire in due scatole quadrate e una rotonda?

[○○○●] [ ] ( )	[○○○] [●] ( )	[○○] [○●] ( )	[○○●] [○] ( )
[○○○] [ ] (●)	[○○] [○] (●)	[○○●] [ ] (○)	[○○] [●] (○)
[○●] [○] (○)	[○●] [ ] (○○)	[○] [●] (○○)	[○○] [ ] (○●)
[○] [○] (○●)	[●] [ ] (○○○)	[○] [ ] (○○●)	[ ] [ ] (○○○●)

Siano A e B insiemi finiti e sia G un gruppo di permutazioni di A (o, più in generale, un gruppo finito che agisce su A). Chiameremo *colori* gli elementi di B. Il gruppo G agisce sull'insieme B^A delle applicazioni

$f : A \to B$ se, per $\sigma \in G$ e $f \in B^A$, definiamo $\sigma(f) \in B^A$ mediante

$$(\sigma(f))(x) := f(\sigma^{-1}(x)).$$

Nelle prime tre questioni precedenti vogliamo contare le orbite di un opportuno gruppo G sull'insieme B^A.

(L'uso di σ^{-1}, anziché di σ, nel membro destro non è un errore. Serve a garantire che $\sigma(\tau(f)) = (\sigma\tau)(f)$, condizione necessaria per avere un'autentica «azione» di G su B^A. Formalmente, abbiamo un omomorfismo di G nel gruppo simmetrico su B^A.)

Nel problema delle collane prendiamo come A l'insieme dei vertici di un n-gono, e come G il suo gruppo di automorfismi rappresentato come gruppo di permutazioni dei vertici (cioè il gruppo diedrale D_n, di ordine $2n$, nella sua rappresentazione usuale). Un problema leggermente diverso si presenta quando le perline non sono rotonde ma, per esempio, piatte da un lato. Le collane non possono allora essere capovolte, e quelle in (37.1) si considerano distinte.

In questo caso prendiamo come G il gruppo ciclico di ordine n nella sua rappresentazione regolare; cfr. l'Esempio 10.5.

Chiedere il numero delle orbite di applicazioni è la domanda più semplice che possiamo porre. Potremmo inoltre voler conoscere il numero delle orbite di un dato «peso»: per esempio, il numero delle collane di n perline di cui k bianche, oppure il numero dei grafi su n vertici con k spigoli. Potremmo introdurre un gruppo di permutazioni H su B e chiedere, rispetto a una relazione di equivalenza più generale, il numero delle «configurazioni». (Questo sarebbe necessario per il problema della distribuzione.) Orig. 524

Per cominciare, ricordiamo il lemma di Burnside, Teorema 10.5: il numero delle orbite di un gruppo finito G su un insieme X è il numero medio dei punti fissi:

$$\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma), \tag{37.2}$$

dove $\psi(\sigma)$ denota il numero dei punti di X fissati dalla permutazione σ.[1] Ricordiamo che questa formula si otteneva contando le coppie ordinate $(x, \sigma) \in X \times G$ tali che $\sigma(x) = x$.

Teorema 37.1. Siano A e B insiemi finiti e supponiamo che G agisca su A. Indichiamo con $c_k(G)$ il numero delle permutazioni di G che hanno esattamente k cicli nella loro decomposizione in cicli su A. Il numero delle orbite di G sull'insieme B^A di tutte le applicazioni $f : A \to B$ è allora

$$\frac{1}{|G|}\sum_{k=1}^{\infty} c_k(G)|B|^k.$$

Dimostrazione. Per il lemma di Burnside, il numero delle orbite è dato da (37.2), dove ora $\psi(\sigma)$ è il numero delle applicazioni $f : A \to B$ tali che $\sigma(f) = f$, cioè $f(a) = f(\sigma^{-1}(a))$ per ogni $a \in A$. Ma un'applicazione f è fissata da σ se e solo se è costante su ogni ciclo di σ; il lettore verifichi questa affermazione. Tali applicazioni si ottengono assegnando un elemento di B a ciascun ciclo di σ; quindi, se σ ha k cicli, il numero delle applicazioni f fissate da σ è $|B|^k$. □

Invitiamo il lettore a fermarsi qui e a verificare che il Teorema 37.1 fornisce la risposta 13 quando viene applicato al problema delle collane della Questione 1.

Poiché ne faremo largo uso nel seguito, è opportuno introdurre ora l'*indice dei cicli* di un gruppo di permutazioni. Anzitutto, in questo capitolo sarà comodo usare la tradizionale notazione $(1^{k_1}2^{k_2}\cdots n^{k_n})$ per la partizione dell'intero n che ha k_i parti di grandezza i, per $i = 1, 2, \ldots, n$. Non si devono calcolare potenze né eseguire moltiplicazioni: si tratta soltanto di una notazione. Per una permutazione σ di un insieme A, sia $z_i(\sigma)$ il numero dei cicli di σ di lunghezza i; dunque $(1^{z_1(\sigma)}2^{z_2(\sigma)}\cdots)$ è una partizione di $n = |A|$, detta *tipo* di σ. Dato un gruppo G che agisce su A, definiamo il suo indice dei cicli Z_G come il polinomio nelle n indeterminate $X_1, X_2, \ldots, X_n$ dato da Orig. 525

$$Z_G(X_1, X_2, \ldots, X_n) := \frac{1}{|G|}\sum_{\sigma\in G} X_1^{z_1(\sigma)}\cdots X_n^{z_n(\sigma)}.$$

Il Teorema 37.1 afferma che il numero delle orbite di G su B^A è

$$Z_G(b, b, \ldots, b) = \frac{1}{|G|}\sum_{\sigma\in G} b^{z_1(\sigma)+z_2(\sigma)+\cdots+z_n(\sigma)},$$

[1] Nell'originale, in questa frase, compare S al posto di X.

dove $b := |B|$.

Esempio 37.1. Un gruppo ciclico C_n di ordine n ha $\varphi(d)$ elementi di ordine d per ogni divisore d di n. Come permutazione nella rappresentazione regolare di C_n, un elemento di ordine d ha n/d cicli di lunghezza d. Per la rappresentazione regolare di C_n abbiamo quindi

$$Z_{C_n}(X_1, \ldots, X_n) = \frac{1}{n} \sum_{d|n} \varphi(d) X_d^{n/d}.$$

Possiamo ora contare le collane «a una faccia» di n perline di due colori. La risposta è $Z_{C_n}(2, 2, \ldots, 2) = \frac{1}{n} \sum_{d|n} \varphi(d) 2^{n/d}$; cfr. l'equazione (10.12). Per $n = 6$ otteniamo 14, una in più che con l'equivalenza diedrale (le due collane in (37.1) sono ora distinte). Per $n = 10$ otteniamo 108.

Esempio 37.2. Per trovare l'indice dei cicli del gruppo diedrale D_n nella sua rappresentazione usuale su n punti, dobbiamo tener conto delle permutazioni (riflessioni) che non appartengono al suo sottogruppo ciclico di ordine n. Vi sono due casi, secondo la parità di n:

$$Z_{D_n} = \begin{cases} \dfrac{1}{2n} \left(\displaystyle\sum_{d|n} \varphi(d) X_d^{n/d} + n X_1 X_2^{(n-1)/2} \right), & n \text{ dispari}, \\ \dfrac{1}{2n} \left(\displaystyle\sum_{d|n} \varphi(d) X_d^{n/d} + \frac{n}{2} X_1^2 X_2^{n/2-1} + \frac{n}{2} X_2^{n/2} \right), & n \text{ pari}. \end{cases}$$

Il numero delle collane «a due facce» con n perline di due colori è $Z_{D_n}(2, 2, \ldots, 2)$. Per $n = 6$ otteniamo 13, verificando così l'elenco che segue la Questione 1. Per $n = 10$ otteniamo 78. Orig. 526

Problema 37A. Calcolare l'indice dei cicli del gruppo delle rotazioni del cubo, rappresentate come permutazioni delle sei facce. (Vi sono 24 rotazioni, compresa l'identità, che portano il cubo, considerato come corpo rigido nello spazio tridimensionale, su se stesso. Non consideriamo le 24 riflessioni del cubo.) In quanti modi essenzialmente diversi si possono colorare le facce del cubo con 2 colori? Con 3 colori? Con n colori?

Prima di procedere, scriviamo l'indice dei cicli dei gruppi simmetrici. Nell'equazione (13.3) abbiamo dato la formula per il numero delle partizioni di un tipo assegnato $(1^{k_1} 2^{k_2} \cdots n^{k_n})$. Su ogni blocco di grandezza i si può scegliere una permutazione ciclica in $(i-1)!$ modi; abbiamo quindi

$$Z_{S_n} = \sum_{(1^{k_1} 2^{k_2} \cdots)} \frac{X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}}{1^{k_1} 2^{k_2} \cdots n^{k_n} k_1! k_2! \cdots k_n!}.$$

Ecco i primi polinomi:

$$\begin{aligned}
1! Z_{S_1} &= X_1, \\
2! Z_{S_2} &= X_1^2 + X_2, \\
3! Z_{S_3} &= X_1^3 + 3X_1X_2 + 2X_3, \\
4! Z_{S_4} &= X_1^4 + 6X_1^2X_2 + 3X_2^2 + 8X_1X_3 + 6X_4, \\
5! Z_{S_5} &= X_1^5 + 10X_1^3X_2 + 15X_1X_2^2 + 20X_1^2X_3 + 20X_2X_3 \\
&\quad + 30X_1X_4 + 24X_5, \\
6! Z_{S_6} &= X_1^6 + 15X_1^4X_2 + 45X_1^2X_2^2 + 40X_3^2 + 40X_1^3X_3 + 15X_2^3 \\
&\quad + 120X_1X_2X_3 + 90X_1^2X_4 + 90X_2X_4 + 144X_1X_5 + 120X_6.
\end{aligned}$$

Esempio 37.3. Il Teorema 37.1 si può usare per enumerare i grafi. Sia V un insieme fissato di n vertici e sia E l'insieme di tutti i sottoinsiemi di V con 2 elementi. I grafi semplici con insieme dei vertici V possono essere visti come applicazioni $f : E \to \{0, 1\}$: il grafo corrispondente a f ha come insieme degli spigoli $f^{-1}(1) = \{e : f(e) = 1\}$. Due grafi su V sono isomorfi se e solo se esiste una permutazione di V che porta gli spigoli dell'uno sugli spigoli dell'altro. Per esprimere ciò in una forma adatta ad applicare il Teorema 37.1, sia S_n il gruppo simmetrico su V e sia $S_n^{(2)} = \{\sigma^{(2)} : \sigma \in S_n\}$ il gruppo indotto, isomorfo a S_n, di permutazioni di E, dove Orig. 527

$$\sigma^{(2)} : \{x, y\} \longmapsto \{\sigma(x), \sigma(y)\}.$$

Allora $S_n^{(2)}$ agisce su $\{0,1\}^E$, e osserviamo che $f, g : E \to \{0,1\}$ corrispondono a grafi isomorfi se e solo se appartengono alla stessa orbita di $S_n^{(2)}$ su $\{0,1\}^E$.

Calcolare i tipi di tutte le permutazioni di $S_n^{(2)}$ non è un compito piacevole. Per esempio, se $\sigma \in S_5$ ha tipo $(2^1 3^1)$, risulta che $\sigma^{(2)}$ ha tipo $(1^1 3^1 6^1)$ sui 10 spigoli di K_5. L'indice dei cicli di $S_5^{(2)}$ è

$$\frac{1}{120}\big(X_1^{10} + 10X_1^4X_2^3 + 15X_1^2X_2^4 + 20X_1X_3^3 + 20X_1X_3X_6 + 30X_2X_4^2 + 24X_5^2\big).$$

In generale avremo una somma su tutte le partizioni di n. Sostituendo 2 a tutte le indeterminate, si trova che il numero dei grafi non isomorfi su cinque vertici è 34.

Generalizziamo ora il Teorema 37.1 per ammettere dei pesi. Sia A un insieme di n elementi, sia G un gruppo che agisce su A, e sia B un insieme finito di colori. Sia R un anello commutativo contenente i razionali e sia $w : B \to R$ un'applicazione che assegna un peso $w(b) \in R$ a ciascun colore $b \in B$. Per $f : A \to B$, definiamo

$$W(f) := \prod_{a \in A} w(f(a)) \in R;$$

$W(f)$ è il *peso* della funzione f. Si osservi che due applicazioni che rappresentano la stessa orbita di G su B^A hanno lo stesso peso, cioè $W(\sigma(f)) = W(f)$ per ogni $\sigma \in G$. La somma

$$\sum_{f \in \mathcal{R}} W(f),$$

estesa a un sistema di rappresentanti $\mathcal{R}$ delle orbite, si chiama *serie enumeratrice delle configurazioni*. (Le orbite sono spesso dette configurazioni; il termine serie diventa appropriato quando i pesi sono monomi.) Se tutti i pesi $w(b)$ sono uguali a 1, il teorema seguente si riduce al Teorema 37.1. Orig. 528

Teorema 37.2. Con la terminologia appena introdotta, la serie enumeratrice delle configurazioni è data da

$$\sum_{f \in \mathcal{R}} W(f) = Z_G\left(\sum_{b \in B} w(b), \sum_{b \in B} [w(b)]^2, \ldots, \sum_{b \in B} [w(b)]^n\right).$$

Dimostrazione. Sia $N = \sum W(f)$, dove la somma è estesa a tutte le coppie (σ, f) con $\sigma \in G$, $f \in B^A$ e $\sigma(f) = f$. Abbiamo

$$N = \sum_{f \in B^A} W(f)|G_f|,$$

dove G_f è lo stabilizzatore di f. Consideriamo i termini $W(f)|G_f|$ mentre f varia in un'orbita O di G su B^A: ciascuno è uguale a $W(f_0)|G|/|O|$, dove f_0 rappresenta l'orbita O, perciò la loro somma è $|G|W(f_0)$. È ora chiaro che N è il prodotto di $|G|$ per la serie enumeratrice delle configurazioni.

D'altra parte,

$$N = \sum_{\sigma \in G}\left(\sum_{\sigma(f)=f} W(f)\right).$$

Ricordando la definizione di Z_G, vediamo che la dimostrazione sarà completa se mostreremo che

$$\sum_{\sigma(f)=f} W(f) = \left(\sum_{b \in B} w(b)\right)^{k_1}\left(\sum_{b \in B} [w(b)]^2\right)^{k_2} \cdots \left(\sum_{b \in B} [w(b)]^n\right)^{k_n}$$

quando σ è una permutazione di tipo $(1^{k_1} 2^{k_2} \cdots n^{k_n})$.

Un'applicazione $f : A \to B$ è fissata da σ se e solo se è costante su ogni ciclo di σ su A. Siano

$$C_1, C_2, \ldots, C_k, \qquad k := k_1 + k_2 + \cdots + k_n,$$

i cicli di σ. Le applicazioni $f \in B^A$ fissate da σ sono in corrispondenza biunivoca con le k-uple $(b_1, b_2, \ldots, b_k)$ di elementi di B (l'applicazione corrispondente associa b_i a tutti gli elementi di C_i). Il peso dell'applicazione f corrispondente a $(b_1, \ldots, b_k)$ è Orig. 529

$$W(f) = \prod_{i=1}^{k} [w(b_i)]^{|C_i|},$$

e, sommando su tutte le k-uple $(b_1, b_2, \dots, b_k)$,

$$\begin{aligned}\sum_{\sigma(f)=f} W(f) &= \sum_{b_1,b_2,\dots,b_k} [w(b_1)]^{|C_1|}[w(b_2)]^{|C_2|}\cdots[w(b_k)]^{|C_k|} \\ &= \left(\sum_{b_1}[w(b_1)]^{|C_1|}\right)\left(\sum_{b_2}[w(b_2)]^{|C_2|}\right)\cdots \\ &= \prod_{c=1}^{n}\left(\sum_{b}[w(b)]^{c}\right)^{k_c},\end{aligned}$$

come volevamo. □

Esempio 37.4. Consideriamo il problema delle collane con equivalenza ciclica. In questo caso $G = C_n$ e $B = \{\text{nero}, \text{bianco}\}$. Prendiamo come R l'anello di polinomi $\mathbb{Q}[X]$ e definiamo $w(\text{nero}) = 1$, $w(\text{bianco}) = X$. Il peso di una colorazione $f : A \to B$ è allora

$$W(f) = X^k,$$

dove k è il numero delle perline bianche.

Quindi il numero delle collane cicliche essenzialmente diverse con n perline, di cui k bianche, è il coefficiente di X^k nella serie enumeratrice delle configurazioni

$$\begin{aligned}Z_{C_n}(1+X, 1+X^2, 1+X^3, \dots, 1+X^n) &= \frac{1}{n}\sum_{d|n}\varphi(d)[1+X^d]^{n/d} \\ &= \frac{1}{n}\sum_{d|n}\varphi(d)\sum_{r=0}^{n/d}\binom{n/d}{r}X^{rd}.\end{aligned}$$

Questo coefficiente è

$$\frac{1}{n}\sum_{d|(k,n)}\varphi(d)\binom{n/d}{k/d}.$$

Orig. 530

Se k e n sono coprimi, il numero è dunque semplicemente $\frac{1}{n}\binom{n}{k}$, mentre per $n = 12$, $k = 4$ si hanno $\frac{1}{12}\left[\varphi(1)\binom{12}{4} + \varphi(2)\binom{6}{2} + \varphi(4)\binom{3}{1}\right] = 43$ collane.

Problema 37B. In quanti modi essenzialmente diversi si possono colorare le facce di un cubo in modo che una faccia sia rossa, due siano blu e le altre tre siano verdi? Risolvere il problema «a mano» (il che potrebbe essere più rapido) e anche usando il Teorema 37.2, quindi confrontare le risposte.

Siano A e B insiemi finiti, $|A| = n$, e siano G e H gruppi finiti, con G agente su A e H su B. Il prodotto diretto $G \times H$ agisce su B^A se, per $f \in B^A$ e $(\sigma, \tau) \in G \times H$, definiamo $(\sigma, \tau)(f)$ mediante

$$((\sigma, \tau)(f))(a) = \tau(f(\sigma^{-1}(a))).$$

Teorema 37.3. Il numero delle orbite di $G \times H$ su B^A è

$$\frac{1}{|H|}\sum_{\tau\in H} Z_G(m_1(\tau), m_2(\tau), \dots, m_n(\tau)),$$

dove

$$m_i(\tau) := \sum_{j|i} j z_j(\tau), \qquad i = 1, 2, \dots, n.$$

Dimostrazione. Per il lemma di Burnside, il numero delle orbite è

$$\frac{1}{|G||H|}\sum_{\sigma\in G,\tau\in H}\psi(\sigma, \tau),$$

dove $\psi(\sigma,\tau)$ è il numero delle applicazioni $f \in B^A$ tali che $(\sigma,\tau)(f) = f$. Per completare la dimostrazione basterà mostrare che, per ogni $\tau \in H$,

$$\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma,\tau) = Z_G(m_1(\tau), m_2(\tau), \ldots, m_n(\tau)). \tag{37.3}$$

Fissiamo $\sigma \in G$ e $\tau \in H$ e siano

Orig. 531

$$C_1, C_2, \ldots, C_k, \qquad k := z_1(\sigma) + z_2(\sigma) + \cdots + z_n(\sigma),$$

i cicli di σ su A. Un'applicazione $f : A \to B$ è fissata da (σ,τ) se e solo se sono fissate tutte le restrizioni $f_i := f|C_i$, $1 \le i \le k$. Quindi $\psi(\sigma,\tau)$ è il prodotto, per $1 \le i \le k$, dei numeri di applicazioni $f_i : C_i \to B$ che soddisfano

$$f_i(\sigma(a)) = \tau(f_i(a)) \qquad \text{per ogni } a \in C_i.$$

Sia ℓ la lunghezza di C_i e fissiamo $a_0 \in C_i$. Supponiamo che $f_i : C_i \to B$ sia fissata da $(\sigma|C_i, \tau)$ e che $f_i(a_0) = b$. Allora f_i è completamente determinata: $f_i(\sigma^t(a_0)) = \tau^t(b)$. Inoltre, $b = f_i(a_0) = f_i(\sigma^\ell(a_0)) = \tau^\ell(b)$, e quindi il ciclo di τ che contiene b deve avere una lunghezza ℓ' che divide ℓ.

Viceversa, se b è un elemento di B appartenente a un ciclo di τ di lunghezza divisore di $\ell := |C_i|$, possiamo definire su C_i l'applicazione $f_i(\sigma^t(a_0)) := \tau^t(b)$ (si verifichi che è ben definita), e questa f_i è fissata da $(\sigma|C_i, \tau)$.

In conclusione, quando $|C_i| = \ell$, le applicazioni fissate $f_i : C_i \to B$ sono tante quanti gli elementi di B appartenenti a cicli di τ la cui lunghezza divide ℓ. Il numero di tali elementi è, naturalmente,

$$m_\ell(\tau) = \sum_{j|\ell} j z_j(\tau).$$

Pertanto

$$\psi(\sigma,\tau) = \prod_{i=1}^{k} m_{|C_i|}(\tau) = [m_1(\tau)]^{z_1(\sigma)}[m_2(\tau)]^{z_2(\sigma)}\cdots[m_n(\tau)]^{z_n(\sigma)},$$

da cui segue immediatamente l'equazione (37.3). □

Esempio 37.5. In quanti modi si possono distribuire 2 palline rosse, 2 gialle e 4 verdi in 1 scatola rotonda e 3 quadrate? Prendiamo

$$A = \{R_1, R_2, Y_1, Y_2, G_1, G_2, G_3, G_4\},$$

Orig. 532

$$G = S_2 \times S_2 \times S_4, \qquad B = \{r, s_1, s_2, s_3\}, \qquad H = S_1 \times S_3.$$

È facile vedere che l'indice dei cicli di G è il prodotto degli indici dei cicli dei gruppi simmetrici di cui G è prodotto; quindi

$$\begin{aligned} Z_G &= Z_{S_2}\cdot Z_{S_2}\cdot Z_{S_4} \\ &= \frac{1}{2!2!4!}(X_1^2 + X_2)^2(X_1^4 + 6X_1^2X_2 + 3X_2^2 + 8X_1X_3 + 6X_4). \end{aligned} \tag{37.4}$$

Vi sono tre tipi di permutazioni in H. Se τ è l'identità,

$$m_1(\tau) = 4, \quad m_2(\tau) = 4, \quad m_3(\tau) = 4, \quad m_4(\tau) = 4;$$

se τ scambia due elementi di $\{s_1, s_2, s_3\}$,[2]

$$m_1(\tau) = 2, \quad m_2(\tau) = 4, \quad m_3(\tau) = 2, \quad m_4(\tau) = 4;$$

se τ fissa soltanto r,

$$m_1(\tau) = 1, \quad m_2(\tau) = 1, \quad m_3(\tau) = 4, \quad m_4(\tau) = 1.$$

[2]Nell'originale l'insieme è stampato erroneamente come $\{s_2, s_2, s_3\}$.

Per il Teorema 37.3, il numero delle distribuzioni è

$$\frac{1}{3!2!2!4!}\big[(4^2+4)^2(4^4+6\cdot 4^2\cdot 4+3\cdot 4^2+8\cdot 4\cdot 4+6\cdot 4)$$
$$+3(2^2+4)^2(2^4+6\cdot 2^2\cdot 4+3\cdot 4^2+8\cdot 2\cdot 2+6\cdot 4)$$
$$+2(1^2+1)^2(1^4+6\cdot 1^2\cdot 1+3\cdot 1^2+8\cdot 1\cdot 4+6\cdot 1)\big]=656$$

(se abbiamo eseguito correttamente i calcoli).[3]

Problema 37C. Dati G su A e H su B, trovare un'espressione per il numero delle orbite delle applicazioni iniettive $f : A \to B$.

Enunciamo senza dimostrazione l'estensione del Teorema 37.3 che ammette dei pesi. Per una dimostrazione si veda de Bruijn (1964). Se tutti i pesi sono 1, essa si riduce al Teorema 37.3.

Teorema 37.4. Siano G agente su A e H su B, sia R un anello commutativo e sia $w : B \to R$. Supponiamo che w sia costante su ogni orbita di H su B. Posto $W(f) := \prod_{a\in A} w[f(a)]$, la somma $\sum W(f)$, estesa a un sistema di rappresentanti delle orbite di $G \times H$ su B^A, è uguale a

Orig. 533

$$\frac{1}{|H|}\sum_{\tau\in H} Z_G\big(M_1(\tau), M_2(\tau), \dots, M_n(\tau)\big),$$

dove

$$M_i(\tau) = \sum_{\tau^i(b)=b} [w(b)]^i.$$

Esempio 37.6. Proseguiamo l'Esempio 37.5.[4] Prendiamo

$$w(r) = r, \qquad w(s_1) = w(s_2) = w(s_3) = s,$$

dove $R = \mathbb{Q}[r, s]$. Il numero delle distribuzioni con t palline nella scatola rotonda e le altre $8 - t$ nelle scatole quadrate è il coefficiente di $r^t s^{8-t}$ in

$$\frac{1}{6}\big[Z_G(r+3s, r^2+3s^2, r^3+3s^3, r^4+3s^4)$$
$$+3Z_G(r+s, r^2+3s^2, r^3+s^3, r^4+3s^4)$$
$$+2Z_G(r, r^2, r^3+3s^3, r^4)\big],$$

dove Z_G è il polinomio della (37.4).

Problema 37D. Identificare le collane di perline di due colori con le loro duali, ottenute scambiando i colori delle perline. (Possiamo ora distinguere i due colori, ma non possiamo stabilire quale sia l'uno e quale l'altro.) Quante sono queste configurazioni ridotte? (Per esempio, per $n = 6$ ed equivalenza diedrale vi sono 8 configurazioni distinte.) Quante collane sono autoduali?

Problema 37E. Si vogliono colorare le facce del cubo con s colori e i vertici con t colori (che si possono supporre diversi, benché ciò non abbia importanza). In quanti modi essenzialmente diversi, rispetto al gruppo delle rotazioni del cubo, si può farlo?

* * *

I teoremi di questo capitolo sono anche fonti di identità algebriche. Consideriamo il caso della «distribuzione di oggetti uguali in caselle distinte». (Stiamo richiamando una questione discussa nel Capitolo 13.) Per esempio, in quanti modi possiamo distribuire 23 mele a Fred, Jane e George? Più in generale, consideriamo le distribuzioni di un insieme A di n mele a un insieme B di x persone (gli elementi di A sono «uguali», mentre quelli di B restano distinti, cioè sono «diversi»). Una distribuzione del genere equivale alla scelta di una famiglia $(k_b : b \in B)$ di interi non negativi k_b con $\sum_{b\in B} k_b = n$, in cui alla persona b vanno k_b mele.

Orig. 534

[3] Nella prima riga dell'originale compare $2 \cdot 4^2$ invece di $3 \cdot 4^2$. La correzione, imposta dalla (37.4), dà effettivamente 656.
[4] L'originale rinvia erroneamente all'Esempio 13.5.

Il numero delle distribuzioni è dunque, come mostrato nel Teorema 13.3,

$$\binom{n+x-1}{n}.$$

Tuttavia la migliore definizione formale di una simile distribuzione è quella di orbita di applicazioni $f : A \to B$ rispetto al gruppo simmetrico S_n agente su A. (Due applicazioni $f, g \in B^A$ determinano la stessa distribuzione se e solo se «differiscono» per una permutazione delle mele.) Per il Teorema 37.1 il numero delle distribuzioni è

$$\frac{1}{n!}\sum_{k=0}^{n} c_k(S_n)x^k,$$

dove $c_k(S_n)$ è il numero delle permutazioni di n lettere con esattamente k cicli. Nel Capitolo 13 i numeri $c_k(S_n)$ erano chiamati numeri di Stirling di prima specie senza segno e denotati con $c(n, k)$. Per il Teorema 37.2, per ogni intero non negativo x,

$$(x+n-1)_{(n)} = \sum_{k=0}^{n} c_k(S_n)x^k,$$

e quindi questa uguaglianza deve valere come identità polinomiale. Abbiamo così dimostrato nuovamente la formula (13.7).

Prendiamo come G il gruppo S_n su un insieme A di n elementi; sia B finito e sia w l'inclusione di B nell'anello di polinomi $\mathbb{Q}[B]$. In questo caso il peso di un'applicazione $f : A \to B$ è un monomio e due applicazioni sono equivalenti, cioè rappresentano la stessa configurazione, se e solo se hanno lo stesso peso. La serie enumeratrice delle configurazioni

Orig. 535

$$\sum W(f) = Z_{S_n}\left(\sum_{b\in B} b, \sum_{b\in B} b^2, \ldots, \sum_{b\in B} b^n\right) \tag{37.5}$$

esprime le cosiddette funzioni simmetriche omogenee complete come polinomi nelle funzioni simmetriche somme di potenze. Per esempio, per $n = 3$ e $B = \{X, Y\}$,

$$6(X^3 + X^2Y + XY^2 + Y^3) = (X+Y)^3 + 3(X+Y)(X^2+Y^2) + 2(X^3+Y^3).$$

Per $n = 4$ e $B = \{X, Y, Z\}$, la (37.5) esprime

$$\sum_{i+j+k=4} X^iY^jZ^k$$

come polinomio in

$$X+Y+Z, \quad X^2+Y^2+Z^2, \quad X^3+Y^3+Z^3, \quad X^4+Y^4+Z^4.$$

Note

Osserviamo che $Z_{S_n}(X_1, \ldots, X_n)$ è il coefficiente di Y^n in

$$\exp\left(X_1Y + \frac{1}{2}X_2Y^2 + \frac{1}{3}X_3Y^3 + \cdots\right),$$

considerato come elemento di $(\mathbb{Q}[X_1, X_2, \ldots])[[Y]]$.

Le risposte fornite dalla teoria di Pólya hanno il vantaggio (per esempio rispetto al principio di inclusione-esclusione) che la formula ottenuta è una somma di termini positivi, anziché una somma a segni alterni.

G. Pólya (1887–1985) fu un matematico ungherese il cui libro *Problems and Theorems in Analysis*, scritto nel 1924 con G. Szegő, è tuttora un classico. Ma è forse più noto per *How to Solve It*, che ha venduto oltre un milione di copie. Scrisse lavori di teoria dei numeri, analisi complessa, combinatoria, teoria della probabilità, geometria e fisica matematica.

Riferimenti bibliografici

- N. G. de Bruijn (1964), Pólya's theory of counting, in: E. F. Beckenbach (a cura di), *Applied Combinatorial Mathematics*, Wiley.
- F. Harary e E. D. Pulver (1966), The power group enumeration theorem, *J. Combinatorial Theory* **1**.

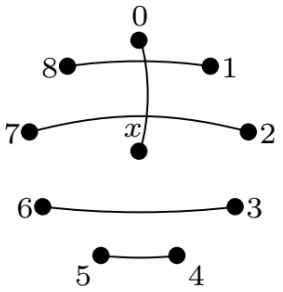
Capitolo 38

Il teorema di Baranyai

In questo capitolo daremo un'elegante applicazione del teorema di integralità dei flussi a un problema di «disegni combinatori». Orig. 536

Esempio 38.1. Supponiamo che ci sia stato affidato il compito di preparare il calendario degli incontri delle squadre di football della «Big Ten». Ogni fine settimana esse devono dividersi in 5 coppie e giocare. Al termine di 9 settimane vogliamo che ogni possibile coppia di squadre si sia affrontata esattamente una volta.

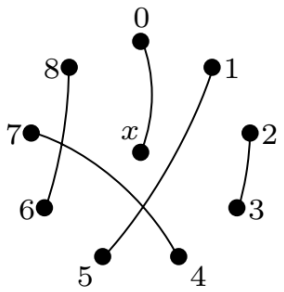
Ecco una soluzione. Disponiamo 9 squadre sui vertici di un 9-gono regolare e una nel centro. Partiamo dall'accoppiamento indicato qui sotto e otteniamo gli altri ruotando la figura di multipli di $2\pi/9$.



Esplicitamente, ecco il calendario:

x–0	x–1	x–2	x–3	x–4	x–5	x–6	x–7	x–8
1–8	2–0	3–1	4–2	5–3	6–4	7–5	8–6	0–7
2–7	3–8	4–0	5–1	6–2	7–3	8–4	0–5	1–6
3–6	4–7	5–8	6–0	7–1	8–2	0–3	1–4	2–5
4–5	5–6	6–7	7–8	8–0	0–1	1–2	2–3	3–4

Vi sono molti altri modi di procedere. Per esempio, si può partire dall'accoppiamento iniziale mostrato qui sotto. Orig. 537



Un accoppiamento perfetto in un grafo è detto anche *1-fattore*. Una partizione dell'insieme degli spigoli di un grafo in 1-fattori è una *1-fattorizzazione*. Nell'esempio precedente abbiamo costruito delle 1-fattorizzazioni di K_{10}. Vi sono 396 1-fattorizzazioni non isomorfe di K_{10}: è un risultato ottenuto al calcolatore da E. N. Gelling (1973). Si veda anche Mendelsohn e Rosa (1985).

Esempio 38.2. Sia Γ un qualunque gruppo abeliano di ordine dispari. Consideriamo il grafo completo sull'insieme dei vertici $\Gamma \cup \{\infty\}$. Per $g \in \Gamma$, poniamo

$$M_g := \{\{g, \infty\}\} \cup \{\{a, b\} : a + b = 2g,\ a \neq b\}.$$

Allora $\{M_g : g \in \Gamma\}$ è una 1-fattorizzazione del grafo completo.

Consideriamo la seguente generalizzazione del problema: con il termine *classe parallela* di sottoinsiemi di k elementi di un insieme di n elementi indichiamo una famiglia di n/k sottoinsiemi di k elementi che costituiscono una partizione dell'insieme. È possibile ripartire l'insieme di tutti i sottoinsiemi di k elementi in classi parallele? Naturalmente ciò richiede che k divida n. Il numero delle classi parallele necessarie sarebbe $\frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$.

Per $k = 2$ il problema non era difficile. È molto più difficile per $k = 3$, ma fu risolto da R. Peltesohn nel 1936, e per $k = 4$ da J.-C. Bermond (risultato non pubblicato). Il lettore potrebbe provare a trovare opportune classi parallele per $n = 9$, $k = 3$. Non è affatto evidente che la nostra generalizzazione ammetta sempre una soluzione; fu dunque sorprendente quando Zs. Baranyai dimostrò il Teorema 38.1 nel 1973. Tutte le dimostrazioni note usano una forma o una conseguenza del Teorema 7.2 o del Teorema 7.4. La dimostrazione che presentiamo è dovuta ad A. E. Brouwer e A. Schrijver (1979).

Teorema 38.1. Se k divide n, l'insieme di tutti i $\binom{n}{k}$ sottoinsiemi di k elementi di un insieme di n elementi può essere ripartito in classi parallele disgiunte $\mathcal{A}_i$, $i = 1, 2, \ldots, \binom{n-1}{k-1}$.

Dimostrazione. In questa dimostrazione useremo il termine *m-partizione* di un insieme X per indicare un multiinsieme $\mathcal{A}$ di m sottoinsiemi di X a due a due disgiunti, alcuni dei quali possono essere vuoti, la cui unione è X. (Nell'uso abituale il termine «partizione» esclude l'insieme vuoto, ma qui è importante ammetterlo, eventualmente con una molteplicità, in modo che il numero totale dei sottoinsiemi sia m.) Orig. 538

Per far funzionare una dimostrazione induttiva dimostriamo qualcosa di apparentemente più forte dell'enunciato originale. Siano dati n e k, supponiamo che k divida n, e poniamo $m := n/k$, $M := \binom{n-1}{k-1}$. Affermiamo che, per ogni intero ℓ, $0 \leq \ell \leq n$, esiste una famiglia

$$\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_M$$

di m-partizioni di $\{1, 2, \ldots, \ell\}$ tale che ogni sottoinsieme $S \subseteq \{1, 2, \ldots, \ell\}$ compaia esattamente in

$$\binom{n-\ell}{k-|S|} \tag{38.1}$$

delle m-partizioni $\mathcal{A}_i$. (Naturalmente il coefficiente binomiale si interpreta come zero se $|S| > k$; per $S = \varnothing$, le m-partizioni contenenti $\varnothing$ si contano con molteplicità uguale al numero delle volte in cui vi compare l'insieme vuoto.)

Dimostreremo l'affermazione per induzione su ℓ. Si osservi che è banalmente vera per $\ell = 0$, quando ciascuna $\mathcal{A}_i$ consiste in m copie dell'insieme vuoto. Si osservi inoltre che il caso $\ell = n$ dimostrerà il Teorema 38.1, poiché allora il coefficiente binomiale in (38.1) è

$$\binom{0}{k-|S|} = \begin{cases} 1 & \text{se } |S| = k, \\ 0 & \text{altrimenti.} \end{cases}$$

Osservazione. Questo enunciato, piuttosto tecnico, non è in realtà più generale: seguirebbe facilmente dal Teorema 38.1. Se esistono M classi parallele come nell'enunciato del Teorema 38.1, allora, per ogni insieme L di ℓ punti di X, le intersezioni con L dei membri delle classi parallele forniscono m-partizioni di L con la proprietà precedente.

Supponiamo che, per un certo valore $\ell < n$, esistano m-partizioni $\mathcal{A}_1, \ldots, \mathcal{A}_M$ con la proprietà richiesta. Costruiamo una rete di trasporto nel modo seguente. Introduciamo un vertice sorgente σ, un vertice chiamato $\mathcal{A}_i$ per ogni $i = 1, 2, \ldots, M$, un vertice chiamato S per ogni sottoinsieme $S \subseteq \{1, 2, \ldots, \ell\}$ e un vertice pozzo τ. Vi è uno spigolo orientato da σ a ogni $\mathcal{A}_i$, con capacità 1. Vi sono spigoli orientati da $\mathcal{A}_i$ ai vertici corrispondenti ai membri di $\mathcal{A}_i$ (si usino j spigoli verso $\varnothing$ se $\varnothing$ compare j volte in $\mathcal{A}_i$); a questi si può assegnare una qualunque capacità intera ≥ 1. Infine vi è uno spigolo orientato dal vertice corrispondente a un sottoinsieme S a τ, di capacità

Orig. 539

$$\binom{n-\ell-1}{k-|S|-1}.$$

Esibiamo un flusso in questa rete: assegniamo valore 1 agli spigoli uscenti da σ, valore $(k-|S|)/(n-\ell)$ agli spigoli da $\mathcal{A}_i$ a ciascuno dei suoi membri S, e valore $\binom{n-\ell-1}{k-|S|-1}$ allo spigolo da S a τ. È facile verificare che si tratta di un flusso: la somma dei valori sugli spigoli uscenti da un vertice $\mathcal{A}_i$ è

$$\sum_{S\in\mathcal{A}_i} \frac{k-|S|}{n-\ell} = \frac{1}{n-\ell}\left[mk - \sum_{S\in\mathcal{A}_i} |S|\right] = \frac{1}{n-\ell}(mk-\ell) = 1.$$

La somma dei valori sugli spigoli entranti in un vertice S è

$$\sum_{i:S\in\mathcal{A}_i} \frac{k-|S|}{n-\ell} = \frac{k-|S|}{n-\ell}\binom{n-\ell}{k-|S|} = \binom{n-\ell-1}{k-|S|-1}.$$

Poiché tutti gli spigoli uscenti da σ sono saturi, questo è un flusso massimo di valore M. Anche gli spigoli entranti in τ sono saturi in questo flusso, e quindi in ogni flusso massimo. Per il Teorema 7.2, la rete ammette un flusso massimo f a valori interi. Tutti gli spigoli uscenti da σ saranno saturi; è quindi chiaro che, per ogni i, f assegna valore 1 a uno degli spigoli uscenti da $\mathcal{A}_i$ e 0 a tutti gli altri. Supponiamo che f assegni 1 allo spigolo da $\mathcal{A}_i$ al suo membro S_i. Per ogni sottoinsieme S, il numero dei valori di i tali che $S_i = S$ è $\binom{n-\ell-1}{k-|S|-1}$.

Orig. 540

(Il flusso intero f desiderato si sarebbe anche potuto ottenere senza introdurre esplicitamente le capacità e senza usare il Teorema 7.2: sarebbe bastato applicare il Teorema 7.4 al flusso razionale esibito, completato a una circolazione mediante uno spigolo aggiuntivo da τ a σ con valore del flusso M.)

Infine otteniamo una famiglia di m-partizioni $\mathcal{A}'_1, \ldots, \mathcal{A}'_M$ dell'insieme $\{1, 2, \ldots, \ell+1\}$, facendo sì che $\mathcal{A}'_i$ si ottenga da $\mathcal{A}_i$ sostituendo il membro prescelto S_i con $S_i \cup \{\ell+1\}$, per $i = 1, \ldots, M$. Il lettore verifichi che ogni sottoinsieme T di $\{1, 2, \ldots, \ell+1\}$ compare esattamente

$$\binom{n-(\ell+1)}{k-|T|}$$

volte in $\mathcal{A}'_1, \ldots, \mathcal{A}'_M$. Questo conclude il passo induttivo. □

Problema 38A. Siano v e u interi con $v \geq 2u$ e v pari, e si consideri il grafo completo K_u come sottografo di K_v. Supponiamo che gli spigoli di K_u siano colorati con $v-1$ colori in modo che spigoli distinti dello stesso colore siano disgiunti. Dimostrare che questa colorazione si può estendere a una colorazione di $E(K_v)$ con $v-1$ colori in modo che gli spigoli dello stesso colore siano disgiunti. (Una tale colorazione di $E(K_v)$ equivale a una 1-fattorizzazione di K_v, nella quale gli spigoli di ogni colore formano un 1-fattore.)

Note

Zsolt Baranyai (1948–1978) fu un matematico ungherese che era anche un flautista dolce professionista. Teneva concerti in tournée in Ungheria con il Barkfark Consort e morì in un incidente automobilistico su una strada di campagna dopo uno di essi. La sua opera matematica comprendeva molti altri splendidi risultati sugli «ipergrafi uniformi completi».

Le 1-fattorizzazioni dei grafi completi sono legate ai quadrati latini simmetrici: si veda il Capitolo 17. Il risultato del Problema 38A è dovuto a Cruse (1974). Generalizzazioni si trovano in Baranyai e Brouwer (1977). Orig. 541

Riferimenti bibliografici

- Zs. Baranyai e A. E. Brouwer (1977), Extension of colourings of the edges of a complete (uniform hyper) graph, *Math. Centrum Dep. Pure Math. ZW.* **91**, 10 pp.
- A. E. Brouwer e A. Schrijver (1979), Uniform hypergraphs, in: A. Schrijver (a cura di), *Packing and Covering in Combinatorics*, Mathematical Centre Tracts **106**, Amsterdam.
- A. Cruse (1974), On embedding incomplete symmetric Latin squares, *J. Combinatorial Theory (A)* **16**, 18–22.
- E. N. Gelling (1973), On 1-factorizations of the complete graph and the relationship to round robin schedules, tesi di laurea magistrale, University of Victoria.
- E. Mendelsohn e A. Rosa (1985), One-factorizations of the complete graph—a survey, *Journal of Graph Theory* **9**.
- R. Peltesohn (1936), Das Turnierproblem für Spiele zu je dreien, dissertazione, Berlino, August Pries, Lipsia.

Appendice 1
Suggerimenti e commenti sui problemi

Orig. 542

Problema 1A. Mostrare che le $\binom{5}{2}$ coppie di $\{1,\dots,5\}$ si possono usare per etichettare i vertici in modo che una regola semplice determini quando esiste uno spigolo. Per trovare l'intero gruppo degli automorfismi, considerare il sottogruppo che fissa un vertice e i suoi tre vicini. Questo grafo è noto come grafo di Petersen. Fu studiato per la prima volta dal matematico danese J. P. C. Petersen (1839–1910). Si veda anche il Capitolo 21.

Problema 1B. Sia l'insieme dei vertici V l'unione disgiunta di V_1 e V_2, senza spigoli da V_1 a V_2. Qual è il massimo numero possibile di spigoli?

Problema 1C. Usare (1.1). (i) Considerare un vertice di grado 1; usare l'induzione. (ii) Un circuito ha tanti spigoli quanti vertici; se il grafo è connesso, ogni vertice ha grado ≥ 1.

Problema 1D. Chiamare i vertici a_1, a_2, a_3 e b_1, b_2, b_3. Dapprima omettere a_3 e mostrare che vi è un solo modo di disegnare nel piano il grafo con i sei spigoli rimanenti. Un metodo migliore consiste nell'usare la formula di Eulero (si veda il Capitolo 33).

Problema 1E. Ogni colore compare un numero pari di volte in un circuito. Si veda J. A. Bondy, Induced subsets, *J. Combinatorial Theory (B)* **12** (1972), 201–202. Il problema si può anche formulare così: data una matrice quadrata di 0 e 1 con righe distinte, è possibile eliminare una colonna in modo che la matrice risultante abbia righe distinte. Anche questo fatto si dimostra facilmente per induzione.

Problema 1F. Considerare i vertici a distanza 2 da un vertice fissato. Si veda la Fig. 1.4.

Orig. 543

Problema 1G. Usare il principio dei cassetti.

Problema 1H. Considerare quando $a_{ij} = a_{jk} = 1$.

Problema 1I. Trovare un procedimento induttivo per costruire il circuito richiesto.

Problema 1J. Per (i), stabilire una corrispondenza biunivoca tra i vertici adiacenti a x e quelli adiacenti a y.

Problema 2B. Qualunque ordinamento di 22335 funziona.

Problema 2C. Sia A_i il numero delle arborescenze ricoprenti con radice x_i e sia r_i il numero degli spigoli uscenti da x_i. Si può dimostrare l'affermazione mostrando che il numero dei diversi circuiti euleriani in G è

$$A_i \prod_{j=1}^{n} (r_j - 1)!.$$

A questo scopo, prendere $i = 1$ e considerare un'arborescenza ricoprente con radice x_1. Fissare uno spigolo uscente da x_1 come primo spigolo di un circuito euleriano. Numerare arbitrariamente gli altri spigoli uscenti da x_1. Per $i = 2, 3, \dots, n$, numerare arbitrariamente gli spigoli uscenti da x_i, ma in modo che lo spigolo dell'arborescenza ricoprente abbia numero r_i. Questa numerazione conduce naturalmente alla costruzione di un circuito euleriano, e il procedimento è reversibile. Si veda il Capitolo 9 di J. H. van

Lint, *Combinatorial Theory Seminar Eindhoven University of Technology*, Lecture Notes in Mathematics **382**, Springer-Verlag, 1974.

Problema 2D. Un approccio è il seguente. Mostrare che T_n ha la proprietà che ogni suo spigolo a ha gli estremi in componenti diverse di $G : \{e \in E(G) : c(e) < c(a)\}$. Mostrare poi che ogni albero ricoprente T con questa proprietà è un albero ricoprente di costo minimo.

Problema 2E. Vi è un solo modo di ottenere la differenza $n-1$, ecc.

Problema 2F. Usare il Problema 1C.

Problema 2G. Mostrare che, se G è un grafo con questa proprietà, esiste un grafo G' con la stessa proprietà, lo stesso numero di spigoli, e nel quale il vertice di grado m è collegato a tutti gli altri vertici di grado > 1. Usare poi l'induzione ($m \to m+2$). La costruzione si può effettuare induttivamente con la stessa idea. Orig. 544

Problema 3A. Per la parte (ii), se la conclusione non vale, H si può scrivere come unione di due sottografi A, B senza spigoli comuni, che si intersecano in due vertici s, t. Applicare l'ipotesi induttiva ai grafi A', B' ottenuti aggiungendo rispettivamente ad A e a B uno spigolo che unisce s, t.

Problema 3B. Si può usare lo stesso tipo di argomento dato per K_6 (sotto questo problema). Mostrare che deve esistere un vertice appartenente a due triangoli monocromatici. Ragionare poi sui sei vertici rimanenti. L'argomento sarà lungo e delicato. Il lettore che ha «barato» e ha continuato a leggere conosce il Corollario al Teorema 3.2.

Problema 3C. Chiamare n_1 e n_2 i termini, entrambi pari, del membro destro. Supporre che valga l'uguaglianza e considerare un grafo con $n_1 + n_2 - 1$ vertici. Se non vi è alcun K_p rosso né alcun K_q blu, qual è il grado rosso di ogni vertice? Quanti spigoli rossi vi sono nel grafo?

Problema 3D. In $\mathbb{Z}_{17}$ considerare $\pm 2^i$, con $i = 0, 1, 2, 3$. Per l'altro problema usare $\mathbb{Z}_{13}$. Applicare (3.4).

Problema 3E. (a) Fissare un vertice e considerare tutti gli spigoli diretti verso quel vertice e, rispettivamente, quelli uscenti da esso. Scegliere l'insieme più grande e usare l'induzione.

(b) Usare il metodo probabilistico. Una soluzione si trova nel Teorema 1.1 di P. Erdős e J. Spencer (1974), dove questo problema serve a illustrare il metodo.

Problema 3F. Prendere come vertici $\{1, 2, \ldots, n\}$. Colorare $\{i, j\}$ con il colore di $|i - j|$. Per evitare una terna con due colori, se 1 è rosso, 2 deve essere blu e quindi 4 deve essere rosso, ecc. Si ha $N(2) = 5$. Separare due di queste configurazioni a due colori con cinque numeri di un terzo colore per stimare $N(13)$.[1] Si veda I. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod p$, *Jber. Deutsche Math. Ver.* **25** (1916), 114–116.

Problema 3G. Colorare con quattro «colori» nel modo seguente:

$$\{i, j\} \longmapsto (a_{ij}, a_{ji}) \qquad (i < j).$$

Orig. 545

Problema 3H. Usare l'argomento impiegato per K_6 e due colori.

Problema 3I. Far dipendere il colore da $\nu \pmod 3$. Mostrare che la somma di due cubi in $\mathbb{F}_{16}^*$ non è un cubo.

Problema 3J. Considerare un sottografo massimale con la proprietà richiesta e poi contare i vertici che non vi appartengono.

Problema 3K. Considerare i vertici di un colore fissato ed eliminare spigoli in modo che sia possibile ricolorare.

Problema 4A. (i) Colorare K_{10} in modo che il rosso corrisponda a uno spigolo di G e il blu a una coppia non adiacente. Vi sono triangoli con 3 spigoli rossi, con 2 rossi e 1 blu, con 2 blu e 1 rosso, e

[1] L'originale stampa $N(13)$; il contesto della costruzione con tre colori suggerisce $N(3)$.

infine con 3 blu. Siano a_i, $i = 1, 2, 3, 4$, i rispettivi numeri. Impostare per questi numeri un sistema di equazioni e disequazioni espresse mediante i gradi dei vertici di G. Esse dovrebbero mostrare che vi sono almeno quattro triangoli in G; l'uguaglianza si può poi escludere esaminando ancora le equazioni.

(ii) Una seconda soluzione è la seguente. Mostrare che esiste un triangolo. Considerare poi un triangolo, l'insieme complementare di 7 vertici e gli spigoli tra i due. Ciò dà un certo numero di nuovi triangoli di due tipi; stimare questo numero.

Problema 4B. Usare l'induzione. Prima riesaminare la dimostrazione del Teorema 4.1.

Problema 4C. Il numero dei triangoli contenenti uno spigolo a con estremi x e y è almeno $\deg(x) + \deg(y) - n$. Sommare su tutti gli spigoli a.

Problema 4D. Fissare un vertice qualsiasi x e indicare con D_i l'insieme dei vertici a distanza i da x in G.

Per $g = 2t + 1$, si ha $|V(G)| \geq 1 + r + r(r-1) + \cdots + r(r-1)^{t-1}$, poiché è facile vedere che $|D_i| = r(r-1)^{i-1}$ per $i = 1, 2, \ldots, t$.

Per $g = 2t$, abbiamo ancora $|D_i| = r(r-1)^{i-1}$ per $i = 1, 2, \ldots, t-1$. Possiamo anche ottenere il limite inferiore $|D_t| \geq \frac{r-1}{r}|D_{t-1}|$, poiché ogni vertice $y \in D_{t-1}$ è adiacente a $r-1$ vertici di D_t, mentre un vertice $y \in D_t$ può naturalmente essere adiacente ad al più r vertici di D_{t-1}.[2]

Problema 4E. Il grafo è bipartito.

Problema 4F. Per il Teorema 4.3 esiste un circuito hamiltoniano H. Supponiamo che H non contenga uno spigolo e con estremi x e y. Siano x' e y' i successori di x e di y, rispettivamente, lungo H. Considerare il cammino P che va da x' a y lungo H, poi percorre $\{y, x\}$ e va da x a y' lungo H nel verso opposto. Se lo spigolo $\{x', y'\}$ appartiene a G, abbiamo finito. Altrimenti ragionare come nella dimostrazione del Teorema 4.3 per mostrare che P si può completare a un circuito eliminando uno spigolo e aggiungendone altri due. Orig. 546

Per un'ulteriore generalizzazione, si veda L. Lovász (1979).

Problema 4G. Mostrare che il valore massimo di S si ottiene quando $z_i > 0$ soltanto sui punti di una cricca.

Problema 4H. Contare in due modi le coppie di spigoli con un vertice comune.

Problema 5A. (i) Dato $A \subseteq X$, dove X è una delle parti di una bipartizione, contare gli spigoli che hanno un estremo in A e l'altro in $\Gamma(A)$.

(ii) Un grafo trivalente senza accoppiamento perfetto è il grafo su quattro vertici e sei spigoli con un vertice incidente a tre spigoli non cappi e con cappi incidenti agli altri tre vertici. Sostituire i cappi con opportuni grafi semplici.

(iii) Lo stesso suggerimento della parte (i).

Problema 5B. Costruire una successione di insiemi A_i di grandezza m_i, usando elementi nuovi soltanto quando è necessario per mantenere soddisfatta la condizione H. Una soluzione è data a p. 41 di van Lint (1974).

Problema 5C. Usare l'induzione sul numero degli elementi non nulli della matrice. L'argomento del Teorema 5.5 si può usare in modo analogo.

Problema 5D. Teorema 5.5.

Problema 5E. Esprimere il numero dei sistemi di rappresentanti distinti nei quali 1, rispettivamente 2, rappresenta A_1 in funzione degli S_i con $i < n$. Si veda il Problema 14A.

Problema 5F. Contare gli insiemi $\{x_1, x_2, \ldots, x_n\}$ con $x_k \in A_k$ per ogni k e con $x_i = x_j$.

Problema 5G. (i) è facile, ma (ii) diventa più laborioso. Consultare l'Esempio 10.1.

Problema 6A. Definire un insieme parzialmente ordinato usando sia l'indice sia la grandezza degli interi a_i. Orig. 547

[2] Nell'originale mancano le barre di cardinalità attorno a D_{t-1} nel limite inferiore.

Problema 6B. (i) Considerare A e $\overline{A}$. (ii) Fare in modo che x appartenga a tutti gli insiemi.

Problema 6C. Mostrare che gli insiemi grandi si possono sostituire con i loro complementari, e applicare il Teorema 6.5.

Problema 6D. (i) Due qualsiasi dei sottoinsiemi non appartengono alla stessa catena. (ii) Usare l'induzione.

Problema 6E. Si veda C. Greene e D. Kleitman, Strong versions of Sperner's Theorem, *J. Combinatorial Theory (A)* **20** (1976), 80–88.

Problema 7A. Si tratta di un'applicazione diretta dell'algoritmo. La capacità minima di un taglio è 20.

Problema 7B. Dato un flusso f di valore non nullo, mostrare che gli spigoli e con $f(e) \neq 0$ contengono gli spigoli di un cammino orientato semplice da s a t. Sottrarre un multiplo scalare del corrispondente flusso elementare per ottenere un flusso f' che si annulla su più spigoli di f, e procedere per induzione.

Per l'esempio richiesto bastano quattro vertici.

Problema 7C. Considerare un flusso massimo f. Dall'equazione (7.1), gli spigoli da X_i a Y_i sono saturi e quelli da Y_i a X_i hanno valore del flusso nullo.

Problema 7D. Dato il grafo bipartito G con vertici $X \cup Y$, costruire una rete aggiungendo due vertici s e t, spigoli orientati da s agli elementi di X di capacità 1, e spigoli orientati dagli elementi di Y a t di capacità 1. Orientare tutti gli spigoli originali da X a Y; conviene assegnare loro una capacità grande, per esempio $|X| + 1$, così che nessuno di essi compaia in un taglio minimo. Spiegare perché esiste un accoppiamento completo da X a Y in G se e solo se il valore del flusso massimo nella rete è $|X|$.[3]

Problema 7E. Per (iv), applicare il Teorema 7.2, con $d = 2$, alla matrice d'incidenza del grafo. (Questo risultato è anche una conseguenza immediata del Teorema 1.2.) Per (v), considerare la *matrice d'incidenza bipartita* M di un grafo bipartito G, definita come segue. Supponiamo che G abbia bipartizione (X, Y). Le righe di M sono indicizzate dai vertici di X e le colonne da quelli di Y. L'elemento nella riga $x \in X$ e nella colonna $y \in Y$ è il numero degli spigoli che uniscono x e y (0 oppure 1 se G è semplice). Orig. 548

Problema 7F. Sia T un albero ricoprente in D. Mostrare che, per qualunque assegnazione di numeri reali ai $|E(D)| - |V(D)| + 1$ spigoli di D non appartenenti a T, vi è un unico modo di estenderla a una circolazione f su D. Può essere utile ricordare che un albero con almeno uno spigolo ha un vertice monovalente.

Problema 8A. Supporre che una sottosuccessione di n elementi consecutivi compaia due volte. Mostrare che α soddisfa un'equazione di grado minore di n.

Problema 8B. I vertici del digrafo sono le coppie ordinate di elementi di $\{0, 1, 2\}$; gli spigoli sono le 27 terne ordinate.

Problema 8C. La successione deve contenere quattro 0 e quattro 1. Tre 0 consecutivi impongono 00010111, che non funziona; la coppia 00 deve comparire due volte, e questo impone 00110011, che non funziona neppure.

Problema 8D. Poiché ogni vertice di G_n ha grado entrante 2 e grado uscente 2, otteniamo effettivamente un cammino chiuso da $00\cdots0$ a $00\cdots0$. L'ultimo spigolo deve provenire da $10\cdots0$ (che identifichiamo con l'intero 1 in notazione binaria). Il fatto che questo spigolo venga usato implica che è già stato usato lo spigolo da $1 = 10\cdots0$ a $0\cdots01$. Siamo quindi entrati due volte nel vertice 1, cioè da $2 = 010\cdots0$ e da $3 = 110\cdots0$. Per lo stesso motivo siamo entrati due volte sia in 2 sia in 3. Procedendo per induzione, vediamo che tutti i vertici sono stati visitati due volte nel cammino attraverso G_n, dimostrando l'affermazione.

Problema 9A. Applicare l'algoritmo.

Problema 9B. Si trova facilmente un indirizzamento banale di lunghezza n come nel Teorema 9.2. Qual è il diametro del grafo?

[3] L'originale stampa X al posto di $|X|$ nell'ultima frase.

Problema 9C. Usare i Teoremi 9.1 e 9.6. A un certo punto del calcolo comparirà $\sum k\cos(kx)$. Questa è la derivata di $\sum \sin(kx)$, e tale somma si determina moltiplicando per $\sin(\frac{1}{2}x)$.

Problema 9D. Si veda il Teorema 9.7.4.[4]

Problema 10A. Usare il Teorema 10.1, dove E_i, $i = 1, 2, 3, 4$, sono gli interi ≤ 1000 divisibili rispettivamente per $2, 3, 5, 7$.

Orig. 549

Problema 10B. Usare l'inclusione-esclusione e il fatto che, se $f(i) = 0$, allora $(x - i)$ divide $f(x)$.

Problema 10C. Usare $\lfloor x \rfloor = \sum_{k \leq x} 1$ e il Teorema 10.3.

Problema 10D. Moltiplicare $\sum a_n n^{-s}$ e $\sum b_m m^{-s}$. Determinare il coefficiente di k^{-s} e usare il Teorema 10.3.

Problema 10E. Determinare $\sum_{d|n} \log f_d(z)$; usare il Teorema 10.3 o 10.4.

Problema 10F. Vi sono evidentemente $2n+1$ colorazioni. Usare l'inclusione-esclusione, dove l'insieme E_i consiste nelle colorazioni in cui i è rosso e $i-1$ è blu. Per determinare N_j, usare l'Esempio 10.6.

Per una soluzione diretta, calcolare

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} (-1)^k \binom{2n-k}{k} 2^{2n-2k} x^{2n}.$$

A questo scopo, usare (10.6) e il fatto che $\sum (2n+1)x^{2n} = \left(\frac{x}{1-x^2}\right)'$.

Problema 10G. Usare il Teorema 10.1.

Problema 10H. Contare le permutazioni di $1, 2, \ldots, n$ che non fissano alcuno degli elementi $1, 2, \ldots, n-k$.

Problema 11A. Considerare una matrice $n \times k$ di soli 1. Aggiungere una colonna di 0 e poi completare a una matrice quadrata aggiungendo righe del tipo $(0, \ldots, 0, 1)$.

Problema 11B. (i) Teorema 5.3; (ii) Teorema 11.5; (iii) usare un prodotto diretto di matrici J_k.

Problema 11C. Determinare $A = (a_{ij})$ con $a_{ij} = |A_i \cap B_j|$. Per trovare il permanente di questa matrice, confrontare con il *problème des ménages*.

Problema 11D. Usare il Teorema 11.7.

Problema 11E. Calcolare il permanente corrispondente B_n sviluppando rispetto alla prima riga e alla prima colonna. Mostrare che $B_n = B_{n-1} + B_{n-2} - 2$. Quindi $\{B_n - 2 : n \geq 3\}$ è una successione di Fibonacci. Si veda anche il Problema 5E.

Orig. 550

Problema 12A. Usare il Teorema 12.1.

Problema 12B. Supporre che AA^{T} sia decomponibile. Spiegare il blocco di elementi nulli considerando una riga di A, i suoi elementi non nulli e i prodotti scalari con le altre righe.

Problema 12C. Effettuare quattro operazioni di media su coppie di righe e altrettante sulle colonne. Si osservi che l'elemento a_{55} non cambia durante queste operazioni. Determinare il permanente e minimizzarlo. Ciò mostra che la matrice era fin dall'inizio $\frac{1}{5}J$.

Problema 13A. Usare il Teorema 13.1.

Problema 13B. (i) Moltiplicare due potenze di $(1 - x)$. (ii) Mettere k nella posizione $a + 1$; che cosa può precedere questo termine?

Problema 13C. (i) Scegliere A_1 e poi scegliere A_2 come sottoinsieme del suo complementare; determinare la somma dei prodotti di coefficienti binomiali. (ii) Considerare una matrice $2 \times n$ le cui righe

[4] Rinvio riportato come nell'originale.

siano le funzioni caratteristiche rispettivamente di A_1 e A_2. Tradurre la condizione su A_1 e A_2 in una condizione sulla matrice.

Problema 13D. Fissare dapprima l'unione U degli insiemi di $\mathcal{A}$. Applicare l'Esempio 13.6 e poi sommare su tutte le scelte di U. La risposta mostra che avremmo potuto trovare una soluzione migliore. Per trovarla, rappresentare ancora $\mathcal{A}$ mediante una matrice $k \times n$ di 0 e 1. Aggiungere a questa matrice una riga «speciale», cioè la funzione caratteristica dell'unione degli insiemi di $\mathcal{A}$. Calcolare il numero di queste matrici di 0 e 1 che hanno un 1 in una posizione assegnata della riga «speciale».

Problema 13E. In ogni cammino considerare l'ultimo passo del tipo $(x, y) \to (x + 1, y + 1)$. Usare il Teorema 13.1. Per l'ultima domanda, inserire k palline in $n + k$ posizioni possibili; sia x_k la lunghezza dell'intervallo che precede la k-esima pallina.

Problema 13F. (i) Dimostrare per induzione. Se una permutazione di $1, \ldots, n-1$ è scritta come prodotto di cicli, vi sono n modi di aggiungere l'elemento n, uno dei quali dà un ciclo in più. (ii) Nel Teorema 13.7 sommare entrambi i membri rispetto a k; usare (13.5). Orig. 551

Problema 13G. Inserire (13.13) in (13.11) e scambiare l'ordine delle somme.

Problema 13H. Usare (10.6).

Problema 13I. Usare la relazione $F(a) = G(a)$ di p. 123.

Problema 13J. Usare la formula binomiale con $x = \zeta$, dove $\zeta^3 = 1$.

Problema 13K. Contare direttamente le partizioni di un insieme di n elementi in $n - 2$ parti.

Problema 14A. (i) Le successioni terminano con 10 oppure con 1. Stabilire la ricorrenza di Fibonacci e risolverla provando $a_n = t^n$ come soluzione (usare la linearità). Si può anche usare il metodo dell'Esempio 14.3.

(ii) Esprimere b_n in funzione dei numeri c_n di tali successioni che terminano con un 1. Trovare una ricorrenza per c_n. La costante c sarà la radice maggiore di un'equazione polinomiale di grado 4; vale circa 1,22075.

Problema 14B. Considerare un albero piano piantato trivalente T. Costruire un nuovo albero T' nel modo seguente. Prendere come vertici la radice di T e tutti i suoi vertici di grado 3. Unire due vertici in T' se esiste in T un cammino dall'uno all'altro che usa esattamente uno spigolo inclinato verso sinistra (si veda la Fig. 14.3). Infine aggiungere una nuova radice in basso. Mostrare come invertire questa applicazione. Mostrare che il numero dei vertici di T' è uguale al numero dei vertici di grado 1 di T. Si veda p. 25 di J. H. van Lint, *Combinatorial Theory Seminar, Eindhoven University of Technology*, Lecture Notes in Mathematics **382**, Springer-Verlag, 1974.

Problema 14C. Fissare un lato; denominare gli altri ciclicamente $a, b, c, \ldots$. Dare alle corde i nomi ovvi; prestare attenzione all'ordine in cui si assegnano questi nomi. Si veda anche p. 25 di van Lint (1974), ibidem.

Problema 14D. Usare il metodo della Fig. 2.2. Un punto fisso produce un'arborescenza; ciò che resta è un'applicazione senza punti fissi. Si veda (14.15). Porre $M_1(0) = 1$, $A(0) = 0$. Orig. 552

Problema 14E. Fissare un lato e poi considerare il quadrilatero al quale appartiene. Gli altri tre lati dividono l'$(n+1)$-gono in poligoni eventualmente vuoti; si veda (14.10). Risolvere $f = x + f^3$ applicando il Teorema 14.3.

Si può dare nel modo seguente una dimostrazione combinatoria del fatto che il numero dei modi di dividere un $(n+1)$-gono in quadrilateri mediante diagonali non intersecantisi è 0 se n è pari e $\frac{1}{3k+1}\binom{3k+1}{k}$ se $n = 2k + 1$. Poiché il caso di n pari è banale, supponiamo $n = 2k + 1$. La suddivisione contiene $k - 1$ diagonali e k quadrilateri. Porre un vertice in ogni quadrilatero e su ogni lato; fissare come radice uno dei vertici sui lati. I vertici dei quadrilateri si uniscono con uno spigolo se i quadrilateri hanno una diagonale comune; un vertice su un lato si unisce al vertice del suo quadrilatero. Descrivere una passeggiata attorno all'albero appena definito mediante una successione di simboli x e y, usando una x ogni volta che si raggiunge un vertice di quadrilatero non visitato prima, e analogamente una y per i vertici sui lati. Otteniamo una successione di k simboli x e $2k + 1$ simboli y. Sappiamo, dall'Esempio 10.6, che vi sono $\frac{1}{3k+1}\binom{3k+1}{k}$ successioni circolari di questo tipo. Resta da mostrare una corrispondenza biunivoca

tra queste successioni circolari e le successioni che descrivono gli alberi. Rappresentare la successione di x e y nel modo seguente: una x corrisponde a un passo nel piano X-Y di un'unità verso destra e un'unità verso l'alto; una y a un passo di un'unità verso destra e $k/(2k+1)$ unità verso il basso. La passeggiata parte da $(0,0)$ e termina in $(3k+1,0)$, senza incontrare nel frattempo l'asse X. Se rappresentiamo allo stesso modo una successione circolare del tipo dato, essa avrà un unico minimo, perché $(k, 2k+1) = 1$. Questo ci dà l'unico punto iniziale che la fa corrispondere a uno degli alberi.

Problema 14F. Per le operazioni formali si veda l'Appendice 2. Prendere i logaritmi e usare il Teorema 10.3.

Problema 14G. Mostrare l'equivalenza con l'Esempio 14.11.

Problema 14H. Costruire un cammino come nell'Esempio 14.8 e trovare un punto di altezza minima.

Problema 14I. (i) Si veda (14.10). (ii) Porre un vertice sulla circonferenza, per esempio tra 1 e $2n$. Sarà la radice di un albero. Porre un vertice in ogni regione e unire i vertici nel modo ovvio. Mostrare l'equivalenza con uno dei problemi di Catalan. Si veda van Lint (1974), p. 26.

Orig. 553

Problema 14J. Un grafo regolare etichettato di valenza 2 è un'unione di poligoni etichettati. Applicare il Teorema 14.2.

Problema 14K. Chiamare A_{4n} il numero delle passeggiate e definire $A(z) := 1 + \sum_{n=1}^{\infty} A_{4n} z^{4n}$. Se B_{2n} è il numero delle passeggiate da $(0,0)$ a (n,n) che evitano i punti (i,i), sappiamo da (14.12) che $B(z) := \sum_{n=1}^{\infty} B_{2n} z^{2n} = 1 - \sqrt{1-4z^2}$. Trovare una relazione tra $A(z)$ e $B(z)$ considerando, per ogni passeggiata, il primo attraversamento di $x = y$.

È anche possibile dimostrare il risultato trovando una corrispondenza biunivoca tra le passeggiate contate da A_{4n} e quelle contate nell'Esempio 14.8. Questo è difficile. Per una soluzione si veda la soluzione del Problema 3096 di W. Nichols in *American Mathematical Monthly* **94** (1987).

Problema 14L. Mostrare che $a_n = 3a_{n-1} - a_{n-2}$ e che F_{2n} soddisfa la stessa ricorrenza.

Problema 14M. Per le g con k punti fissi, contare il loro numero e il numero delle f adatte, e sommare su k; per le f con immagine di grandezza i, suddividere $\{1, 2, \ldots, r\}$ nelle controimmagini, contare le f e il numero delle g adatte, e sommare su i. Usare (13.9) e (13.11). Questa è la soluzione del Problema 3057 dell'*American Mathematical Monthly* **94** (1988), data da J. M. Freeman, S. C. Locke e H. Niederhausen.

Problema 14N. Introdurre $b_{k,n}$:= numero delle passeggiate da $(0,0)$ a (n,n) che incontrano per la seconda volta la retta $x = y$ in (k,k).

Problema 15A. Distinguere i casi $x_k = 1$ e $x_k > 1$; nel secondo porre $y_i = x_i - 1$. Usare l'induzione.

Problema 15B. Siano E, I e S i numeri rispettivamente dei triangoli equilateri, isosceli e scaleni. Calcolare E e $I + E$, ed esprimere $\binom{n}{3}$ mediante E, I, S.

(Questa dimostrazione è dovuta a J. S. Frame, *Amer. Math. Monthly* **47** (1940), 664.)

Problema 15C. Usare la decomposizione in fratti semplici. Trovare c usando il coefficiente di $(1-x)^{-t}$ e (10.6).

Problema 15D. Contare le composizioni di n in k parti che hanno un 3 nella posizione j. Farlo per tutti i j e sommare; una composizione con m parti uguali a 3 viene così contata m volte. Una seconda soluzione, che dà un risultato più generale, è la seguente. Mostrare anzitutto che un elenco di tutte le composizioni possibili contiene esattamente $(n+1)2^{n-2}$ interi. Lo si può fare usando l'argomento delle palline rosse. Dimostrare poi per induzione su n che, per $1 \le m < n$, un elenco delle 2^{n-1} composizioni di n contiene l'intero m esattamente $(n-m+3)2^{n-m-2}$ volte. A questo scopo usare la formula $1 + \sum_{k=1}^{n-1}(k+3)2^{k-2} = (n+1)2^{n-2}$, anch'essa dimostrabile per induzione.

Orig. 554

Problema 15E. Omettere la prima colonna.

Problema 15F. Per le parti dispari distinte, usare figure a forma di «gancio» per formare un diagramma di Ferrers e leggerlo nel modo abituale.

Problema 15G. Mostrare una corrispondenza con l'Esempio 14.8.

Problema 15H. Si veda il Capitolo 13.

Problema 15I. Generalizzare il Teorema 15.4.

Problema 15J. Applicare il Teorema 15.10 a un quadrato $n \times n$.

Problema 16A. Usare l'induzione; confrontare due segmenti iniziali di $\mathbf{r}$ e $\mathbf{s}$.

Problema 16B. Determinare la prima colonna di una matrice con somme di riga $\mathbf{r}$ e somme di colonna $\mathbf{r}^*$. Usare l'induzione.

Problema 16C. Usare il Problema 16A e scambiare spigoli. Un'altra possibilità è descrivere il grafo mediante la sua matrice di adiacenza e usare la stessa idea della dimostrazione del Teorema 16.2.

Problema 16D. Stimare il numero delle soluzioni di $s_1 + \cdots + s_n = \frac{1}{2}n^2$ usando soltanto il fatto che ogni s_i è al più n.

Problema 16E. Per la sufficienza, osservare anzitutto che esiste un torneo con successione dei gradi $(n-1, \ldots, 2, 1, 0)$. Usare poi il Problema 16A. Mostrare che, se in un torneo il grado uscente di x è maggiore di quello di y, esiste un torneo sullo stesso insieme di vertici e con gli stessi gradi uscenti, tranne che il grado uscente di x è diminuito di 1 e quello di y è aumentato di 1. Lo si può ottenere cambiando il verso di al più due spigoli.

Problema 16F. Per la generalizzazione, considerare l'ipergrafo ottenuto scegliendo i primi m sottoinsiemi di k elementi nell'ordine lessicografico. Per le parti di sufficienza, usare ancora il Problema 16A.

Orig. 555

Problema 16G. Si ha $A(5,3) = A(5,2)$. Si veda (16.2). Un conteggio diretto è possibile nel modo seguente: (i) fissare la prima riga come $(1,1,0,0,0)$; ciò significa che il risultato finale va moltiplicato per 10. (ii) Mettere un 1 nella posizione $(2,1)$; ciò significa che occorre moltiplicare anche per 4. (iii) Distinguere due casi: un 1 nella posizione $(2,2)$, ecc., oppure un 1 nella posizione $(2,3)$, nel qual caso si introduce un fattore 3, ecc.

Un'altra soluzione si ottiene osservando che $\mathcal{A}^*(5,2)$ ha cardinalità $\frac{1}{2}5!4! = 1440$ e che in $\mathcal{A}(5,2)$ vi sono $\binom{5}{2}^2 \cdot 3! = 600$ matrici decomponibili.

Problema 16H. Nel caso 1 vi sono $n-1$ scelte possibili. Nel caso 2 eliminare la riga 1 e la colonna 1, sostituire un elemento di $\mathcal{A}(n-1,2)$ e ottenere poi in due modi un elemento di $\mathcal{A}(n,2)$.

Problema 16I. Sostituzione diretta.

Problema 17A. Indicizzare le prime due righe con x, y e le prime due colonne con u, v, sempre nell'ipotesi che si tratti della tavola di moltiplicazione di un gruppo di ordine 5. Mostrare che $(v^{-1}u)^2 = 1$.

Problema 17B. Questo è già difficile, nonostante le piccole dimensioni del quadrato! Prendere $a = 1$. Si osservi che l'1 nell'angolo superiore sinistro appartiene a sottoquadrati del tipo $\left[\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right]$ per $i = 2,3,4,5$. Considerare un qualunque quadrato latino con questa proprietà. Se l'elemento $(2,3)$ non è 4, scambiando le righe 4 e 5, le colonne 4 e 5 e i simboli 4 e 5 si trasforma il quadrato in uno equivalente con un 4 nella posizione $(2,3)$. A questo punto vi è un solo modo di completare il quadrato. Quindi, se un quadrato latino ha una qualunque casella con una proprietà analoga a quella menzionata per l'1 in alto a sinistra, esso è equivalente a questo.

Usando lo stesso tipo di argomento si può mostrare che vi sono soltanto pochi quadrati di ordine 5 potenzialmente non equivalenti. Per alcuni occorre poi stabilire l'equivalenza, compito tedioso.

Problema 17C. A questo punto si prescrive di procedere per tentativi. Si veda però il Capitolo 22.

Problema 17D. La sufficienza si mostra con un esempio (si può usare il Teorema 17.1, ma non è necessario). Per la necessità, osservare che anche soltanto aggiungere una colonna a un quadrato latino di ordine m richiede m simboli nuovi.

Orig. 556

Problema 17E. Applicare l'algoritmo.

Problema 17F. Per la parte (i), descrivere un algoritmo che recuperi il quadrato latino originale di ordine n dal quadrato latino costruito di ordine $n+1$ con diagonale secondaria costante. Per (ii), spiegare perché il numero dei quadrati latini di ordine n con n sulla diagonale secondaria è uguale a $N(n)/n!$.

Problema 17G. (a) Per $n = 6$ un esempio è $6, 1, 5, 2, 4, 3$.

(b) Sommare le differenze.

(c) Supporre che due coppie siano uguali e risolvere.

Problema 17H. Cominciare sostituendo con $n + 1$ gli elementi diagonali del quadrato più piccolo.

Problema 17I. Si veda l'Esempio 10.6.

Problema 17J. (i) Usare l'inclusione-esclusione. Se k interi sono al posto sbagliato, scrivere $k = 2i + j$, dove vi sono i coppie al posto sbagliato, ecc.

(ii) Usare $J - I$ di ordine n.

Problema 18A. Per mostrarlo direttamente, ragionare come nel Teorema 18.1 sulle prime tre righe. Mostrare che nessun'altra riga può cominciare con tre $+1$. Quindi le righe 5, 6 e 7 cominciano tutte con $++-$ (perché?). Esse si possono poi completare in un unico modo, ecc. Per un'altra soluzione, si veda il Problema 19D.

Problema 18B. Usare il metodo del Teorema 18.1. Si osservi che una permutazione delle righe e delle colonne che conserva la diagonale nulla non aiuta a rendere una matrice simmetrica o antisimmetrica. Servono dunque soltanto moltiplicazioni per -1. Normalizzare la prima riga e rendere la prima colonna (tranne l'elemento di indice 0) tutta di 1 o tutta di -1. Basta ora mostrare che gli elementi $(2, 3)$ e $(3, 2)$ sono uguali, rispettivamente opposti, quando $n \equiv 2 \pmod 4$, rispettivamente $n \equiv 0 \pmod 4$.

Problema 18C. Un esercizio banale!

Problema 18D. Abbiamo $28 = 1+9+9+9$ e $28 = 1+1+1+25$. Usare la prima uguaglianza. Si osservi che ogni W_i ha 1 sulla diagonale e che, se $w_{ij} = 2$, anche $w_{7-i,j}$ è 2; analogamente per -2. L'osservazione sulle occorrenze delle U^i nelle matrici W_j impone allora completamente la scelta delle quattro matrici W_i. Esse risultano funzionare. Orig. 557

Problema 18E. Mostrare per induzione che $M_n^{(i)} \cdots M_n^{(m)} = H_{2^{m-i+1}} \otimes I_{2^{i-1}}$. Per la seconda parte, contare gli elementi non nulli di $M_n^{(i)}$. Si veda il riferimento E. C. Posner (1968).

Problema 18F. Per entrambe le domande usare l'induzione.

Problema 18G. Per (2), mostrare che il numero delle righe con prima coordinata 0 (oppure 1) è al più n.

Problema 18H. Diretto; si veda il Teorema 18.4.

Problema 18I. Riesaminare le proprietà di Q.

Problema 19A. Per l'isomorfismo nella parte (i), etichettare i vertici di K_6 con 0000, 1000, 0100, 0010, 0001, 1111 in $\mathbb{F}_2^4$, ed etichettare ogni spigolo con la somma in $\mathbb{F}_2^4$ delle etichette dei suoi estremi. Questo dà una corrispondenza biunivoca tra gli spigoli di K_6 e i 15 vettori non nulli di $\mathbb{F}_2^4$.

Per la parte (ii), considerare le configurazioni formate da tre spigoli (ve ne sono quattro tipi). La costruzione è dovuta a E. S. Kramer (1990), *Discrete Math.* **81**, 223–224.

Problema 19B. Calcolare b_i, per $i = 3, 2, 1, 0$; si ha $b_1 \notin \mathbb{Z}$.

Problema 19C. È il Teorema 19.4.

Problema 19D. (i) Siano c_i le somme di colonna di N. Allora $\sum c_i = 66$. La somma di tutti i prodotti scalari tra righe è $\sum \binom{c_i}{2}$. Usare la disuguaglianza di Cauchy–Schwarz. Concludere che tutte le somme di colonna sono 6 e tutti i prodotti scalari sono 3. (ii) Per mostrare l'unicità, considerare il complementare: un disegno 2-$(11, 5, 2)$. Senza perdita di generalità, la prima riga è (11111000000); le altre dieci righe iniziano con le $\binom{5}{2}$ coppie $(110\cdots)$, $(1010\cdots)$, ecc. Mostrare poi che le righe da 2 a 5 si possono completare in un unico modo. Resta da completare un quadrato 6×6. A prima vista sembrano esserci due modi per farlo. Trovare una permutazione che trasformi l'uno nell'altro. Orig. 558

Problema 19E. Indicare con a_i il numero dei blocchi che incontrano B in i punti. Calcolare $\sum a_i$, $\sum i a_i$ e $\sum \binom{i}{2} a_i$. Ricavare una disuguaglianza per a_0 usando la forma $\sum (i - c)^2 a_i$. Confrontare con il Teorema 19.9.

Problema 19F. L'applicazione $x \mapsto 2x$ ha sei orbite, due delle quali sono troppo lunghe per poter essere usate (per esempio $(1, 2, 4, 8, 16, 11)$). Si veda l'Esempio 28.2.

Problema 19G. Usare lo schieramento ortogonale corrispondente. Usare la consueta applicazione da $\{0, 1\}$ a $\{1, -1\}$.

Problema 19H. Per (1) usare (19.2) o (19.4). Per (3) contare le coppie $p, q \notin B$ contenute in blocchi che incontrano p. Trovare così i parametri di D^B. Per (4), supporre dapprima che D^B sia costituito da un unico blocco. Considerare l'Esempio 19.3. Nell'altro caso la disuguaglianza di Fisher dà $k \geq (\lambda+1)(\lambda+2)$. Esprimere ora b_0 come frazione in k e λ e dedurre che k deve dividere $2(\lambda + 1)(\lambda + 2)$.

Problema 19I. (i) Fissare un punto x di O. Contare le coppie (y, L), con $y \in O$ e L retta passante per x e y. (ii) Da (i) vediamo che, se $|O| = n+2$, ogni retta che incontra O lo incontra in due punti. Prendere un punto $z \notin O$ e contare le rette per z che incontrano O. (iii) Prendere quattro punti qualsiasi, senza che tre siano allineati. Essi determinano sei rette, che contengono complessivamente 19 punti del piano.

Problema 19J. Per $p_1, \ldots, p_5$ prendere $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 1)$ e $(1, t, t^2)$, e mostrare che vi sono due modi di raggrupparli per produrre $p_6 = (1, x, x^2)$, dove $x = t/(1 + t)$.

Problema 19K. Sia $B_1 \sim B_2$. Quanti blocchi incontrano B_1? Prendere $x \in B_1$, $y \in B_2$; quanti blocchi incontrano sia B_1 sia B_2? Vi sono $n + 1$ classi di equivalenza, ciascuna con n rette (blocchi). A ogni classe associare un punto da aggiungere come punto supplementare a ogni retta di quella classe, ecc.

Problema 19L. Usare il Teorema 19.11. Considerare l'equazione modulo 3.

Problema 19M. Per v pari, usare forme quadratiche come nella dimostrazione del Teorema 19.11. Si veda J. H. van Lint e J. J. Seidel (1966), Equilateral point sets in elliptic geometry, *Proc. Kon. Nederl. Akad. Wetensch.* **69**, 335–348.

Orig. 559

Problema 19N. (a) Il metodo dell'Esempio 19.14 funziona anche se $|V| = 1$; si ha $85 = 7(13 - 1) + 1$. (b) $15 = 7(3 - 1) + 1$.

Problema 19O. Considerare la matrice d'incidenza N di dimensioni $n \times b$, dove $b = |\mathcal{A}|$. Verificare che nel caso (i) $N^{\mathsf{T}}N$ è non singolare modulo 2. Per la parte (ii), sia N_1 ottenuta aggiungendo a N una colonna di soli 1; mostrare che $N_1^{\mathsf{T}}N_1$ ha rango almeno b modulo 2.

Problema 19P. L'ultima delle somme esposte deve risultare nulla. Ciò implica che ogni μ_i è 1 oppure 2.

Problema 19Q. Usare l'induzione, partendo da $t = 2$. Contare in due modi le terne ordinate (x, A, B), dove A e B sono blocchi distinti che contengono entrambi il punto x.

Problema 19R. Rappresentare le rette come nell'Esempio 19.6 e usare il fatto che la rappresentazione è ciclica. Distinguere i casi secondo il numero degli elementi «primi» usati nel sistema di rappresentanti distinti.

Problema 19S. Si può dare una costruzione per induzione su k, ma è più rapido dare una costruzione diretta usando $\mathbb{F}_2^k$ come insieme dei punti. Riesaminare l'Esempio 19.1.

Problema 19T. Usare il risultato del Problema 19H. Le estensioni compariranno nel Capitolo 20.

Problema 19U. Applicare il Teorema 5.5.

Problema 20A. Usare (20.5).

Problema 20B. Applicare il principio dei cassetti agli ultimi due bit delle parole. Un codice binario con tre parole è facile da trattare!

Problema 20C. Per ognuno dei tre modi in cui possono essere violate le condizioni per una parola del codice, modificare una coordinata opportuna per rimediare.

Problema 20D. (i) Le righe della matrice generatrice corrispondono a $\pm\mathbf{a}_i$, $i = 1, \ldots, n$, dove le $\mathbf{a}_i$ sono le righe di una matrice di Hadamard. Sia $\mathbf{u} \in \mathbb{F}_2^n$, dove $n = 2^{2k}$. Con $\mathbf{u}^*$ indichiamo la rappresentazione mediante ± 1. Calcolare $\sum \langle \mathbf{u}^*, \mathbf{a}_i \rangle^2$ per trovare il limite superiore.

(ii) Per l'uguaglianza, trovare dapprima il peso di $\mathbf{z}$. Usare poi il fatto che le parole del codice corrispondono a funzioni lineari e che aggiungere una funzione lineare a $\mathbf{x}$ dà una forma quadratica equivalente.

Orig. 560

Problema 20E. (i) Si veda il Problema 20A. (ii) Contare le parole di peso 5 «coperte» da parole del codice di peso 7; le altre parole di peso 5 sono coperte da parole del codice di peso 8. Usando questa idea, impostare un sistema di equazioni lineari per gli A_i.

Problema 20F. Una parola del codice a distanza $\leq e$ da una parola di peso $e+1$ deve avere peso $2e+1$.

Problema 20G. Le parole del duale del codice binario di Hamming di lunghezza 2^r-1 si possono identificare con i funzionali lineari su $\mathbb{F}_2^r$ (cfr. la descrizione geometrica dei codici di Reed–Muller nel Capitolo 18); ogni parola non nulla ha peso 2^{r-1}.

Problema 20H. Usare (19.6) e il fatto che G_{24} è lineare e ha peso minimo 8; si osservi che vi sono $\binom{21}{2}$ coppie di rette. Se $\alpha=1$, considerare nel piano la configurazione B^* di 7 punti. Ogni retta che incontra B^* deve incontrarlo in 1 oppure in 3 punti. Quante lo incontrano in 3 punti?

Problema 20I. (i) Trovare la matrice generatrice standard di C. (ii) Le condizioni (1) e (2) definiscono evidentemente un codice lineare. In (1) abbiamo due scelte per la parità; in (2) abbiamo 4^3 scelte per la parola del codice; in cinque delle colonne di A abbiamo poi due possibilità (ma non nell'ultima!). Per la scelta «pari» è chiaro che una parola non nulla di C impone peso ≥ 8; lo zero va trattato separatamente. Per la scelta «dispari» è chiaro che otteniamo peso almeno 6; la condizione (1) impedisce l'uguaglianza. Per approfondire questa splendida descrizione del codice di Golay e le sue numerose conseguenze, si veda J. H. Conway, The Golay codes and the Mathieu groups, Capitolo 11 in J. H. Conway e N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

Problema 20J. L'autodualità si dimostra come nell'Esempio 20.6. Tutti i pesi in Sym_{12} sono divisibili per 3. Considerare le combinazioni lineari di due righe della matrice generatrice e poi dedurre che cosa accade combinandole con una terza riga. Usare (20.5).

Problema 20K. Dimostrare la generalizzazione per induzione su r. Per ogni r, trovare una tale matrice nessuna delle cui colonne sia un vettore costante. Per il passo induttivo, concatenare tre copie della matrice con r righe, alle quali siano state aggiunte rispettivamente una riga di soli 0, una di soli 1 e una di soli 2, e aggiungere poi tre colonne opportune.

Orig. 561

Problema 20L. Il suggerimento nel capitolo dovrebbe bastare.

Problema 21A. L'argomento è lo stesso che per (21.4), ora con disuguaglianze.

Problema 21B. Usare la condizione di integralità. Si veda anche il riferimento A. J. Hoffman e R. R. Singleton (1960) del Capitolo 4.

Problema 21C. Usare (19.2); si veda il Problema 20F. Se due blocchi sono disgiunti, contare i blocchi che li incontrano entrambi, ciascuno in due punti. Quanti ne incontrano uno solo? Argomenti di conteggio analoghi (distinguere alcuni casi!) servono a mostrare che $\mu=6$.

Problema 21D. Supporre che un tale grafo esista. Scegliere un vertice x e considerare gli insiemi $\Gamma(x)$ e $\Delta(x)$. Li consideriamo come i punti e i blocchi di un disegno. Mostrare che questo è un disegno 2-$(9,4,3)$. Fissare poi un blocco del disegno e sia a_i il numero dei blocchi che lo incontrano in i punti. Mostrare che $a_0\leq 1$ (si veda il Problema 19E) e che il fatto che $\Delta(x)$ abbia grado 5 implica che a_0 dovrebbe essere almeno 5.

Problema 21E. Le prime due domande sono dirette. Per la terza rinviamo ai testi di teoria delle matrici (si veda «interlacciamento») oppure al Capitolo 31. Il teorema al quale alludiamo afferma che gli autovalori di una sottomatrice principale B di una matrice simmetrica A sono compresi tra il massimo e il minimo autovalore di A. Per dimostrarlo, basta considerare un vettore qualsiasi $\mathbf{x}$ e calcolare $\mathbf{x}^{\mathsf{T}}A\mathbf{x}/\mathbf{x}^{\mathsf{T}}\mathbf{x}$. Specializzare poi scegliendo $\mathbf{x}$ come un autovettore di B completato con zeri.

Problema 21F. Riesaminare la dimostrazione del Teorema 21.5. Mostrare che $\Gamma(x)=\overline{K_{n-1,n-1}}$. Definire una *grande cricca* come una cricca di grandezza n e mostrare che ogni spigolo appartiene esattamente

a una grande cricca. Mostrare che vi sono esattamente $2n$ grandi cricche, suddivise in due classi di n, in modo che le grandi cricche della stessa classe siano disgiunte. Si veda S. S. Shrikhande, The uniqueness of the L_2 association scheme, *Ann. Math. Stat.* **30** (1959), 781–798.

Problema 21G. Contare bandiere e altre configurazioni, per esempio due rette incidenti e un punto su una di esse.

Orig. 562

Problema 21H. Per v si veda il Problema 21E; k è ovvio. Prendere due punti sulla retta L. I punti collegati a entrambi appartengono a L oppure a una delle altre $R-1$ rette per uno dei due punti. Un argomento analogo dà μ. Per r e s si veda (21.6).

Problema 21I. Su $\Gamma(x)$ usare il fatto che $\mu = 1$. Considerare poi $\{x\} \cup \Gamma(x)$.

Problema 21J. L'equazione (21.8) conduce a un'equazione simile alla (21.6), con t al posto di k. Benché A non sia simmetrica, gli autovettori relativi ad autovalori diversi da k sono ortogonali a $\mathbf{j}$.

Problema 21K. Mostrare che, se $(\lambda-\mu)^2+4(t-\mu)$ non è un quadrato, gli autovalori hanno molteplicità $1, f, g$, dove $f = g = \frac{1}{2}(v-1)$. Mostrare poi che $A + A^{\mathsf{T}} = J - I$ e $AA^{\mathsf{T}} = lJ + (l+1)I$, dove $v = 4l+3$.[5] Definire $Q := A - A^{\mathsf{T}}$.

Problema 21L. Sia $d := \sqrt{(\lambda-\mu)^2 + 4(t-\mu)}$. Applicare (21.8) a $\mathbf{j}$ e mostrare poi che d divide $(k-1)^2$. Usando $4k - 7 = d^2$, dimostrare che d deve dividere 9.

Per $v = 18$, usare la matrice

$$\begin{pmatrix} cI & (c-1)I + J \\ (\overline{c}-1)I + J & \overline{c}I \end{pmatrix}$$

e sostituire c con la matrice C dell'Esempio 21.11 e $\overline{c}$ con C^2, per ottenere una matrice A di dimensioni 18×18.[6]

Problema 21M. (i) Considerare $\Gamma(x) \cap \Gamma(y)$, dove (xy) è uno spigolo. (ii) Dimostrare che anche $\overline{G}$ è regolare negli intorni.

Problema 21N. (i) $\Gamma(x_1) = C \cup B$ è regolare di grado a, quindi $|CB| = a|C| - |CC|$, ecc.

(ii) Eliminare $|BC|$ e $|BD|$ dalle relazioni di (i).

(iii) Scambiare x_1 e x_2. Usare $d_1 \neq d_2$.

(iv) Esprimere d_i mediante k_i, a, $\overline{a}$ e il numero n dei vertici di G. Dimostrare poi che $k_1 + k_2 = 2n - 3\overline{a} - a - 5$.

Problema 21O. La parte (i) è diretta. Per esempio, $\lambda = (n+3)/2$. (ii) Se quattro terne di una cricca C contengono un punto x, tutte le terne della cricca devono contenere x. (iii) Se $n > 15$, le cricche di grandezza $(n-1)/2$ nel grafo di un sistema di terne sono in corrispondenza biunivoca con i punti del sistema di terne.

Orig. 563

Problema 21P. L'uguaglianza implicherebbe l'esistenza di uno $\mathrm{srg}(a^2 + a + 1, a + 1, 1, 1)$. Usare il Teorema 21.1. È possibile soltanto $a = 1$, e un K_3 evidentemente non ha un circuito su quattro vertici.

Problema 21Q. Il grafo G che rappresenta la relazione di amicizia è un'unione di triangoli con un vertice comune a tutti, oppure è regolare. Usare il Teorema 21.1.

Problema 22A. Mostrare mediante calcolo che il complementare del grafo di una rete (n, n) ha i parametri del grafo di una rete $(n, 1)$. Mostrare poi che è il grafo di una rete $(n, 1)$, cioè che esiste una partizione dei punti in n insiemi di grandezza n, nessuno dei quali contiene due punti collineari.

(Più in generale, una rete (n, r) si può completare a una rete $(n, n+1)$ se e solo se il complementare del grafo della rete (n, r) è il grafo di una rete $(n, n+1-r)$.)

Problema 22B. Usare le costruzioni mediante campi descritte prima del problema. Per esempio, per q dispari prendere $S(x, y) := (x + y)/2$.

Per q pari possiamo usare A e S per organizzare incontri di doppio misto di tennis. Supponiamo di avere q coppie di coniugi: la signora i e il signor i, per $i \in \mathbb{F}_q$. Far giocare la signora i e la signora j

[5] L'originale stampa $A = A^{\mathsf{T}} = J - I$; il primo segno va corretto in $+$.

[6] L'originale dice di sostituire d con C^2, benché nella matrice compaia $\overline{c}$, non d.

l'una contro l'altra, con compagni rispettivamente il signor $A(i,j)$ e il signor $A(j,i)$, nel turno $S(i,j)$. Vi saranno $q-1$ turni, etichettati dai simboli fuori diagonale di S, durante i quali ciascuno gioca esattamente un incontro. Si vedrà che nessuno incontra il proprio coniuge come compagno o avversario nell'intero torneo, ma incontra ogni altra persona esattamente una volta come avversario e ha ogni persona dell'altro sesso esattamente una volta come compagno. Per q dispari possiamo avere q turni, con una coppia a riposo in ciascun turno.

Problema 22C. Mostrare che ciascuno dei numeri $m, m+1, t, u$ ha la proprietà di essere, per ogni primo $p < x$, coprimo con p oppure divisibile per p^x.

Problema 22D. Riesaminare il legame tra insiemi di quadrati latini a due a due ortogonali e disegni trasversali.

Orig. 564

Problema 22E. Usare il Teorema 22.6.

Problema 22F. Le colonne di A sono formate da interi tra 1 e k. Per ogni colonna di A e di S, sostituire un intero i nella colonna di A con l'i-esimo elemento della colonna di S. Aggiungendo colonne opportune e una riga, completare a un $\mathrm{OA}(v, c+1)$.

Problema 22G. La dimostrazione è simile a quella del Teorema 22.6. Ora serve anche un $(\mathcal{V}, \mathcal{K}, \mathcal{D})$, un $\mathrm{TD}(v,k)$.

Problema 22H. Usare il Problema 22F.

Problema 22I. Usare il Problema 22G.

Problema 22J. Usare il Problema 22G.

Problema 23A. Si osservi che la chiusura di un insieme S di spigoli consiste in tutti gli spigoli i cui estremi appartengono alla stessa componente connessa del sottografo ricoprente di G con insieme degli spigoli S.

Problema 23B. Le rette di $\mathrm{AG}_r(2)$ hanno grandezza 2.

Problema 23C. Trattare prima i casi in cui l'unione di due rette è l'intero insieme dei punti. Mostrare poi come stabilire una corrispondenza biunivoca tra i punti di due rette qualsiasi.

Problema 23D. La parte più difficile è mostrare che $\mathcal{F} = \{F_1 \cup F_2 : F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2\}$. Dimostrare che $\overline{F_1 \cup F_2} = F_1 \cup F_2$ usando il fatto che il rango di $\overline{F_1 \cup F_2}$ è la somma dei ranghi di F_1 e F_2.

Per una discussione completa della connessione delle geometrie combinatorie e dell'irriducibilità dei reticoli geometrici, si veda H. Crapo e G.-C. Rota (1970).

Problema 23E. Supporre che $A \cap F = \varnothing$ e $\mathrm{rank}(A) + \mathrm{rank}(F) = \mathrm{rank}(\overline{A \cup F})$. Mostrare che queste uguaglianze restano valide sostituendo A con $A' := \overline{A \cup \{x\}}$, dove x è un qualunque punto non appartenente a $\overline{A \cup F}$.

Problema 23F. Usare (23.4).

Problema 23G. Possiamo lavorare in $\mathrm{PG}_2(\mathbb{F})$ e supporre senza perdita di generalità che $L_1 = [1,0,0]$ e $L_2 = [0,1,0]$. Allora (spiegare perché) $a_1 = \langle 0, \alpha_1, 1\rangle$, $b_1 = \langle 0, \beta_1, 1\rangle$, $c_1 = \langle 0, \gamma_1, 1\rangle$, mentre $a_2 = \langle \alpha_2, 0, 1\rangle$, $b_2 = \langle \beta_2, 0, 1\rangle$, $c_2 = \langle \gamma_2, 0, 1\rangle$.

Orig. 565

Problema 23H. Si veda il Capitolo 13.

Problema 23I. Usare semplicemente la definizione di λ.

Problema 24A. Si veda il Capitolo 13.

Problema 24B. Una risposta è $e_i = i(m-k+i)$. Considerare le matrici $k \times (n+m)$ di rango k in forma a scala. Quante hanno i elementi direttori uguali a 1 nelle prime n colonne?

Problema 24C. Verificare che $\mathbf{x}$ e $\mathbf{y}$ appartengono a una classe laterale di un sottospazio U se e solo se $\mathbf{x} - \mathbf{y}$ appartiene a U.

Problema 24D. Contare tutte le matrici $n \times n$.

Problema 24E. Si veda il Teorema 6.4.

Problema 25A. Per un sottospazio U dello spazio r-dimensionale W, sia $f(U)$ il numero dei sottospazi di dimensione k che intersecano W in U. Usare (25.5).

Problema 25B. Per un sottospazio U, sia $f(U)$ il numero delle applicazioni non singolari il cui insieme dei vettori fissi è esattamente U, e sia $h(U)$ il numero delle applicazioni lineari non singolari che fissano almeno i vettori di U. È facile dare una formula per $h(U)$ in funzione di n, q e della dimensione di U. Ci occorre una formula per $f(\{0\})$.

Problema 25C. Usare (25.2) per calcolare $\mu(0, x)$ per x di rango 1 o 2.

Problema 25D. Vi sono soltanto $n-1$ partizioni $x \neq 0_L$, ciascuna formata da un blocco di grandezza 2 e da $n-2$ singoletti, che soddisfano $x \wedge a = 0_L$.

Problema 25E. Per $x < z < y$, una catena di lunghezza k da x a z si estende a una catena di lunghezza $k+1$ da x a y.

Problema 25F. Si veda il Teorema 25.1(iii). Contare le applicazioni iniettive da V a S e poi far variare $|S|$.

Problema 26A. Il numero delle rette per un punto $x \notin A$ che incontrano A è costante, cioè indipendente da x.

Problema 26B. Ogni retta disgiunta dall'arco si può usare per ottenere una partizione dei blocchi in classi parallele, una per ciascun punto della retta.

Orig. 566

Problema 26C. Per esempio, il punto d'intersezione della retta per $\langle 1,0,0\rangle$ e $\langle 0,1,0\rangle$ con la retta per $\langle 0,0,1\rangle$ e $\langle 1,1,1\rangle$ è $\langle 1,1,0\rangle$.

Problema 26D. Sia μ_i la cardinalità dell'intersezione dell'i-esima retta con S. La disuguaglianza è facile se qualche $\mu_i \geq \sqrt{n}+1$; supporre dunque il contrario e considerare $\sum_i(\mu_i - 1)(\mu_i - \sqrt{n} - 1)$.

Problema 26E. Che la caratteristica sia pari o dispari, f è degenere se e solo se $\mathbf{x}(C + C^{\mathsf{T}}) = 0$ per qualche $\mathbf{x}$ con $f(\mathbf{x}) = 0$. Per trovare un tale $\mathbf{x}$ quando f è degenere, prendere l'ultima riga di una matrice non singolare A tale che ACA^{T} abbia l'ultima riga e l'ultima colonna nulle; tale matrice esiste perché, per esempio, x_n non compare in una forma proiettivamente equivalente. Si veda anche J. W. P. Hirschfeld (1979).

Problema 26F. Per il Teorema 26.6, con $q = 2$ e $n = 2m-1$, le forme quadratiche non degeneri in $2m$ variabili hanno $2^{2m-1} - 2^{m-1}$ oppure $2^{2m-1} + 2^{m-1}$ zeri, contando qui anche il vettore nullo. Quindi le parole del codice corrispondenti a tali forme (vettori di lunghezza 2^{2m})[7] hanno peso $2^{2m-1} + 2^{m-1}$ oppure $2^{2m-1} - 2^{m-1}$. Poiché, come funzioni su $\mathbb{F}_2$, si ha $x_i^2 = x_i$, possiamo considerare i polinomi $f(\mathbf{x}) + a(\mathbf{x})$ come forme quadratiche, oppure come i loro complementari se vi è un termine costante 1. Mostrare che tutte queste forme sono non degeneri.

In alternativa, mostrare che esiste una «sostituzione affine invertibile» (nella quale, per esempio, x_i può essere sostituito con $x_i + 1$) che porta $f(\mathbf{x}) + a(\mathbf{x})$, come funzione su $\mathbb{F}_2^{2m}$, in $f(\mathbf{x})$ oppure in $f(\mathbf{x}) + 1$.

Problema 26G. È relativamente diretto mostrare che Q' è una quadrica non degenere in W. Se n è dispari, non occorre altro. Per n pari si può usare il Teorema 26.5 per completare la dimostrazione. È facile vedere che, se Q' è iperbolica, anche Q lo è. Usare poi l'equazione (26.4) per mostrare che ogni punto p su una quadrica iperbolica Q in $\mathrm{PG}_{n-1}(q)$ è contenuto in un sottospazio $F \subseteq Q$ di dimensione proiettiva $n/2-1$. Verificare che un tale sottospazio è contenuto in T_p, così che il sottospazio $F \cap W \subseteq Q'$ ha dimensione inferiore di uno a quella di F.

Problema 26H. Se il punto x non appartiene alla retta ℓ, considerare il piano determinato da x e ℓ.

Problema 26I. I punti di un triangolo appartengono a una retta. Per (iii) si veda il Capitolo 21.

Orig. 567

Problema 26J. Si veda l'argomento per gli archi nei piani proiettivi.

[7] L'originale indica erroneamente lunghezza $2m$; le coordinate sono indicizzate dai 2^{2m} elementi di $\mathbb{F}_2^{2m}$.

Problema 26K. Considerare tre punti. Sia x_i il numero dei blocchi del disegno complementare che contengono i di questi punti. Usare il consueto argomento di conteggio per mostrare che $x_0 + x_3 = \lambda$.[8]

Problema 27A. Non è difficile vedere che le affermazioni di numero pari sono equivalenti tra loro, e analogamente quelle di numero dispari. Per mostrare, per esempio, che (3) e (4) sono equivalenti, introdurre una matrice d'incidenza N e mostrare che una equivale all'equazione matriciale $NN^{\mathsf{T}} = (k-\lambda)I + \lambda J$ e l'altra a $N^{\mathsf{T}}N = (k-\lambda)I + \lambda J$.

Problema 27B. Considerare $(\mathbb{Z}_2)^4$ come spazio vettoriale sul campo $\mathbb{F}_2$. Possiamo supporre che l'insieme di differenze contenga il vettore nullo. Esso genera $(\mathbb{Z}_2)^4$ e quindi contiene una base.

Problema 27C. Contare separatamente quante volte un elemento non nullo di $G \times H$ si può scrivere come differenza di due elementi di $A \times (H \setminus B)$, come differenza di due elementi di $(G \setminus A) \times B$, e come differenza di un elemento di ciascuno di questi insiemi.

Problema 27D. Moltiplicare per un qualunque quadrato la somma degli elementi che vogliamo mostrare essere nulla.

Problema 27E. Abbiamo già detto che questo problema è simile al calcolo illustrato di λ_2.

Problema 27F. Usare il Teorema 27.5. (Una tabella di insiemi di differenze ciclici si trova in L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math. **182**, Springer-Verlag, 1971.)

Problema 27G. Uno zero ω del polinomio $y^3 + 3y + 2$, a coefficienti in $\mathbb{F}_7$, è un elemento primitivo di $\mathbb{F}_{7^3}$.

Problema 27H. La cardinalità dell'intersezione di un traslato $D+g$ di D con l'insieme $-D$ è il numero delle volte in cui g si ottiene come somma di elementi di D.

Problema 27I. Per $i \neq j$, le differenze $\mathbf{x} - \mathbf{y}$, con $\mathbf{x} \in U_i$, $\mathbf{y} \in U_j$, percorrono tutti i vettori di V, ciascuno esattamente una volta.

Orig. 568

Problema 28A. L'automorfismo di Frobenius di $\mathbb{F}_{p^{t(n+1)}}$ è un automorfismo del disegno simmetrico dei sottospazi di dimensione 1 e n di $\mathbb{F}_{p^{t(n+1)}}$ su $\mathbb{F}_{p^t}$.[9]

Problema 28B. Possiamo prendere $S(x)$ come nel Lemma 28.4 con $D = \{1, 2, 4\}$, ma scegliendo α che non sia un moltiplicatore.

Problema 28C. Se, per esempio, $n \equiv 0 \pmod{10}$, allora per ogni $x \in D$ si ha $\{x, 2x, 4x, 5x\} \subseteq D$, e si vede che la differenza x compare due volte, a meno che $3x = 0$. Se $3x = 0$ per ogni $x \in D$, allora $3x = 0$ per ogni x del gruppo, e quindi $n^2 + n + 1$ deve essere una potenza di 3. Mostrare che $n^2 + n + 1$ non è mai divisibile per 9.

Problema 28D. I numeri degli insiemi di differenze normalizzati con questi parametri sono, rispettivamente, $2, 2, 4, 2, 0, 4$.

Problema 28E. Vi sono due insiemi di differenze normalizzati $(15, 7, 3)$; sono equivalenti perché l'uno è formato dagli opposti degli elementi dell'altro. Non vi sono insiemi di differenze normalizzati per nessuno degli altri parametri. Per dimostrarlo in ciascun caso, trovare dapprima un moltiplicatore mediante il Teorema 28.7.

Per esempio, per $(v, k, \lambda) = (25, 9, 3)$, l'Esempio 28.3 mostra che 2 è un moltiplicatore di un ipotetico insieme di differenze normalizzato D. Se il gruppo è ciclico, D è un'unione dei cicli di $x \mapsto 2x$ su $\mathbb{Z}_{25}$, che sono

$$\{0\}, \qquad \{5, 10, 20, 15\}, \qquad \mathbb{Z}_{25} \setminus \{0, 5, 10, 15, 20\};$$

ma nessuna unione di questo tipo ha nove elementi. Se il gruppo è abeliano elementare, di esponente 5, allora D deve essere formato da 0 e da due cicli della forma $\{x, 2x, 4x, 8x = 3x\}$; ma la differenza x compare già cinque volte tra 0 e gli elementi di uno di questi cicli.

Problema 28F. Supporre che $D(x^{-1}) = D(x)$ e usare il Lemma 28.2 con $p = 2$.

[8] Questo suggerimento è etichettato 26K nell'originale, ma il riferimento al disegno complementare corrisponde al Problema 26L.

[9] Nell'originale, nella seconda occorrenza del campo esteso, compare s al posto di t.

Problema 28G. Ricordare la costruzione di un disegno simmetrico con quei parametri a partire da un quadrato latino di ordine 6 nel Problema 19G.

Problema 28H. Supporre che $D(x^q) = D(x)$. Si osservi che $q^3 \equiv -1 \pmod{|H|}$. Mostrare che $D(x^\alpha) \equiv 0 \pmod{q, H}$ e concludere che uno dei coefficienti di $D(x^\alpha)$ è $q+1$ e tutti gli altri sono 1. Orig. 569

Problema 28I. La prima parte è simile al Problema 28H. Mostrare poi che, se in $\mathrm{PG}_3(q)$ una retta incontra un insieme S di grandezza q^2+1 in $k \geq 3$ punti, uno dei $q+1$ piani per quella retta contiene più di $q+1$ punti di S.

Problema 29A. Riesaminare la dimostrazione del Teorema 20.6.

Problema 29B. Riesaminare l'ultima parte della dimostrazione della Proposizione 29.5.

Problema 29C. La risposta è $(v,k,\lambda) = (4n-1, 2n-1, n-1)$ oppure $(4n-1, 2n, n)$, cioè Hadamard o il complementare di Hadamard. Riesaminare la dimostrazione del Teorema 29.7.

Problema 30A. $A_1A_2 = 8A_1 + 8A_2 + 9A_3$ e $A_1^3 = 90A_0 + 83A_1 + 56A_2 + 36A_3$.

Problema 30B. Per (30.3), $A_iA_j = \sum_{\alpha=0}^k P_i(\alpha)P_j(\alpha)E_\alpha$. Quindi, per (30.4),

$$NA_iA_j = \sum_{\alpha=0}^k P_i(\alpha)P_j(\alpha) \sum_{\beta=0}^k Q_\alpha(\beta)A_\beta,$$

e dunque evidentemente $p_{ij}^\ell = \frac{1}{N}\sum_{\alpha=0}^k P_i(\alpha)P_j(\alpha)Q_\alpha(\ell)$. La seconda matrice degli autovalori Q si può calcolare invertendo P (si veda anche il Teorema 30.2).

Problema 30C. Per i grafi di quadrati latini,

$$P = \begin{pmatrix} 1 & (n-1)r & (n-1)(n-r+1) \\ 1 & n-r & -n+r-1 \\ 1 & -r & r-1 \end{pmatrix}.$$

Problema 30D. Per calcolare gli elementi $P_\ell(0)$ della prima riga di P, prendere il prodotto scalare (introdotto nella dimostrazione del Teorema 30.2) di entrambi i membri di (30.3) con E_0.

Problema 30E. È il duale del Problema 30B.

Problema 30F. Provare $|A| = |B| = 3$.

Problema 30G. Si osservi che, per ogni automorfismo σ, si ha $|A \cap \sigma(B)| \leq 1$. Contare gli automorfismi di G.

Problema 30H. Dato uno schema metrico proveniente da un grafo regolare rispetto alla distanza G, osservare anzitutto che A_1^i è una combinazione lineare di $A_0, A_1, \ldots, A_i$ nella quale il coefficiente di A_i è positivo. Dato uno schema P-polinomiale, definire un grafo G stabilendo che x e y siano adiacenti se e solo se sono primi associati nello schema, e mostrare che due punti sono i-esimi associati se e solo se sono a distanza i in G. Orig. 570

Problema 30I. Usare dapprima l'argomento di conteggio del Problema 20K per le parole di peso 8; trovare poi le altre parole che soddisfano la condizione. Usare i sottocodici con j fissato e il sottocodice del Problema 20K.

Problema 30J. Se un tale codice esistesse, sarebbe equivalente a un codice con matrice generatrice avente $(1111100\cdots0)$ come prima riga e, sotto di essa, $(A\ B)$, dove B genera un codice di lunghezza 8, dimensione 5 e distanza minima almeno 3. Usare ora il fatto che il codice di Hamming $[7,4,3]$ è unico a meno di equivalenza.

Problema 30K. (i) La distanza dipende soltanto dalla grandezza dell'intersezione: basta contare. (ii) Il grafo ha grado 4, e due terne corrispondenti al piano di Fano si incontrano in un punto.

Problema 30L. Per $J(k,v)$ mostrare che è necessario che $1 + k(v-k)$ divida $\binom{v}{k}$.

Problema 31A. Considerare l'intersezione degli autospazi di A_1 e A_2 corrispondenti all'autovalore 1.

Problema 31B. Poiché la matrice di adiacenza del complementare di un grafo G con matrice di adiacenza A è $J - I - A$, gli autovalori di $\overline{G}$ si determinano facilmente da quelli di G. I primi esempi del Capitolo 21 sono casi nei quali può verificarsi l'uguaglianza.

Problema 31C. (i) Il grafo di Petersen contiene artigli a tre rami, cioè sottografi indotti su quattro vertici formati da tre spigoli incidenti a un vertice comune e nessun altro spigolo. Spiegare perché un grafo degli spigoli non può contenere un tale artiglio. (ii) La matrice $N^{\mathsf{T}}N$ è semidefinita positiva ed è uguale a $2I + A$, dove A è la matrice di adiacenza.

Problema 31D. Dall'equazione che segue (31.1), scegliendo $\mathbf{x}$ come il vettore di tutti 1, segue che il massimo autovalore di un grafo è almeno il grado minimo del grafo. Per il Lemma 31.5, il massimo autovalore di un grafo G è almeno il grado minimo di ogni sottografo indotto H di G. Se $\chi(H) = \chi(G)$ e l'eliminazione di un qualunque vertice x di H diminuisce il numero cromatico, allora $\deg(x) \geq \chi(H) - 1$. Orig. 571

Problema 31E. Se in un digrafo G con matrice di adiacenza A non vi sono cammini orientati da x a y, sia S l'insieme dei vertici z per i quali esiste un cammino orientato in G da x a z. Allora $A(a, b) = 0$ ogni volta che $a \in S$ e $b \in V(G) \setminus S$, quindi A non è irriducibile.[10] Il viceversa è ancora più facile.

Problema 31F. (i) Mostrare mediante calcolo diretto che $\mathbf{u}_j A = \lambda_j \mathbf{u}_j$, dove

$$\mathbf{u}_j = (1, \omega^j, \omega^{2j}, \ldots, \omega^{(n-1)j}).$$

Per (ii), definire, per ogni carattere χ, un vettore $\mathbf{u}_\chi$ le cui coordinate sono indicizzate da G e per il quale $\mathbf{u}_\chi(g) = \chi(g)$, e mostrare che $\mathbf{u}_\chi A = \lambda_\chi \mathbf{u}_\chi$.[11]

Problema 31G. Per dimostrare il lemma, mostrare che, se $\mathbf{x}$ è un vettore riga tale che $\mathbf{x}S = 0$, allora $\mathbf{xa} = 0$. Applicare il lemma a $S = A + I$, dove A è la matrice di adiacenza del grafo. Il lemma si trova in B. Bagchi e N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes, *Geometriae Dedicata* **22** (1987), 137–147. Il problema sui grafi, formulato in termini di «conoscenze», è il Problema 10851, di D. Beckworth, dell'*American Mathematical Monthly* **108**.

Problema 31H. Gran parte del lavoro è stata fatta nella dimostrazione del Teorema 31.10: se gli autovalori distinti di G sono il suo grado d e μ_i, $i = 1, 2$, allora $(A - \mu_1 I)(A - \mu_2 I) = \frac{1}{v}(d - \mu_1)(d - \mu_2)J$, dove A è la matrice di adiacenza di G. Ciò significa che A^2 appartiene all'algebra generata da I, J, A. Quindi G è fortemente regolare.

Problema 31I. Gli autovalori di $\Delta(x)$ si interlacciano con gli autovalori

$$k, r, r, \ldots, r, s, s, \ldots, s \qquad \text{(diciamo } r > s\text{)}$$

di G, dove G è uno $\mathrm{srg}(v, k, \lambda, \mu)$. Una successione che si interlaccia con questa può avere al più un termine maggiore di r.

Tranne che nel caso metà, r e s sono interi con $rs = \mu - k$; in particolare, $r \leq k - \mu$ (anche nel caso metà). Il grafo $\Delta(x)$ è regolare di grado $k - \mu$. Se non fosse connesso, $k - \mu$ sarebbe un autovalore di $\Delta(x)$ di molteplicità maggiore di uno. Orig. 572

Problema 31J. L'autospazio di A corrispondente all'autovalore 1 e quello di B corrispondente a -1 hanno entrambi dimensione 5, ma sono contenuti nello spazio di dimensione 9 dei vettori ortogonali al vettore di tutti 1; esiste quindi un vettore non nullo $\mathbf{u}$ nell'intersezione dei due autospazi. Mostrare che la connessione di K contraddice il Teorema 31.11.

Problema 31K. (i) Segue dal Teorema 31.13 o da una parte della sua dimostrazione. (ii) Moltiplicare (31.6) per J. (iii) Il numero degli spigoli non orientati è metà della traccia di A^2. (iv) Mostrare che gli spigoli non orientati non hanno un vertice comune e non sono collegati da uno spigolo. A meno di invertire i versi, resta un solo modo di completare il grafo.

Problema 32A. Uno dei grafi ha due vertici, uno ne ha tre e due ne hanno quattro.

[10] L'originale stampa $A(x, y)$ al posto di $A(a, b)$ nella frase quantificata.

[11] Anche questo suggerimento riprende il problema di segno segnalato nella nota alla Proposizione 31.14: con autovettori riga occorre il carattere inverso nella formula dell'autovalore.

Problema 32B. Sia X l'insieme dei vertici raggiungibili da s mediante un cammino orientato con $f(e) > 0$ su tutti i suoi spigoli, e sia Y l'insieme dei vertici rimanenti, se ve ne sono. Se $t \notin X$, otteniamo una contraddizione con l'equazione (7.1) (perché?). Per la parte (ii), usare l'induzione su k.

Problema 32C. Assegnare capacità 1 a tutti gli spigoli di D. Usare il Teorema 7.1.

Problema 32D. Se (H, K) è una ℓ-separazione e l'eliminazione degli ℓ vertici di $S := V(H) \cap V(K)$ non sconnette il grafo, almeno uno fra H e K ha l'insieme dei vertici contenuto in S.

Problema 33A. Spiegare brevemente perché gli alberi ricoprenti di G contenenti lo spigolo e sono in corrispondenza biunivoca con gli alberi ricoprenti di G''_e, e perché quelli che non contengono e sono in corrispondenza biunivoca con gli alberi ricoprenti di G'_e.

Problema 33B. Trovare una risposta della forma $f(\lambda) + (-1)^n g(\lambda)$. Usare l'induzione, l'equazione (32.1) e l'Esempio 32.1.[12]

Problema 33C. Più precisamente, una suddivisione di $K_{3,3}$, in cui gli spigoli sono sostituiti da cammini, compare come sottografo del grafo di Petersen.

Orig. 573

Problema 33D. Supporre che un vertice di G''_S sia incidente a tre spigoli distinti e_1, e_2, e_3. Tale vertice è una componente connessa C di $G : S$. Quindi e_i ha un estremo x_i in C, per $i = 1, 2, 3$ (questi estremi non sono necessariamente distinti). Spiegare perché la connessione di C implica che esistono un vertice x e cammini in C, eventualmente degeneri ma internamente disgiunti, da x a ciascuno di x_1, x_2, x_3. In altri termini, abbiamo un sottografo di C isomorfo a una suddivisione della lettera Y, con gli x_i agli estremi dei rami se tutti i cammini hanno lunghezza ≥ 1; altrimenti alcuni rami possono essere degeneri. Questa osservazione conduce immediatamente a una soluzione della prima parte del problema.

Dati quattro vertici x_i, $i = 1, 2, 3, 4$, di un grafo connesso C, mostrare che esiste un sottografo isomorfo a una suddivisione della lettera X oppure della lettera I, con rami eventualmente degeneri e con gli x_i agli estremi dei rami.

Verificare che, se un vertice di K_5, diciamo 1, viene sostituito con due vertici 1_L e 1_R uniti da uno spigolo, e gli spigoli che univano 1 agli altri vertici vengono ripartiti, per esempio unendo 1_L a 2 e 3 e 1_R a 4 e 5, il grafo risultante contiene $K_{3,3}$ come sottografo. Combinare questo fatto con l'osservazione del paragrafo precedente per concludere.

Problema 33E. Usare la formula di Eulero. Le uniche coppie (d_1, d_2) che compaiono, oltre a $(3,3), (3,4), (3,5), (4,3), (5,3)$, corrispondenti ai cinque solidi platonici, sono $(2, n)$ e $(n, 2)$, con $n \geq 2$, corrispondenti ai poligoni e ai grafi a fascio.

Problema 34A. Abbiamo un'applicazione lineare dallo spazio vettoriale su $\mathbb{F}_2$ di tutti i sottoinsiemi X dell'insieme dei vertici $V(G)$ sullo spazio dei tagli di G, precisamente $X \mapsto \times(X, V(G) \setminus X)$. (La matrice di questa applicazione è N, la matrice d'incidenza.) Quali insiemi X appartengono al nucleo? La dimensione dello spazio dei tagli è il numero dei vertici meno la dimensione del nucleo.

Problema 34B. Usare l'induzione sulla cardinalità del supporto delle parole del codice.

Problema 34C. I circuiti di G'_e sono esattamente i circuiti di G che non contengono e. Quali sono i legami di H''_e?

Orig. 574

Problema 34D. Un modo consiste nel dimostrare prima due fatti sui sottoinsiemi S dell'insieme degli spigoli di un grafo connesso K: (1) S è l'insieme degli spigoli di un albero ricoprente di K se e solo se nessun circuito di K è contenuto in S e S è massimale rispetto a questa proprietà; (2) S è l'insieme degli spigoli di un albero ricoprente di K se e solo se ogni legame di K incontra S non banalmente e S è minimale rispetto a questa proprietà.

Problema 34E. Mostrare anzitutto che le due componenti ottenute eliminando un istmo da un grafo connesso trivalente hanno ciascuna un numero dispari di vertici.

Problema 34F. Ecco un'idea per costruire legami. Eliminando un qualunque spigolo di un albero ricoprente di G resta un sottografo con due componenti; l'insieme degli spigoli con un estremo in ciascuna componente è un legame di G.

[12] I rinvii sono quelli dell'originale; per il polinomio cromatico si intendono l'equazione (33.1) e l'Esempio 33.1.

Problema 34G. Eliminare gli spigoli di un legame S da un grafo connesso G dà sempre un grafo con due componenti, ma si ricordi che nella definizione di G'_S abbiamo scelto di eliminare i vertici isolati. Nella parte (ii), un'equivalenza di codici dà una corrispondenza biunivoca tra gli insiemi degli spigoli di H e G che porta circuiti in circuiti e legami in legami. Usare la parte (i) e il fatto che un grafo senza vertici isolati è non separabile se e solo se due spigoli qualsiasi sono contenuti insieme in un circuito; cfr. il Teorema 32.2.

Problema 34H. Dato un poligono P in G, si possono considerare i sottografi H, K, dove $H = P$ e K è il sottografo ricoprente di G contenente tutti gli spigoli di G tranne quelli di P.

Considerare un legame B di G formato da tutti gli spigoli con un estremo in X e uno in Y, dove X, Y partizionano $V(G)$ e inducono ciascuno un sottografo connesso. Supporre per assurdo che G sia k-connesso nel senso di Tutte, ma che $|B| = \ell < k$. Sia ℓ_1 il numero dei vertici di X incidenti a spigoli di B. Se il sottografo indotto da X ha almeno ℓ_1 spigoli, troviamo facilmente una ℓ_1-separazione di G. Trattare la situazione rimanente.

Problema 34I. Diamo suggerimenti indipendenti, anche se si può dedurre (i) da (ii) oppure, come abbiamo detto, le prime due parti da (iii). (i) Se A e B sono gli insiemi degli spigoli di poligoni P e Q, cominciare a percorrere P nei due versi, partendo dallo spigolo y, e fermarsi non appena si raggiungono vertici di Q. Orig. 575

(ii) Se A e B sono i supporti di parole del codice $\mathbf{a}$ e $\mathbf{b}$, il supporto S di una certa combinazione lineare di $\mathbf{a}$ e $\mathbf{b}$ contiene la coordinata y ma non x. Mostrare per induzione su $|S|$ che ogni supporto S di una parola del codice è unione di supporti minimali di parole del codice.

(iii) Mostrare che, in generale, se $z \in \overline{S}$, esiste un insieme dipendente minimale D tale che $z \in D \subseteq S \cup \{z\}$. (Riesaminare il Lemma 23.2.) Mostrare poi che y appartiene alla chiusura di $(A \cup B) \setminus \{x, y\}$.

Problema 35A. Prendere come vertici di K_n gli elementi di $\mathbb{Z}_n$. Per $n = 5$, usare tutti gli spostamenti ciclici (traslati) di $[1, 2, 4, 3] \pmod 5$.

Problema 35B. Eliminiamo l'ultima coordinata nella descrizione dell'Esempio 21.4 e descriviamo il grafo di Clebsch mediante l'insieme dei vertici $\mathbb{F}_2^4$, dove $\mathbf{x}$ e $\mathbf{y}$ sono adiacenti quando $\mathbf{x} + \mathbf{y}$ ha peso 3 o 4. Provare a scegliere una passeggiata w e a ottenere le altre come traslati di w mediante tutti gli elementi di $\mathbb{F}_2^4$.

Problema 35C. La parte (i) è simile al Teorema 33.5. Per dimostrare l'unicità della maglia, possiamo prendere $V(K_7) = \{0, 1, \ldots, 6\}$ e supporre senza perdita di generalità che le passeggiate che attraversano 0 siano

$$[6, 0, 1],\ [1, 0, 2],\ [2, 0, 3],\ [3, 0, 4],\ [4, 0, 5],\ [5, 0, 6].$$

La passeggiata che percorre lo spigolo $(6, 1)$ ha come terzo vertice 3 oppure 4 (altrimenti la condizione sui vertici è violata in 1 o in 6), e in entrambi i casi le altre passeggiate sono determinate univocamente.

Problema 35D. I vertici del grafo M_x sono gli spigoli incidenti a x. Questi spigoli formano l'insieme degli spigoli di un legame di G e sono quindi gli spigoli di un circuito di H.

Problema 35E. Usiamo il termine *bandiera* per una terna (x, e, F) formata da un vertice x, uno spigolo e incidente a x e una faccia F incidente a e. Vi è esattamente un altro vertice x' tale che (x', e, F) sia una bandiera, esattamente un altro spigolo e' tale che (x, e', F) sia una bandiera, ed esattamente un'altra faccia F' tale che (x, e, F') sia una bandiera; questi oggetti devono quindi essere fissati da ogni automorfismo α che fissa gli elementi di (x, e, F). Orig. 576

Problema 35F. Usare il Teorema 35.1. Il minimo valore di $n > 2$ per il quale $K_{n,n}$ si immerge in una superficie orientabile con tutte le facce quadrilatere è $n = 6$; n deve essere pari, ma $K_{4,4}$ non si immerge in questo modo in T_0. Occorrono qualche idea e/o un'analisi dei casi.[13]

Problema 35G. Tutte le facce avranno la stessa grandezza. Considerare la passeggiata che percorre lo spigolo $(0, 1)$. Gli spigoli successivi sono $(1, 1-\omega)$, $(1-\omega, 1-\omega+\omega^2)$, $(1-\omega+\omega^2, 1-\omega+\omega^2-\omega^3)$, ecc. Se, per esempio, $m \equiv 2 \pmod 4$, la passeggiata ha lunghezza $m/2$.

[13] Il suggerimento originale è problematico: dalla formula di Eulero, per una tale immersione di $K_{n,n}$ si ricava $g = (n-2)^2/4$, che per $n = 4$ dà $g = 1$, non 0. In effetti $K_{4,4}$ ammette una quadrangolazione del toro T_1, e il minimo corretto è $n = 4$. Manteniamo il testo originale segnalando l'errore.

Problema 36A. La somma dei determinanti di tutte le sottomatrici principali $(n-1)\times(n-1)$ di M è, a meno di un opportuno segno, il coefficiente di x nel polinomio caratteristico $\det(xI-M)$ di M.

Problema 36B. Vi è una tale arborescenza per ogni applicazione $f:\{2,3,\ldots,n\}\to\{1,2,\ldots,n-1\}$ tale che $f(i)<i$ per ogni i.

Problema 36C. Se un vettore $\mathbf{g}$ con coordinate indicizzate da $E(H)$ ha la proprietà che, per ogni passeggiata chiusa w, la somma con segno dei valori di $\mathbf{g}$ sugli spigoli di w è nulla, definire un vettore $\mathbf{h}$ indicizzato da $V(H)$ nel modo seguente. (Per comodità supponiamo H connesso; altrimenti si lavora separatamente su ogni componente.) Fissare un vertice x, porre $\mathbf{h}(x):=0$ e, per ogni vertice y, definire $\mathbf{h}(y)$ come la somma con segno dei valori di $\mathbf{g}$ sugli spigoli di una qualunque passeggiata da x a y. Verificare che $\mathbf{h}$ è ben definito e che $\mathbf{g}$ è il cobordo di $\mathbf{h}$.

Problema 36D. Siano Z lo spazio dei cicli e B lo spazio dei cobordi. Sono complementi ortogonali, quindi la loro somma diretta è $\mathbb{R}^m$, lo spazio di tutti i vettori con coordinate indicizzate da $E(D)$. Mostrare che la trasformazione lineare R è iniettiva su Z e che $ZR\cap B=\{0\}$, così che $\mathbb{R}^m$ è somma diretta di questi sottospazi.

Problema 36E. Le dimensioni di tutti i quadrati della Fig. 36.4 si possono esprimere come combinazioni lineari intere delle dimensioni x,y,z dei tre quadrati indicati. Per esempio, il quadrato più piccolo ha dimensione $z-x$ e quello immediatamente successivo ha dimensione $x+z-y$. Si troverà che le dimensioni di alcuni quadrati si possono esprimere in più modi, ottenendo così relazioni lineari tra x,y,z. Alla fine potremo esprimere la dimensione di ogni quadrato come multiplo razionale di x, e il minimo comune denominatore di questi numeri razionali è il valore da assegnare a x.

Orig. 577

Problema 36F. La via più rapida può essere procedere come nel Problema 36E: siano, per esempio, x,y,z i valori della corrente su tre spigoli, ecc. Si possono però anche calcolare determinanti come nell'equazione (36.3) per trovare le soluzioni.

Problema 37A. Le rotazioni comprendono: l'identità (1); le rotazioni di 90, 180 e 270 gradi attorno a un asse passante per i centri di due facce opposte $(3+3+3)$; le rotazioni di 180 gradi attorno a un asse passante per i punti medi di due spigoli opposti (6); e le rotazioni di 120 e 240 gradi attorno a un asse passante per due vertici opposti $(2+2+2+2)$. Queste ultime otto rotazioni, per esempio, contribuiscono con $8X_3^2$ all'indice dei cicli.

Problema 37B. Usare il Teorema 37.2 e il Problema 37A.

Problema 37C. Spiegare perché il numero delle applicazioni iniettive f fissate da (σ,τ) dipende soltanto dalla struttura dei cicli di σ e τ, cioè dai numeri z_i dei cicli di lunghezza i per ogni i, e trovare un'espressione per tale numero mediante gli $z_i(\sigma)$ e gli $z_i(\tau)$.

Problema 37D. Nel Teorema 37.3, prendere come G il gruppo diedrale e come H il gruppo simmetrico S_2.

Problema 37E. Se una rotazione ρ del cubo ha a cicli sulle facce e b cicli sui vertici, il numero delle colorazioni fissate da ρ è s^at^b.[14] Usare il lemma di Burnside.

Problema 38A. Sia $m:=v/2$. Per ciascuno degli $M:=v-1$ colori i, otteniamo una m-partizione di $V(K_u)$[15] prendendo gli spigoli di colore i, tutti i singoletti $\{x\}$ per x non incidente a uno spigolo di colore i, e un numero sufficiente di copie dell'insieme vuoto per ottenere una m-partizione. Verificare che vale la condizione (38.1). Riesaminare la dimostrazione del Teorema 38.1.

[14] L'originale stampa t^as^b, scambiando i colori assegnati nel Problema 37E a facce e vertici.

[15] L'originale stampa $V(K_v)$. La costruzione iniziale riguarda i vertici già colorati di K_u; viene poi estesa ai v vertici mediante la dimostrazione del Teorema 38.1.

Appendice 2
Serie formali di potenze

Orig. 578

Prima di introdurre l'argomento di questa appendice, osserviamo che molte delle affermazioni che faremo non saranno dimostrate. In questi casi la dimostrazione costituirà un facile esercizio per il lettore.

Consideriamo l'insieme

$$\mathbb{C}^{\mathbb{N}_0} := \{(a_0, a_1, a_2, \ldots) : \forall i \in \mathbb{N}_0 \ [a_i \in \mathbb{C}]\}.$$

Su questo insieme introduciamo un'operazione di addizione e una moltiplicazione come segue:

$$\begin{aligned}(a_0, a_1, \ldots) + (b_0, b_1, \ldots) &:= (a_0 + b_0, a_1 + b_1, \ldots),\\ (a_0, a_1, \ldots)(b_0, b_1, \ldots) &:= (c_0, c_1, \ldots),\end{aligned}$$

dove $c_n := \sum_{i=0}^{n} a_i b_{n-i}$.

Questa definizione produce un anello che denotiamo con $\mathbb{C}[[z]]$ e chiamiamo *anello delle serie formali di potenze*. Il nome si spiega nel modo seguente. Poniamo $z := (0, 1, 0, 0, \ldots)$. Allora z^n è la successione $(0, \ldots, 0, 1, 0, \ldots)$ con un 1 nella posizione n-esima. Formalmente abbiamo dunque

$$a = (a_0, a_1, \ldots) = \sum_{n=0}^{\infty} a_n z^n =: a(z).$$

Useremo entrambe le notazioni, a e $a(z)$, per indicare la successione. Diciamo che a_n è il *coefficiente di* z^n in a (o in $a(z)$). Si osservi che $\mathbb{C}[z]$, l'anello dei polinomi a coefficienti in $\mathbb{C}$, è un sottoanello di $\mathbb{C}[[z]]$. Alcune serie di potenze saranno convergenti nel senso dell'analisi. Per queste possiamo usare i risultati che conosciamo dall'analisi. Molto spesso tali risultati si possono dimostrare in senso formale, cioè senza usare la convergenza o altri strumenti dell'analisi.

Orig. 579

Esempio 1. Sia $f := (1, 1, 1, \ldots)$. Usando la definizione della moltiplicazione e $1 - z = (1, -1, 0, \ldots)$, troviamo $(1 - z)f = (1, 0, 0, \ldots) = 1$. Quindi in $\mathbb{C}[[z]]$ abbiamo $f = (1 - z)^{-1}$, cioè

$$\frac{1}{1 - z} = \sum_{n=0}^{\infty} z^n,$$

un risultato già noto dall'analisi.

Gli elementi invertibili di $\mathbb{C}[[z]]$ sono le serie di potenze con $a_0 \neq 0$.[16] Lo si vede immediatamente dalla definizione della moltiplicazione. Dalla relazione $a(z)b(z) = 1$ possiamo calcolare i coefficienti b_n, poiché $b_0 = a_0^{-1}$ e $b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i}$. Da ciò vediamo che il campo dei quozienti di $\mathbb{C}[[z]]$ si può identificare con l'insieme delle cosiddette *serie di Laurent* $\sum_{n=k}^{\infty} a_n z^n$, dove $k \in \mathbb{Z}$. Poiché avrà un ruolo speciale nel seguito, diamo al coefficiente di z^{-1} un nome familiare dall'analisi. Se la serie è $a(z)$, diciamo che a_{-1} è il *residuo* di $a(z)$, e lo indichiamo con $\operatorname{Res} a(z)$.

Siano $f_n(z) = \sum_{i=0}^{\infty} c_{ni} z^i$, per $n = 0, 1, 2, \ldots$, elementi di $\mathbb{C}[[z]]$ con la proprietà

$$\forall i \ \exists n_i \ [n > n_i \Rightarrow c_{ni} = 0].$$

[16] L'originale usa qui «regular elements». Il significato necessario è «elementi invertibili»; nel significato algebrico usuale di «non divisori dello zero», tutti gli elementi non nulli di $\mathbb{C}[[z]]$ sono regolari.

Possiamo allora definire formalmente

$$\sum_{n=0}^{\infty} f_n(z) = \sum_{i=0}^{\infty} \left(\sum_{n=0}^{n_i} c_{ni} \right) z^i. \tag{1}$$

Questa definizione ci permette di introdurre la sostituzione di una serie di potenze $b(z)$ alla «variabile» z di una serie di potenze $a(z)$. Se $b_0 = 0$, condizione che scriviamo anche $b(0) = 0$, le potenze $b^n(z) := (b(z))^n$ soddisfano la condizione per l'addizione formale; dunque ha senso porre

$$a(b(z)) := \sum_{n=0}^{\infty} a_n b^n(z).$$

Orig. 580

Esempio 2. Siano $f(z) := (1-z)^{-1}$ e $g(z) = 2z - z^2$. Formalmente,

$$\begin{aligned} h(z) := f(g(z)) &= 1 + (2z - z^2) + (2z - z^2)^2 + \cdots \\ &= 1 + 2z + 3z^2 + 4z^3 + \cdots . \end{aligned}$$

Dal calcolo infinitesimale sappiamo che questo è lo sviluppo in serie di potenze di $(1-z)^{-2}$, e ciò deve dunque essere vero anche in $\mathbb{C}[[z]]$. Infatti abbiamo

$$(1-z)h(z) = \sum_{n=0}^{\infty} z^n = (1-z)^{-1}.$$

Questo segue anche da una manipolazione algebrica legittima:

$$f(g(z)) = \big(1 - (2z - z^2)\big)^{-1} = (1-z)^{-2}.$$

Molte delle serie di potenze che usiamo spesso rappresentano funzioni ben note, e in molti casi anche la funzione inversa è rappresentata da una serie di potenze. Anche questo si può interpretare formalmente, per serie $f(z)$ con $f_0 = 0$ e $f_1 \neq 0$. «Risolviamo» l'equazione $f(g(z)) = z$ mediante sostituzione. Otteniamo $f_1 g_1 = 1$, $f_1 g_2 + f_2 g_1^2 = 0$,[17] e, in generale, un'espressione per il coefficiente di z^n che comincia con $f_1 g_n$ e i cui altri termini coinvolgono soltanto coefficienti f_i e coefficienti g_k con $k < n$. Ponendola uguale a 0 possiamo calcolare g_n.

Esempio 3. Il lettore che ama le sfide combinatorie può dare una dimostrazione mediante conteggio della formula

$$\sum_{k=0}^{n} \binom{2k}{k} \binom{2n-2k}{n-k} = 4^n.$$

Ciò equivale a dimostrare che la serie formale di potenze $f(z) := \sum_{n=0}^{\infty} \binom{2n}{n} (z/4)^n$ soddisfa la relazione $f^2(z) = (1-z)^{-1}$. Con argomenti analoghi o mediante manipolazioni algebriche si può poi trovare la serie formale di potenze che merita il nome $(1+z)^{1/2}$.

Consideriamo ora la serie formale di potenze $f(z) := 2z + z^2$. Il procedimento della «funzione inversa» descritto sopra produce una serie di potenze $g(z)$ che soddisfa $2g(z) + g^2(z) = z$, cioè $(1+g(z))^2 = 1+z$. Pertanto $1 + g(z)$ dovrebbe essere la serie che abbiamo appena chiamato $(1+z)^{1/2}$.[18] Non dovrebbe più sorprenderci che relazioni algebriche valide per serie di potenze convergenti valgano anche nella teoria delle serie formali di potenze.

Orig. 581

Osservazione. Sottolineiamo che sostituzioni perfettamente sensate nel calcolo infinitesimale potrebbero essere vietate nella teoria presente. La serie di potenze $\sum_{n=0}^{\infty} z^n/n!$ riceverà naturalmente il nome $\exp(z)$. Nel calcolo infinitesimale potremmo sostituire $z = 1+x$ e trovare la serie di potenze di $\exp(1+x)$. Non lo ammettiamo nel quadro dell'addizione formale.

Introduciamo ora la derivazione formale delle serie di potenze.

Definizione. Se $f(z) \in \mathbb{C}[[z]]$, definiamo la *derivata*

$$(Df)(z) = f'(z)$$

[17] Nell'originale manca il fattore f_2 nel secondo termine.

[18] L'originale dice «questa dovrebbe essere la serie», con un riferimento ambiguo a $g(z)$; la serie con quadrato $1+z$ e termine costante 1 è $1 + g(z)$.

come la serie di potenze $\sum_{n=1}^{\infty} n f_n z^{n-1}$.

Il lettore non dovrebbe avere difficoltà a dimostrare le regole seguenti usando le definizioni di questa appendice:

$$\begin{aligned}
&\text{(D1)} \quad (f(z)+g(z))' = f'(z)+g'(z);\\
&\text{(D2)} \quad (f(z)g(z))' = f'(z)g(z)+f(z)g'(z);\\
&\text{(D3)} \quad (f^k(z))' = kf^{k-1}(z)f'(z);\\
&\text{(D4)} \quad (f(g(z)))' = f'(g(z))g'(z).
\end{aligned}$$

La regola di derivazione delle funzioni composte (D4) è un esempio di un'affermazione più generale, cioè

$$D\left(\sum_{n=0}^{\infty} f_n(z)\right) = \sum_{n=0}^{\infty} D(f_n(z)).$$

Quando interviene la convergenza, questo è un teorema difficile che richiede ipotesi aggiuntive; per le serie formali di potenze, invece, è banale!

Anche la consueta regola di derivazione di un quoziente si dimostra facilmente. Possiamo quindi estendere la teoria alle serie di Laurent. Ci serviranno i due fatti seguenti. Ancora una volta lasciamo la dimostrazione per esercizio.

Se $w(z)$ è una serie di Laurent, allora:

(R1) $\operatorname{Res}(w'(z)) = 0$;

(R2) il residuo di $w'(z)/w(z)$ è il minimo intero ℓ tale che il coefficiente di z^ℓ in $w(z)$ sia non nullo.

Orig. 582

Abbiamo già menzionato l'idea di «funzione inversa» e abbiamo mostrato come calcolarne ricorsivamente i coefficienti. Il prossimo teorema fornisce un'espressione per tali coefficienti.

Teorema 1. Sia $W(z) = w_1 z + w_2 z^2 + \cdots$ una serie di potenze con $w_1 \neq 0$. Sia $Z(w) = c_1 w + c_2 w^2 + \cdots$ una serie di potenze in w tale che $Z(W(z)) = z$. Allora

$$c_n = \operatorname{Res}\left(\frac{1}{nW^n(z)}\right).$$

Dimostrazione. Si osservi che $c_1 = w_1^{-1}$. Usiamo ora la derivazione formale e applichiamola alla relazione $Z(W(z)) = z$. Otteniamo

$$1 = \sum_{k=1}^{\infty} k c_k W^{k-1}(z) W'(z). \tag{2}$$

Consideriamo la serie ottenuta dividendo il membro destro di (2) per $nW^n(z)$. Se $n \neq k$, il termine $W^{k-1-n}(z)W'(z)$ è una derivata per (D3) e ha quindi residuo 0 per (R1). Applicando (R2) al termine con $n = k$, troviamo l'affermazione del teorema. □

Questo teorema ci permette di dimostrare la formula di inversione di Lagrange (si veda il Teorema 14.3) nell'ambito della teoria delle serie formali di potenze. Sia $f(z)$ una serie di potenze con $f_0 \neq 0$. Allora $W(z) := z/f(z)$ è una serie di potenze con $w_1 \neq 0$. Applichiamo ora il Teorema 1. Troviamo che $z = \sum_{n=1}^{\infty} c_n w^n$, con

$$c_n = \operatorname{Res} \frac{f^n(z)}{nz^n} = \frac{1}{n!}(D^{n-1} f^n)(0),$$

che è la (14.19). Questo approccio si basa su P. Henrici, An algebraic proof of the Lagrange–Bürmann formula, *J. Math. Anal. and Appl.* **8** (1964), 218–224. L'elegante semplificazione è dovuta a J. W. Nienhuys.

Come osservato sopra, definiamo

$$\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}. \tag{3}$$

Dalle conoscenze precedenti ci aspettiamo che sostituire z con $-z$ dia l'elemento inverso nell'anello $\mathbb{C}[[z]]$. Orig. 583

La moltiplicazione formale e il fatto che $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$ per $n > 0$ mostrano che è così.

È ora del tutto naturale definire anche

$$\log(1+z) := \sum_{n=1}^{\infty}(-1)^{n-1}\frac{z^n}{n}. \tag{4}$$

[19] Ancora una volta, il calcolo infinitesimale ci fa attendere una relazione tra le «funzioni» log ed exp. In base alla nostra regola di sostituzione, ha senso considerare la serie di potenze $\log(\exp(z))$. Da (D4) ricaviamo allora

$$D(\log(\exp(z))) = \frac{\exp(z)}{\exp(z)} = 1,$$

cioè $\log(\exp(z)) = z$. (Qui abbiamo usato il fatto che la derivata formale di $\log(1+z)$ è $(1+z)^{-1}$.)

Naturalmente si può dire molto di più sulle serie formali di potenze. Si potrebbe indagare quanti risultati familiari dell'analisi si possano trasferire o dimostrare formalmente. Ci auguriamo che questa trattazione sommaria basti a rendere più chiare le idee.

[19] Nell'originale compare erroneamente $(-1)^n$. Il segno corretto è $(-1)^{n-1}$, coerente con la derivata e con l'identità che seguono.

Indice dei nomi

I numeri rimandano alle pagine dell'edizione originale, indicate a margine della traduzione. Le voci onomastiche sono riprodotte nell'ordinamento originale. Il rinvio «Preface» significa «Prefazione»; «Catherine the Great» indica Caterina la Grande.

Orig. 584

Aardenne–Ehrenfest, T. van 520
Alltop, W.O. 223, 241
André, D. 138, 151
André, J. 320, 324
Assmus, E.F. 249, 259, 260
Appel, K. 24, 34, 35, 466, 471

Baer, R. 255
Bagchi, N. 571
Baker, R.D. 300
Balinski, M. 457, 458
Bannai, E. 413, 431
Baranyai, Zs. 536, 537, 540, 541
Batten, L.M. 324, 363, 368
Baumert, L.D. 204, 214, 294, 295, 567
Beauregard Robinson, G. de 165, 167
Beckworth, D. 571
Beineke, L.W. 281
Belevitch, V. 200, 214, 265
Bermond, J.-C. 537
Bertrand, J.L.F. 151
Best, M.R. 207, 214
Beth, T. 301
Bhattacharya, K.N. 240, 241
Biggs, N. 450, 466, 471
Binet, A. 508, 510
Birkhoff, G. 48, 51, 52, 111
Block, R.E. 371, 382
Blokhuis, A. 367, 368
Bollobás, B. 38, 41, 57
Bondy, J.A. 9, 542
Bose, R.C. 240, 264, 271, 272, 279, 280, 284, 288, 300, 301, 365, 367, 368, 409
Bouwkamp, C.J. 520, 521
Brégman, L.M. 101, 108
Brooks, R.L. 24, 35
Brouwer, A.E. 85, 87, 88, 272, 279, 280, 355, 368, 407, 431, 537, 541
Brouwer, L. E. J. 458
Bruck, R.H. 230, 241, 280, 381, 382, 383, 398
Bruijn, N.G. de 55, 59, 71, 75, 76, 216, 241, 433, 513, 514, 520, 532, 535
Buekenhout, F. 281
Bürmann, H. 582
Burnside, W. 94, 370

Cameron, P.J. 259, 260, 279, 280, 281
Catalan, E. 150, 151
Catherine the Great 284
Cauchy, A.L. 94, 108, 508, 510
Cayley, A. 12, 22, 504, 505, 508

Orig. 585

Chakravarti, I.M. 367, 368
Chandrasekharan, K. 167, 230, 241
Chang, L.C. 271, 280, 281
Chartrand, G. 462, 471, 491, 505
Chowla, S. 230, 241, 301, 383, 398
Chvátal, V. 70
Clebsch, A. 263, 279, 498, 505, 575
Cohen, A.M. 407, 431
Cohen, G.D. 241
Connor, W.S. 228, 241, 280, 281
Conway, J.H. 216, 560
Crapo, H. 324, 490, 564
Crawley, P. 304, 313, 319,324
Cruse, A. 541
Cvetković, D.M. 440, 450

Da Silva, D.A. 96
De Clerck, F. 280, 281
Dedekind, J.W.R. 167
Dehn, M. 520, 521
Delsarte, P. 279, 280, 281, 405, 412, 413, 419, 422, 424, 431
Dembowski, P. 324, 368
Dénes, J. 197
Denniston, R.H.F. 223, 242, 252, 268
Desargues, G. 317, 323
Diaconis, P. 181
Diestel, R. 462, 463, 471
Dilworth, R.P. 53, 60, 304, 313, 319, 324
Dinitz, J.H. 294, 301, 469
Dirac, G.A. 40
Doob, M. 450
Dowling, T. 341, 342, 349
Duijvestijn, A.J.W. 517, 520, 521
Dulmage, A.L. 295, 302
Duval, A.M. 276, 281

Ebbenhorst Tengbergen, C. van 55, 59
Edmonds, J. 69, 503, 505
Egoritsjev, G.P. 110
Eğecioğlu, Ö. 16, 23
Elspas, B. 446, 450
Erdős, P. *Preface*, 5, 10, 33, 35, 51, 59, 216, 241, 301, 331, 418, 430, 433, 520, 544
Euler, L. 6, 10, 136, 157, 166, 182, 284, 290, 300, 465, 466, 480, 491, 497, 513 542, 573
Evans, T. 189, 197

Falikman, D.I. 110
Fan, K. 491, 505
Fano, G. 225, 240, 242, 492
Fekete, M. 103, 109
Ferrers, N.M. 166, 327
Fibonacci 150
Fisher, R.A. 222, 240, 558
Flye Sainte-Marie, C. 75, 76
Ford, L.R. 64, 66, 70
Fourier, J.B. 212
Frame, J.S. 165, 167, 553
Frankl, P. 59, 60, 331, 332
Franklin, F. 157, 167
Fréchet, M. 491, 505
Freeman, J.M. 553
Frobenius, G. 94, 167, 442, 568
Fulkerson, D.R. 64, 66, 69

Gale, D. 181
Galvin, F. 194, 197, 469
Gantmacher, F.R. 442, 450
Gardner, M. 521
Garey, M. 9, 10
Gauss, C.F. 97, 325, 332
Gelling, E.N. 537, 541

Gewirtz, A. 267, 281
Gödel, K. 458
Godlewski, P. 241
Godsil, C.D. 227, 281
Goethals, J.-M. 266, 279, 280, 281
Golay, M.J.E. 252, 259, 417, 429
Golomb, S.W. 204, 214
Gordon, B. 381, 382
Goulden, I.P. 150, 151
Graham, R.L. 32, 35, 78, 88, 332, 432, 521
Granell, M.J. 223, 242
Greene, C. 59, 60, 312, 334, 547
Griggs, T.S. 223, 242
Grinstead, C.M. 35
Grossman, J.W. 10
Grünbaum, B. 349, 350, 456, 457, 458
Gustin, W. 504, 506
Guthrie, Francis 465
Guthrie, Frederick 465

Hadamard, J. 213, 268, 375
Haemers, W. 280, 435, 450
Haken, W. 24, 34, 35, 466, 471
Hall, M. 51, 60, 196, 204, 214, 281, 298, 302, 319, 324, 383, 394, 395
Hall, P. 43, 51, 52
Halmos, P.R. 51, 52
Hamilton, W.R. 8, 10, 465
Hamming, R.W. 259, 406, 417
Harary, F. 535
Hardy, G.H. 166, 167
Hautus, M.L.J. 51
Heawood, P.J. 433, 466, 493, 494, 498, 505
Henrici, P. 582
Hickerson, D. 150
Higman, D.G. 267, 279, 281
Hilbert, D. 470
Hirschfeld, J.W.P. 358, 359, 368, 566
Hoffman, A.J. 41, 280, 282, 434, 440, 450, 561
Hoffman, D. 197
Hsieh, W.N. 331, 332
Hu, T.C. 70
Hubaut, X. 279, 282
Hughes, D.R. 321, 324

Ito, T. 413, 431

Jackson, D.M. 150, 151, 181, 280, 431
Jacobi, C.G.J. 167
Jeans, J.H. 519, 521
Johnson, D. 295, 302
Johnson, D.S. 9, 10
Johnson, S. 35, 406
Jones, B.W. 80, 88
Joyal, A. 141, 151
Jungnickel, D. 227, 242, 301, 404

Karp, R.M. 69
Katona, G.O.H. 59, 60
Keedwell, A.D. 197
Kempe, A.B. 466, 467, 470
Kirchhoff, G.R. 500, 515
Kirkman, T.P. 240, 242
Klarner, D.A. 132, 151
Klein, F. 285, 499
Kleitman, D.J. 59, 60, 547
Knuth, D. 87, 163, 167, 181
Ko, Chao 51, 331, 418, 430
Koch, J. 466, 470, 471
König, D. 51, 52
Körner, J. 258
Koornwinder, T.H. 280, 282
Kramer, E.S. 557
Krause, M. 172, 181

Orig. 587

Kreher, D.L. 224, 242
Krein, M.G. 267, 279, 280
Kronecker, L. 201, 268
Kruyswijk, D. 55, 59
Kuratowski, K. 462, 470

Lagrange, J.L. 145, 151, 230, 240, 582
Lam, C.W.H. 242
Lander, E.S. 394, 398, 404
La Poutré, J.A. 86, 88
Laurent, P.M.H. 579
Leavitt, D.W. 224, 242
Leeb, K. 332
Lenz, H. 301
Leonardo of Pisa 150
Lesniak, L. 462, 491, 505
Lewin, M. 35, 36
Lint, J.H. van 51, 52, 60, 86, 88, 108, 109, 110, 118, 166, 167, 259, 260, 279, 280, 281, 282, 431, 543, 546, 551, 552, 558
Lloyd, E.K. 466, 471
Lloyd, S.P. 425, 427, 431
Locke, S.C. 553
London, D. 114, 118
Lorentz, H.A. 118
Lovász, L. 41, 42, 436, 437, 438, 450, 546
Lubell, D. 54, 60
Lucas, F.E.A. 95, 97, 150

MacLane, S. 480, 490
MacMahon, P.A. 166, 167
MacNeish, H.F. 288, 290, 300, 302
MacWilliams, F.J. 248, 258, 259, 260
Magliveras, S.S. 224, 242
Maldeghem, H. Van 280, 282
Mann, H.B. 298, 302, 394, 395
Mantel, W. 37, 42
Marcus, M. 112, 114, 118
Mathieu, É. 260
Mathon, R. 280
Mattson, H.F. 249, 259, 260
McFarland, R.L. 381, 382
McKay, B.D. 176, 181, 277, 281
Medema, P. 520, 521
Mendelsohn, E. 537, 541
Mendelsohn, N.S. 295, 302
Menger, K. 454, 455, 458
Merkx, F. 241
Mesner, D.M. 264, 279, 280, 409
Mills, W.H. 223, 242, 381, 382
Minc, H. 101, 108, 109, 118
Mirsky, L. 54, 60
Möbius, A.F. 97, 333, 362
Moivre, A. de 108
Montmort, P.R. de 97
Moon, J.W. 108, 109
Moore, E.H. 300, 302
Morgan, A. de 465
Muir, T. 108
Muller, D.E. 199ff, 213, 214, 261
Muzychuk, M. 448

Narasima Sasbry, N.S. 571
Nešetřil, J. 521
Neumaier, A. 270, 272, 282, 407, 431
Neumann, P.M. 97
Newman, M. 112, 114, 118
Nichols, W. 553
Niderhausen, H. 553
Nienhuys, J.W. 582
Niven, I. 150, 151
Nordstrom, A.W. 419

Ohm, G.S. 515
Ostrand, P. 51, 52

Paige, L.J. 298, 302
Paley, R.E.A.C. 203, 213, 214, 262, 375
Paola, J. di 368
Pappus of Alexandria 318, 323
Parker, E.T. 284, 288, 301
Pasch, M. 314, 323
Payne, S.E. 280, 282
Pedoe, D. 319, 324
Peltesohn, R. 537, 541
Perron, O. 442
Petersen, J.P.C. 261, 433, 462, 465,477, 483, 491ff, 508, 542
Petrenjuk, A.Ya. 222, 242
Pierce, J.R. 88
Piper, F.C. 321, 324
Pless, V. 252, 260, 404
Plotkin, M. 212
Plücker, J. 239
Pollak, H.O. 78, 88, 432
Pólya, G. 522, 535
Posner, E.C. 213, 214, 557
Prüfer, H. 13, 23
Pulver, E.D. 535
Pythagoras 166

Rademacher, H. 166, 167
Rado, R. 51, 331, 418, 430
Radziszowski, S.P. 35, 36, 224, 242
Ramanujan, S. 166, 167
Ramsey, F.P. 28, 35, 36
Raney, G.N. 151
Ray-Chaudhuri, D.K. 222, 242, 367, 368, 425, 431
Reed, I.S. 213, 214, 361
Rees, G.M.J., van 294, 302
Remmel, J.B. 16, 23
Riemann, G.F.B. 97
Ringel, G. 493, 494, 502, 506
Roberts, S.M. 35
Robertson, N. 463
Robinson, J.P. 419
Rogers, D.G.E.D. 181
Rosa, A. 537, 541
Rota, G.-C. 151, 324, 349, 350, 378, 490, 564
Rothschild, B.L. 32, 33, 35, 332
Ryser, H.J. *Preface*, 99, 108, 109, 181, 187, 197, 213, 229, 230, 241, 292, 383, 394, 395, 398

Sachs, H. 450
Schellenberg, P.J. 294, 302
Schläfli, L. 275
Schönheim, J. 59, 60
Schrijver, A. 65, 101, 107, 108, 109, 280, 282, 355, 368, 537, 541
Schur, I. 22, 34, 544
Schutzenberger, M.P. 240, 242
Schwenk, A.J. 450
Scott, L.L. 279
Seberry, J. 213
Segner, J.A. von 136
Seidel, J.J. 266, 279, 280, 281, 282, 558
Seymour, P. 463
Shannon, C.E. 259, 260, 436
Shimamoto, T. 279
Shrikhande, S.S. 284, 288, 301, 561
Simonyi, G. 258
Sims, C.C. 267, 279, 281
Singer, J. 377, 378, 382
Singleton, R.R. 41, 561
Skolem, Th. 241, 242
Sloane, N.J.A. 258, 259, 260, 560
Smetaniuk, B. 189, 197
Smith, C. A. B. 520
Spencer, J.L. 33, 35, 59, 60, 332, 544

Sperner, E. 54, 59, 60, 326
Sprott, D.A. 376, 384
Stanley, R.P. 150, 151, 349, 350, 460, 471
Stanton, R.G. 376, 384
Staudt, K.G.C. von 240
Steiner, J. 217, 240, 242
Steinitz, E. 465, 470, 471, 486
Stinson, D.R. 284, 302
Stirling, J. 108, 128
Strauss, E.G. 301
Swiercz, S. 241
Sylvester, J.J. 96, 166, 432
Szegő, G. 535
Szekeres, G. 33, 35

Tait, P.G. 481–486, 490
Tarry, G. 284
Tarsy, M. 35
Teirlinck, L. 224, 242
Thas, J.A. 280, 287
Thiel, L. 242
Thomas, S. 330, 332
Thomassen, C. 469, 471
Thompson, J.G. 259, 260
Thompson, T.M. 258, 263
Thrall, R.M. 165, 167
Tits, J. 221, 242
Todd, J.A. 375
Turán, P. 38, 41, 42
Turner, J. 446, 450
Tutte, W.T. 457, 458, 462, 471, 483, 489, 490, 512, 517, 520
Tverberg, H. 53, 60

Valiant, W.G. 107, 109
Vallée-Poussin, C.J. De La 213
Vandermonde, A.-T. 163
Vanstone, S.A. 181, 227, 242, 280, 294, 302, 431
Vaughan, H.E. 51

Veblen, O. 279, 290
Vedder, K. 362
Voigt, M. 470
Voorhoeve, M. 105, 109

Waerden, B.L. van der 32, 36, 76, 110, 118, 197
Wald, A. 458
Wallis, J.S. 213, 214
Watkins, J.J. 10, 11
Watson, G.N. 151
Wedderburn, J.H.M 319, 402
Weisner, L. 335, 339, 350
Welch, L.R. 381, 382
Welsh, D.J.A. 490
White, A.T. 506
Whitney, H. 454, 458, 472ff, 490
Whittaker, E.T. 151
Wilbrink, H.A. 396, 404
Wilf, H. 450
Williamson, J. 204, 214
Wilson, R.J. 10, 11, 281, 466, 471
Wilson, R.M. 222, 242, 279, 282, 301, 302, 331, 334, 341, 350, 412, 430
Winkler, P. 80, 88
Witt, E. 223, 242, 397
Woolhouse, W.S.B. 240, 243
Wright, E.M. 160, 166, 167, 168

Yamamoto, K. 395
Young, A. 167, 168
Young, J.W. 313, 324
Youngs, J.W.T. 493, 494, 502, 506

Indice analitico

Le voci sono tradotte e ordinate alfabeticamente in italiano; le voci duplicate dell'originale sono riunite. I numeri si riferiscono alle pagine originali, riconoscibili dai richiami «Orig.» a margine. I numeri di pagina sono collegamenti cliccabili ai corrispondenti richiami nel testo. «ss.» significa «e seguenti». L'indice originale occupa le pagine 590–602.

1-fattore di un grafo 537
1-fattorizzazione di un grafo 537
1-scheletro di un politopo 456
2-disegni 224 ss., 311
2-disegno di Hadamard 218
3-artiglio 570
3-disegno di Hadamard 218, 220, 252
5-disegni 223, 242, 249, 252–253, 255, 266
6-disegni 224
Accoppiamento completo in un grafo bipartito 43 ss., 56
Accoppiamento in un grafo 43
Accoppiamento massimo 69
Accoppiamento perfetto 44, 546
Alberi e foreste radicati 15, 19, 145–146
Alberi piani piantati 139
Albero binario 139
Albero o foresta etichettati 12 ss., 141, 145
Albero piano 139
Albero ricoprente di costo minimo 18, 543
Albero ricoprente 12 ss., 81, 479, 507 ss., 519, 543, 548, 572, 574
Albero trivalente 139
Albero 6, 12–22, 77–80, 459
Alfabeto di un codice 244
Algebra booleana 303
Algebra di Bose–Mesner di un grafo fortemente regolare 264 ss.
Algebra di Bose–Mesner di uno schema 409 ss., 419, 430
Algebra di incidenza di un insieme parzialmente ordinato 333 ss.
Algebra semisemplice 402
Algoritmo goloso 18
Anello di gruppo 383 ss.
Antenato 20
Anticatena 53 ss., 327
Applicazione completa di un gruppo 298
Arborescenza ricoprente 16 ss., 512, 543
Arborescenza 15, 145
Archi di Jordan 472 ss.
Arco duale nei piani proiettivi 352–353
Arco massimale in un piano proiettivo 367
Arco perfetto 351–353, 367
Arco 351–353, 367
Artiglio 218, 500
Asse di prospettività 317

Assegnazione di liste 194
Assioma di Pasch 314 ss.
Assioma di scambio 309
Associati in uno schema 406 ss.
Automorfismo di Frobenius 568
Automorfismo di un albero 13
Automorfismo di un codice 260
Automorfismo di un disegno simmetrico 316, 329 ss., 379, 566
Automorfismo di un grafo 3, 422, 542, 569
Automorfismo di una mappa 499, 575
Autospazi 264, 410
Autovalore dominante 444
Autovalori di un grafo 264, 433 ss.
Bandiere di una struttura di incidenza 215
Base di un diagramma di Ferrers 158
Basi in una geometria combinatoria 310 ss.
Biplano 267
Blocchi base 236, 241
Blocchi di una struttura di incidenza 215
Blocchi ripetuti 215, 223
Blocco di formaggio 41
Bottiglia di Klein 499
Calcolo delle differenze finite 97
Cammini nel piano X,Y 122, 130, 138, 149, 552
Cammino aumentante; si veda anche cammino speciale 63, 69
Cammino chiuso semplice 5
Cammino chiuso 5
Cammino in un grafo 5
Cammino orientato 16
Cammino semplice 5, 25
Cammino speciale 63 ss.
Cancellazione di spigoli 459
Capacità di Shannon di un grafo 436–437
Capacità di un taglio 62 ss.
Capacità di uno spigolo 62 ss.
Cappio di un grafo 1
Carattere 202, 248, 394
Caratteristica di Eulero 497
Cardinalità dei blocchi di un t-disegno 216
Casella 162
Caso metà dei grafi fortemente regolari 265, 277
Catena di Kempe 467
Catena massimale in un insieme parzialmente ordinato 53–54, 306, 325
Catena simmetrica 55, 57, 58
Catena 53 ss., 305, 348
Centro di prospettività 317
Chiusura in una geometria combinatoria 308 ss.
Cicli di un grafo 475 ss.
Cicli di una permutazione 123, 127, 524 ss.
Ciclo completo 72–75
Ciclo elementare 514
Circolazione in un grafo orientato 66 ss.
Circuiti di un grafo 475 ss.
Circuito euleriano orientato 16, 71, 75
Circuito euleriano 6–9, 71, 513
Circuito hamiltoniano 8, 40–41, 449, 483, 545
Classe parallela di insiemi 537
Classe parallela in un piano affine 227, 273

Classe parallela in un sistema di Steiner 353
Coalbero 462, 473
Cocricca in un grafo 434–435, 440
Cocricca in uno schema 421
Coda di uno spigolo orientato 2, 460
Codice a distanza massima separabile (MDS) 248, 259, 347–348
Codice autoduale 246, 396 ss.
Codice binario di Golay 243, 252–255, 259, 417, 560
Codice binario 244
Codice correttore di errori 208, 244–246, 258–259
Codice di distanza d in uno schema metrico 422
Codice di Hamming 246–247, 376, 560
Codice di Nordstrom–Robinson 419
Codice di Prüfer 13
Codice di Reed–Muller del primo ordine 210–212, 361
Codice di ripetizione 209, 245
Codice di simmetria 252
Codice di un disegno 256–258, 396 ss.
Codice di un grafo 475 ss.
Codice duale 246
Codice esteso 246
Codice in uno schema 422
Codice lineare 244 ss., 398
Codice perfetto 245, 248, 250, 254, 259, 405, 425, 427, 430
Codice q-ario 244
Codice simplesso 247
Codice ternario di Golay 256, 417
Codice ternario 244
Codice trifferente 258
Codice 244 ss., 396 ss.
Codici autoortogonali 246, 396 ss.
Codici di Golay 241–244, 252–255, 259, 279, 417, 429, 560
Codici di Reed–Muller 210–213, 361, 560
Codici equivalenti 246
Codifica hash 84
Coefficienti gaussiani 325
Coefficienti multinomiali 16, 120
Colinea 309
Collane 94–95, 522, 525–530, 533
Collineari 272
Collineazione centrale 367
Collineazione di un piano proiettivo 353, 366
Colonna di un quadrato latino 182
Colorazione di Tait di un grafo 481–483
Colorazione propria di un grafo 24, 341, 459
Colorazioni degli spigoli 27
Colorazioni dei grafi 24, 306, 459 ss.
Combinazione convessa di matrici di permutazione 49, 111
Complementare di un disegno simmetrico 401
Complementare di un disegno 220, 251, 569
Complementare di un grafo 393, 563, 570
Complementare di un insieme di differenze 391
Complementare di una struttura di incidenza 215
Complemento modulare 314
Complessità di un grafo 460, 519
Completo per colonne 196
Completo per righe 196
Componente 5

Composizione di un numero 154, 553
Condizione di integrità per grafi fortemente regolari 265, 561
Condizione di Krein 267, 269, 273, 279, 280
Condizione sui vertici 497
Configurazione di Desargues 317
Configurazione o piano di Fano 225, 237, 255, 258, 354, 394, 430, 434, 492
Congettura di Dinitz 194, 469
Congettura di Eulero 281 ss., 288, 300
Congettura di Evans 189–193
Congettura di Heawood 493, 498
Congettura di Minc 101–103, 108
Congettura di Van der Waerden 104, 108, 110–118, 186, 197
Congiunzione di vertici in un grafo 1
Coniugata di una partizione 156, 169
Coniugati di un quadrato latino 183
Connettività di Tutte 451, 457, 458
Connettività di un grafo 451 ss.
Connettività per vertici 451
Conservazione del flusso 62
Conteggio in due modi 4, 207, 212, 219, 262
Contrazione di spigoli 462 ss.
Controesempio minimale 24–26
Coordinate omogenee 317
Copertura in un insieme parzialmente ordinato 303, 305, 335
Costo di uno spigolo 17
Cricca in un grafo 271, 435
Cricca in uno schema 421
Crivello di Lovász 31
Decodificare 209, 212
Derivata formale 145, 581
Derivazione 146
Determinante della matrice delle distanze 80
Determinante di Vandermonde 163
Diagramma di Ferrers 156 ss., 170–171, 327–328
Diagramma di Young 156
Dimensione di una geometria combinatoria 304
Dimostrazioni combinatorie di identità 121–122, 125, 138, 147, 552
Discendente 20
Disegni equivalenti 221
Disegni in uno schema 422
Disegni isomorfi 221
Disegni simmetrici 224, 299, 367, 369, 396 ss., 568
Disegni trasversali risolubili 291
Disegno a blocchi associativo 83 ss.
Disegno a blocchi incompleto bilanciato (BIBD) 217 ss.
Disegno a blocchi 217 ss.
Disegno combinatorio 351
Disegno derivato 228
Disegno di un grafo 1, 461
Disegno di Witt 223, 255, 256, 266
Disegno esteso 239
Disegno indotto 463
Disegno non immergibile 228–229, 240
Disegno parzialmente bilanciato 430
Disegno proiettivo 224
Disegno proprio di un grafo 461 ss.
Disegno quadrato 224
Disegno quasiresiduale 228, 275

Disegno quasisimmetrico 266, 275
Disegno residuo 228, 275
Disegno semplice 215 ss., 223
Disegno stretto (tight) 223, 425, 428
Disegno trasversale 273, 290, 563
Distanza di Hamming 77, 244
Distanza fra vertici 5
Distanza in un codice 244
Distanza minima di un codice 211, 244
Disuguaglianza di Cauchy 115
Disuguaglianza di Fisher 222, 226, 353, 364, 405, 430
Disuguaglianza di Wilson–Petrenjuk 222
Disuguaglianze di Delsarte 405, 416, 418
Dodecaedro 8, 492
Duale di un disegno simmetrico 228
Duale di Whitney di un grafo 472 ss.
Eccesso di una matrice di Hadamard 207
Enumeratore dei pesi di un codice 248
Estremi di uno spigolo 1
Estremo inferiore in un reticolo (meet) 305
Estremo superiore in un reticolo (join) 305 ss.
Etichettatura graziosa 22
Faccia di un grafo o di un'immersione 463
Faccia di un politopo convesso 456
Fattori invarianti 399
Fattoriale decrescente 119
Fibratura (spread) 320, 330
Flusso ammissibile 61 ss.
Flusso elementare 64
Flusso intero 64–66, 171, 540
Flusso massimo 62
Flusso 61
Foresta 17
Forma a scala 246, 327–328
Forma hermitiana 364 ss.
Forma normale di Smith 399
Forma quadratica ellittica 359 ss.
Forma quadratica iperbolica 359 ss.
Forma quadratica non degenere 356
Forma quadratica parabolica 359 ss.
Forma quadratica 78–80, 231, 355, 558, 559, 566
Forme hermitiane proiettivamente equivalenti 364
Forme quadratiche proiettivamente equivalenti 356 ss.
Formula di Eulero 349, 464, 465, 466, 480, 491, 542, 573
Formula di inversione di Lagrange 145, 151, 582
Formula di Stirling 32, 107, 108, 187, 208
Forza di uno schieramento ortogonale 423
Frazioni parziali 153, 553
Funzione delle partizioni 155 ss., 166
Funzione di discrepanza 82
Funzione di Eulero 92
Funzione di Möbius aritmetica 92–94, 333
Funzione di Möbius di un insieme parzialmente ordinato 333 ss., 344
Funzione eta di Dedekind 167
Funzione generatrice esponenziale 129 ss.
Funzione generatrice ordinaria 129
Funzione generatrice 126, 129 ss.
Funzione hash 84

Funzione razionale 132
Funzione zeta di Riemann 93, 97
Funzione zeta di un insieme parzialmente ordinato 333
Funzioni simmetriche 535
Ganci nelle tabelle di Young 165
Genere di una superficie 491
Genitore 20
Geometria affine 304
Geometria combinatoria connessa 313, 564
Geometria combinatoria modulare 313 ss.
Geometria combinatoria 306 ss.
Geometria parziale duale 272
Geometria parziale propria 273, 280
Geometria parziale 271 ss., 363
Geometria proiettiva 225, 303, 304, 313, 351
Geometrie dei cerchi 365
Gradi di uno schema 406
Grado di un vertice 4
Grado di una faccia 465
Grafi di Chang 271, 280
Grafi di De Bruijn 71 ss.
Grafi di tipo quadrato latino negativo 414
Grafi estremali 38–40
Grafi isomorfi 2, 411, 466
Grafi omeomorfi 453
Grafo 3-connesso 483–484
Grafo a fascio 451, 473
Grafo bipartito completo 6, 39, 432
Grafo bipartito regolare 44
Grafo bipartito 24, 43, 55, 69, 196, 324
Grafo circolante 446, 448
Grafo colorato per liste 194
Grafo completo 3, 12, 24, 27–28, 30, 33, 37 ss., 78, 217, 261, 432, 491, 492, 494, 500, 502, 508, 540
Grafo connesso 5–6, 347, 451
Grafo degli spigoli (line graph) 194, 435–436, 570
Grafo dei blocchi di un disegno 266
Grafo dei punti di una geometria parziale 272
Grafo di Cayley 446, 504–505
Grafo di Clebsch 263, 276, 279, 440, 447, 498, 505, 575
Grafo di dipendenza 31
Grafo di Gewirtz 267
Grafo di Heawood 433, 434, 492
Grafo di Higman–Sims 267, 279
Grafo di Hoffman–Singleton 41
Grafo di Paley 262, 265
Grafo di Petersen 9, 40, 261, 263, 276, 430, 433–434, 436, 449, 462, 465, 477, 483, 485, 486, 491, 492, 508, 542, 570, 572
Grafo di Schläfli 275
Grafo di un politopo 456
Grafo di un quadrato latino 274, 276, 414
Grafo dispari (odd graph) 430
Grafo duale 466 ss., 472 ss.
Grafo etichettato 12, 149
Grafo euleriano 6
Grafo finito 4
Grafo fortemente regolare connesso 261
Grafo fortemente regolare 261 ss., 405, 407, 449
Grafo geometrico 272

Grafo k-connesso 451
Grafo multipartito completo 38
Grafo non separabile 451 ss., 483 ss., 499
Grafo orientato fortemente connesso 442
Grafo orientato semplice 2
Grafo orientato 2, 194, 454
Grafo pesato 17, 434
Grafo planare 1, 461 ss., 479, 480
Grafo pseudogeometrico 272, 280
Grafo regolare nei vicinati 277
Grafo regolare rispetto alla distanza 407
Grafo regolare 4, 40, 149, 422, 445
Grafo reticolare 262
Grafo semplice 2
Grafo triangolare 262, 270, 275
Grafo trivalente 481–482, 546, 551, 574
Grafo 1
Grafo-spigolo 451, 471, 453
Grande cricca in un grafo fortemente regolare 271, 280, 561
Gruppi di Mathieu 259, 560
Idempotenti nell'algebra di Bose–Mesner 236, 410
Idempotenti nell'anello di gruppo 402
Idempotenti ortogonali di uno schema 410
Identità del triplo prodotto di Jacobi 160
Identità di Eulero 157
Immersione cellulare di un grafo 463, 473, 494–495
Immersione di un grafo 461 ss.
Immersione triangolare di un grafo 500, 505
Incidenza in un grafo 1
Inclusione ed esclusione 89–97, 98, 122, 177, 337, 535, 549, 556
Incontri di tennis 563
Indice ciclico 524
Indice di un disegno 216
Indice di uno schieramento ortogonale 216, 423
Insieme bloccante in un piano proiettivo 355
Insieme di differenze ciclico 373 ss., 386, 567
Insieme di differenze di Hadamard 375–377, 380, 569
Insieme di differenze non banale 372
Insieme di differenze normalizzato 374, 388
Insieme di differenze planare 372, 388–389, 396, 403
Insieme di differenze semplice 372
Insieme di differenze 369 ss., 389 ss.
Insieme indipendente 37
Insieme parzialmente ordinato (poset) 53, 333 ss.
Insieme parzialmente ordinato duale 307
Insieme parzialmente ordinato euleriano 350
Insieme quoziente 372–373
Insieme sferico a due distanze 269
Insiemi di differenze di Paley–Todd 375–377
Insiemi di differenze di Singer 378–380
Insiemi di differenze di Stanton–Sprott 376
Insiemi di differenze equivalenti 374
Insiemi di differenze isomorfi 380
Instant Insanity 7
Interlacciamento degli autovalori 439–440, 561, 571
Interrogazione a corrispondenza parziale 84
Intervallo di un insieme parzialmente ordinato 307
Inversione di Möbius 93, 136, 298, 333, 336, 337, 339, 346, 347, 370

Involuzione 323
Ipercubo 77
Ipergrafo uniforme completo 540
Iperovale 227, 248, 255, 258, 266–267, 274
Iperpiani nelle geometrie combinatorie 309 ss.
Iperpiano affine 211
Iperpiano di supporto 446
Istmo di un grafo 20, 482
k-connettività di Tutte 457, 489
k-connettività per vertici 451, 454
Legame di un grafo 475 ss.
Legge di Ohm 515
Legge di Sylvester 96, 432
Legge modulare 313
Legge semimodulare 311
Leggi di Kirchhoff 500, 515
Lemma di Block 371
Lemma di Burnside 94, 97, 370, 524
Lemma di Fekete 103, 106, 108, 130, 150, 436
Limite assoluto per grafi fortemente regolari 270, 273
Limite dell'artiglio 272–273
Limite dell'impacchettamento di sfere 245, 419, 425
Limite della programmazione lineare 406, 418, 419
Limite di Hamming 245
Limite di Plotkin 212
Limite di Singleton 247
Linea di una matrice 48
Lunghezza di una passeggiata 5
Lunghezza di uno spigolo 17
Lunghezze dei ganci 165–166
Maggiorazione di vettori 169–170
Maglia di un grafo (girth) 9, 39–40
Maglia di un grafo immerso (mesh) 494
Maglia orientabile 497
Maglia triangolare 494
Manico di una rappresentazione 437
Mappa su una superficie 491
Matrice completamente indecomponibile 111
Matrice delle distanze di un grafo 79–80
Matrice di adiacenza di un grafo orientato 432
Matrice di adiacenza di un grafo 263 ss., 391–402, 449 ss.
Matrice di adiacenza di un multigrafo 507
Matrice di adiacenza di un torneo 432
Matrice di adiacenza di uno schema 409
Matrice di conferenza 200 ss., 233, 265, 402
Matrice di controllo di parità di un codice 246
Matrice di Hadamard normalizzata 199
Matrice di Hadamard regolare 208, 218, 226, 375
Matrice di Hadamard 199 ss., 218, 279, 411–412, 424
Matrice di incidenza di un disegno simmetrico 228 ss.
Matrice di incidenza di un disegno 221 ss., 225
Matrice di incidenza di un grafo orientato 62, 509
Matrice di incidenza di un grafo 475
Matrice di incidenza 221
Matrice di Paley 203, 252–253, 256, 374
Matrice di Vandermonde 251
Matrice doppiamente stocastica 49, 104, 108, 110 ss.
Matrice generatrice di un codice 246, 570

Matrice irriducibile 442
Matrice minimizzante 110 ss.
Matrice parzialmente decomponibile 111
Matrici (0,1) 48, 100 ss., 169 ss.
Matrici degli autovalori di uno schema 413, 415
Matrici di associazione di uno schema 409 ss.
Matrici di incidenza superiori di un t-disegno 222
Matrici di permutazione 48, 83, 114, 148, 205, 221, 193, 329
Matrici non negative 111 ss., 442 ss.
Matrici totalmente unimodulari 510
Matroide 324, 489, 490
Memoria scrivibile una sola volta 237
Metodi algebrici 264, 267, 432 ss.
Metodi delle differenze 234, 240, 288, 294 ss., 498
Metodi di composizione 288
Metodi di crivello 96
Metodo delle differenze si vedano metodi delle differenze
Metodo di Williamson 204, 206
Metodo probabilistico 30–32, 35, 544
Metodo ricorsivo 201, 233
Minore di un grafo 462
Molteplicità di uno schema 411
Moltiplicatore di Hall 386
Moltiplicatore di un insieme di differenze 386 ss.
Moltiplicatore numerico di un insieme di differenze 386
Multigrafo 2
NP-completo 9
Numeri di Bell 125, 149
Numeri di Catalan 136–141, 150, 16
Numeri di Stirling senza segno 123, 534
Numeri di Stirling 123–127, 534
Numeri gaussiani 312, 325 ss.
Numeri o successione di Fibonacci 97, 149, 150, 550
Numeri pentagonali 157
Numero cromatico 24, 327, 398, 466, 571
Numero dei quadrati latini 186–187, 192
Numero delle suriezioni 90, 125, 337
Numero di Erdős 5, 10
Numero di indipendenza di un grafo 436
Numero di replicazione 219, 240, 430
Omomorfismi dell'anello di gruppo 385 ss.
Operazione di prodotto non associativa 136
Orbite di un gruppo 95, 370, 407, 523, 528, 530, 532
Ordine di raffinamento sulle partizioni 307
Ordine di un piano proiettivo 225
Ordine di una matrice di Hadamard 199
Ordine di uno schieramento ortogonale 183
Ordine lineare 53
Ordine totale 53
Orientazione bilanciata di un grafo 68
Orientazione di un grafo 21, 460
Orientazioni acicliche di un grafo 461
Ortomorfismo di un gruppo abeliano 297–298, 339
Ovale in un disegno simmetrico 367
Ovale in un piano proiettivo 227, 381
Ovoide nello spazio proiettivo tridimensionale 362, 394
Parametri ammissibili per grafi fortemente regolari 265
Parametri di Krein di uno schema 420

Parametri di uno schema 406
Parole confondibili 436
Parole di codice 244
Partizione non ordinata 152
Partizioni autoconiugate 162
Partizioni di un insieme 49, 106–107, 126, 537 ss.
Partizioni di un numero 152 ss., 169, 327–329
Passeggiata chiusa 5, 515
Passeggiata in un grafo 5
Passeggiate nel piano X,Y 122, 130, 138, 149, 552
Pendenza di un diagramma di Ferrers 158
Permanente di una matrice 98 ss., 549
Permanenti di matrici (0,1) 100–104
Permanenti di matrici intere non negative 105 ss.
Permutazione complementante 342
Peso di una parola di codice 244
Peso minimo 245
Piani desarguesiani 319, 352
Piani pappiani 319
Piano affine di traslazione 320
Piano affine 227, 273, 287
Piano all'infinito 367
Piano di Möbius 362
Piano di traslazione 320, 331
Piano inversivo 362
Piano proiettivo reale 226, 492, 496
Piano proiettivo 225, 232, 256, 280, 287, 290, 313, 351–355, 396
Pioggia in Olanda 97
Poligono convesso di n lati 33, 139, 146
Poligono di n lati 6, 153, 460
Poligono 5, 83, 475
Polinomi gaussiani 326
Polinomio cromatico 341, 349, 459
Poliomino orizzontalmente convesso 132
Poliomino 132, 150
Politopo convesso 336, 349, 456, 465, 486
Ponte 20, 482
Ponti di Königsberg 6, 7, 10, 59
Poset si veda insieme parzialmente ordinato; 53, 333 ss.
Pozzo in una rete di trasporto 61
Principio dei cassetti 55, 559
Principio di riflessione di André 118
Principio di sostituzione 114, 117
Problema degli incontri 97
Problema dei 36 ufficiali 284
Problema dei ménages 95, 549
Problema dei quattro colori 459 ss.
Problema del tamburo rotante 71
Problema dell'indirizzamento 77 ss.
Problema della commutazione ad anello 88
Problema delle 15 scolarette 240
Problema delle scolarette di Kirkman 240
Problema dello scrutinio 150
Prodotto di Hadamard di matrici 268–269, 409, 415, 419
Prodotto di Kronecker 201, 208, 213, 268, 287, 309, 437
Prodotto forte di grafi 436
Prodotto interno o scalare 115–116, 396 ss., 415
Profondità di uno schieramento ortogonale 183

Progettazione degli esperimenti 240
Programmazione lineare 69, 457
Progressione aritmetica 32
Prospettività da un punto 317
Prospettività da una retta 317
Punti fissi di un automorfismo 353, 369
Punto di un reticolo 305
Punto di una geometria combinatoria 303, 309
Punto di una struttura di incidenza 215
q-analoghi 326, 337, 408
Quadrangolo generalizzato 273–274, 280, 363, 367
Quadrati latini a due a due ortogonali 285, 300
Quadrati latini equivalenti 183
Quadrati latini isomorfi 183
Quadrati latini mutuamente ortogonali 300
Quadrati latini ortogonali 283 ss., 563
Quadrato greco-latino 284
Quadrato latino parziale 185
Quadrato latino unipotente 288
Quadrato latino 182 ss., 226, 273, 358
Quadrato magico 300
Quadrato quadrato 507
Quadrica ellittica 359 ss.
Quadrica iperbolica 359 ss.
Quadrica nello spazio proiettivo 356 ss., 566
Quadrica parabolica 359 ss.
Quasi fascio (near pencil) 216, 313, 354
Quasigruppo idempotente 28 ss.
Quasigruppo 182, 288 ss.
Quoziente di Rayleigh 434
Raggio di ricoprimento 245, 247
Rango di un grafo connesso 453
Rango di un sottospazio chiuso 309
Rango di una forma hermitiana 364
Rango di una forma quadratica 356
Rango in una geometria combinatoria 309 ss.
Rappresentazione ortonormale di un grafo 437
Rappresentazione ottimale di un grafo 437
Regioni di un'immersione 463, 472
Relazione binaria su un insieme 406
Relazione di ricorrenza 124, 134 ss., 159, 329
Relazioni di MacWilliams 249
Relazioni di ortogonalità 415
Rete come geometria parziale (net) 273, 280, 286, 287, 563
Rete di trasporto 61 ss., 170, 538
Rete elettrica 507, 514, 515
Rete speciale 517
Reticolo atomico 305
Reticolo come insieme parzialmente ordinato 305 ss., 333 ss.
Reticolo delle contrazioni 308, 340
Reticolo delle partizioni 307–308, 336, 344–346
Reticolo geometrico 305 ss., 340, 342, 490, 564
Reticolo semimodulare 306 ss., 342
Retta di prospettività 317
Retta di un disegno a blocchi 323
Retta di un piano proiettivo 225
Retta di uno spazio lineare 215
Rettangolo latino 186

Rettangolo quadrato 516 ss.
Ricolorazione 24, 467
Ricorrenza di Fibonacci 150, 159, 551
Ricorrenza lineare 130–134
Riga 182
Ripetizione 177
Risposte semplici 288
Rotazioni del cubo 526, 577
Schema ciclotomico 408
Schema cometrico 422
Schema di associazione a k classi 406
Schema di associazione 279, 405 ss.
Schema di Hamming 406, 411 ss.
Schema di Johnson 406, 413 ss.
Schema metrico 407, 422
Schema P-polinomiale 422
Schema polinomiale 422
Schema Q-polinomiale 422
Schema 405 s.
Schemi formalmente duali 420
Schieramenti ortogonali isomorfi 183
Schieramento ortogonale 182, 294, 423
Scompigli 90, 97, 129, 142, 149
Semidefinita positiva o definita positiva 223, 435, 439
Semiregolarità 44
Serie di Laurent 579, 581
Serie enumeratrice delle configurazioni 528
Serie formali di potenze 130–151, 578 ss.
Simbolo di controllo di parità 246
Simbolo 182
Sistema di passeggiate in un grafo 487 ss.
Sistema di rappresentanti distinti (SDR) 43 ss., 100, 106–108, 186
Sistema di Steiner generalizzato 238–239, 304
Sistema di Steiner risolubile 353
Sistema di Steiner 216 ss., 221, 223, 303, 351 ss., 362, 364–365
Sistema di terne di Steiner 233–241, 276, 278
Sistemi di rappresentanti distinti e permanenti 100
Solidi platonici 465, 499, 573
Somma di riga 169
Somme di linea delle matrici (0,1) 100–101, 173–181
Sorgente in una rete di trasporto 61
Sostituzione di serie di potenze 579
Sottogeometria 304
Sottografo indotto 4, 77
Sottografo ricoprente 4
Sottografo 4
Sottoinsieme generatore in geometrie combinatorie 310
Sottoinsieme indipendente di una geometria combinatoria 309 ss.
Sottopiano di Baer 255, 355, 394
Sottopiano di un piano proiettivo 353 ss.
Sottoquadrati di quadrati latini ortogonali 298
Sottoquadrato di un quadrato latino 185
Sottoquadrato latino 185
Sottospazi chiusi (flat) 303, 309, 315
Sottospazio affine 304
Sottospazio di dimensione k 325
Sottostruttura di una struttura di incidenza 353
Sottosuccessione monotona 55

Spazio dei cicli di un grafo orientato 514
Spazio dei cicli di un grafo 453
Spazio dei cobordi di un grafo orientato 514
Spazio dei tagli di un grafo 476 ss.
Spazio di Lorentz 115–118
Spazio lineare 215, 289 ss., 303, 313
Spigoli di un grafo 1
Spigoli indipendenti in un grafo 18
Spigoli multipli 2
Spigoli paralleli 2
Spigolo aciclico 482
Spigolo saturo 63 ss.
Struttura di incidenza 215
Successione di Ford 75
Successioni circolari 94–95, 120
Successioni di De Bruijn 71 ss., 513
Successioni di Skolem 241
Suddivisione di un grafo 452 ss.
Supporto di una parola di codice 249, 475
t-disegni 216 ss., 223, 249–253, 255, 266, 330, 405, 423
Tabella di Young 162–167
Tabelle standard 162
Tagli di un grafo 475 ss.
Taglio in una rete di trasporto 62
Taglio minimo 64 ss.
Tangente 367
Tasso di informazione 209
Teorema cinese del resto 293
Teorema dei cinque colori 34, 466, 469
Teorema dei matrimoni 43, 65
Teorema dei moltiplicatori 386 ss., 390 ss.
Teorema dei quattro colori 24, 34, 427, 466, 482
Teorema dei rappresentanti distinti si veda teorema di Hall
Teorema dei sei colori 467
Teorema del flusso massimo e taglio minimo 64, 171, 540
Teorema dell'amicizia 279
Teorema della curva di Jordan 464
Teorema di Assmus–Mattson 249
Teorema di Baranyai 536 ss.
Teorema di Birkhoff 48, 65, 111
Teorema di Brooks 24, 34
Teorema di Bruck–Ryser–Chowla 230, 241, 383, 398
Teorema di Cauchy–Binet 508, 510
Teorema di Cayley 12 ss., 145, 508
Teorema di De Bruijn–Erdős 216, 433
Teorema di Desargues 318, 321, 322
Teorema di Dilworth 53, 55
Teorema di Erdős–Ko–Rado 56, 59, 331, 418, 430
Teorema di Hall 43–47, 65
Teorema di König 48, 51
Teorema di Kuratowski 462
Teorema di Lloyd 405, 427
Teorema di MacWilliams 248, 418
Teorema di Mantel 37
Teorema di Menger 454, 455
Teorema di Pappo 318
Teorema di Perron–Frobenius 442–443
Teorema di Ramsey 27 ss., 37, 332

Teorema di Ringel–Youngs 494
Teorema di Schröder–Bernstein 51
Teorema di Singer 377, 381
Teorema di Sperner 54, 56, 59, 326, 484
Teorema di Turán 37 ss.
Teorema di Weisner 335, 339, 344
Teorema di Whitney 479, 480
Teorema e congettura di MacNeish 288, 290
Teorema matrice-albero 507
Teoremi formalmente duali 424
Teoria dei codici 244 ss.
Teoria dei disegni 215
Teoria di Joyal 141 ss.
Teoria di Pólya 522 ss.
Teoria estremale degli insiemi 56, 59
Testa di uno spigolo orientato 2, 460
Tipo di una partizione di un insieme 346, 526
Tipo di una permutazione 370, 525–528
Torneo transitivo 33
Torneo 33, 432
Toro di genere g 491
Toro 492
Totalmente isotropo 397
Trasformata veloce di Fourier 212
Triangoli in un grafo 27, 37–39, 543, 544
Triangoli monocromatici 27–28
Unitale 365
Valenza di un vertice 4
Valore di un flusso 62
Varietà hermitiana 364 ss.
Varietà sperimentali 240
Vertice di grado uno 13
Vertice isolato 1
Vertici adiacenti in un grafo 4
Vertici di un grafo 1
Vertici indipendenti in un grafo 37, 434–435
Vettore di distribuzione in uno schema 406, 416–417
Vettore isotropo 115
Vettori positivi e negativi 115
Vicini di un vertice 4
Visita in ampiezza 19, 81
Visita in profondità 19, 81