Matematica Discreta

basato sull'omonimo corso
tenuto dai proff. Roberto Dvornicich e Giovanni Gaiffi

Anno Accademico 2014/15 - II semestre

Oscar Papini

Indice

Simboli e notazioni utilizzati

$\mathbb{N}$	Insieme dei numeri naturali ($0 \in \mathbb{N}$)
$\mathbb{K}, \mathbb{F}_q$	Campo, campo finito con q elementi
$\mathcal{M}_{m\times n}(R)$	Spazio delle matrici $m \times n$ a coefficienti in R
$\mathcal{S}_n, \mathcal{A}_n$	Gruppo simmetrico, gruppo alterno su n elementi
S^n, D^n	Sfera, disco (chiuso) n-dimensionali
$R[X]$, $R(X)$, $R[\![X]\!]$	Polinomi, funzioni razionali, serie formali a coefficienti in R (X può essere un insieme arbitrario di indeterminate)
$\mathcal{H}om(V, W)$	Spazio degli omomorfismi da V in W
$\mathcal{E}nd(V)$	$= \mathcal{H}om(V, V)$, spazio degli endomorfismi di V
$\mathsf{GL}(V)$	Gruppo generale lineare di V (gruppo degli automorfismi lineari di V)
$\mathsf{GL}_n(\mathbb{K})$	$= \mathsf{GL}(\mathbb{K}^n)$ visto come sottogruppo di $\mathcal{M}_n(\mathbb{K})$
$\mathrm{rk}(A)$	Rango di A
$\mathrm{tr}(A)$	Traccia di A
$\mathrm{sp}(A)$	Spettro di A, cioè $\{\lambda \mid \lambda \text{ autovalore per } A\}$
$\mathrm{sgn}(\sigma)$	Segno di σ
$\#(V)$	Cardinalità dell'insieme V
$\wp(V)$, $\wp_k(V)$	Insieme delle parti di V, insieme delle parti di V di cardinalità k
$A \sqcup B$	Unione disgiunta di A e B
$\langle V \rangle$	Struttura generata dall'insieme V (dipende dal contesto)
$\langle\, \mathbf{a}, \mathbf{b} \,\rangle$	Prodotto scalare tra $\mathbf{a}$ e $\mathbf{b}$
$\mathrm{GCD}(a, b)$	Massimo comun divisore fra a e b
o, $\mathcal{O}$	Notazione o-piccolo, o-grande

Nota. Le variabili indicate in corsivo (come x) indicano oggetti con una sola componente, quelle in grassetto (come $\mathbf{x}$) indicano oggetti con più componenti, come vettori o n-uple. Incognite o valori precisi sono generalmente indicati in minuscolo, mentre le indeterminate dei polinomi sono sempre indicate in maiuscolo.

Una versione duale di un teorema ha lo stesso numero del teorema a cui si riferisce, seguito da un asterisco. Le versioni duali non sono dimostrate.

Introduzione

Questo testo è basato sul corso di *Matematica Discreta* tenuto dai proff. Roberto Dvornicich e Giovanni Gaiffi durante il secondo semestre dell'anno accademico 2014/2015. Esso ripercorre quanto svolto durante il corso, seguendo la traccia degli appunti presi in classe.

Purtroppo per problemi di sovrapposizione di orario non mi è stato possibile seguire tutte le lezioni del corso; ringrazio perciò tutti coloro che mi hanno permesso di usare i loro appunti per completare il lavoro, in ordine rigorosamente alfabetico: Elena, Francesca, Gianluca, Giulio, Pia e Sabino.

Ovviamente mi assumo ogni responsabilità per gli eventuali errori presenti nel testo: invito chiunque ne trovi, sia di natura concettuale che ortografica, a segnalarmeli.

Oscar Papini
papini@dm.unipi.it

Ultima revisione: 11 febbraio 2016

Capitolo 1

Funzioni generatrici

In questo capitolo ci occuperemo di *funzioni generatrici* associate a una successione (che nel nostro caso sarà definita da un qualche problema combinatorio). Le funzioni generatrici sono un modo condensato di rappresentare l'informazione combinatoria contenuta in una successione numerica; tuttavia la loro forma permette, attraverso opportune manipolazioni algebriche, di studiare le proprietà della successione pur non avendo necessariamente, ad esempio, una formula chiusa per l'n-esimo termine. ▹ *23/02/2015*

Nonostante la prima sezione rappresenti solo un'infarinatura di quello che studieremo, per comprenderla meglio introduciamo subito gli oggetti protagonisti del capitolo.

Definizione 1.1. Sia $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ una successione. Definiamo *funzione generatrice (ordinaria)* di $\mathbf{a}$ la serie formale

$$A(X) := \sum_{n=0}^{\infty} a_n X^n. \tag{1.1}$$

Definizione 1.2. Sia $\mathbf{b} = (b_n)_{n\in\mathbb{N}}$ una successione. Definiamo *funzione generatrice esponenziale* di $\mathbf{b}$ la serie formale

$$B(X) := \sum_{n=0}^{\infty} \frac{b_n}{n!} X^n. \tag{1.2}$$

1.1 Primi esempi

In questa sezione presenteremo una breve carrellata di esempi che useranno tecniche descritte più avanti. È utile comunque iniziare in questo modo per avere già in partenza un'idea di ciò che affronteremo.

Esempio 1.1 (Successioni ricorrenti I). Vediamo un primo esempio di successione definita per ricorrenza.

$$\begin{cases} a_0 = 0 \\ a_{n+1} = 2a_n + 1 \quad \text{per } n \in \mathbb{N}. \end{cases}$$

Calcoliamo un po' di termini: $a_0 = 0$, $a_1 = 1$, $a_2 = 3$, $a_3 = 7$, $a_4 = 15\ldots$ Ci sembra di riconoscere un *pattern*:

$$a_n = 2^n - 1. \tag{1.3}$$

Come possiamo dimostrare che la formula chiusa (1.3) è corretta? In questo caso è facile per induzione; vediamo invece come usare le funzioni generatrici.

Dalla formula ricorsiva otteniamo

$$\sum_{n=0}^{\infty} a_{n+1} X^n = 2 \sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} X^n$$

cioè (osservando che la prima sommatoria è $A(X)$ traslata, mentre la terza è una serie geometrica formale)

$$\frac{A(X) - a_0}{X} = 2A(X) + \frac{1}{1-X}$$

da cui (ricordando che $a_0 = 0$)

$$A(X) = \frac{X}{(1-X)(1-2X)}.$$

Ora imponiamo che

$$\frac{X}{(1-X)(1-2X)} = \frac{\alpha}{1-X} + \frac{\beta}{1-2X}$$

per qualche α, β. Un semplice conto mostra che

$$A(X) = \frac{X}{(1-X)(1-2X)} = \frac{1}{1-2X} - \frac{1}{1-X} = \sum_{n=0}^{\infty} 2^n X^n - \sum_{n=0}^{\infty} X^n = \sum_{n=0}^{\infty} (2^n - 1) X^n$$

e possiamo dunque concludere che la formula (1.3) è corretta.

Esempio 1.2 (Successioni ricorrenti II). Nell'esempio precedente la formula chiusa già si intuiva dopo pochi termini. Vediamone un altro meno evidente.

$$\begin{cases} a_0 = 1 \\ a_{n+1} = 2a_n + n \quad \text{per } n \in \mathbb{N}. \end{cases}$$

Sostituendo la definizione per ricorrenza nella funzione generatrice abbiamo

$$\sum_{n=0}^{\infty} a_{n+1}X^n = 2\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} nX^n.$$

A questo punto ci accorgiamo che

$$nX^n = X \cdot nX^{n-1} = X \cdot \frac{d}{dX}(X^n)$$

dunque

$$\frac{A(X)-1}{X} = 2A(X) + X\frac{d}{dX}\frac{1}{1-X} = 2A(X) + \frac{X}{(1-X)^2},$$

da cui con pochi conti

$$A(X) = \frac{1-2X+2X^2}{(1-X)^2(1-2X)} = \frac{2}{1-2X} - \frac{1}{(1-X)^2}.$$

Ricordiamo che la serie binomiale è

$$(1+X)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} X^n,$$

dove compare il coefficiente binomiale generalizzato

$$\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

in cui α è un qualsiasi numero complesso. Nel nostro caso abbiamo

$$(1-X)^{-2} = \sum_{n=0}^{\infty} \binom{-2}{n} (-1)^n X^n$$

ed esplicitando il coefficiente binomiale

$$\binom{-2}{n} = \frac{(-2)(-3)\cdots(-n-1)}{n!} = (-1)^n(n+1)$$

arriviamo infine a

$$A(X) = 2\sum_{n=0}^{\infty} 2^n X^n - \sum_{n=0}^{\infty} (n+1)X^n.$$

Il generico termine della successione è allora $a_n = 2^{n+1} - n - 1$.

1.1.1 I numeri di Fibonacci

La successione di Fibonacci è definita da

$$\begin{cases} f_0 = 0 \\ f_1 = 1 \\ f_{n+2} = f_{n+1} + f_n \quad \text{per } n \in \mathbb{N}. \end{cases}$$

La funzione generatrice $F(X)$ si ottiene facilmente dalla terza equazione:

$$\sum_{n=0}^{\infty} f_{n+2} X^n = \sum_{n=0}^{\infty} f_{n+1} X^n + \sum_{n=0}^{\infty} f_n X^n$$

cioè

$$\frac{F(X) - f_1 X - f_0}{X^2} = \frac{F(X) - f_0}{X} + F(X)$$

da cui concludiamo

$$F(X) = \frac{X}{1 - X - X^2}.$$

La successione di Fibonacci è un caso particolare di *ricorrenza lineare*, cioè una successione definita da

$$\begin{cases} a_0 = \alpha_0 \\ \vdots \\ a_{k-1} = \alpha_{k-1} \\ a_{j+k} = \displaystyle\sum_{i=0}^{k-1} r_i a_{j+i} \qquad \text{per } j \in \mathbb{N} \end{cases} \tag{1.4}$$

in cui sono fissate le condizioni iniziali $\alpha_0, \ldots, \alpha_{k-1}$. Vediamo solo un accenno di questa teoria, dal momento che anche per lo studio delle ricorrenze lineari useremo le funzioni generatrici.

Definizione 1.3. Data una ricorrenza lineare della forma (1.4), definiamo *polinomio caratteristico* il polinomio

$$p(X) := X^k - (r_{k-1} X^{k-1} + \cdots + r_0).$$

Proposizione 1.4. *Se il polinomio caratteristico ha k radici distinte $\gamma_1, \ldots, \gamma_k$, allora il termine generale della successione per ricorrenza lineare è*

$$a_n = c_1 {\gamma_1}^n + \cdots + c_k {\gamma_k}^n$$

dove i coefficienti $c_1, \ldots, c_k$ sono determinati dalle condizioni iniziali.

La proposizione precedente non è più vera nel caso in cui $p(X)$ abbia radici multiple. Ad esempio, è possibile dimostrare che se $p(X) = (X-2)^2(X-3)$, il termine generale è $a_n = c_1 2^n + n c_2 2^n + c_3 3^n$. In effetti, se γ_t è una radice di molteplicità m_t, abbiamo

$$a_n = \cdots + \lambda_{m_t-1}(n)\gamma_t{}^n + \cdots$$

in cui $\lambda_{m_t-1}(n)$ è un polinomio di grado $m_t - 1$ in n.

1.1.2 Partizioni

In questa sezione ci poniamo la seguente domanda: fissati n e k, in quanti modi è possibile partizionare l'insieme $\{1, \ldots, n\}$ in esattamente k sottoinsiemi non vuoti? Indichiamo con

$$\left\{ n \atop k \right\}$$

questo numero, e poniamo per convenzione

$$\left\{ 0 \atop 0 \right\} = 1, \quad \left\{ n \atop 0 \right\} = 0 \text{ per } n > 0, \quad \left\{ 0 \atop k \right\} = 0 \text{ per } k > 0.$$

Ad esempio: in quanti modi possiamo spezzare in due parti un insieme di 5 elementi? Possiamo separare $\{1, \ldots, 5\}$ in

- $1 + 4$ elementi in $\binom{5}{1} = 5$ modi;
- $2 + 3$ elementi in $\binom{5}{2} = 10$ modi;

per un totale di

$$\left\{ 5 \atop 2 \right\} = 15.$$

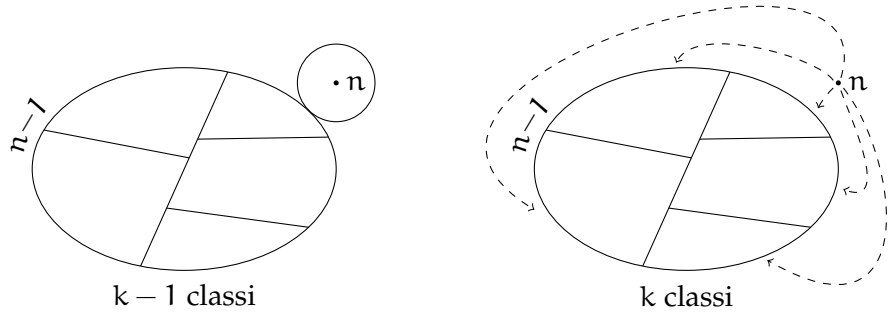
In generale è un calcolo abbastanza complicato, inoltre questi numeri crescono molto velocemente al crescere di n e k. Tuttavia soddisfano una relazione per ricorrenza abbastanza semplice. In effetti, possiamo considerare $\{1, \ldots, n\} = \{1, \ldots, n-1\} \cup \{n\}$; di conseguenza, le partizioni di n elementi in k classi sono date dalla somma di:

1. le partizioni in cui $\{n\}$ è una classe, che sono tante quante le partizioni di $n-1$ in $k-1$ classi;
2. le partizioni di $n-1$ in k classi, in cui ne scegliamo una in cui mettere n (ed abbiamo k possibili scelte).

In altre parole, vale che

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

(si veda anche la Figura 1.1).



(a) $\{n\}$ è una classe a sé stante. (b) n è messo in una classe già esistente.

Figura 1.1: I due casi per passare da $n-1$ a n.

Abbiamo allora una successione che dipende da due parametri, n e k: fissandone uno per volta, otteniamo due funzioni generatrici

$$A_n(Y) := \sum_{k=0}^{\infty} \left\{ {n \atop k} \right\} Y^k \quad \text{e} \quad B_k(X) := \sum_{n=0}^{\infty} \left\{ {n \atop k} \right\} X^n.$$

Usando la formula ricorsiva

$$\begin{aligned} B_k(X) &= \sum_{n=0}^{\infty} \left\{ {n-1 \atop k-1} \right\} X^n + k \sum_{n=0}^{\infty} \left\{ {n-1 \atop k} \right\} X^n = \\ &= X \cdot B_{k-1}(X) + kX \cdot B_k(X) \end{aligned}$$

cioè otteniamo

$$\begin{cases} B_k(X) = \dfrac{X}{1-kX} B_{k-1}(X) \\ B_0(X) = 1 \end{cases}$$

da cui, induttivamente,

$$B_k(X) = \frac{X^k}{(1-X)(1-2X)\cdots(1-kX)}.$$

Come nell'Esempio 1.1, vorremmo usare le funzioni razionali; quindi cerchiamo $\alpha_1, \ldots, \alpha_k$ tali che

$$\frac{1}{(1-X)(1-2X)\cdots(1-kX)} = \sum_{j=1}^{k} \frac{\alpha_j}{(1-jX)}. \tag{1.5}$$

Per determinare α_r moltiplichiamo ambo i membri di (1.5) per $(1 - rX)$ e poi valutiamo in $X = 1/r$. Così, nella sommatoria a destra, tutti gli addendi sono nulli tranne l'r-esimo (perché $(1 - rX)$ si è semplificato), lasciando solo α_r. Di conseguenza

$$\begin{aligned}\alpha_r &= \frac{1}{\left(1-\frac{1}{r}\right)\left(1-\frac{2}{r}\right)\cdots\left(1-\frac{r-1}{r}\right)\left(1-\frac{r+1}{r}\right)\cdots\left(1-\frac{k}{r}\right)} = \\ &= (-1)^{k-r}\frac{1}{(r-1)!}\frac{r^{k-1}}{(k-r)!}.\end{aligned}$$

Ora, $\left\{ {n \atop k} \right\}$ è il coefficiente di X^n in $B_k(X) = X^k \sum_{j=1}^{k} \frac{\alpha_j}{1-jX}$, che è il coefficiente di X^{n-k} in $\sum_{j=1}^{k} \frac{\alpha_j}{1-jX}$. Esplicitando la serie geometrica otteniamo

$$\sum_{r=1}^{k} \frac{\alpha_r}{1-rX} = \sum_{r=1}^{k} \alpha_r \sum_{i=0}^{\infty} r^i X^i$$

ed il coefficiente cercato è

$$\sum_{r=1}^{k} \alpha_r r^{n-k} = \sum_{r=1}^{k} (-1)^{k-r} \frac{r^n}{r!(k-r)!}.$$

A questo punto ci dedichiamo a contare le partizioni *totali* di $\{1, \ldots, n\}$, cioè vogliamo sapere in quanti modi possiamo partizionare n elementi. Ovviamente tale numero è

$$b(n) := \sum_{k=1}^{n} \left\{ {n \atop k} \right\} = \sum_{k=1}^{n} \sum_{r=1}^{k} (-1)^{k-r} \frac{r^n}{r!(k-r)!}.$$

Se $k > n$, il numero di partizioni è 0; di conseguenza, possiamo scrivere

$$b(n) = \sum_{k=1}^{N} \sum_{r=1}^{k} (-1)^{k-r} \frac{r^n}{r!(k-r)!}$$

per ogni $N \geqslant n$, e potremo eventualmente estendere questa somma all'infinito, dopo averla manipolata.

Per prima cosa scambiamo gli ordini delle sommatorie, cambiando gli indici. La Figura 1.2 ci aiuta a visualizzare la situazione: in un caso si sommano prima

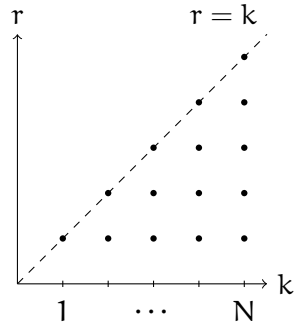


Figura 1.2: Coppie (k, r) interessate dalla sommatoria.

le coppie in verticale, nell'altro prima le coppie in orizzontale. Si ottiene

$$\begin{aligned} b(n) &= \sum_{k=1}^{N} \sum_{r=1}^{k} (-1)^{k-r} \frac{r^n}{r!(k-r)!} = \\ &= \sum_{r=1}^{N} \sum_{k=r}^{N} (-1)^{k-r} \frac{r^n}{r!(k-r)!} = \\ &= \sum_{r=1}^{N} \frac{r^n}{r!} \sum_{k=r}^{N} \frac{(-1)^{k-r}}{(k-r)!} = \\ &= \sum_{r=1}^{N} \frac{r^n}{r!} \sum_{h=0}^{N-r} \frac{(-1)^h}{h!} \end{aligned}$$

dove nell'ultimo passaggio abbiamo cambiato la variabile in $h := k - r$. A questo punto mandiamo $N \to \infty$: è noto che la serie $\sum (-1)^h/h!$ converge a $1/e$. Il risultato finale è

$$b(n) = \frac{1}{e} \sum_{r=1}^{\infty} \frac{r^n}{r!}. \tag{1.6}$$

Vediamo cosa succede provando a calcolare la funzione generatrice esponenziale $B(X)$ per la successione $b(n)$, usando il risultato (1.6):

$$B(X) = \frac{1}{e} \sum_{n=0}^{\infty} \frac{X^n}{n!} \sum_{r=1}^{\infty} \frac{r^n}{r!}.$$

L'addendo con $n = 0$ dà

$$\frac{1}{e} \sum_{r=1}^{\infty} \frac{1}{r!} = \frac{1}{e} \cdot e = 1,$$

mentre il resto della serie può essere scritto come

$$\begin{aligned}\frac{1}{e}\sum_{n=1}^{\infty}\frac{X^n}{n!}\sum_{r=1}^{\infty}\frac{r^n}{r!} &= \frac{1}{e}\sum_{r=1}^{\infty}\frac{1}{r!}\sum_{n=1}^{\infty}\frac{X^n}{n!}r^n = \\ &= \frac{1}{e}\sum_{r=1}^{\infty}\frac{1}{r!}\left(e^{rX}-1\right) = \\ &= \frac{1}{e}\sum_{r=1}^{\infty}\left(\frac{\left(e^X\right)^r}{r!}-\frac{1}{r!}\right) = \\ &= \frac{1}{e}\left(e^{e^X}-e\right) = e^{e^X-1}-1.\end{aligned}$$

In conclusione possiamo scrivere

$$B(X) = e^{e^X-1}$$

che è una formula estremamente compatta rispetto all'informazione contenuta in essa (ricordiamo che il coefficiente dell'n-esimo termine nella sua espansione in serie esponenziale è il numero di partizioni totali di n).

1.1.3 Parentesi di Catalan

Studiamo ora un esempio classico di combinatoria. Supponiamo di avere un prodotto non associativo; se per esempio abbiamo cinque simboli $x_1, \ldots, x_5$ possiamo calcolare

$$\begin{gathered}(((x_1x_2)x_3)x_4)x_5\\ ((x_1x_2)x_3)(x_4x_5)\\ ((x_1x_2)(x_3x_4))x_5\\ \vdots\end{gathered}$$

e ottenere risultati diversi. La domanda è: in quanti modi possiamo disporre delle parentesi (bilanciate) su n simboli? Denoteremo questo numero con c_n, per $n \geqslant 1$.[1] I primi casi sono ovvi: $c_1 = c_2 = 1$, infatti gli unici modi sono rispettivamente (x_1) e (x_1x_2).[2]

Esiste una formula ricorsiva: per $n \geqslant 2$

$$c_n = c_1c_{n-1} + c_2c_{n-2} + \cdots + c_{n-1}c_1. \tag{1.7}$$

In effetti, nel calcolo del prodotto finale, l'ultimo passaggio consiste nell'effettuare l'operazione sugli ultimi due prodotti parziali, in qualunque modo essi siano

[1] Normalmente, in letteratura c_n denota il numero di modi in cui si possono disporre parentesi intorno a $n+1$ simboli. Il lettore presti attenzione a questa piccola discrepanza.

[2] Consideriamo uguali due modi che nel prodotto portano allo stesso risultato, ad esempio $(x_1)x_2$ e (x_1x_2).

stati ottenuti: il primo con i simboli $x_1, \ldots, x_i$, il secondo con $x_{i+1}, \ldots, x_n$. In termini di parentesi questo vuol dire

pattern con n simboli = (*pattern* con i simboli)(*pattern* con $n-i$ simboli)

per ogni $i = 1, \ldots, n-1$.

Per calcolare c_n definiamo la funzione generatrice della successione

$$C(T) := \sum_{n=1}^{\infty} c_n T^n$$

che, sostituita nella relazione (1.7), soddisfa l'equazione

$$C(T) = c_1 T + (C(T))^2$$

ottenuta dall'espressione del prodotto di serie formali. Ricordando che $c_1 = 1$ abbiamo

$$(C(T))^2 - C(T) + T = 0$$

che ha per soluzioni (sceglieremo il segno più avanti)

$$C(T) = \frac{1 \pm \sqrt{1-4T}}{2}. \tag{1.8}$$

Espandiamo in serie di potenze la radice:

$$\sqrt{1-4T} = (1-4T)^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-4)^n T^n.$$

Il coefficiente di T^n in questa espressione è

$$\frac{\frac{1}{2} \cdot \left(-\frac{1}{2}\right) \cdots \left(-\frac{2n-3}{2}\right)}{n!} \cdot (-4)^n \tag{1.9}$$

che è negativo (se n è pari ho un numero dispari di segni meno nel binomiale generalizzato; viceversa se n è dispari, il segno meno è dato da $(-4)^n$). Quindi scegliamo il segno meno nella formula (1.8), in modo da avere $C(T)$ a termini positivi.

Ora, si verifica che il prodotto dei primi $n-1$ dispari (1 compreso) è

$$\prod_{k=1}^{n-1} (2k-1) = 1 \cdot 3 \cdots (2n-3) = \frac{(2n-2)!}{2^{n-1}(n-1)!},$$

quindi in definitiva c_n, che in base alla Formula (1.8) è dato da (1.9) moltiplicando per $-1/2$, vale

$$c_n = \frac{1}{2} \cdot \frac{1}{2^n} \cdot \frac{(2n-2)!}{2^{n-1}(n-1)!} \cdot \frac{4^n}{n!} = \frac{1}{n} \cdot \frac{(2n-2)!}{(n-1)!(n-1)!} = \frac{1}{n} \binom{2n-2}{n-1}.$$

È facile mostrare che c_n, nonostante la presenza di $1/n$, è un numero intero: abbiamo

$$nc_n = \binom{2n-2}{n-1} \in \mathbb{Z}$$

e dalle proprietà dei coefficienti binomiali

$$(n-1)c_n = \binom{2n-2}{n} \in \mathbb{Z},$$

quindi anche $c_n = nc_n - (n-1)c_n \in \mathbb{Z}$.

Osservazione. I numeri di Catalan emergono in molti contesti combinatori. Ad esempio: supponiamo di avere un poligono convesso di $n+1$ lati e di volerlo suddividere in triangoli tracciandone le diagonali (senza che esse si intersechino). Il numero di possibili suddivisioni[3] è proprio c_n.

Figura 1.3: Le 5 possibili suddivisioni in triangoli di un pentagono.

1.2 Serie formali

Ricordiamo in questa sezione la definizione e alcune proprietà dell'anello delle serie formali in una indeterminata. ▹ *04/03/2015*

Definizione 1.5. Sia R un anello (commutativo con identità). Si definisce *serie formale* a coefficienti in R una scrittura del tipo

$$\sum_{n=0}^{\infty} a_n X^n,$$

dove $a_n \in R$ per ogni $n \in \mathbb{N}$ e X è un simbolo di indeterminata.

L'insieme delle serie formali a coefficienti in R è indicato con $R[\![X]\!]$.[4] Su tale insieme si può mettere una struttura di anello (commutativo con identità) definendo la somma puntualmente

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) + \left(\sum_{n=0}^{\infty} b_n X^n\right) := \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

[3] Attenzione! Due suddivisioni che differiscono per una rotazione o una simmetria sono considerate diverse!

[4] Noi tratteremo sempre le serie a coefficienti in $\mathbb{C}$, se non diversamente specificato.

e il prodotto alla Cauchy

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n X^n\right) := \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j}\right) X^n.$$

Rispetto a queste operazioni, l'elemento neutro della somma è la serie con tutti i coefficienti uguali a 0, mentre quello del prodotto è la serie 1, cioè quella con $a_n = 0$ per $n \neq 0$ e $a_0 = 1$.

Proposizione 1.6. *In* $R[\![X]\!]$*, la serie* $\sum a_n X^n$ *è invertibile se e solo se* a_0 *è invertibile in* R*.*

Dimostrazione. $\boxed{\Rightarrow}$ Supponiamo che $\sum b_n X^n$ sia l'inversa di $\sum a_n X^n$. Dalla definizione di prodotto di serie si ha $a_0 b_0 = 1$, quindi a_0 è invertibile.
$\boxed{\Leftarrow}$ Supponendo che a_0 sia invertibile, si possono costruire i coefficienti b_n dell'inversa. Infatti, ammettendo che la serie inversa $\sum b_n X^n$ esista e imponendo $(\sum a_n X^n)(\sum b_n X^n) = 1$, si ottengono le relazioni

$$\begin{cases} a_0 b_0 = 1 \\ \displaystyle\sum_{j=0}^{n} a_{n-j} b_j = 0 \quad \text{per } n > 0 \end{cases}$$

da cui si ricava $b_0 = {a_0}^{-1}$ e, supponendo di aver costruito induttivamente $b_0, \ldots, b_{n-1}$,

$$b_n = {a_0}^{-1} \left(- \sum_{j=0}^{n-1} a_{n-j} b_j \right).$$

Questo dimostra la tesi. □

Sulle serie formali è possibile definire anche un'operazione di composizione: se $f(X) = \sum a_n X^n$ e $g(X) = \sum b_n X^n$, poniamo

$$(f \circ g)(X) := f(g(X)) = \sum_{n=0}^{\infty} a_n (g(X))^n.$$

Questa operazione, tuttavia, non è sempre ben definita: se $b_0 \neq 0$, infatti, il termine noto di $f \circ g$ è

$$(f \circ g)_0 = \sum_{n=0}^{\infty} a_n (b_0)^n$$

che non è una quantità ben definita. D'altra parte, se $b_0 = 0$, la composizione è ben definita: in tal caso il primo termine di $(g(X))^n$ ha grado n, quindi tale serie

non contribuisce ai termini di grado inferiore nella composizione $f \circ g$, i quali dunque sono il risultato di una somma finita.

Esiste un'identità per il prodotto di composizione, che è chiaramente la "serie" $\mathrm{Id}(X) = X$. D'altra parte, l'insieme delle serie formali con la somma usuale e il prodotto di composizione *non* è un anello: in generale non vale la proprietà distributiva, cioè esistono serie f, g e h tali che $f \circ (g + h) \neq f \circ g + f \circ h$.

Proposizione 1.7. *Sia* $f(X) = \sum a_n X^n \in \mathbb{C}[\![X]\!]$ *con* $a_0 = 0$. *La serie* f *è invertibile rispetto alla composizione se e solo se* $a_1 \neq 0$.

Dimostrazione. $\boxed{\Rightarrow}$ Supponiamo che $g(X) := \sum b_n X^n$ sia tale che $(f \circ g)(X) = X$ e siano $r \geqslant 1$, $s \geqslant 1$ i più piccoli indici per i quali rispettivamente $a_r \neq 0$ e $b_s \neq 0$.

Scrivendo esplicitamente la composizione $f \circ g$ osserviamo che il termine di grado minimo è $a_r b_s X^{rs}$. Imponendo che $f \circ g = \mathrm{Id}$ si ha

$$\begin{cases} rs = 1 & r, s \in \mathbb{N} \setminus \{0\} \\ a_r b_s = 1, \end{cases}$$

da cui otteniamo $r = s = 1$ e $a_1 \neq 0$ (e anche $b_1 \neq 0$).
$\boxed{\Leftarrow}$ Si procede in modo simile alla dimostrazione della Proposizione 1.6. Abbiamo visto nella prima parte della dimostrazione che, se esiste l'inversa compositiva $\sum b_n X^n$, dev'essere $b_1 := {a_1}^{-1}$. A questo punto ci chiediamo: chi è il generico termine di grado k in $f \circ g$? Un semplice conto mostra che

$$(f \circ g)_k = a_1 b_k + \text{polinomio in } a_i \text{ e } b_j \text{ con } j < k.$$

Imponendo che tale coefficiente sia nullo si ricava b_k in funzione di $b_1, \ldots, b_{k-1}$. □

Terminiamo questa breve presentazione delle serie formali con un'operazione unaria: la derivata formale. Se

$$f(X) = \sum_{n=0}^{\infty} a_n X^n$$

è una serie, definiamo la sua derivata come

$$\frac{d}{dX} f(X) = f'(X) := \sum_{n=1}^{\infty} n a_n X^{n-1}.$$

È immediato osservare che

1. $f' = 0$ se e solo se $f = a_0$;

2. $f' = f$ se e solo se $f = ce^X$, dove c è una costante e

$$e^X := \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

In effetti, da $f' = f$ si ha che $(n+1)a_{n+1} = a_n$, da cui $a_{n+1} = a_n/(n+1)$; fissato $a_0 = c$, induttivamente si ricava $a_n = c/n!$.

1.3 Proprietà delle funzioni generatrici ordinarie

Abbiamo visto la definizione di funzione generatrice ordinaria (Definizione 1.1 a pagina 1). Per noi a_n sarà il valore della soluzione di un problema combinatorio nel caso n. In questa sezione esporremo qualche proprietà che ci permette di calcolare funzioni generatrici di successioni più complicate a partire da mattoncini semplici. In ogni proprietà, $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ sarà una successione e $f(X) := \sum a_n X^n$ la corrispondente funzione generatrice.

Proprietà 1 (*shift*)**.** Se $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ è una successione, definiamo *shiftata* la successione $\mathcal{S}\mathbf{a}$ il cui termine n-esimo è $(\mathcal{S}\mathbf{a})_n := a_{n+1}$ per ogni $n \in \mathbb{N}$. La funzione generatrice associata a $\mathcal{S}\mathbf{a}$ è

$$\frac{f(X) - f(0)}{X}.$$

Dimostrazione. Naturalmente $f(X) - f(0) = \sum_{n=0}^{\infty} a_{n+1} X^{n+1}$, da cui la tesi. □

Proprietà 2 (*shift* iterato)**.** Se $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ è una successione e $h \in \mathbb{N}$, definiamo *shiftata di* h la successione $\mathcal{S}_h\mathbf{a}$ il cui termine n-esimo è $(\mathcal{S}_h\mathbf{a})_n := a_{n+h}$ per ogni $n \in \mathbb{N}$. La funzione generatrice associata a $\mathcal{S}_h\mathbf{a}$ è

$$\frac{1}{X^h}\left(f(X) - \sum_{j=0}^{h-1} a_j X^j\right).$$

Dimostrazione. È un'applicazione iterata della Proprietà 1. Più esplicitamente, si ha

$$f(X) - \sum_{j=0}^{h-1} a_j X^j = \sum_{n=0}^{\infty} a_{n+h} X^{n+h}$$

da cui la tesi. □

Proprietà 3 (moltiplicazione per n)**.** Alla successione $(na_n)_{n\in\mathbb{N}}$ è associata la funzione generatrice

$$X \cdot \frac{d}{dX} f(X).$$

Dimostrazione. Per il termine n-esimo vale

$$X \cdot \frac{d}{dX}(a_n X^n) = X \cdot n a_n X^{n-1} = n a_n X^n. \qquad \square$$

Proprietà 4 (moltiplicazione per un polinomio in n)**.** Se $p(T) \in \mathbb{C}[T]$ è un polinomio, allora alla successione $(p(n)a_n)_{n\in\mathbb{N}}$ è associata la funzione generatrice

$$p\left(X \cdot \frac{d}{dX}\right) f(X).$$

Dimostrazione. È un'applicazione iterata della Proprietà 3. Attenzione! In questo caso

$$\left(X \cdot \frac{d}{dX}\right)^2 f(X) = X \cdot \frac{d}{dX}\left(X \cdot \frac{d}{dX}(f(X))\right)$$

cioè è una potenza di composizione dell'operatore $X \cdot d/dX$. $\square$

Esempio 1.3. Sia data la successione

$$\begin{cases} a_0 = 1 \\ (n+1)a_{n+1} = 3a_n + 1 \quad \text{per } n \in \mathbb{N}. \end{cases}$$

Notiamo che $(n+1)a_{n+1}$ è il termine n-esimo di $\mathcal{S}((na_n)_{n\in\mathbb{N}})$. Se $f(X) = \sum a_n X^n$ è la funzione generatrice per (a_n), applicando prima la Proprietà 3 e poi la Proprietà 1 abbiamo che la funzione generatrice per $\mathcal{S}((na_n)_{n\in\mathbb{N}})$ è

$$\frac{g(X) - g(0)}{X},$$

dove $g(X) = X \cdot \frac{d}{dX} f(X)$. Esplicitando i conti risulta che tale funzione generatrice non è altro che $f'(X)$, quindi per trovare f è sufficiente risolvere l'equazione differenziale

$$f'(X) = 3f(X) + \frac{1}{1-X}$$

in cui la serie geometrica è data dal contributo del termine $+1$. Se per esempio sostituiamo tale termine con $+1/n!$ nella formula ricorsiva, l'equazione differenziale da risolvere diventa

$$f'(X) = 3f(X) + e^X.$$

Esempio 1.4. Vogliamo calcolare

$$\sum_{n=0}^{\infty} \frac{n^2 + 4n + 9}{n!}.$$

Lavoriamo per gradi:

1. sappiamo che la serie e^X corrisponde alla successione $(1/n!)$;
2. dalle Proprietà 3 e 4 abbiamo che a $(n/n!)$ corrisponde $X \cdot e^X$, mentre a $(n^2/n!)$ corrisponde $(X + X^2) \cdot e^X$;
3. di conseguenza alla successione $((n^2 + 4n + 9)/n!)$ corrisponde $(X^2 + 5X + 9) \cdot e^X$.

Notiamo ora che, se $f(X) = \sum a_n X^n$,

$$\sum_{n=0}^{\infty} a_n = f(1).$$

Quindi la somma richiesta è 15e.

1.3.1 Somme parziali

Studieremo qui ulteriori proprietà che legano le funzioni generatrici di una successione con quelle delle loro somme parziali.

Iniziamo con un esempio: al primo anno di matematica generalmente viene data una formula che esprime "la somma delle prime N potenze k-esime" e viene richiesto di dimostrare la formula per induzione. Ma come si fa a trovare la formula?

Sappiamo che

$$\sum_{n=0}^{N} X^n = \frac{X^{N+1} - 1}{X - 1}$$

e la prima è la serie generatrice per la successione che vale 1 per $n \leqslant N$ e 0 altrove. Allora possiamo moltiplicare la successione per n^k (Proprietà 4) e ottenere la serie

$$\sum_{n=0}^{N} n^k X^n = \left(X \cdot \frac{d}{dX} \right)^k \left(\frac{X^{N+1} - 1}{X - 1} \right).$$

Un computer è in grado di calcolare l'espressione sulla destra e valutarla in $X = 1$ per ottenere la formula chiusa richiesta.

Proprietà 5 (Prodotto di serie)**.** Se $f(X)$ è la funzione generatrice della successione (a_n) e $g(X)$ è quella per (b_n), allora $f(X) \cdot g(X)$ è la funzione generatrice per

$$\left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}}$$

Dimostrazione. Discende immediatamente dalla definizione di prodotto tra serie formali. □

Proprietà 6 (Potenza di serie)**.** Alla serie $f(X)^k$ è associata la successione

$$\left(\sum_{\substack{i_1,\dots,i_k\in\mathbb{N}\\ i_1+\cdots+i_k=n}} a_{i_1}\cdots a_{i_k}\right)_{n\in\mathbb{N}}$$

Dimostrazione. È un'applicazione iterata della Proprietà 5. □

Esempio 1.5. Se $f(X) = 1/(1-X) = \sum X^n$, allora il termine di grado n in $f(X)^k = 1/(1-X)^k$ è il numero di modi in cui si può scrivere n come somma di k numeri naturali. Ma noi sappiamo chi è il coefficiente del termine di grado n in $(1-X)^{-k}$: è

$$\binom{-k}{n}(-1)^n = \frac{(-k)(-k-1)\cdots(-k-n+1)}{n!}(-1)^n = \binom{k+n-1}{n}.$$

Proprietà 7 (Prodotto per la serie geometrica)**.** Se $f(X)$ è la funzione generatrice per (a_n), allora

$$\frac{1}{1-X}\cdot f(X)$$

è quella associata alla successione di somme parziali

$$\left(\sum_{j=0}^{n} a_j\right)_{n\in\mathbb{N}}$$

Dimostrazione. Dalla Proprietà 5, il termine di grado k in $(\sum X^n)(\sum a_n X^n)$ è

$$1\cdot a_0 + 1\cdot a_1 + \cdots + 1\cdot a_k.$$ □

Esempio 1.6. Ricaviamo la nota formula per la somma dei primi n quadrati. Iniziamo dalla successione costante $(1)_{n\in\mathbb{N}}$, cui è associata la serie geometrica. Dalla Proprietà 4 ricaviamo la serie associata a (n^2), che è

$$\left(X\cdot\frac{d}{dX}\right)^2\left(\frac{1}{1-X}\right).$$

Quindi per la Proprietà 7 alla successione delle somme $(\sum j^2)$ è associata la serie

$$\frac{1}{1-X} \cdot \left(X \cdot \frac{d}{dX}\right)^2 \left(\frac{1}{1-X}\right),$$

la quale si può riscrivere dopo qualche conto come

$$\frac{X(1+X)}{(1-X)^4}. \tag{1.10}$$

Ora, il coefficiente di X^n in $(1-X)^{-4}$ è

$$\binom{-4}{n}(-1)^n = \frac{4 \cdot 5 \cdots (n+3)}{n!} = \binom{n+3}{n}.$$

Riscrivendo (1.10) come

$$\frac{X}{(1-X)^4} + \frac{X^2}{(1-X)^4}$$

ci accorgiamo che il coefficiente di X^n in (1.10) è dato dalla somma di uno *shift* di 1 (moltiplicazione per X) e uno *shift* di 2 (moltiplicazione per X^2) rispetto a quello nella serie $(1-X)^{-4}$. In definitiva, dunque, la formula chiusa è

$$\binom{n+2}{3} + \binom{n+1}{3} = \frac{n(n+1)(2n+1)}{6}.$$

Esempio 1.7. Vediamo qual è la funzione generatrice associata alla serie armonica troncata, ovvero alla successione

$$H_n := 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Il termine n-esimo di questa successione è asintotico a $\ln n$:[5] questo fatto discende dal criterio del confronto integrale, in quanto H_n si stima con

$$\int_1^n \frac{1}{t} dt.$$

In effetti, la successione $(1/n)$ ha come funzione generatrice

$$\sum_{n=1}^{\infty} \frac{X^n}{n} = -\ln(1-X)$$

da cui ricaviamo che la funzione generatrice per (H_n) è

$$\frac{-\ln(1-X)}{1-X}.$$

[5] In effetti, possiamo scrivere

$$H_n = \ln n + \gamma + o\left(\frac{1}{n}\right)$$

dove $\gamma \approx 0.577$ è la *costante di Eulero-Mascheroni*. Si suppone che γ sia un numero trascendente; al momento non sappiamo nemmeno se sia razionale.

1.3.2 Fontana di monete

La fontana di monete è un gioco combinatorio che consiste nell'impilare delle monete seguendo alcune regole. Si comincia con n monete; si sceglie un numero $0 \leqslant k \leqslant n-1$ e si dispongono k monete consecutivamente sopra le prime n monete; quindi si sceglie un numero $0 \leqslant m \leqslant k-1$ di monete da disporre sul secondo piano e così via (si veda la Figura 1.4). La domanda è: quante fontane distinte si possono costruire se al piano terra ci sono n monete?

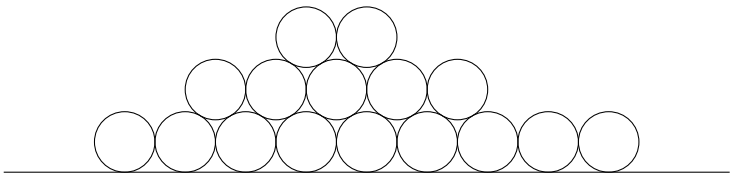
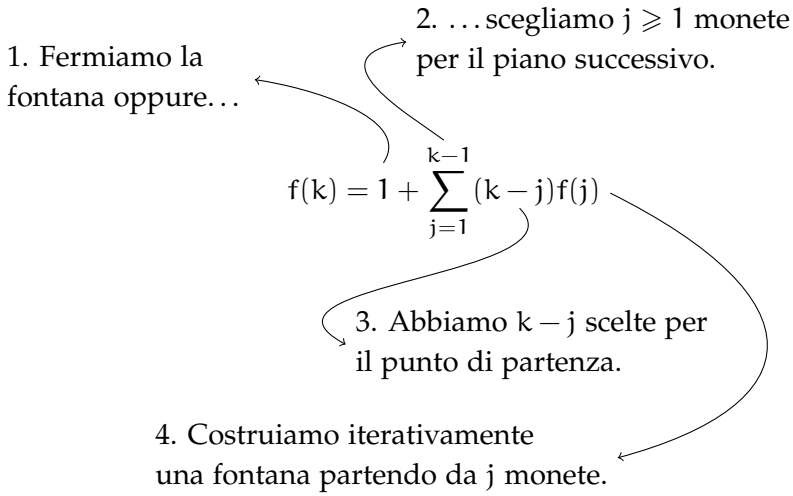


Figura 1.4: Una possibile fontana di monete.

Sia $f(n)$ il numero di fontane costruibili a partire da n monete. Per convenzione poniamo $f(0) := 1$ (la "fontana vuota"). Esiste una relazione di ricorrenza per f: se $k > 0$ vale che



Chiamiamo $F(X)$ la funzione generatrice associata a $(f(n))$. Notiamo che, se calcoliamo il prodotto di serie

$$\left(\sum_{n=0}^{\infty} f(n)X^n\right) \cdot \left(\sum_{n=0}^{\infty} nX^n\right),$$

il termine n-esimo risulta

$$c_n := \sum_{j=0}^{n}(n-j)f(j) = 0 \cdot f(n) + n \cdot f(0) + \sum_{j=1}^{n-1}(n-j)f(j) = n + \sum_{j=1}^{n-1}(n-j)f(j).$$

Quindi $f(n) = 1 - n + c_n$ e

$$F(X) = \sum_{n=0}^{\infty}(1-n+c_n)X^n = \sum_{n=0}^{\infty}(1-n)X^n + F(X)\cdot\left(\sum_{n=0}^{\infty}nX^n\right) = \\ = \frac{1-2X}{(1-X)^2} + F(X)\frac{X}{(1-X)^2}.$$

Con pochi passaggi si arriva infine a

$$F(X) = \frac{1-2X}{1-3X+X^2}.$$

Proviamo a calcolare $f(n)$ per qualche valore di n (Tabella 1.1). Si riconosce una certa regolarità? In effetti, sono tutti numeri di Fibonacci, e precisamente

n	0	1	2	3	4	5	6
$f(n)$	1	1	2	5	13	34	89

Tabella 1.1: Valori di $f(n)$ per $n \leqslant 6$.

quelli di indice dispari. Congetturiamo allora

$$f(n) = F_{2n-1}$$

(ponendo $F_{-1} = 1$ per convenzione, in modo che $F_{-1} + F_0 = F_1$).

Proviamo a dimostrarlo con le funzioni generatrici. Se

$$\mathcal{F}(X) = \frac{X}{1-X-X^2}$$

è la funzione generatrice per i numeri di Fibonacci (vedi Sezione 1.1.1), allora la sua parte dispari è

$$\frac{\mathcal{F}(X)-\mathcal{F}(-X)}{2} = \sum_{n=0}^{\infty}F_{2n+1}X^{2n+1}.$$

Quindi

$$X\frac{\mathcal{F}(X)-\mathcal{F}(-X)}{2} + F_{-1} = F_{-1} + \sum_{n=0}^{\infty}F_{2n+1}X^{2n+2} = \sum_{k=0}^{\infty}F_{2k-1}X^{2k}$$

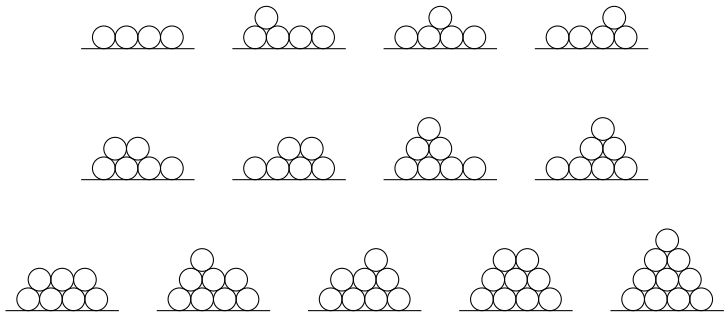


Figura 1.5: Le 13 possibili fontane a partire da 4 monete.

dove nell'ultimo passaggio abbiamo posto $k := n+1$. Per avere la tesi è sufficiente verificare che quest'ultima espressione sia uguale a $F(X^2)$. Proviamo a calcolarla:

$$X\frac{\mathcal{F}(X)-\mathcal{F}(-X)}{2}+F_{-1}=\frac{X}{2}\left(\frac{X}{1-X-X^2}+\frac{X}{1+X-X^2}\right)+1=\frac{1-2X^2}{1-3X^2+X^4}$$

che è proprio $F(X^2)$. La congettura è dunque dimostrata.

1.4 Proprietà delle funzioni generatrici esponenziali

Vediamo quali sono le proprietà analoghe a quelle della Sezione 1.3 per le funzioni generatrici esponenziali, definite a pagina 1. Al solito, supporremo che $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ sia una successione e $f(X) := \sum a_n X^n/n!$ la corrispondente funzione generatrice esponenziale. ▹ *09/03/2015*

Proprietà E1 (*shift*)**.** La funzione generatrice esponenziale associata a $\mathcal{S}\mathbf{a}$ è

$$f'(X) = \frac{d}{dX}f(X).$$

Dimostrazione. Basta verificarlo sui monomi:

$$\frac{d}{dX}\left(a_n\frac{X^n}{n!}\right) = \frac{a_n}{(n-1)!}X^{n-1}. \qquad \square$$

Proprietà E2 (*shift* iterato)**.** La funzione generatrice esponenziale associata a $\mathcal{S}_h\mathbf{a}$ è

$$f^{(h)}(X) = \left(\frac{d}{dX}\right)^h f(X).$$

Dimostrazione. È un'applicazione iterata della Proprietà E1. $\square$

Proprietà E3 (moltiplicazione per n)**.** Alla successione $(na_n)_{n\in\mathbb{N}}$ è associata la funzione generatrice esponenziale

$$X \cdot \frac{d}{dX} f(X).$$

Dimostrazione. Per il termine n-esimo vale

$$X \cdot \frac{d}{dX}\left(a_n \frac{X^n}{n!}\right) = X \cdot \frac{a_n}{(n-1)!} X^{n-1} = n a_n \frac{X^n}{n!}. \qquad \square$$

Proprietà E4 (moltiplicazione per un polinomio in n)**.** Se $p(T) \in \mathbb{C}[T]$ è un polinomio, allora alla successione $(p(n)a_n)_{n\in\mathbb{N}}$ è associata la funzione generatrice esponenziale

$$p\left(X \cdot \frac{d}{dX}\right) f(X).$$

Dimostrazione. È un'applicazione iterata della Proprietà E3. $\square$

Proprietà E5 (Prodotto di serie)**.** Se $f(X)$ è la funzione generatrice esponenziale della successione (a_n) e $g(X)$ è quella per (b_n), allora $f(X) \cdot g(X)$ è la funzione generatrice esponenziale per

$$\left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}\right)_{n\in\mathbb{N}}$$

Dimostrazione. Per la definizione di prodotto di serie, il termine n-esimo è

$$\sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} X^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a_k b_{n-k} \frac{X^n}{n!}. \qquad \square$$

1.4.1 Numeri di Bell

Nella Sezione 1.1.2 abbiamo calcolato il numero $b(n)$ di partizioni totali di un insieme di n elementi. Tali numeri sono detti *numeri di Bell*. Ora che abbiamo un po' più di teoria, proviamo a calcolare direttamente la funzione generatrice esponenziale.

Per i numeri $b(n)$ vale una formula ricorsiva: per $n \in \mathbb{N}$,

$$b(n+1) = \sum_{k=0}^{n} \binom{n}{k} b(k) \tag{1.11}$$

e per convenzione $b(0) = 1$ (la "partizione vuota"). Infatti, per contare le partizioni basta:

1. isolare un sottoinsieme appartenente alla partizione;
2. considerare ricorsivamente le partizioni del complementare di quel sottoinsieme.

Al variare dei possibili sottoinsiemi isolati si hanno tutte le partizioni. Attenzione, però: in questo modo si conta la stessa partizione più volte prendendo sottoinsiemi isolati disgiunti (se A, B sono sottoinsiemi disgiunti, le due partizioni $A \cup \{\text{partizione di } A^c \text{ che contiene } B\}$ e $B \cup \{\text{partizione di } B^c \text{ che contiene } A\}$ in realtà sono la stessa).

Il trucco è fissare un elemento di $\{1, \dots, n+1\}$ e isolare solo sottoinsiemi che contengono quell'elemento. In questo modo siamo sicuri di contare le partizioni una sola volta. Dunque, fissiamo $a \in \{1, \dots, n+1\}$ e consideriamo i sottoinsiemi di $\{1, \dots, n+1\}$ di cardinalità h che contengono a. Il loro numero è $\binom{n}{h-1}$ e h varia tra 1 (a vi appartiene sempre) e $n+1$. Per ognuno di essi, il complementare ha cardinalità $n+1-h$ e può essere partizionato in $b(n+1-h)$ modi. Quindi

$$\begin{aligned} b(n+1) &= \sum_{h=1}^{n+1} \binom{n}{h-1} b(n+1-h) = \\ &= \sum_{h=1}^{n+1} \binom{n}{n-h+1} b(n+1-h) = \sum_{k=0}^{n} \binom{n}{k} b(k) \end{aligned}$$

in cui nell'ultimo passaggio si è posto $k := n-h+1$.

A questo punto calcoliamo la funzione generatrice esponenziale per entrambi i membri dell'Equazione (1.11): detta

$$B(X) = \sum_{n=0}^{\infty} b(n) \frac{X^n}{n!},$$

a sinistra abbiamo $B'(X)$ per la Proprietà E1, mentre a destra

$$\begin{aligned} \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} b(k) \frac{X^n}{n!} &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{k!(n-k!)} b(k) X^n = \\ &= \left(\sum_{n=0}^{\infty} b(n) \frac{X^n}{n!} \right) \cdot \left(\sum_{n=0}^{\infty} \frac{X^n}{n!} \right) = B(X) e^X \end{aligned}$$

per la Proprietà E5. Abbiamo dunque l'equazione differenziale

$$\begin{cases} B'(X) = B(X) e^X & \text{(1.12a)} \\ B(0) = b_0 = 1. & \text{(1.12b)} \end{cases}$$

Dall'Equazione (1.12a) si ha $B'(X)/B(X) = e^X$, da cui integrando otteniamo $\ln B(X) = e^X + c$ (con c costante che determineremo fra poco) e finalmente $B(X) = e^{e^X+c}$. Imponendo le condizioni (1.12b) troviamo $c = -1$ e possiamo scrivere infine

$$B(X) = e^{e^X-1}$$

in accordo con quanto visto nella Sezione 1.1.2.

1.4.2 Permutazioni senza punti fissi

Sia $\mathfrak{S}_n$ il gruppo simmetrico su n elementi, cioè il gruppo delle permutazioni di $\{1, \ldots, n\}$. Vogliamo contare le *dismutazioni* all'interno di $\mathfrak{S}_n$, cioè le permutazioni senza punti fissi. Chiamiamo

$$d_n := \#\{\sigma \in \mathfrak{S}_n \mid \forall k = 1, \ldots, n\ \sigma(k) \neq k\}.$$[6]

I valori iniziali sono $d_0 = 1$ (la permutazione su 0 elementi, in effetti, non ha punti fissi...) e $d_1 = 0$ (l'unica permutazione di un elemento lo lascia ovviamente fisso). Anche in questo caso esiste una formula ricorsiva:

$$n! = \sum_{k=0}^{n} \binom{n}{k} d_{n-k}.$$

Infatti il numero totale di permutazioni (che è $\#(\mathfrak{S}_n) = n!$) è la somma dei numeri di permutazioni che lasciano fissi esattamente k elementi, per $k = 0, \ldots, n$. Questi sono dati dalla scelta dei k punti da fissare (in $\binom{n}{k}$ modi) e, una volta scelti, da d_{n-k} modi di permutare i restanti elementi (senza lasciarne alcuno fisso).

Detta $D(X)$ la funzione generatrice esponenziale per i d_n, dalla formula ricorrente si ha

$$\frac{1}{1-X} = e^X D(X)$$

perché a sinistra il fattoriale si semplifica e resta una serie geometrica, mentre a destra riconosciamo ancora una volta un prodotto di serie. In definitiva

$$D(X) = \frac{e^{-X}}{1-X}.$$

Quest'espressione, unitamente all'espansione di e^{-X} e alla Proprietà 7 sul prodotto per una serie geometrica, ci permette di calcolare una formula chiusa per d_n:

$$\frac{d_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

[6] Questo numero è a volte chiamato *subfattoriale* di n ed indicato con $!n$.

1.5 Serie di Dirichlet

Esistono altri modi per associare una serie a una successione di valori, alcuni migliori di altri a seconda del contesto. Vediamone uno usato particolarmente in Teoria Analitica dei Numeri.

Definizione 1.8. Data una successione $(a_n)_{n\in\mathbb{N}\setminus\{0\}}$, definiamo *serie di Dirichlet* la serie formale

$$A(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

La serie di Dirichlet più famosa è probabilmente quella associata alla successione che vale costantemente 1 ed è nota come *funzione zeta di Riemann*:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Proprio come succedeva con le serie di potenze, in cui trattando l'indeterminata X come numero complesso aveva senso porsi domande sulla convergenza della serie, possiamo chiederci cosa succede se il parametro formale s è visto come numero complesso. A differenza delle serie di potenze, in questo caso non c'è un raggio di convergenza, ma una *retta di convergenza*: in particolare la serie converge per il semipiano $\mathfrak{Re}(s) > r$ per un certo valore r che naturalmente dipende dalla serie. Ad esempio, $\zeta(s)$ converge per $\mathfrak{Re}(s) > 1$.

Ci piacerebbe ora che il prodotto di due serie di Dirichlet sia ancora una serie di Dirichlet. In effetti, così è: moltiplicando tra loro il generico termine h-esimo di $\sum a_n/n^s$ e quello k-esimo di $\sum b_n/n^s$ si ottiene

$$\frac{a_h}{h^s}\frac{b_k}{k^s} = \frac{a_h b_k}{(hk)^s}$$

che è una parte del termine (hk)-esimo. Osserviamo dunque che i contributi al termine n-esimo del prodotto sono dati dai termini h-esimi della prima serie e k-esimi della seconda per ogni h, k tali che $hk = n$. In altre parole, se

$$\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

allora

$$c_n = \sum_{hk=n} a_h b_k = \sum_{d|n} a_d b_{n/d}. \tag{1.13}$$

Questo è chiamato *prodotto di convoluzione di Dirichlet*.

Le serie di Dirichlet sono importanti soprattutto per lo studio di un tipo di successioni che si incontra spesso in Teoria dei Numeri.

Definizione 1.9. La successione $f(n)$ è detta *moltiplicativa* se $f(mn) = f(m)f(n)$ ogni volta che $\mathrm{GCD}(m, n) = 1$; *completamente moltiplicativa* se $f(mn) = f(m)f(n)$ per ogni $m, n \in \mathbb{N}$.

Ovviamente le successioni moltiplicative sono univocamente determinate dal valore che assumono sulle potenze dei primi, in virtù del Teorema Fondamentale dell'Aritmetica. Ci aspettiamo che anche le serie di Dirichlet associate a una successione moltiplicativa abbia un comportamento analogo.

Teorema 1.10. *Sia $f(n)$ una successione moltiplicativa. Allora*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ primo}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \dots\right). \tag{1.14}$$

L'idea è che tutti i termini nella serie a sinistra di (1.14) si ottengono in modo unico scegliendo uno e un solo termine da ciascun fattore sulla destra, proprio grazie all'unicità della fattorizzazione in primi.

Se inoltre $f(n)$ è completamente moltiplicativa, possiamo scrivere $f(p^m) = f(p)^m$ per ogni p primo e per ogni m, ottenendo serie geometriche nei fattori a destra in (1.14).

Corollario 1.11. *Se $f(n)$ è completamente moltiplicativa, allora*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ primo}} \left(1 - \frac{f(p)}{p^s}\right)^{-1}.$$

Ad esempio, per la zeta di Riemann vale

$$\zeta(s) = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{1.15}$$

Notiamo che, poiché $\mathrm{GCD}(n, 1) = 1$ per ogni n, affinché $f(n) = f(n \cdot 1) = f(n)f(1)$ dev'essere $f(1) = 1$. L'insieme delle funzioni moltiplicative dotato del prodotto di convoluzione, definito in (1.13) ed indicato con $f \star g$, formano un gruppo in cui l'elemento neutro è

$$\varepsilon(n) := \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1. \end{cases}$$

Se chiamiamo $\mathbb{1}(n)$ la successione associata a $\zeta(z)$, cioè $\mathbb{1}(n) = 1$ per ogni n, allora possiamo calcolare $\mathbb{1}^{-1}$ grazie alla Formula (1.15): infatti

$$\zeta(s)^{-1} = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

in cui $\mu(n)$ è la *funzione di Möbius* definita sulle potenze dei primi da

$$\mu(p^a) := \begin{cases} 1 & \text{se } a = 0 \\ -1 & \text{se } a = 1 \\ 0 & \text{se } a \geqslant 2 \end{cases}$$

ed estesa per moltiplicatività. In altre parole, $\mu(1) = 1$, $\mu(n) = (-1)^k$ se n è libero da quadrati e prodotto di k primi, e $\mu(n) = 0$ se n non è libero da quadrati. Quindi vale

$$\mathbb{1} \star \mu = \mu \star \mathbb{1} = \varepsilon. \tag{1.16}$$

Dalla relazione precedente otteniamo che per f, g funzioni aritmetiche[7] vale che $g = f \star \mathbb{1}$ se e solo se $f = g \star \mu$; questo risultato è noto come *formula di inversione di Möbius*.

Proposizione 1.12 (Formula di Inversione di Möbius)**.** *Siano* $f(n)$ *e* $g(n)$ *funzioni aritmetiche. Allora si ha*

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

per ogni $n \geqslant 1$ *se e solo se*

$$f(n) = \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big)$$

sempre per ogni $n \geqslant 1$.

Ad esempio, se $\varphi(n)$ è la funzione di Eulero (cioè $\varphi(n) := \#\{k \leqslant n \mid \mathrm{GCD}(n,k) = 1\}$), è un risultato noto che

$$n = \sum_{d|n} \varphi(d),$$

quindi, posto $\mathrm{Id}(n) := n$ per ogni n, in termini di prodotto di convoluzione vale che $\mathrm{Id} = \mathbb{1} \star \varphi$. Convolvendo ambo i membri di quest'espressione per $\mathbb{1}^{-1} = \mu$ si ottiene $\mu \star \mathrm{Id} = \varphi$, da cui

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Esempio 1.8 (Stringhe binarie primitive). Vediamo un esempio di applicazione delle serie di Dirichlet. Consideriamo l'insieme delle stringhe binarie, cioè sequenze di 0 e 1. Definiamo *primitiva* una stringa che non è esprimibile come concatenazione di una stringa più piccola ripetuta più volte (e *periodica* una stringa non primitiva). Ad esempio, 10100 è primitiva, mentre 001001 no. La domanda è: quante stringhe binarie di lunghezza n sono primitive?

[7] *Non* necessariamente moltiplicative.

Il numero totale di stringhe binarie di lunghezza n è naturalmente 2^n. Sia $f(n)$ il numero di stringhe primitive. Ogni stringa di lunghezza n è esprimibile in modo unico come concatenazione di un certo numero n/d di stringhe primitive di lunghezza d (eventualmente $d = n$ se la stringa è già primitiva), con d un divisore di n. Quindi

$$2^n = \sum_{d|n} f(d) = (\mathbb{1} \star f)(n).$$

Dalla relazione (1.16) ricaviamo allora $\mu \star (2^n) = f$, cioè

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) 2^d.$$

Esempio 1.9 (Parole circolari). In questo esempio parliamo ancora di stringhe, ma stavolta scegliamo un alfabeto con m simboli. Siamo interessati alle cosiddette *parole circolari*, cioè alle classi di equivalenza in cui consideriamo uguali due parole se si possono ottenere una dall'altra applicando uno *shift* delle lettere. La Figura 1.6 illustra il motivo per cui queste classi sono dette "circolari".

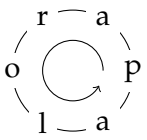


Figura 1.6: Esempio di parola circolare: è la classe di equivalenza delle parole lineari "parola", "arolap", "rolapa", "olapar", "laparo", "aparol".

Ci chiediamo: quante parole circolari di lunghezza n ci sono? Innanzitutto osserviamo che nel caso di lettere ripetute è possibile che non ci siano esattamente n parole lineari in una parola circolare: ad esempio, la classe di equivalenza di "papa" contiene in più solamente "apap". Diciamo che una parola circolare di lunghezza n ha *periodo* $p \leqslant n$ se si ripete uguale a sé stessa dopo p *shift*, cioè se la sua classe di equivalenza ha p elementi. Notiamo che $p \mid n$.

Detto $M(p)$ il numero di parole circolari di lunghezza n e periodo p, si ha che ciascuna di esse dà origine a p stringhe ordinarie. Dato che a ogni stringa è associata almeno una parola circolare, dev'essere

$$m^n = \sum_{p|n} pM(p).$$

Analogamente a quanto fatto precedentemente, possiamo invertire la formula convolvendo con μ: detta $m^*(k) := m^k$ si ha che $nM(n) = (\mu \star m^*)(n)$; prendendo

il p-esimo termine otteniamo

$$M(p) = \frac{1}{p} \sum_{d|p} \mu\Big(\frac{p}{d}\Big) m^d.$$

Possiamo allora ricavare il numero totale di parole circolari di lunghezza n: basta sommare su tutti i possibili periodi. Tale numero è

$$\begin{aligned} \sum_{p|n} M(p) &= \frac{1}{n} \sum_{p|n} \frac{n}{p} (\mu \star m^*)(p) = \frac{1}{n} (\mathrm{Id} \star \mu \star m^*)(n) \\ &= \frac{1}{n} (\varphi \star m^*)(n) = \frac{1}{n} \sum_{d|n} \varphi(d) m^{n/d}. \end{aligned}$$

Esempio 1.10 (Polinomi ciclotomici). Le serie di Dirichlet e le loro proprietà non sono utili solo per contare. Ad esempio, permettono di ricavare una formula più o meno esplicita per l'n-esimo polinomio ciclotomico.

Ricordiamo che l'n-esimo polinomio ciclotomico $\Phi_n(X)$ è il polinomio di grado $\varphi(n)$ le cui radici sono tutte e sole le radici primitive n-esime dell'unità.[8]

La formula che ci interessa qui è

$$\prod_{d|n} \Phi_d(X) = X^n - 1.$$

In effetti, le radici di $X^n - 1$ sono tutte le radici n-esime dell'unità e ciascuna di esse è una radice primitiva d-esima per esattamente un $d \leqslant n$ tale che $d \mid n$.

Passando ai logaritmi trasformiamo il prodotto in somma:

$$\sum_{d|n} \ln(\Phi_d(X)) = \ln(X^n - 1)$$

e la formula di inversione ci dà dunque

$$\ln(\Phi_n(X)) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \ln(X^d - 1)$$

da cui, esponenziando,

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

[8] Cioè le radici di $X^n - 1$ che non sono radici di $X^m - 1$ se $m < n$; sono della forma $e^{2\pi i r/n}$, per $0 \leqslant r \leqslant n-1$ con $\mathrm{GCD}(r, n) = 1$.

1.6 Carte, mani e mazzi (versione etichettata)

Introduciamo in questa sezione alcuni strumenti che, usati in combinazione con le funzioni generatrici esponenziali, permettono di risolvere una grande quantità di problemi combinatori. Definiremo un modello che, nella più ampia generalità, ci permette di rispondere alla seguente domanda: abbiamo una struttura fatta con dei mattoncini semplici; quante sono le possibili strutture che è possibile assemblare, supponendo di saper contare quanti sono i mattoncini di ciascun tipo?

Per essere più concreti, iniziamo con un esempio. Sappiamo che ogni grafo è unione di grafi connessi; in questo caso la struttura è il grafo e i mattoncini sono i grafi connessi. Di grafi etichettati connessi ne esistono esattamente 1 con un vertice, 1 con due vertici e 4 con tre vertici. D'altra parte esistono 8 possibili grafi etichettati con tre vertici (connessi e non). Come possiamo legare tra loro questi numeri?

In partenza è dato un insieme astratto P di *configurazioni* (*pictures*). Cosa siano effettivamente queste configurazioni, dipende dal problema specifico: per una maggiore chiarezza, si rimanda agli esempi.

Definizione 1.13. Una *carta* (*card*) è una coppia $\mathcal{C}(S, p)$, dove $S \subset \mathbb{N} \setminus \{0\}$ è un insieme finito di *etichette* (*labels*) e $p \in P$ è una configurazione. Il *peso* di una carta è $\#(S)$, e la carta è detta *standard* se $S = \{1, \dots, n\}$.

Definizione 1.14. Una *mano* (*hand*) è un insieme finito di carte in cui gli insiemi di etichette formano una partizione di $\{1, \dots, n\}$ per qualche n. Il *peso* di una mano è la somma dei pesi delle carte di cui è composta (cioè n).

Definizione 1.15. Una *rietichettatura* (*relabeling*) di una carta $\mathcal{C}(S, p)$ è una carta $\mathcal{C}(S', p)$ con la stessa configurazione e $\#(S') = \#(S)$. Se $S' = \{1, \dots, \#(S)\}$ la rietichettatura è detta *standard*.

Definizione 1.16. Un *mazzo* (*deck*) $\mathcal{D}$ è un insieme finito di carte con lo stesso peso e configurazioni distinte. Il *peso* di un mazzo è il peso comune delle sue carte.

Definizione 1.17. Una *famiglia esponenziale* $\mathcal{F}$ è una collezione (eventualmente infinita) di mazzi $\mathcal{D}_1, \mathcal{D}_2, \dots$ tale che ogni mazzo $\mathcal{D}_i$ ha peso i.

Definizione 1.18. Siano $\mathcal{F} = \{\mathcal{D}_1, \mathcal{D}_2, \dots\}$ una famiglia esponenziale e $d_n := \#(\mathcal{D}_n)$. Definiamo *contatore dei mazzi* (*deck enumerator*) la funzione generatrice esponenziale $\mathcal{D}(X)$ della successione $(d_n)_{n \in \mathbb{N} \setminus \{0\}}$, cioè

$$\mathcal{D}(X) := \sum_{n=1}^{\infty} d_n \frac{X^n}{n!}.$$

Vediamo subito un esempio. Consideriamo le permutazioni di $\{1, \dots, n\}$: come è noto esse si scrivono in modo unico come prodotto di cicli disgiunti. Proviamo allora a rappresentare le permutazioni in termini di carte e mani.

L'insieme delle configurazioni è formato dai *cicli standard*, cioè è

$$P = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \{\sigma \in \mathcal{S}_n \mid \sigma \text{ è un } n\text{-ciclo}\}.$$

Una carta di peso n è un n-ciclo non necessariamente etichettato con i numeri $1, \dots, n$: ad esempio

$$(2\ 5\ 3\ 17\ 9).$$

Questo ciclo è rappresentato come una carta di peso 5 che ha $S = \{2, 3, 5, 9, 17\}$ e $p = (1\ 3\ 2\ 5\ 4)$. Osserviamo che la rietichettatura del ciclo standard per ottenere il ciclo particolare *preserva l'ordine delle etichette*.

A questo punto è facile vedere che una mano rappresenta una generica permutazione: si ha corrispondenza tra le carte nella mano e i cicli che compongono la permutazione.

Un altro esempio è quello con cui abbiamo aperto questa sezione: i grafi etichettati. Ricordiamo che il numero di grafi etichettati con n vertici è

$$2^{\binom{n}{2}}$$

perché assegnare un grafo equivale a dare una funzione definita sulle coppie (che sono $\binom{n}{2}$) che dica se esiste un arco tra i due vertici oppure no.

Ogni grafo si può ottenere come unione di sottografi connessi; l'idea allora è di rappresentare i grafi connessi con le carte e quelli generici con le mani.

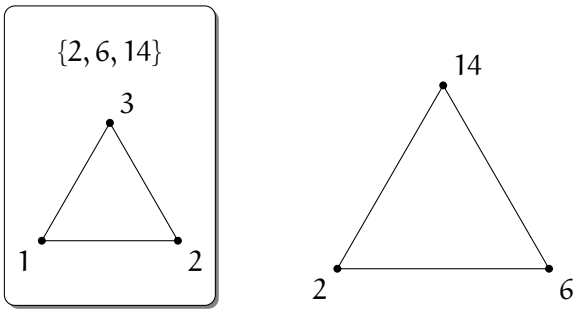


Figura 1.7: Esempio di carta per rappresentare un grafo etichettato connesso. A sinistra la carta, a destra l'oggetto che rappresenta.

Definizione 1.19. Sia $\mathcal{F}$ una famiglia esponenziale. Indichiamo con $h(n, k)$ il numero di mani di peso n formate da k carte, tali che ciascuna carta sia una

rietichettatura di una qualche carta in un qualche mazzo di $\mathcal{F}$. Sono ammesse ripetizioni, nel senso che possiamo prendere più copie della stessa carta, purché ciascuna copia sia rietichettata in modi diversi.

L'obiettivo finale è determinare $h(n,k)$ in funzione della successione (d_n). Per fare ciò, si usa una funzione generatrice in due variabili "mista", in parte ordinaria e in parte esponenziale:

$$\mathcal{H}(X,Y) := \sum_{n,k=0}^{\infty} h(n,k)\frac{X^n}{n!}Y^k.$$

Chiamiamo questa funzione *contatore delle mani* (*hand enumerator*). Definendo inoltre

$$h(n) := \sum_{k=0}^{\infty} h(n,k)$$

come il numero delle mani di peso n, indipendentemente dal numero di carte di cui sono formate, indicheremo con $\mathcal{H}(X)$ la funzione generatrice esponenziale per $(h(n))$, cioè

$$\mathcal{H}(X) := \mathcal{H}(X,1) = \sum_{n=0}^{\infty} h(n)\frac{X^n}{n!}.$$

Il seguente teorema ci permette di collegare i due contatori $\mathcal{D}(X)$ e $\mathcal{H}(X,Y)$. È un teorema di fondamentale importanza per raggiungere il nostro obiettivo.

Teorema 1.20 (Formula esponenziale)**.** *Vale che*

$$\mathcal{H}(X,Y) = e^{Y\mathcal{D}(X)}. \tag{1.17}$$

Corollario 1.21. *Valutando* (1.17) *per* $Y = 1$ *otteniamo*

$$\mathcal{H}(X) = e^{\mathcal{D}(X)}$$

Esempio 1.11. Riprendiamo la rappresentazione delle permutazioni in cicli. Il numero di n-cicli in $\mathfrak{S}_n$ è $d_n := (n-1)!$ (fissato il primo elemento, ho $n-1$ scelte per il secondo, $n-2$ per il terzo e così via). Quindi

$$\mathcal{D}(X) = \sum_{n=1}^{\infty} \frac{X^n}{n} = -\ln(1-X).$$

Per il Teorema 1.20 dunque

$$\mathcal{H}(X,Y) = e^{-Y\ln(1-X)} = \frac{1}{(1-X)^Y}.$$

Esempio 1.12. Contiamo ancora una volta il numero di partizioni di $\{1,\dots,n\}$. In questo caso possiamo prendere un insieme di configurazioni $P = \{*\}$, perché tutta l'informazione è contenuta nelle etichette.

Ora, $d_n = 1$ per ogni n (l'unica carta di peso n è quella etichettata con $\{1,\dots,n\}$) e una mano rappresenta una partizione. Quindi

$$\mathcal{D}(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!} = e^X - 1$$

da cui ricaviamo

$$\mathcal{H}(X) = e^{e^X - 1}$$

che è lo stesso risultato delle Sezioni 1.1.2 e 1.4.1.

Prima di procedere con la dimostrazione del Teorema 1.20 occorre enunciare un lemma. ▹ *11/03/2015*

Lemma 1.22 (Lemma fondamentale, versione etichettata)**.** *Siano $\mathcal{F}'$, $\mathcal{F}''$ due famiglie esponenziali. Definiamo una nuova famiglia $\mathcal{F} := \mathcal{F}' \oplus \mathcal{F}''$,* fusione *(*merge*) di $\mathcal{F}'$ e $\mathcal{F}''$, come unione disgiunta di $\mathcal{F}'$ e $\mathcal{F}''$ (cioè $\mathcal{D}_n = \mathcal{D}'_n \sqcup \mathcal{D}''_n$ per ogni n: si può fare ridefinendo eventualmente l'insieme delle configurazioni in modo che carte provenienti da famiglie diverse siano diverse fra loro; naturalmente $d_n = d'_n + d''_n$). Detti $\mathcal{H}$, $\mathcal{H}'$, $\mathcal{H}''$ i contatori delle mani rispettivamente di $\mathcal{F}$, $\mathcal{F}'$, $\mathcal{F}''$, si ha*

$$\mathcal{H} = \mathcal{H}'\,\mathcal{H}''\,.$$

Dimostrazione. In una mano di $\mathcal{F}$ di peso n con k carte, alcune di esse provengono da $\mathcal{F}'$ e altre da $\mathcal{F}''$. Le carte di $\mathcal{F}'$ formano una "sottomano" di peso n' con k' carte (eventualmente rietichettate con un certo sottoinsieme $S \subset \{1,\dots,n\}$). Quindi una mano di $\mathcal{F}$ di peso n con k carte è univocamente determinata da:

- una mano di $\mathcal{F}'$ di peso n' con k' carte;
- una rietichettatura con $S \subset \{1,\dots,n\}$;
- la rimanente mano di $\mathcal{F}''$ di peso $n'' = n - n'$ con $k'' = k - k'$ carte, rietichettata con $\{1,\dots,n\} \setminus S$.

Quindi

$$h(n,k) = \sum_{n' \leqslant n} \sum_{k' \leqslant k} \binom{n}{n'} h'(n',k') h''(n'',k'').$$

Ma ora calcoliamo il prodotto

$$\mathcal{H}'\,\mathcal{H}'' = \left(\sum_{n',k'=0}^{\infty} h'(n',k') \frac{X^{n'}}{n'!} Y^{k'} \right) \cdot \left(\sum_{n'',k''=0}^{\infty} h''(n'',k'') \frac{X^{n''}}{n''!} Y^{k''} \right).$$

Il coefficiente di $X^n Y^k$ è

$$\sum_{\substack{n'+n''=n \\ k'+k''=k}} \frac{1}{n'!}\frac{1}{n''!} h'(n',k') h''(n'',k'')$$

e notiamo che $\dfrac{1}{n'!}\dfrac{1}{n''!} = \dfrac{1}{n!}\binom{n}{n'}$. Questo termina la dimostrazione del lemma. □

Dimostrazione del Teorema 1.20. Dividiamo la dimostrazione in tre casi.
Caso 1. Consideriamo la famiglia $\mathcal{F}_0$ in cui tutti i mazzi sono vuoti, tranne l'r-esimo che consta di una sola carta. Cioè

$$d_n = \begin{cases} 1 & \text{se } n = r \\ 0 & \text{se } n \neq r, \end{cases} \qquad \mathcal{D}(X) = \frac{X^r}{r!}.$$

Quante mani è possibile creare con questa famiglia? Abbiamo a disposizione una sola carta, che eventualmente può essere ripetuta k volte. In particolare le mani possono avere solamente peso kr, quindi $h(n,k) = 0$ se $n \neq kr$. Se invece $n = kr$, il numero di mani coincide con il numero di partizioni di n elementi in k sottoinsiemi di cardinalità r: per la prima carta della mano abbiamo $\binom{n}{r}$ scelte, per la seconda ne abbiamo $\binom{n-r}{r}$ e così via fino alla k-esima per la quale abbiamo $\binom{n-(k-1)r}{r} = \binom{r}{r} = 1$ scelta. Visto che l'ordine delle carte in una mano non conta, dobbiamo dividere il tutto per $k!$. In definitiva, se $n = kr$

$$h(n,k) = \frac{1}{k!}\binom{n}{r}\cdot\binom{n-r}{r}\cdots\binom{n-(k-1)r}{r} = \frac{n!}{k!(r!)^k}.$$

Per vedere quest'ultima uguaglianza, notiamo che sviluppando i coefficienti binomiali si hanno cancellazioni:

$$\frac{n!}{r!(n-r)!}\frac{(n-r)!}{r!(n-2r)!}\frac{(n-2r)!}{r!(n-3r)!}\cdots$$

Ricapitolando

$$\mathcal{H}(X,Y) = \sum_{k=0}^{\infty} \frac{1}{k!(r!)^k} X^{kr} Y^k = \sum_{k=0}^{\infty} \frac{1}{k!}\left(\frac{X^r Y}{r!}\right)^k = e^{X^r Y/r!} = e^{Y\mathcal{D}(X)}.$$

Caso 2. C'è sempre un solo mazzo non vuoto (supponiamo $\mathcal{D}_r$), ma con un numero di carte d_r qualsiasi. La tesi discende abbastanza velocemente dal

Lemma 1.22: in questo caso $\mathcal{F}$ è la fusione di d_r copie della famiglia $\mathcal{F}_0$ introdotta nel Caso 1, quindi

$$\mathcal{H}(X,Y) = (\mathcal{H}_0(X,Y))^{d_r} = \left(e^{X^r Y/r!}\right)^{d_r} = e^{d_r X^r Y/r!} = e^{Y\mathcal{D}(X)}.$$

Caso 3. Una famiglia arbitraria $\mathcal{F}$ formata da mazzi con d_r carte può essere sempre vista come fusione delle famiglie $\mathcal{F}_1, \mathcal{F}_2, \dots$ tali che $\mathcal{F}_r$ ha un solo mazzo non vuoto di peso r con d_r carte. Dal Lemma 1.22 e dal Caso 2 otteniamo dunque

$$\mathcal{H}(X,Y) = \prod_r \mathcal{H}_r(X,Y) = \prod_r e^{Y\mathcal{D}_r(X)} = e^{Y\sum \mathcal{D}_r(X)} = e^{Y\mathcal{D}(X)}. \qquad \square$$

Esempio 1.13 (Esempio 1.11, parte II). Abbiamo visto che, costruendo le mani-permutazioni a partire dalle carte-cicli, si ottiene

$$\mathcal{H}(X,Y) = (1-X)^{-Y}.$$

Il coefficiente $h(n,k)$ rappresenta il numero di permutazioni su n che si scrivono con esattamente k cicli. Per trovare questo coefficiente applichiamo l'usuale regola della potenza di binomio:

$$(1-X)^{-Y} = \sum_{n=0}^{\infty} \binom{-Y}{n} (-1)^n X^n = \sum_{n=0}^{\infty} Y\cdot(Y+1)\cdots(Y+n-1)\frac{X^n}{n!}.$$

Quindi $h(n,k)$ è il coefficiente di Y^k nel polinomio $Y\cdot(Y+1)\cdots(Y+n-1)$.

Verifichiamo di aver fatto i conti giusti: il coefficiente di $X^n/n!$ in $\mathcal{H}(X,1)$ dovrebbe essere il numero di permutazioni su n elementi che si scrivono come prodotto di cicli (e quindi dovrebbero essere $n!$, cioè tutte...). In effetti

$$\mathcal{H}(X,1) = (1-X)^{-1} = \sum_{n=0}^{\infty} X^n = \sum_{n=0}^{\infty} n!\frac{X^n}{n!}.$$

1.6.1 Sottoclassi di permutazioni

Forti del risultato dell'esempio precedente, possiamo chiederci quante permutazioni abbiano delle determinate proprietà. Ad esempio: quante permutazioni si possono scrivere usando solamente cicli di lunghezza dispari?

Possiamo risolvere questo problema cambiando di poco la famiglia esponenziale. Infatti le limitazioni del testo ci impongono di poter pescare una carta solo da un mazzo $\mathcal{D}_n$ con n dispari. In altre parole

$$d_n = \begin{cases} (n-1)! & \text{se } n \text{ è dispari} \\ 0 & \text{se } n \text{ è pari.} \end{cases}$$

In questo contesto

$$\mathcal{D}(X) = \sum_{n \text{ dispari}} \frac{(n-1)!}{n!} X^n = \sum_{k=0}^{\infty} \frac{X^{2k+1}}{2k+1}.$$

Questa è la parte dispari di $-\ln(1-X)$, dunque possiamo scrivere

$$\mathcal{D}(X) = \frac{-\ln(1-X) - (-\ln(1+X))}{2} = \ln \sqrt{\frac{1+X}{1-X}}$$

da cui ricaviamo $\mathcal{H}(X,Y)$ senza problemi.

Ci spingiamo ora un pochino oltre: vogliamo contare quante permutazioni hanno tutti cicli di lunghezza dispari e sono formate da un numero pari di cicli.[9] In questo caso stiamo limitando i possibili valori k, cioè il numero di carte presenti nella mano: possiamo prendere solo k pari.

Proposizione 1.23. *Sia $T \subseteq \mathbb{N}$. Definiamo*

$$\exp_T(X) := \sum_{k \in T} \frac{X^k}{k!}.$$

Detto $h_n(T)$ il numero di mani di peso n che hanno un numero di carte $k \in T$, allora la funzione generatrice esponenziale per la successione $(h_n(T))$ è $\exp_T(\mathcal{D}(X))$.

Dimostrazione. È un corollario del Teorema 1.20. Infatti esplicitando l'Equazione (1.17):

$$\sum_{k=0}^{\infty} \frac{\mathcal{D}(X)^k}{k!} Y^k = \sum_{n,k=0}^{\infty} h(n,k) \frac{X^n}{n!} Y^k$$

e in particolare

$$\frac{\mathcal{D}(X)^k}{k!} = \sum_{n=0}^{\infty} h(n,k) \frac{X^n}{n!}$$

quindi $h(n,k)$ è il coefficiente di $X^n/n!$ in $\mathcal{D}(X)^k/k!$. Sommando solamente sui $k \in T$ si ha la tesi. □

Nel nostro caso $T = \{\text{pari}\}$, ed $\exp_T(X)$ è la parte pari di e^X, che risulta essere

$$\exp_T(X) = \frac{e^X + e^{-X}}{2} = \cosh(X).$$

Riutilizzando il risultato dell'esempio precedente si ha

$$\mathcal{H}(X) = \frac{1}{2}\left(\sqrt{\frac{1+X}{1-X}} + \sqrt{\frac{1-X}{1+X}}\right) = \frac{1}{\sqrt{1-X^2}}$$

[9] Osserviamo che n deve essere necessariamente pari.

che è un binomio; possiamo sviluppare ulteriormente il calcolo:

$$(1-X^2)^{-1/2} = \sum_{m=0}^{\infty} \binom{-1/2}{m} (-1)^m X^m = \sum_{m=0}^{\infty} \binom{2m}{m} \frac{(2m!)}{2^{2m}} \frac{X^{2m}}{(2m!)}.$$

In altre parole, il numero di permutazioni su n elementi formate da un numero pari di cicli tutti di lunghezza dispari è 0 se n è dispari e

$$\binom{n}{n/2} \frac{n!}{2^n}$$

se n è pari. Visto che tutte le permutazioni sono $n!$, la probabilità di sceglierne una con queste caratteristiche è

$$\binom{n}{n/2} \frac{1}{2^n}$$

che è uguale alla probabilità di ottenere esattamente $n/2$ "testa" e $n/2$ "croce" lanciando una moneta non truccata n volte.

Un ultimo esempio sulle permutazioni: quante sono le *involuzioni* su n elementi, cioè permutazioni σ tali che $\sigma^2 = \mathrm{Id}$? Più in generale, fissato m, quante sono le permutazioni tali che $\sigma^m = \mathrm{Id}$?

È un risultato noto che $\sigma^m = \mathrm{Id}$ se e solo se tutte le lunghezze dei cicli di σ sono divisori di m. In altre parole, possiamo pescare carte solo dai mazzi dei cicli $\mathcal{D}_r$ tali che $r \mid m$. Il contatore dei mazzi per questa famiglia è

$$\mathcal{D}(X) = \sum_{r|m} \frac{X^r}{r}.$$

Come caso speciale, $m = 2$ dà

$$\mathcal{D}(X) = X + \frac{X^2}{2}, \qquad \mathcal{H}(X) = e^{X+X^2/2}.$$

1.6.2 Esempi sui grafi

Studiamo alcuni esempi sui grafi. Ricordiamo che in questo caso i grafi si intendono con vertici etichettati e le carte sono i grafi connessi.

Quanti sono i grafi 2-regolari, cioè i grafi per cui da ogni vertice partono esattamente due archi? Per un grafo 2-regolare connesso non c'è molta scelta: è costretto ad essere un poligono, cioè un ciclo. Quindi ogni grafo 2-regolare è unione disgiunta di cicli.

Ora, $d_n = 0$ per $n = 1, 2$, mentre per $n \geqslant 3$

$$d_n = \frac{(n-1)!}{2}.$$

La differenza con i cicli delle permutazioni è la non-orientazione dei grafi: un ciclo di grafo percorso in senso orario o antiorario è lo stesso. Questa è l'origine del 2 a denominatore. A questo punto i conti sono facili:

$$\mathcal{D}(X) = \sum_{n=3}^{\infty} \frac{(n-1)!}{2} \frac{X^n}{n!} = \frac{1}{2} \sum_{n=3}^{\infty} \frac{X^n}{n} = \frac{1}{2}\left(-\ln(1-X) - X - \frac{X^2}{2}\right),$$

da cui

$$\mathcal{H}(X) = \frac{1}{\sqrt{1-X}} e^{(1/2)(-X-X^2/2)}.$$

Analizziamo ora un caso a rovescio: abbiamo i numeri h_n e vogliamo trovare i d_k. La domanda è: quanti grafi *connessi* con n vertici ci sono?

È facile contare la totalità dei grafi: sono

$$h_n := 2^{\binom{n}{2}}$$

da cui

$$\mathcal{H}(X) = \sum_{n=0}^{\infty} \frac{2^{\binom{n}{2}}}{n!} X^n.$$

Ora, la Formula (1.17) permette di ricavare i numeri h_n in funzione dei d_k o viceversa. Infatti vale il seguente lemma.

Lemma 1.24. *Per h_n numero di mani di peso n e d_k numero di carte nel mazzo D_k vale*

$$n h_n = \sum_{k=0}^{n} \binom{n}{k} k d_k h_{n-k}.$$

Dimostrazione. A partire da $\mathcal{H}(X) = e^{\mathcal{D}(X)}$, si applicano ad ambo i membri in ordine gli operatori di logaritmo, derivata e moltiplicazione per X: si arriva a

$$X \frac{\mathcal{H}'(X)}{\mathcal{H}(X)} = X\,\mathcal{D}'(X).$$

Per le varie proprietà delle funzioni generatrici esponenziali

$$\frac{\displaystyle\sum_{n=0}^{\infty} n h_n \frac{X^n}{n!}}{\displaystyle\sum_{n=0}^{\infty} h_n \frac{X^n}{n!}} = \sum_{n=0}^{\infty} n d_n \frac{X^n}{n!}.$$

Moltiplicando per togliere il denominatore e ricordando la formula di prodotto di serie si ha la tesi. □

Applicando il lemma precedente al nostro caso otteniamo una formula ricorsiva per i d_k:

$$n2^{\binom{n}{2}} = \sum_{k=0}^{n} \binom{n}{k} k d_k 2^{\binom{n-k}{2}}.$$

I primi valori di d_k sono $1, 1, 4, 38, 728 \ldots$

Passiamo ad analizzare alcune strutture di grafo più particolari rispetto a quelle viste finora. Ad esempio: quanti sono i grafi (etichettati) bipartiti con n vertici? ▹ *16/03/2015*

Un *grafo bipartito* è un grafo in cui l'insieme dei vertici V può essere partizionato come $V = A \sqcup B$ in modo che gli archi connettano solamente vertici in A con quelli in B (cioè non ci sono archi che uniscano due vertici di A o due vertici di B tra loro).

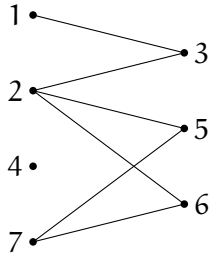


Figura 1.8: Esempio di grafo bipartito. Qui $A = \{1, 2, 4, 7\}$ e $B = \{3, 5, 6\}$.

Un grafo bipartito è unione disgiunta di grafi bipartiti connessi (in cui la partizione è data dall'unione delle partizioni). È naturale allora rappresentare i grafi bipartiti come mani e quelli connessi come carte.

Il problema è che in questo caso non c'è un modo ovvio per contare né le carte dei mazzi né le mani possibili. Una prima idea è: fissiamo una partizione $V = A \sqcup B$ e per ogni $(a, b) \in A \times B$ possiamo scegliere se mettere un arco tra a e b, quindi il numero di grafi bipartiti in totale sarebbe

$$2^{\#(A \times B)} = 2^{\#(A) \cdot \#(B)}.$$

In questo ragionamento c'è un intoppo: si conta più volte lo stesso oggetto. Si pensi anche solo al fatto che un grafo viene contato due volte scambiando tra loro A e B.

In generale, un grafo bipartito con c componenti connesse viene contato 2^c volte con questo metodo; questo perché per ogni componente connessa i del grafo possiamo scegliere quale dei due insiemi della partizione A_i o B_i mettere in A oppure in B nella partizione totale dei vertici (si veda anche la Figura 1.9).

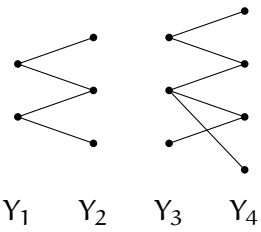


Figura 1.9: Scegliendo $A = Y_1 \cup Y_3$ e $B = Y_2 \cup Y_4$ oppure $A = Y_1 \cup Y_4$ e $B = Y_2 \cup Y_3$ si conta più volte lo stesso grafo.

Per rimediare a questo problema aggiungiamo informazioni che ci permettono di distinguere grafi diversi e che poi trascureremo quando andremo a tirare le somme. Definiamo *grafo bipartito 2-colorato* un grafo bipartito con una 2-colorazione dei vertici (supponiamo in "rosso" e "verde") tale che se esiste un arco tra i vertici v e w, allora essi hanno colore diverso. Osserviamo che per ogni grafo bipartito connesso ne esistono due 2-colorati (prima assegno ad A un colore e a B l'altro, poi li scambio) e in generale per un grafo con c componenti connesse abbiamo 2^c grafi 2-colorati.

Ora che i nostri grafi sono colorati è facile contarli: infatti il numero di mani di peso n (cioè il numero di grafi bipartiti 2-colorati) è

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

Infatti per ogni k tra 0 e n scegliamo k vertici a cui assegnare il colore "rosso" (e di conseguenza gli $n-k$ "verdi") e solo a quel punto stabiliamo quali siano gli archi.

A questo punto la Formula (1.17) ci permette di ricavare la funzione generatrice esponenziale per i mazzi (cioè otteniamo i grafi bipartiti 2-colorati *connessi*):

$$\mathcal{D}(X) = \ln\left(\sum_{n=0}^{\infty} \gamma_n \frac{X^n}{n!}\right).$$

Ma ora sappiamo che il numero dei grafi bipartiti connessi *non colorati* è esattamente la metà di quelli colorati, quindi abbiamo la funzione generatrice esponenziale dei mazzi per il nostro problema originale: è esattamente

$$\frac{\mathcal{D}(X)}{2} = \ln\left(\sqrt{\sum_{n=0}^{\infty} \gamma_n \frac{X^n}{n!}}\right).$$

Applicando ancora una volta la Formula (1.17) possiamo dunque trovare la funzione generatrice esponenziale delle mani, che ci dice quanti grafi bipartiti

con n vertici ci sono: tale numero è il coefficiente di $X^n/n!$ in

$$\sqrt{\sum_{n=0}^{\infty} \gamma_n \frac{X^n}{n!}}.$$

Ci dedicheremo ora agli *alberi* (etichettati), cioè a grafi connessi etichettati senza cicli. Il risultato a cui vogliamo arrivare è: il numero di alberi etichettati con n vertici è n^{n-2}.

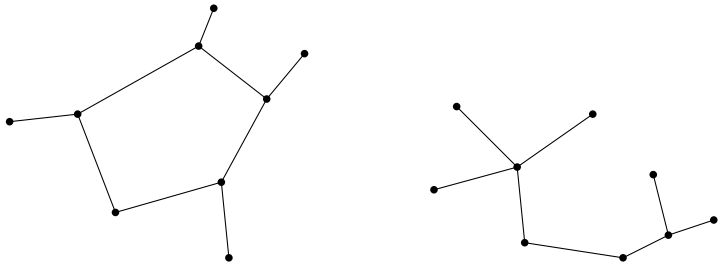


Figura 1.10: Il grafo a sinistra *non* è un albero, quello a destra sì.

In realtà conteremo i cosiddetti *alberi con radice*, cioè alberi in cui è selezionato un vertice (la radice, appunto). Dato che la radice può essere uno qualsiasi degli n vertici, abbiamo che

$$\#\{\text{alberi su } n \text{ vertici con radice}\} = n \cdot \#\{\text{alberi su } n \text{ vertici}\}$$

quindi ci basta dimostrare che il numero di alberi con radice è n^{n-1}.

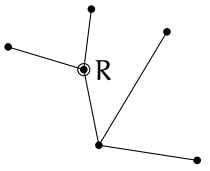


Figura 1.11: Un albero con radice R.

Ora, se le carte della nostra famiglia rappresentano gli alberi con radice, una mano corrisponde a una *foresta* (etichettata, con radici), cioè a un'unione disgiunta di alberi con radice. Quindi abbiamo due funzioni generatrici esponenziali:

$$\mathcal{D}(X) = \sum_{n=0}^{\infty} t_n \frac{X^n}{n!}$$

che contiene informazioni sugli alberi, e

$$\mathcal{H}(X) = \sum_{n=0}^{\infty} f_n \frac{X^n}{n!}$$

che invece corrisponde alle foreste.[10] Purtroppo siamo ancora nel caso in cui nessuno dei coefficienti (né i t_n né gli f_n) si contano facilmente ed abbiamo la Formula (1.17)

$$\mathcal{H}(X) = e^{\mathcal{D}(X)}$$

che lega due serie incognite. Tuttavia siamo fortunati: esiste un'altra relazione tra i t_n e gli f_n.

Proposizione 1.25 (dovuta a Pólya)**.** *Per ogni* $n \in \mathbb{N}$ *vale che* $t_{n+1} = (n+1)f_n$.

Dimostrazione. Sia F una foresta con n vertici. Introduciamo un nuovo vertice v e lo etichettiamo con j ($1 \leqslant j \leqslant n+1$). Rietichettiamo i vertici di F con le etichette in $\{1, \dots, j-1, j+1, \dots, n+1\}$, mantenendo l'ordinamento, quindi colleghiamo v con le radici degli alberi contenuti in F (vedi Figura 1.12). Fissiamo la radice dell'albero ottenuto in v.

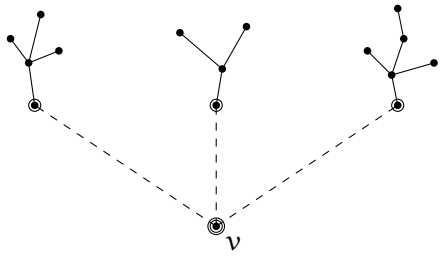


Figura 1.12: Come ottenere un albero da una foresta (e viceversa).

Abbiamo ottenuto un albero con radice su $n+1$ vertici. Al variare di j abbiamo costruito $n+1$ alberi a partire dalla foresta F.

Viceversa, dato un albero con radice, possiamo costruire una foresta eliminando la radice e tutti i rami che partono da essa, e definendo le nuove radici nelle altre estremità degli archi cancellati. Dato che queste costruzioni sono una l'inversa dell'altra, l'uguaglianza è dimostrata. □

Possiamo allora scrivere

$$\mathcal{H}(X) = \sum_{n=0}^{\infty} f_n \frac{X^n}{n!} = \sum_{n=0}^{\infty} \frac{t_{n+1}}{n+1} \frac{X^n}{n!} = \sum_{n=0}^{\infty} \frac{t_{n+1}}{(n+1)!} X^n = \frac{1}{X} \sum_{n=0}^{\infty} t_n \frac{X^n}{n!} = \frac{1}{X} \mathcal{D}(X).$$

[10] Si conviene che il grafo su zero vertici *non* sia un albero, ma una foresta (unione di 0 alberi), quindi $t_0 = 0$ e $f_0 = 1$.

Combinando quest'ultima relazione con quella data dalla formula esponenziale si ottiene che $\mathcal{D}(X)$ risolve l'equazione

$$\mathcal{D}(X) = Xe^{\mathcal{D}(X)}.$$

Ora, c'è una tecnica basata sulla Formula di Inversione di Lagrange che ci permette di risolvere equazioni come quella precedente. La accenneremo solamente.

Teorema 1.26. *Siano* $f, \varphi \in \mathbb{C}[\![T]\!]$ *serie formali con* $\varphi(0) = 1$. *Esiste ed è unica una serie formale* $u(T)$ *che risolve l'equazione*

$$u(T) = T \cdot (\varphi \circ u)(T)$$

e il coefficiente di T^n *in* $(f \circ u)(T)$ *è uguale al coefficiente di* u^{n-1} *in* $f'(u)\varphi(u)^n$ *diviso per* n.

Nel nostro caso, $\varphi(T) = e^T$ e scegliamo $f = \mathrm{Id}$. Allora $f'(u)\varphi(u)^n = e^{nu}$ e il coefficiente di u^{n-1} è $n^{n-1}/(n-1)!$, che diviso per n dà

$$\frac{n^{n-1}}{n!}.$$

Dal teorema precedente, questo coefficiente è uguale a $t_n/n!$, da cui otteniamo infine $t_n = n^{n-1}$.

Cerchiamo ora di ottenere il risultato precedente passando per un'altra strada. Per un generico grafo si definisce *valenza* o *grado* di un vertice il numero di archi che vi confluisce.

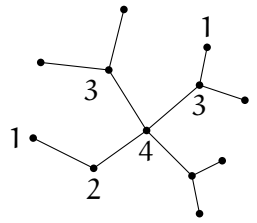


Figura 1.13: Un grafo in cui sono evidenziate alcune valenze.

Detta $\nu(i)$ la valenza dell'i-esimo vertice, si ha ovviamente che

$$\sum_{i=1}^{n} \nu(i) = 2 \cdot \#\{\text{archi}\}.$$

Proposizione 1.27. *Il numero di archi in un albero su* n *vertici è* $n - 1$.

Dimostrazione. Procediamo per induzione sul numero di vertici. Per $n = 1$, il risultato è ovvio. Supponiamo allora che ogni albero con k vertici ($k < n$) abbia $k - 1$ archi.

Osserviamo intanto che, se si elimina un nodo (e tutti gli archi che vi giungono) da un albero, esso può rimanere tale oppure può diventare un non-albero (si veda la Figura 1.14).

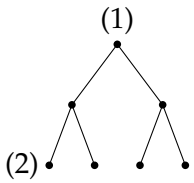


Figura 1.14: Togliendo il vertice in (1), il grafo non è più un albero; togliendo (2), invece, questo non succede.

Possiamo allora ordinare i vertici in modo che i primi k siano quelli che *non* mantengano la struttura ad albero;[11] in altre parole, togliendo un qualsiasi vertice tra il $(k+1)$-esimo e l'n-esimo si ottiene ancora un albero. In particolare, il sottografo formato dai primi k vertici è un albero e, per ipotesi induttiva, ha $k - 1$ archi.

A questo punto riordiniamo gli $n - k$ vertici rimasti in modo che il j-esimo vertice sia collegato ad almeno uno tra i vertici $1, \dots, j - 1$. Questo si può sempre fare, perché altrimenti i due insiemi di vertici $\{1, \dots, j - 1\}$ e $\{j, \dots, n\}$ formerebbero due componenti connesse distinte dell'albero di partenza. In particolare, il $(k+1)$-esimo vertice dev'essere collegato a *esattamente uno* dei vertici $1, \dots, k$: infatti per ogni coppia di vertici (i, j) in un albero esiste un'unica successione di archi che collega i e j;[12] se quindi il vertice $k + 1$ fosse collegato a due vertici distinti i e j (con $i, j \leqslant k$), ci sarebbero due percorsi distinti per andare da i a j (uno passando per $k + 1$, l'altro appartenente al sottoalbero definito dai vertici $1, \dots, k$).

Un ragionamento simile ci permette di concludere che ognuno dei vertici $k + 1, \dots, n$ dev'essere collegato ad esattamente un vertice, di conseguenza contribuiscono con un arco ciascuno al conteggio totale. Il numero di archi dell'albero di partenza è dunque

$$(k - 1) + (n - k) = n - 1$$

e la proposizione è così dimostrata. □

[11] Si può dimostrare che un albero finito ha almeno un vertice di valenza 1 (una *foglia*), quindi dev'essere $k < n$: togliendo una foglia il grafo resta un albero.

[12] L'esistenza è dovuta alla connessione, l'unicità all'assenza di cicli.

Associamo a questo punto ad ogni grafo un monomio: se i vertici sono $1, \dots, n$ con valenze $\nu(1), \dots, \nu(n)$, prendiamo n indeterminate $T_1, \dots, T_n$ e consideriamo il monomio

$$T_1^{\nu(1)} \cdots T_n^{\nu(n)}.$$

Questa associazione non è iniettiva; in Figura 1.15 è mostrato un esempio di due grafi distinti a cui è associato lo stesso monomio.

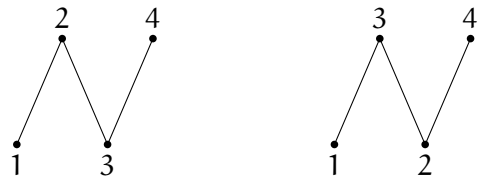


Figura 1.15: Entrambi i grafi hanno come monomio $T_1 T_2^2 T_3^2 T_4$, ma sono grafi diversi (ad esempio, a sinistra i vertici 3 e 4 sono collegati mentre a destra no).

Siamo però in grado di contare quanti siano gli alberi associati a un particolare monomio. Ricordiamo che, alla luce della Proposizione 1.27, la somma delle valenze $\nu(i)$ è pari a $2n-2$.

Proposizione 1.28. *Siano* $d_1, \dots, d_n$ *numeri naturali tali che* $d_i \geqslant 1$ *e* $d_1 + \cdots + d_n = 2n-2$. *Il numero di alberi su* n *vertici tali che* $\nu(i) = d_i$ *per ogni* i *è*

$$f_n(d_1, \dots, d_n) := \frac{(n-2)!}{(d_1-1)! \cdots (d_n-1)!}.$$

Dimostrazione. Procediamo per induzione su n. Per $n = 1$ non c'è nulla da dimostrare; per $n = 2$ l'unica scelta è $d_1 = d_2 = 1$ e si ha

$$f_2(1,1) = \frac{0!}{0!0!} = 1$$

che effettivamente conta l'unico albero possibile.

Abbiamo già visto nella dimostrazione della Proposizione 1.27 che un albero finito ha almeno una foglia, cioè un vertice di valenza 1; quindi almeno uno dei d_i è uguale ad 1 e supponiamo senza perdita di generalità che sia $d_1 = 1$. Diciamo che l'unico vertice collegato a 1 sia j.

Ora, fissato $j \geqslant 2$, gli alberi su n vertici che hanno la successione delle valenze $(d_1, \dots, d_n)$ sono in corrispondenza biunivoca con gli alberi sugli $n-1$ vertici $\{2, \dots, n\}$ con successione delle valenze $(d_2, \dots, d_{j-1}, d_j - 1, d_{j+1}, \dots, d_n)$ in quanto abbiamo tolto il vertice 1 e l'arco che lo unisce a j. Possiamo ora applicare

l'ipotesi induttiva ed ottenere

$$\begin{aligned} f_n(d_1,\dots,d_n) &= \sum_{j=2}^{n} \frac{(n-3)!}{(d_2-1)!\cdots(d_j-2)!\cdots(d_n-1)!} = \\ &= \sum_{j=2}^{n} \frac{(n-3)!(d_j-1)}{(d_2-1)!\cdots(d_j-1)!\cdots(d_n-1)!} = \\ &= \frac{(n-3)!}{(d_2-1)!\cdots(d_n-1)!}\sum_{j=2}^{n}(d_j-1) = \\ &= \frac{(n-3)!}{(d_2-1)!\cdots(d_n-1)!}\big((2n-3)-(n-1)\big) = \\ &= \frac{(n-2)!}{(d_1-1)!\cdots(d_n-1)!}. \end{aligned}$$

□

Il numero totale degli alberi su n vertici è la somma al variare di tutte le possibili n-uple $(d_1,\dots,d_n)$ che possono rappresentare le valenze; definiamo allora una funzione generatrice

$$F_n(T_1,\dots,T_n) := \sum_{\substack{d_1+\cdots+d_n=2n-2 \\ d_1,\dots,d_n\geqslant 1}} f_n(d_1,\dots,d_n)T_1^{d_1}\cdots T_n^{d_n}.$$

Andando a sostituire i risultati della Proposizione 1.28 otteniamo

$$\begin{aligned} F_n(T_1,\dots,T_n) &= \sum_{d_1,\dots,d_n} \frac{(n-2)!}{(d_1-1)!\cdots(d_n-1)!}T_1^{d_1}\cdots T_n^{d_n} = \\ &= (T_1\cdots T_n)\sum_{d_1,\dots,d_n} \frac{(n-2)!}{(d_1-1)!\cdots(d_n-1)!}T_1^{d_1-1}\cdots T_n^{d_n-1} = \\ &= (T_1\cdots T_n)(T_1+\cdots+T_n)^{n-2} \end{aligned}$$

in cui nell'ultima uguaglianza si è usato il Teorema Multinomiale:

$$(x_1+\cdots+x_k)^n = \sum_{r_1+\cdots+r_k=n} \frac{n!}{r_1!\cdots r_k!}x_1^{r_1}\cdots x_k^{r_k}.$$

Il numero totale di alberi etichettati su n vertici si ottiene allora valutando $F_n(T_1,\dots,T_n)$ per $T_1=\cdots=T_n=1$:

$$F_n(1,\dots,1) = n^{n-2}.$$

1.7 Carte, mani e mazzi (versione non etichettata)

Finora abbiamo visto problemi *etichettati*, in cui oggetti con la stessa "figura" ma "etichette" diverse erano distinti. Ci proponiamo ora di studiare problemi

non etichettati, in cui conta solamente la "figura". Possiamo immaginare che la differenza sia nella mancanza di fattori $n!$ che contavano i modi diversi di etichettare gli oggetti...

Comunque, diamo ora le nuove definizioni di carta, mano e mazzo in questa versione non etichettata.

Definizione 1.29. Una *carta* (*card*) *non etichettata* è una coppia $\mathcal{C}(n, p)$, dove $n \in \mathbb{N}$ e $p \in P$ è una configurazione. Il numero n è detto *peso* della carta. In questa versione non è necessario specificare etichette che caratterizzino i punti della configurazione, basta sapere il loro numero.

Definizione 1.30. Un *mazzo* (*deck*) *non etichettato* $\mathcal{D}$ è un insieme finito di carte non etichettate con lo stesso peso e configurazioni distinte. Il *peso* di un mazzo è il peso comune delle sue carte.

Definizione 1.31. Una *mano* (*hand*) *non etichettata* è un multiinsieme[13] finito di carte non etichettate. Il *peso* di una mano è la somma dei pesi delle carte di cui è composta.

Detto $h(n, k)$ il numero di mani di peso n formate da k carte, possiamo scrivere la funzione generatrice di questa successione. Stavolta conviene mantenere la versione ordinaria della serie:

$$\mathcal{H}(X, Y) := \sum_{n,k=0}^{\infty} h(n, k) X^n Y^k.$$

In maniera analoga, indicheremo con il suggestivo nome di *prefabbricato* (*prefab*)[14] un insieme di mazzi non etichettati $\mathcal{D}_1, \mathcal{D}_2, \dots$ tale che ogni mazzo $\mathcal{D}_n$ ha peso n e un numero di carte d_n. Indichiamo con $\mathcal{D}(X) := \sum d_n X^n$ la funzione generatrice ordinaria per il *prefab*. Vogliamo trovare una relazione tra $\mathcal{D}(X)$ e $\mathcal{H}(X, Y)$.

Il primo passo consiste ancora una volta nel considerare un *prefab* in cui tutti i mazzi sono vuoti, tranne l'r-esimo che contiene una sola carta; in tal caso $d_r = 1$ e $d_j = 0$ per $j \neq r$. Ovviamente le uniche mani possibili sono quelle formate da k copie dell'unica carta, quindi

$$h(n, k) = \begin{cases} 1 & \text{se } n = rk \\ 0 & \text{altrimenti.} \end{cases}$$

Dunque la funzione generatrice delle mani è

$$\mathcal{H}(X, Y) = \sum_{k=0}^{\infty} X^{rk} Y^k = \frac{1}{1 - YX^r}.$$

[13] Cioè, sono ammesse ripetizioni nei suoi elementi.

[14] *NdA:* mi sfugge il motivo per cui sia stato scelto proprio questo nome...

Per unire diverse istanze del risultato precedente, abbiamo bisogno ancora una volta di un lemma fondamentale che descrive cosa succede con la fusione di due *prefab*.

Lemma 1.32 (Lemma fondamentale, versione non etichettata)**.** *Siano $\mathcal{P}'$, $\mathcal{P}''$ due* prefab*. Definiamo un nuovo* prefab *$\mathcal{P} := \mathcal{P}' \oplus \mathcal{P}''$,* fusione *(*merge*) di $\mathcal{P}'$ e $\mathcal{P}''$, come nel Lemma 1.22. Detti $\mathcal{H}$, $\mathcal{H}'$, $\mathcal{H}''$ i contatori delle mani rispettivamente di $\mathcal{P}$, $\mathcal{P}'$, $\mathcal{P}''$, si ha*

$$\mathcal{H} = \mathcal{H}'\,\mathcal{H}''\,.$$

Dimostrazione. Considerando una mano di peso n con k carte prese da $\mathcal{P}$, essa sarà formata da una mano di peso n' con k' carte prese da $\mathcal{P}'$ e le rimanenti $n'' = n - n'$ carte di peso totale $k'' = k - k'$ provenienti da $\mathcal{P}''$. Dunque

$$h(n,k) = \sum_{n' \leqslant n} \sum_{k' \leqslant k} h'(n',k')h''(n'',k'')$$

che è proprio il coefficiente di $\mathcal{H}'\,\mathcal{H}''$. □

Quindi, in un *prefab* con un solo mazzo non vuoto formato da d_r carte abbiamo

$$\mathcal{H}(X,Y) = \left(\frac{1}{1-YX^r}\right)^{d_r}$$

e infine racchiudiamo in un teorema il risultato generale.

Teorema 1.33. *Per un* prefab *con mazzi $\mathcal{D}_n$ formati da d_n carte vale che*

$$\mathcal{H}(X,Y) = \prod_{n=1}^{\infty}\left(\frac{1}{1-YX^n}\right)^{d_n}.$$

Il risultato così com'è è molto elegante ma poco pratico per ottenere i numeri h dai numeri d. Per fortuna il metodo standard "passa al logaritmo, deriva e moltiplica per Y" funziona anche in questo caso. Infatti

$$\begin{aligned}\ln \mathcal{H}(X,Y) &= \sum_{n=1}^{\infty} \ln\left(\left(\frac{1}{1-YX^n}\right)^{d_n}\right) = \\ &= \sum_{n=1}^{\infty} d_n \ln\left(\frac{1}{1-YX^n}\right) = \sum_{n=1}^{\infty} d_n \sum_{s=1}^{\infty} \frac{Y^s X^{ns}}{s}.\end{aligned}$$

Ponendo $m := ns$ otteniamo

$$\ln \mathcal{H}(X,Y) = \sum_{m=1}^{\infty} \sum_{s|m} d_{m/s} \frac{Y^s X^m}{s}.$$

Applichiamo l'operatore $Y \cdot \mathcal{H}(X,Y) \cdot \dfrac{\partial}{\partial Y}$: a sinistra rimane

$$Y \cdot \frac{\partial}{\partial Y}\,\mathcal{H}(X,Y)$$

mentre a destra

$$Y \cdot \mathcal{H}(X,Y) \cdot \frac{\partial}{\partial Y}\left(\sum_{m=1}^{\infty}\sum_{s|m} d_{m/s}\frac{Y^s X^m}{s}\right) = \mathcal{H}(X,Y)\sum_{m=1}^{\infty}\sum_{s|m} Y d_{m/s}\, s\frac{Y^{s-1}X^m}{s} =$$

$$= \mathcal{H}(X,Y)\sum_{m=1}^{\infty}\sum_{s|m} d_{m/s} Y^s X^m.$$

Prendendo il coefficiente di $Y^k X^n$ in entrambi i membri porta infine alla formula ricorsiva

$$k \cdot h(n,k) = \sum_{r,k'=1}^{\infty} h(n-rk', k-k')\,d_r.$$

La funzione generatrice $\mathcal{H}(X,Y)$ contiene un sacco di informazioni. Ad esempio, possiamo contare tutte le mani di peso n, indipendentemente dal numero di carte da cui sono composte:

$$h_n := \sum_{k=0}^{\infty} h(n,k).$$

La funzione generatrice $\mathcal{H}(X)$ associata alla successione (h_n) si ottiene valutando $\mathcal{H}(X,Y)$ in $Y = 1$:

$$\mathcal{H}(X) = \prod_{n=1}^{\infty}\left(\frac{1}{1-X^n}\right)^{d_n}.$$

Anche in questo caso è possibile esprimere gli h_n in funzione dei d_r con il solito operatore: applicando il logaritmo si ha

$$\ln \mathcal{H}(X) = \sum_{r=1}^{\infty} d_r \sum_{m=1}^{\infty}\frac{X^{rm}}{m},$$

derivando e moltiplicando per $X \cdot \mathcal{H}(X)$ si giunge a

$$X \cdot \mathcal{H}'(X) = \mathcal{H}(X)\sum_{r=1}^{\infty} d_r \sum_{m=1}^{\infty} r X^{rm}.$$

La formula ricorsiva per gli h_n è allora

$$n h_n = \sum_{m=1}^{\infty} D_m h_{n-m}$$

dove $D_m := \displaystyle\sum_{r|m} r d_r$.

1.7.1 Partizioni di interi

Sia $n \in \mathbb{N}$ un intero fissato. In quanti modi è possibile scrivere

$$n = x_1 + \cdots + x_k$$

al variare di $k, x_1, \ldots, x_k \in \mathbb{N} \setminus \{0\}$? Supporremo $x_1 \geqslant \cdots \geqslant x_k$. Ad esempio, il numero 5 ha 7 partizioni:

$$5, \quad 4+1, \quad 3+2, \quad 3+1+1, \quad 2+2+1, \quad 2+1+1+1, \quad 1+1+1+1+1.$$

In termini del nostro modello di carte e mazzi, ogni carta di peso n rappresenta proprio il numero n ed ogni mazzo è composto da una singola carta: $d_r = 1$ per ogni $r \geqslant 1$, di conseguenza la funzione generatrice per le partizioni degli interi è

$$\mathcal{H}(X) = \prod_{r=1}^{\infty} \frac{1}{1 - X^r}.$$

Il formalismo delle funzioni generatrici permette di rispondere anche a domande più raffinate. Per esempio, in quanti modi è possibile partizionare un intero n come $x_1 + \cdots + x_k$ in modo tale che ogni x_i sia dispari? La risposta è facile: basta fare in modo che i mazzi $\mathcal{D}_r$ con r pari siano vuoti, cioè

$$d_r = \begin{cases} 1 & \text{se } r \text{ è dispari} \\ 0 & \text{se } r \text{ è pari,} \end{cases}$$

dunque in questo caso

$$\mathcal{H}(X) = \prod_{r \text{ dispari}} \frac{1}{1 - X^r}. \tag{1.18}$$

Un'altra cosa che possiamo chiedere è limitare la molteplicità delle carte presenti in una mano. Ad esempio, potremmo volere che sia ammessa solo una singola copia di una carta. Nell'esempio delle partizioni di n, questo equivale a chiedere che tutti gli x_i siano distinti tra loro.

Sia $W \subseteq \mathbb{N}$ con $0 \in W$ l'insieme delle possibili molteplicità che può avere una carta in una mano. Definiamo

$$w(T) := \sum_{k \in W} T^k.$$

Ora, se $h(n, k; W)$ è il numero di mani di peso n con k carte in totale, in cui la molteplicità di ciascuna è un elemento di W, e $\mathcal{H}(X, Y; W)$ è la funzione generatrice ordinaria per gli $h(n, k; W)$, vale un risultato analogo a quello della Proposizione 1.23. La dimostrazione, che ricalca quella dei Teoremi 1.20 e 1.33, si può trovare in [9].

Proposizione 1.34. *Siano $\mathcal{P}$ un* prefab *con mazzi formati da d_n carte, $W \subseteq \mathbb{N}$ con $0 \in W$ un insieme di molteplicità e $w(T)$ definita come sopra. Allora*

$$\mathcal{H}(X, Y; W) = \prod_{r=1}^{\infty} w(YX^r)^{d_r}. \tag{1.19}$$

Nel caso particolare in cui $W = \{0, 1\}$, cioè una carta non può essere presente in più di una copia, la Formula (1.19) si riduce a

$$\mathcal{H}(X, Y; \{0, 1\}) = \prod_{r=1}^{\infty} (1 + YX^r)^{d_r} = \frac{1}{\mathcal{H}(X, -Y)}$$

dove $\mathcal{H}(X, Y) = \mathcal{H}(X, Y; \mathbb{N})$ è la funzione generatrice usuale. Per esempio, le partizioni di n in parti distinte hanno come funzione generatrice

$$\mathcal{H}(X; \{0, 1\}) = \prod_{r=1}^{\infty} (1 + X^r) \overset{\blacktriangleright 15}{=} \prod_{r=1}^{\infty} \frac{1 - X^{2r}}{1 - X^r}.$$

Ma ora i denominatori con r pari si semplificano con i numeratori, lasciando

$$\mathcal{H}(X; \{0, 1\}) = \prod_{r \text{ dispari}} \frac{1}{1 - X^r}$$

che è uguale alla Formula (1.18)! Quindi le partizioni di n in parti dispari sono tante quante quelle in parti distinte. Possiamo generalizzare questo fatto.

Proposizione 1.35. *Sia $m \in \mathbb{N}$ fissato. Le partizioni di n in parti non divisibili per m sono tante quante quelle in parti con molteplicità strettamente minore di m.*

Dimostrazione. Le partizioni di n in parti non divisibili per m hanno come funzione generatrice

$$\prod_{m \nmid r} \frac{1}{1 - X^r}.$$

D'altra parte, considerando $W = \{0, \dots, m - 1\}$, la funzione generatrice con molteplicità limitate è

$$\prod_{r=1}^{\infty} \left(1 + X^r + \cdots + X^{r(m-1)}\right) = \prod_{r=1}^{\infty} \frac{1 - X^{mr}}{1 - X^r}.$$

Dato che nell'ultima espressione i numeratori semplificano esattamente i denominatori con esponente multiplo di m, le due funzioni generatrici coincidono. □

1.7.2 Problema di Frobenius

18/03/2015 ◃ Una generalizzazione del problema delle partizioni di n è il *cambio delle monete*: abbiamo m monete del valore (intero) $1 \leqslant a_1 < \cdots < a_m$ e vogliamo sapere se, prendendone un certo numero di ciascun taglio, sia possibile ottenere una somma n prefissata. In altre parole, vogliamo sapere se esistono $k_1, \ldots, k_m \geqslant 0$ tali che

$$n = \sum_{i=1}^{m} k_i a_i. \tag{1.20}$$

Innanzitutto ci chiediamo per quali n sia possibile farlo. È immediato notare che, se $\mathrm{GCD}(a_1, \ldots, a_m) = d > 1$, il problema non ha soluzione per ogni n non multiplo di d. Se invece n è multiplo di d, ci riconduciamo al caso $\mathrm{GCD}(a_1, \ldots, a_m) = 1$ dividendo tutto per d.

Possiamo allora limitarci a studiare il caso $\mathrm{GCD}(a_1, \ldots, a_m) = 1$. Un teorema dovuto a Issai Schur (che non dimostriamo) ci garantisce che una decomposizione di n è sempre possibile, purché n sia sufficientemente grande.

Teorema 1.36 (Schur)**.** *Se* $\mathrm{GCD}(a_1, \ldots, a_m) = 1$*, allora esiste* n_0 *tale che ogni* $n \geqslant n_0$ *ammette una decomposizione del tipo* (1.20)*.*

Fin qui tutto bene. Le prossime questioni sorgono allora spontanee: vorremmo sapere

1. quale sia l'n_0 minimo per cui vale il Teorema di Schur (tale numero è detto *conduttore* dell'insieme $\{a_1, \ldots, a_m\}$ e indicato con $\kappa(a_1, \ldots, a_m)$);
2. supponendo che n sia decomponibile, in quanti modi sia possibile farlo.

Sfortunatamente non è ancora stata trovata una formula chiusa per trovare il minimo n_0 se $m \geqslant 3$; abbiamo però il risultato per $m = 2$.

Proposizione 1.37. *Siano* $1 \leqslant a < b$ *naturali con* $\mathrm{GCD}(a, b) = 1$*. Il conduttore è* $\kappa = (a-1)(b-1)$*, cioè*

1. *ogni* $n \geqslant \kappa$ *si scrive come* $n = xa + yb$ *per qualche* $x, y \geqslant 0$*;*
2. $\kappa - 1$ *non è esprimibile nella forma precedente.*

Inoltre, esattamente la metà dei numeri $0, \ldots, \kappa - 1$ *è rappresentabile.*

Dimostrazione. Dato che $\mathrm{GCD}(a, b) = 1$, sappiamo che ogni n si può scrivere come $xa + yb$ per qualche $x, y \in \mathbb{Z}$. In particolare, fissati x e y, esistono infinite rappresentazioni di n, che sono date da $n = (x + kb)a + (y - ka)b$ al variare di

[15] Ricorda che $(a+b)(a-b) = a^2 - b^2$…

$k \in \mathbb{Z}$. Se scegliamo $x \in \{0, \dots, b-1\}$, abbiamo che per ogni n esistono unici $x \in \{0, \dots, b-1\}$ e $y \in \mathbb{Z}$ tali che $n = xa + yb$.

In queste condizioni n è rappresentabile con coefficienti positivi se e solo se $y \geqslant 0$.

- Se $y \geqslant 0$, proprio $n = xa + yb$ è una rappresentazione di n.
- Supponiamo che n sia rappresentabile con coefficienti positivi e supponiamo per assurdo che $y < 0$. Per l'ipotesi, esiste $k \in \mathbb{Z}$ tale che

$$\begin{cases} x + kb \geqslant 0 & \text{(1.21a)} \\ y - ka \geqslant 0. & \text{(1.21b)} \end{cases}$$

  Dall'ipotesi $y < 0$ e da (1.21b) ricaviamo che $k \leqslant y/a < 0$ e quindi $kb \leqslant -b$. Ma ora, dato che $x \leqslant b-1$,

$$x + kb \leqslant b - 1 - b = -1$$

  in contraddizione con (1.21a).

Ora, il più grande intero n non rappresentabile con coefficienti positivi si ha per $x = b-1$ e $y = -1$. Infatti, se fosse $x < b-1$, allora

- n non può avere $y \geqslant 0$ (altrimenti sarebbe rappresentabile);
- d'altra parte, se $y < 0$, il numero $(b-1)a + yb$ sarebbe maggiore di n e non rappresentabile per quanto visto poco sopra.

Quindi n deve avere $x = b-1$ e $y < 0$ il più grande possibile, cioè $y = -1$. Dunque si ha

$$\kappa - 1 = (b-1)a - b = ab - a - b$$

e questo dimostra che il conduttore è $\kappa = (a-1)(b-1)$.

Per la seconda parte: sia $0 \leqslant m \leqslant \kappa - 1$ e supponiamo $m = xa + yb$ con $x \in \{0, \dots, b-1\}$. Sia inoltre

$$m' := \kappa - 1 - m = (b - 1 - x)a + (-1 - y)b.$$

Dal momento che $0 \leqslant b - 1 - x < b$, abbiamo che se $y \geqslant 0$ m è rappresentabile e m' no, mentre se $y < 0$ m' è rappresentabile e m no. Dunque, detto h il numero di $m \in \{0, \dots, \kappa/2\}$ rappresentabili, si ha che h è anche il numero di $m' \in \{\kappa/2 + 1, \dots, \kappa - 1\}$ *non* rappresentabili, quindi

$$\#\{m = 0, \dots, \kappa - 1 \mid m \text{ è rappresentabile}\} = h + \frac{\kappa}{2} - h = \frac{\kappa}{2}. \qquad \square$$

Passiamo alla seconda domanda. Impostiamo l'ambiente di lavoro: il *prefab* che studieremo è formato da mazzi quasi tutti vuoti, tranne quelli di peso $a_1, \dots, a_m$ che contengono esattamente una carta. Quindi

$$d_r = \begin{cases} 1 & \text{se } r = a_1, \dots, a_m \\ 0 & \text{altrimenti.} \end{cases}$$

Se $h(n,k)$ è il numero di rappresentazioni di n che usano esattamente k monete, cioè quelle tali che $\sum k_i = k$, allora dal Teorema 1.33 abbiamo

$$\mathcal{H}(X,Y) = \frac{1}{1-YX^{a_1}} \cdots \frac{1}{1-YX^{a_m}}$$

oppure, se non ci interessa il numero k di monete, si può come al solito considerare la somma al variare dei possibili k valutando in $Y = 1$:

$$\mathcal{H}(X) = \frac{1}{1-X^{a_1}} \cdots \frac{1}{1-X^{a_m}}. \tag{1.22}$$

Nei prossimi paragrafi non calcoleremo direttamente h_n ma ne stimeremo il comportamento asintotico.

Definizione 1.38. Si dice che la successione $f(n)$ *si comporta asintoticamente* come la successione $g(n)$ se

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

In tal caso scriviamo $f(n) \sim g(n)$.

Dunque, chi sono i poli di $\mathcal{H}(X)$? Dall'espressione (1.22) sappiamo che devono essere radici dell'unità. In particolare, $X = 1$ è un polo di ordine m, perché ogni fattore del denominatore è divisibile per $(1-X)$. D'altra parte, se $\zeta \neq 1$ è una radice primitiva q-esima dell'unità e un polo di $\mathcal{H}(X)$, essa non può essere radice comune a tutti i fattori del denominatore (altrimenti $q \mid a_i$ per ogni i, contro l'ipotesi di $\mathrm{GCD}(a_1, \dots, a_m) = 1$). In particolare i poli $\zeta \neq 1$ hanno molteplicità *strettamente minore* di m.

Sia ζ un polo di $\mathcal{H}(X)$ di molteplicità r. Il contributo del polo ζ nell'espansione in frazioni parziali di $\mathcal{H}$ è

$$\frac{c_1}{\left(1-\frac{X}{\zeta}\right)^r} + \frac{c_2}{\left(1-\frac{X}{\zeta}\right)^{r-1}} + \cdots + \frac{c_r}{\left(1-\frac{X}{\zeta}\right)} \tag{1.23}$$

dove $c_1, \dots, c_r$ dipendono ovviamente da ζ. A questo punto, ricordando che

$$\frac{1}{(1-X)^{k+1}} = \sum_{n=0}^{\infty} \binom{-k-1}{n} (-1)^n X^n = \sum_{n=0}^{\infty} \binom{n+k}{k} X^n$$

e osservando che il coefficiente di X^n, sviluppando il binomiale, è asintotico a $n^k/k!$, nella somma (1.23) il coefficiente di X^n è asintotico a

$$c\frac{n^{r-1}}{(r-1)!}$$

con c costante opportuna (gli altri addendi della somma sono trascurati perché di ordine inferiore). Dato che il polo $\zeta = 1$ ha molteplicità m, che è la massima possibile, otteniamo infine

$$h_n \sim C\frac{n^{m-1}}{(m-1)!}$$

sempre per C costante opportuna, che ora proviamo a determinare.[16] Per quanto visto finora,

$$\mathcal{H}(X) = \frac{C}{(1-X)^m} + \mathcal{O}\left(\frac{1}{(1-X)^{m-1}}\right).$$

Moltiplicando per $(1-X)^m$ abbiamo

$$C + \mathcal{O}(1-X) = (1-X)^m\,\mathcal{H}(X) = \frac{1-X}{1-X^{a_1}}\cdots\frac{1-X}{1-X^{a_m}}$$

da cui

$$C = \lim_{X\to 1}\frac{1-X}{1-X^{a_1}}\cdots\frac{1-X}{1-X^{a_m}} = \lim_{X\to 1}\prod_{j=1}^{m}\left(\frac{1}{1+X+\cdots+X^{a_j-1}}\right) = \frac{1}{a_1\cdots a_m} \tag{1.24}$$

e infine

$$h_n \sim \frac{n^{m-1}}{(m-1)!a_1\cdots a_m}.$$

Nel caso $m = 2$ possiamo dire qualcosa di più preciso. Siano a, b con $\mathrm{GCD}(a,b) = 1$: sappiamo che

$$\mathcal{H}(X) = \frac{1}{1-X^a}\cdot\frac{1}{1-X^b}. \tag{1.25}$$

L'unico polo con molteplicità massima $m = 2$ è 1; gli altri poli (cioè le radici a-esime e b-esime dell'unità) sono tutti semplici. Quindi l'espansione in frazioni parziali è

$$\mathcal{H}(X) = \frac{A}{(1-X)^2} + \frac{B}{1-X} + \sum_{\substack{\omega^a=1\\ \omega\neq 1}}\frac{C_\omega}{\left(1-\frac{X}{\omega}\right)} + \sum_{\substack{\zeta^b=1\\ \omega\neq 1}}\frac{D_\zeta}{\left(1-\frac{X}{\zeta}\right)} \tag{1.26}$$

[16] Questa formula per il comportamento asintotico in particolare ci dice che definitivamente $h_n \neq 0$, dimostrando il Teorema di Schur.

per opportune costanti A, B, C_ω e D_ζ. Dall'Equazione (1.24) sappiamo che $A = 1/(ab)$; per ottenere B moltiplichiamo per $(1-X)^2$, deriviamo e valutiamo in $X = 1$: nell'espressione (1.26) resta solo $-B$, mentre utilizzando la Formula (1.25) dobbiamo calcolare

$$\frac{d}{dX}\left((1-X)^2\,\mathcal{H}(X)\right) = \frac{d}{dX}\left(\frac{1}{1+X+\cdots+X^{a-1}}\cdot\frac{1}{1+X+\cdots+X^{b-1}}\right) =$$
$$= -\frac{1+2X+\cdots+(a-1)X^{a-2}}{(1+\cdots+X^{a-1})^2(1+\cdots+X^{b-1})} - \frac{1+2X+\cdots+(b-1)X^{b-2}}{(1+\cdots+X^{a-1})(1+\cdots+X^{b-1})^2}.$$

Valutando in $X = 1$ si ottiene

$$-B = -\frac{(a-1)a}{2a^2b} - \frac{(b-1)b}{2ab^2}$$

da cui $B = (a+b-2)/(2ab)$. Per trovare C_ω moltiplichiamo per $(1-X/\omega)$ e valutiamo per $X = \omega$, in modo che si salvi solo il coefficiente cercato: alla fine risulta $C_\omega = 1/(a(1-\omega^b))$. Un procedimento analogo porta a $D_\zeta = 1/(b(1-\zeta^a))$. Possiamo quindi prendere il coefficiente di X^n in (1.26) ottenendo

$$h_n = \frac{n}{ab} + \frac{a+b}{2ab} + \sum_{\substack{\omega^a=1\\ \omega\neq 1}} \frac{C_\omega}{\omega^n} + \sum_{\substack{\zeta^b=1\\ \omega\neq 1}} \frac{D_\zeta}{\zeta^n}$$

cioè: h_n è dato dalla somma di una funzione lineare in n,

$$\frac{n}{ab} + \frac{a+b}{2ab},$$

e una funzione periodica in n,

$$\sum_{\substack{\omega^a=1\\ \omega\neq 1}} \frac{C_\omega}{\omega^n} + \sum_{\substack{\zeta^b=1\\ \omega\neq 1}} \frac{D_\zeta}{\zeta^n}$$

di periodo ab e media nulla (perché è una somma estesa sulle radici dell'unità).

1.8 Funzioni simmetriche

Vediamo un'ultima applicazione delle funzioni generatrici.

Definizione 1.39. Sia $\mathbb{K}$ un campo. Una funzione razionale in n variabili $f \in \mathbb{K}(X_1, \ldots, X_n)$ è detta *simmetrica* se è invariante sotto l'azione di S_n sulle variabili, cioè se

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

per ogni $\sigma \in S_n$.

Tra le funzioni simmetriche rivestono un ruolo di particolare importanza i *polinomi simmetrici elementari*, che sono definiti da

$$e_i(X_1, \dots, X_n) := \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant n} X_{j_1} \cdots X_{j_i}$$

per $i = 0, \dots, n$ ed $e_i(X_1, \dots, X_n) = 0$ per $i > n$ (per convenzione). In altre parole, l'i-esimo polinomio simmetrico elementare è dato dalla somma di tutti i possibili prodotti distinti di i variabili. Ad esempio, per $n = 3$ abbiamo:

$$\begin{aligned} e_0(X_1, X_2, X_3) &= 1 \\ e_1(X_1, X_2, X_3) &= X_1 + X_2 + X_3 \\ e_2(X_1, X_2, X_3) &= X_1X_2 + X_1X_3 + X_2X_3 \\ e_3(X_1, X_2, X_3) &= X_1X_2X_3. \end{aligned}$$

I polinomi simmetrici elementari sono dati dai coefficienti di

$$e(T) := (T - X_1) \cdots (T - X_n) \in \mathbb{K}[X_1, \dots, X_n][T], \tag{1.27}$$

e precisamente vale che

$$e(T) = T^n - e_1T^{n-1} + e_2T^{n-2} - \cdots + (-1)^n e_n.$$

Proposizione 1.40. *Sia $\mathbb{K}$ un campo di caratteristica 0. Sia $\mathbb{E} := \mathbb{K}(X_1, \dots, X_n)^{S_n}$ il campo delle funzioni simmetriche, cioè le funzioni razionali lasciate fisse dall'azione di S_n. Allora*

$$\mathbb{E} = \mathbb{K}(e_1, \dots, e_n),$$

cioè: le funzioni simmetriche elementari generano il campo delle funzioni simmetriche.

Dimostrazione. Ovviamente $\mathbb{K}(e_1, \dots, e_n) \subseteq \mathbb{E}$, quindi dimostriamo l'altro contenimento. Il polinomio $e(T)$ definito in (1.27) ha coefficienti in $\mathbb{K}(e_1, \dots, e_n)$ ed il suo campo di spezzamento è $\mathbb{K}(X_1, \dots, X_n)$; per un risultato noto di teoria di Galois, il grado dell'estensione è

$$[\mathbb{K}(X_1, \dots, X_n) : \mathbb{K}(e_1, \dots, e_n)] \leqslant n!.$$

Ora, l'estensione $\mathbb{K}(X_1, \dots, X_n) \supseteq \mathbb{E}$ è di Galois con gruppo di Galois isomorfo a S_n, dunque ha grado esattamente $n!$. Ma allora da

$$[\mathbb{K}(X_1, \dots, X_n) : \mathbb{K}(e_1, \dots, e_n)] = [\mathbb{K}(X_1, \dots, X_n) : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{K}(e_1, \dots, e_n)] \leqslant n!$$

segue che $[\mathbb{E} : \mathbb{K}(e_1, \dots, e_n)] = 1$ e di conseguenza $\mathbb{E} = \mathbb{K}(e_1, \dots, e_n)$. □

Passiamo ora ai *polinomi simmetrici*. La definizione è la stessa di funzione simmetrica: un polinomio $p \in A[X_1, \ldots, X_n]$ (dove A è un anello commutativo con identità) si dice *simmetrico* se è invariante sotto permutazione delle variabili. Ovviamente rientrano in questa categoria i polinomi simmetrici elementari introdotti sopra. È ancora vero che gli e_i generano tutti i polinomi simmetrici? La risposta è sì, ma prima di dimostrarlo premettiamo una definizione.

Definizione 1.41. Sia $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ un monomio. Definiamo *peso* di $\mathbf{X}^\alpha$ la quantità $w(\mathbf{X}^\alpha) = \alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$. Per un polinomio $p \in A[X_1, \ldots, X_n]$ definiamo *peso* di p, indicato con $w(p)$, il massimo dei pesi dei suoi monomi.

Osserviamo che un polinomio $g \in A[e_1, \ldots, e_n]$ può essere visto anche come polinomio nelle indeterminate "vere" $X_1, \ldots, X_n$. Poiché l'i-esimo polinomio simmetrico elementare ha grado i, si ha che $w(g)$ (visto come polinomio in $e_1, \ldots, e_n$) è uguale a $\deg(g)$ (visto come polinomio in $X_1, \ldots, X_n$).

Proposizione 1.42. *I polinomi simmetrici sono* $A[e_1, \ldots, e_n]$.[17] *Inoltre, se* f *è un polinomio simmetrico con* $\deg(f) = d$ *e vale che* $f = g(e_1, \ldots, e_n)$*, allora* $w(g) \leqslant d$.

Dimostrazione. La dimostrazione procede per induzione doppia: la prima sul numero di variabili n e, per n fissato, sul grado dei polinomi d.

Il caso $n = 1$ è del tutto ovvio; supponiamo allora che la tesi sia vera per i polinomi in $n-1$ variabili. Per prima cosa riprendiamo il polinomio definito in (1.27) e valutiamolo in $X_n = 0$: si ottiene

$$F(T) := (T - X_1) \cdots (T - X_{n-1})T = T^n - (e_1)_0 T^{n-1} + \cdots + (-1)^{n-1}(e_{n-1})_0 T$$

dove $(e_i)_0$ sono i polinomi simmetrici elementari in $n-1$ variabili.

Consideriamo un polinomio simmetrico $f \in A[X_1, \ldots, X_n]$ con $\deg(f) = d$. Abbiamo che $f(X_1, \ldots, X_{n-1}, 0)$ è un polinomio simmetrico in $n-1$ variabili di grado $\deg(f(X_1, \ldots, X_{n-1}, 0)) \leqslant d$, dunque per ipotesi induttiva

$$f(X_1, \ldots, X_{n-1}, 0) = g_1((e_1)_0, \ldots, (e_{n-1})_0)$$

con $w(g_1) \leqslant \deg(f(X_1, \ldots, X_{n-1}, 0)) \leqslant d$. A questo punto riprendiamo i polinomi simmetrici elementari in n variabili $e_1, \ldots, e_n$ e consideriamo il polinomio

$$g_1(e_1, \ldots, e_{n-1}).$$

Esso, visto come polinomio in $X_1, \ldots, X_n$, è simmetrico ed ha grado minore o uguale a d (per l'osservazione sopra).

[17] Notiamo che sono *polinomi* in $e_1, \ldots, e_n$: non è necessario ricorrere alle funzioni razionali!

Definiamo ora $f_1(X_1, \dots, X_n) := f(X_1, \dots, X_n) - g_1(e_1, \dots, e_{n-1})$. Esso è ancora un polinomio simmetrico in $X_1, \dots, X_n$ di grado $\deg(f_1) \leqslant d$. Valutando in $X_n = 0$ otteniamo

$$f_1(X_1, \dots, X_{n-1}, 0) = f(X_1, \dots, X_{n-1}, 0) - g_1((e_1)_0, \dots, (e_{n-1})_0) = 0,$$

dunque X_n divide $f_1(X_1, \dots, X_n)$. Per simmetria f_1 è divisibile anche per X_i per ogni $i = 1, \dots, n$ e di conseguenza anche per

$$\prod_{i=1}^{n} X_i = e_n;$$

possiamo allora scrivere $f_1 = e_n \cdot f_2(X_1, \dots, X_n)$ per un qualche polinomio simmetrico f_2 con $\deg(f_2) \leqslant d - n < d$, a cui poter applicare l'ipotesi induttiva sul grado:

$$f_2(X_1, \dots, X_n) = g_2(e_1, \dots, e_n).$$

Di conseguenza

$$\begin{aligned} f(X_1, \dots, X_n) &= f_1(X_1, \dots, X_n) + g_1(e_1, \dots, e_{n-1}) = \\ &= e_n \cdot f_2(X_1, \dots, X_n) + g_1(e_1, \dots, e_{n-1}) = \\ &= e_n \cdot g_2(e_1, \dots, e_n) + g_1(e_1, \dots, e_{n-1}), \end{aligned}$$

cioè $f \in A[e_1, \dots, e_n]$. □

Si potrebbe dimostrare che $e_1, \dots, e_n$ sono *algebricamente indipendenti*, cioè che non esiste un polinomio in n variabili $p \in A[T_1, \dots, T_n]$ non nullo tale che $p(e_1, \dots, e_n) = 0$. In altre parole, $A[e_1, \dots, e_n]$ è isomorfo a un anello di polinomi "vero" $A[T_1, \dots, T_n]$.

Dove entrano in gioco le funzioni generatrici? Possiamo definirne una per i polinomi simmetrici elementari:

$$E(T) := \sum_{r=0}^{\infty} e_r T^r \overset{(\star)}{=} \prod_{i \geqslant 1} (1 + X_i T). \tag{1.28}$$

Notiamo che, per n fissato, sia la serie che il prodotto in (1.28) hanno un numero finito di termini. In ogni caso, è possibile definire (in modo formale) polinomi simmetrici in infinite variabili, ma non ce ne occuperemo.

La relazione $(\star)$ è dovuta al fatto che, per ogni $i = 1, \dots, n$, possiamo scegliere se mettere la variabile X_i in un termine oppure no; l'indeterminata T conta quante variabili abbiamo scelto. Il coefficiente di T^r, dunque, è dato dalla somma di tutti i prodotti possibili di r variabili distinte, che è proprio e_r.

Introduciamo ora un nuovo tipo di funzioni simmetriche: i *polinomi simmetrici (omogenei) completi* di grado r. Essi sono dati dalla somma di tutti i monomi di grado r:

$$h_r(X_1, \dots, X_n) := \sum_{1 \leqslant j_1 \leqslant \cdots \leqslant j_r \leqslant n} X_{j_1} \cdots X_{j_r}.$$

Ad esempio, per $n = 3$ e $r = 2$ si ha

$$h_2(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2 + X_1X_2 + X_1X_3 + X_2X_3.$$

Anche di questi polinomi possiamo scrivere la funzione generatrice

$$H(T) := \sum_{r=0}^{\infty} h_r T^r,$$

la quale stavolta si estende effettivamente fino all'infinito.

Possiamo scrivere $H(T)$ come prodotto:

$$H(T) = \prod_{i \geqslant 1} (1 + X_i T + X_i^2 T^2 + \cdots) = \prod_{i \geqslant 1} (1 - X_i T)^{-1},$$

infatti per ogni $i = 1, \dots, n$ possiamo scegliere se mettere in un termine la variabile X_i e con quale grado; l'opportuna potenza di T tiene traccia proprio della somma dei gradi scelti.

Ora, non può non colpire il fatto che

$$E(-T)H(T) = 1.$$

Per i termini noti, questa relazione dice semplicemente $h_0 e_0 = 1 \cdot 1 = 1$. Il discorso cambia considerando i termini di grado $r > 0$.

Proposizione 1.43. *Per ogni $r > 0$ e per ogni n vale*

$$\sum_{i=0}^{r} (-1)^i e_i(X_1, \dots, X_n) h_{r-i}(X_1, \dots, X_n) = 0.$$

La proposizione precedente ci dà una formula ricorsiva per calcolare gli h_r a partire dagli e_r e viceversa. Inoltre la mappa

$$\begin{array}{ccc} \omega : A[e_1, \dots, e_n] & \longrightarrow & A[h_1, \dots, h_n] \\ e_i & \longmapsto & h_i \end{array}$$

è un involuzione (cioè $\omega^2 = \mathrm{Id}$), quindi è un isomorfismo di anelli. Ne consegue che anche i polinomi simmetrici completi sono un insieme di generatori per i polinomi simmetrici.

Infine, abbiamo un'ultima categoria di polinomi simmetrici: le *funzioni simmetriche di Newton*. Esse sono definite da[18]

$$p_r(X_1, \dots, X_n) := \sum_{i=1}^{n} X_i^r.$$

La funzione generatrice per i polinomi p_r è leggermente modificata in modo che le formule abbiano un aspetto più carino:

$$P(T) := \sum_{r=1}^{\infty} p_r T^{r-1}.$$

In effetti le manipolazioni non sono difficili:

$$\begin{aligned} P(T) &= \sum_{r=1}^{\infty} \Big(\sum_{i \geqslant 1} X_i^r \Big) T^{r-1} = \sum_{i \geqslant 1} \sum_{r=1}^{\infty} X_i^r T^{r-1} = \sum_{i \geqslant 1} \frac{X_i}{1 - X_i T} = \\ &= \sum_{i \geqslant 1} \frac{d}{dT} \ln\left(\frac{1}{1 - X_i T} \right) = \frac{d}{dT} \sum_{i \geqslant 1} \ln\left(\frac{1}{1 - X_i T} \right) = \frac{d}{dT} \ln\left(\prod_{i \geqslant 1} \frac{1}{1 - X_i T} \right) = \\ &= \frac{d}{dT} \ln(H(T)) = \frac{H'(T)}{H(T)} \end{aligned}$$

e in maniera del tutto analoga

$$P(-T) = \frac{E'(T)}{E(T)}.$$

Da queste relazioni possiamo ottenere le formule ricorsive che legano p_r con h_r ed e_r:

$$r h_r = \sum_{k=1}^{r} p_k h_{r-k}, \qquad r e_r = \sum_{k=1}^{r} (-1)^{k-1} p_k e_{r-k}.$$

[18] La lettera p sta per *power sum*.

Capitolo 2

Poset

Questo capitolo sarà dedicato allo studio dei *poset*, cioè degli insiemi parzialmente ordinati (dall'inglese *partially ordered set*). Vedremo soprattutto tecniche molto generali che possono essere applicate in numerosi casi diversi, evitando soluzioni furbe che però risolvono (magari anche brillantemente) un solo problema specifico. ▹ *23/03/2015*

2.1 Prime definizioni

Iniziamo proprio con il definire il protagonista di questo capitolo.

Definizione 2.1. Un *insieme parzialmente ordinato*, in breve *poset*, è una coppia $(P, \leqslant)$ dove P è un insieme e $\leqslant$ è una relazione d'ordine su P, ovvero una relazione binaria

1. riflessiva, cioè $\forall\, x \in P\ x \leqslant x$;
2. antisimmetrica, cioè $\forall\, x, y \in P\ (x \leqslant y) \wedge (y \leqslant x) \to x = y$;
3. transitiva, cioè $\forall\, x, y, z \in P\ (x \leqslant y) \wedge (y \leqslant z) \to x \leqslant z$.

Notazione 2.2. Come è usuale, useremo alcune abbreviazioni standard: scriveremo "$x < y$" al posto di "$x \leqslant y \wedge x \neq y$" e "$x \leqslant y \leqslant z$" al posto di "$x \leqslant y \wedge y \leqslant z$".

Definizione 2.3. Due elementi $s, t \in P$ si dicono *confrontabili* se vale almeno una tra $s \leqslant t$ e $t \leqslant s$, *non confrontabili* altrimenti.

Esempio 2.1. Vediamo alcuni esempi di poset.

1. Il poset $\{1, \ldots, n\}$ con l'ordinamento standard dei numeri naturali sarà indicato con $[n]$.

2. $\wp(\{1,\dots,n\})$, con l'ordinamento dato dall'inclusione, è un poset detto *algebra booleana standard* B_n.

3. Indichiamo con Π_n l'insieme delle partizioni di $\{1,\dots,n\}$ con l'ordine dato dal raffinamento (se σ, τ sono partizioni, diciamo che σ è più fine di τ se per ogni $S \in \sigma$ esiste $T \in \tau$ tale che $S \subseteq T$; ad esempio, $\sigma = \{\{1,2\},\{3\},\{4,5\},\{6,7\},\{8,9\}\}$ è più fine di $\tau = \{\{1,2,3\},\{4,5,6,7\},\{8,9\}\}$, dunque $\sigma \leqslant \tau$).

4. Infine, $B_n(q)$ sarà il poset degli $\mathbb{F}_q$-sottospazi vettoriali di $(\mathbb{F}_q)^n$ ordinati dall'inclusione.

Definizione 2.4. Due poset $(P,\leqslant)$ e $(Q,\preccurlyeq)$ si dicono *isomorfi* se esiste una funzione biiettiva $f\colon P \to Q$ che rispetta gli ordini, cioè tale che per ogni $p,q \in P$ si ha $p \leqslant q$ se e solo se $f(p) \preccurlyeq f(q)$.

Più delicata è la questione di cosa si intenda per *sottoposet*. Dato un poset $(P,\leqslant)$, potremmo considerare un poset $(P,\preccurlyeq)$ che ha lo stesso insieme supporto ma solo alcune relazioni del poset originale (cioè: se $p \preccurlyeq q$ allora $p \leqslant q$, non necessariamente il viceversa). Questo è il concetto di *sottoposet debole* (*weak subposet*), che noi *non* adotteremo.

Definizione 2.5. Siano $(P,\leqslant)$ e $(\Lambda,\preccurlyeq)$ due poset con $\Lambda \subseteq P$. Diciamo che Λ è un *sottoposet* (*forte*, o *indotto*) di P se per ogni $s,t \in \Lambda$ si ha $s \preccurlyeq t$ se e solo se $s \leqslant t$. Se $\Lambda \subseteq P$ è un sottoposet, indicheremo con lo stesso simbolo gli ordinamenti su Λ e P.

Terminiamo questa sezione introduttiva con le ultime definizioni.

Definizione 2.6. Sia P un poset e siano $s,t \in P$ con $s \leqslant t$. Definiamo *intervallo (chiuso)* di estremi s e t l'insieme $[s,t] := \{u \in P \mid s \leqslant u \leqslant t\}$. Definiamo *intervallo aperto* di estremi s e t l'insieme $(s,t) := \{u \in P \mid s < u < t\}$. Indicheremo con $\mathcal{I}nt(P)$ l'insieme degli intervalli chiusi di P.

Definizione 2.7. Un poset P è *localmente finito* se ogni suo intervallo è un insieme finito.

Osserviamo che l'insieme vuoto non può essere un intervallo chiuso, ma è un intervallo aperto: scelto comunque un $t \in P$, allora $\varnothing = (t,t)$.

Definizione 2.8. Siano P un poset e $s,t \in P$. Diciamo che t *ricopre* s se $s < t$ e non esiste $u \in P$ tale che $s < u < t$. Equivalentemente, t ricopre s se $[s,t] = \{s,t\}$. Useremo il simbolo $s \lessdot t$ per dire che t ricopre s.

Definizione 2.9. Sia P un poset. Un elemento $g \in P$ è detto *massimale* se non esiste $a \in P$ tale che $a > g$; un elemento $m \in P$ è detto *minimale* se non esiste $b \in P$ tale che $b < m$.

Definizione 2.10. Sia P un poset. Un elemento $g \in P$ è detto *massimo* se per ogni $a \in P$ si ha $a \leqslant g$; un elemento $m \in P$ è detto *minimo* se per ogni $b \in P$ si ha $b \geqslant m$.

Un poset P può non avere un elemento massimo (o minimo); tuttavia se tale elemento esiste, è unico. Inoltre un poset può avere più elementi massimali (o minimali), ma se esiste il massimo (o il minimo) in P, esso è l'unico elemento massimale (o minimale) di P.

Definizione 2.11. Una *catena* è un poset in cui ogni coppia di elementi è comparabile. Un sottoinsieme C di un poset P è una *catena* di P se è una catena come sottoposet indotto.

Ad esempio, il poset $[n]$ è una catena, perché l'ordinamento dei numeri naturali è totale.

Definizione 2.12. Una catena $C \subseteq P$ è *massimale* se non è contenuta strettamente in nessun'altra catena di P. Una catena $C \subseteq P$ è *saturata* se non esiste $u \in P \smallsetminus C$ tale che $s < u < t$ per qualche $s, t \in C$ e $C \cup \{u\}$ sia ancora una catena di P.

In altre parole: non possiamo aggiungere un elemento di P in mezzo a una sua catena saturata; possiamo però allungare la catena aggiungendo elementi agli estremi.

Definizione 2.13. Se C è una catena finita, la sua *lunghezza* è $\ell(C) := \#(C) - 1$.[1] Se P è un poset (finito), la sua *lunghezza* è il massimo delle lunghezze delle sue catene, cioè $\ell(P) := \max\{\ell(C) \mid C \text{ catena di } P\}$.

Definizione 2.14. Un poset (finito) P è detto *graduato* di *rango* n se ogni sua catena massimale ha la stessa lunghezza pari a n. In tal caso è definita una funzione *rango* $\rho\colon P \to \{0, \dots, n\}$ tale che $\rho(s) = 0$ se s è minimale e $\rho(t) = \rho(s) + 1$ se $t \gtrdot s$. Vale ovviamente che $\rho(t) - \rho(s) = \ell(s, t)$.

Definizione 2.15. Una *multicatena* in P è una catena in cui sono ammessi elementi ripetuti, cioè è un multiinsieme i cui elementi sono una catena di P.

In particolare, una multicatena di lunghezza n in P è una successione di elementi

$$t_0 \leqslant t_1 \leqslant \cdots \leqslant t_n.$$

[1] Se la catena è un intervallo $[s, t]$, scriveremo $\ell(s, t)$ anziché $\ell([s, t])$ per non appesantire la notazione.

2.2 L'algebra di incidenza

In questa sezione introduciamo una struttura combinatoria molto utile nello studio dei poset.

Definizione 2.16. Siano P un poset localmente finito e $\mathbb{K}$ un campo.[2] L'insieme delle funzioni $f\colon \mathcal{I}nt(P) \to \mathbb{K}$ è una $\mathbb{K}$-algebra, detta *algebra di incidenza* di P e indicata con $\mathcal{I}(P)$.

In realtà nella definizione precedente abbiamo solo detto chi è l'insieme supporto dell'algebra di incidenza: dobbiamo definire le operazioni. Non ci sono problemi per somma e prodotto per scalari di $\mathbb{K}$, perché sono le usuali operazioni che rendono un qualunque insieme di funzioni a valori in $\mathbb{K}$ un $\mathbb{K}$-spazio vettoriale. Il prodotto, invece, è una sorta di convoluzione:[3]

$$(fg)(s,t) := \sum_{u \in [s,t]} f(s,u)g(u,t).$$

A volte scriveremo $s \leqslant u \leqslant t$ anziché $u \in [s,t]$ come indice di sommatoria. Notiamo che il prodotto è ben definito perché P è localmente finito.

L'algebra $\mathcal{I}(P)$ è associativa e non commutativa. Non lo verifichiamo subito: vedremo a breve che è isomorfa a una sottoalgebra dell'algebra delle matrici. Inoltre ha un'identità:

$$\delta(s,t) := \begin{cases} 1 & \text{se } s = t \\ 0 & \text{altrimenti.} \end{cases}$$

Per mostrare l'isomorfismo tra $\mathcal{I}(P)$ e una sottoalgebra di matrici, è comodo pensare a una $f\colon \mathcal{I}nt(P) \to \mathbb{K}$ come a una combinazione $\mathbb{K}$-lineare (formale) di intervalli, cioè a un elemento del $\mathbb{K}$-spazio vettoriale libero generato dagli intervalli:

$$f = \sum_{[s,t] \in \mathcal{I}nt(P)} f(s,t)[s,t]. \tag{2.1}$$

Per definire il prodotto in questo caso basta vedere cosa significa moltiplicare due intervalli: poniamo

$$[s,t][u,v] := \begin{cases} [s,v] & \text{se } t = u \\ 0 & \text{altrimenti.} \end{cases}$$

È immediato verificare che i due modi di vedere le funzioni $f\colon \mathcal{I}nt(P) \to \mathbb{K}$ sono equivalenti.

[2] Se non diversamente specificato, considereremo sempre $\mathbb{K} = \mathbb{C}$, anche se parleremo di un campo generico. (*NdA:* non sono sicuro che quanto è detto nel seguito valga anche per campi $\mathbb{K}$ con $\mathrm{char}(\mathbb{K}) > 0$.)

[3] Per non appesantire la notazione, d'ora in avanti scriveremo $f(s,t)$ al posto di $f([s,t])$.

Prima di passare alle matrici diamo ancora una definizione importante.

Definizione 2.17. Il *diagramma di Hasse* di un poset P è un grafo i cui vertici sono gli elementi di P e c'è un arco tra s e t se t ricopre s. Il grafo normalmente non è orientato e convenzionalmente se $t \geqslant s$ allora t è disegnato più in alto di s.

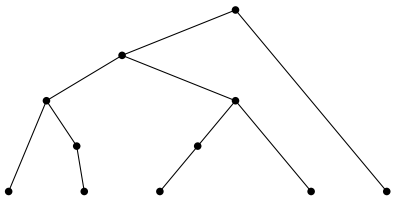


Figura 2.1: Esempio di diagramma di Hasse.

Con l'aiuto di un diagramma di Hasse, se P è un poset finito (cosa che supporremo per il resto della sezione, perché vorremmo lavorare con matrici di dimensione finita...) possiamo etichettare i suoi elementi con $t_1, \ldots, t_{\#(P)}$ in modo che se $t_i < t_j$ in P allora $i < j$. Infatti possiamo procedere nel seguente modo:

1. per ogni $p \in P$ ne calcoliamo l'*altezza*, cioè la massima distanza di p da un elemento minimale;
2. prendiamo gli elementi di altezza 0 (cioè gli elementi minimali) e li ordiniamo con $t_1, \ldots, t_k$;
3. poi prendiamo gli elementi di altezza 1 e li ordiniamo a partire da t_{k+1};
4. proseguiamo ordinando gli elementi di altezza 2 e così via finché non abbiamo esaurito gli elementi.

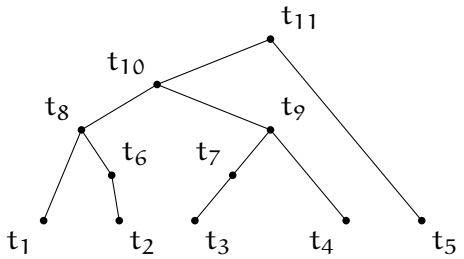


Figura 2.2: Il diagramma di Hasse della Figura 2.1 con i vertici ordinati.

Dopo aver ordinato in questo modo i vertici, possiamo associare a $\mathcal{I}(P)$ una matrice in $\mathcal{M}_{\#(P)}(\mathbb{K})$ triangolare superiore: se m_{ij} è l'elemento di posto (i,j), allora

$$m_{ij} := \begin{cases} 0 & \text{se } t_i \not\leqslant t_j \\ f(t_i, t_j) & \text{altrimenti.} \end{cases}$$

Ovviamente si ha che la matrice è triangolare superiore (se $i > j$, $t_i \not\leqslant t_j$.)

Esempio 2.2. Consideriamo il poset descritto dal diagramma di Hasse in Figura 2.3, in cui abbiamo già rietichettato i vertici. Per inciso, questo non è l'unico modo per etichettare i vertici in modo che se $t_i < t_j$ allora $i < j$ (e naturalmente ci si è chiesti in quanti modi si possa fare!).

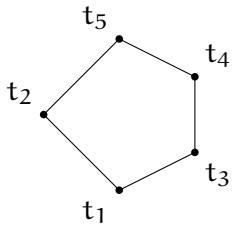


Figura 2.3: Diagramma di Hasse per l'Esempio 2.2.

L'elemento di posto (i,j) identifica l'intervallo $[t_i, t_j]$, quindi la matrice associata a una f deve avere zeri in posti (i,j) in cui t_i e t_j non sono comparabili (oppure se $t_i > t_j$), cioè deve essere della forma

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

dove un simbolo $*$ indica i posti che possono essere occupati da elementi di $\mathbb{K}$ diversi da 0.

Effettivamente, le matrici in cui ci sono zeri in posti prefissati formano una sottoalgebra delle matrici. Se associamo a una $f \in \mathcal{I}(P)$ una matrice nel modo definito sopra, al prodotto fg corrisponde l'usuale prodotto (righe per colonne) tra matrici. È sufficiente mostrarlo per le matrici della forma E_{ij}, cioè matrici con 1 al posto (i,j) e 0 altrove: esse corrispondono alla funzione $f \in \mathcal{I}(P)$ che assegna 1 all'intervallo $[t_i, t_j]$ e 0 agli altri intervalli, o se si preferisce alla funzione

$f = [t_i, t_j]$ nella notazione introdotta in (2.1). Ma è banale dimostrare che

$$E_{ij}E_{st} = \begin{cases} E_{it} & \text{se } j = s \\ 0 & \text{altrimenti.} \end{cases}$$

Perché abbiamo introdotto l'algebra di incidenza? Nella prossima sezione vedremo un particolare elemento di quest'algebra, la *funzione di Möbius* del poset, che avrà numerose applicazioni. Per il momento proseguiamo con lo studio di $\mathcal{I}(P)$ chiedendoci: quando una funzione è invertibile?

Proposizione 2.18. *Sia $f \in \mathcal{I}(P)$. Le seguenti sono equivalenti:*

1. *f ha un'inversa sinistra;*
2. *f ha un'inversa destra;*
3. *f ha un'inversa bilatera (che coincide necessariamente con l'unica inversa sinistra e l'unica inversa destra);*
4. *$f(t,t) \neq 0$ per ogni $t \in P$.*

Se f^{-1} esiste, allora $f^{-1}(s,u)$ dipende solo dai valori assunti da f sui sottointervalli di $[s,u]$.

Dimostrazione. $\boxed{2. \Leftrightarrow 4.}$ Imponendo la relazione $fg = \delta$ si scopre che dev'essere

$$f(s,s)g(s,s) = 1, \tag{2.2a}$$

$$f(s,s)g(s,u) + \sum_{s<t\leqslant u} f(s,t)g(t,u) = 0. \tag{2.2b}$$

Quindi, supponendo $f(s,s) \neq 0$, dall'Equazione (2.2b) si ricava che

$$g(s,u) = -f(s,s)^{-1} \sum_{s<t\leqslant u} f(s,t)g(t,u).$$

Questa formula permette di definire g ricorsivamente, visto che a destra abbiamo g definita su sottointervalli propri di $[s,u]$ (e $g(s,u)$ dipende solo dai valori assunti da f in $[s,u]$). Viceversa, se sappiamo che g esiste, allora da (2.2a) dev'essere $f(s,s) \neq 0$.
$\boxed{1. \Leftrightarrow 4.}$ Imponendo $hf = \delta$ e ripetendo i conti visti nel caso precedente si ha la tesi.
$\boxed{(1. \text{ e } 2.) \Leftrightarrow 3.}$ Ovviamente un'inversa bilatera è sia sinistra che destra. Viceversa, se h è inversa sinistra e g è inversa destra, per associatività si ha

$$h = h\delta = h(fg) = (hf)g = \delta g = g$$

da cui $h = g$ è anche inversa bilatera. □

Presentiamo anche una dimostrazione alternativa (che funziona per poset *finiti*) del fatto che se f ha un'inversa destra g, allora essa è anche inversa sinistra.

Abbiamo visto che f è interpretabile come una matrice; in quanto tale soddisfa il proprio polinomio caratteristico:

$$f^n + a_{n-1}f^{n-1} + \cdots + a_0 = 0. \tag{2.3}$$

Notiamo che $a_0 \neq 0$, perché è (a meno di segno) $\det(f)$ ed f è triangolare superiore con tutti gli elementi sulla diagonale non nulli (f è invertibile a destra per ipotesi). Ora, moltiplichiamo l'espressione (2.3) a destra per l'inversa g: dopo semplici manipolazioni si ottiene

$$g = a_0^{-1}(-a_1\delta - a_2 f - \cdots - f^{n-1}).$$

Dunque g si scrive come combinazione lineare di potenze di f e di conseguenza commuta con f. Ne consegue che g è anche inversa sinistra di f.

A questo punto possiamo introdurre alcune funzioni notevoli in $\mathcal{I}(P)$. La prima, tra le più importanti, è la funzione ζ che è definita da

$$\zeta(t,u) := 1 \quad \forall\, t \leqslant u \text{ in } P.$$

Proviamo a calcolare ζ^2:

$$\zeta^2(s,u) = \sum_{s\leqslant t\leqslant u} \zeta(s,t)\zeta(t,u) = \sum_{s\leqslant t\leqslant u} 1 = \#([s,u]).$$

Se si vuole, $\#([s,u]) = \#\{t \in P \mid s \leqslant t \leqslant u\}$, cioè ζ^2 conta il numero di multicatene di lunghezza 2 con estremi s ed u. Se ora consideriamo ζ^3,

$$\zeta^3(s,u) = \sum_{s\leqslant t\leqslant u} \zeta(s,t)\zeta^2(t,u) = \sum_{s\leqslant t_1\leqslant t_2\leqslant u} \zeta(s,t_1)\zeta(t_1,t_2)\zeta(t_2,u)$$

cioè ζ^3 conta il numero di multicatene di lunghezza 3 con estremi s ed u. Se poi vediamo $\zeta(s,u) = 1$ come la funzione che conta l'unica multicatena $s \leqslant u$, otteniamo per induzione che $\zeta^k(s,u)$ conta il numero di multicatene di lunghezza k con estremi s ed u.

Passiamo alla funzione $\zeta - 1$.[4] Per definizione di ζ si ha

$$(\zeta - 1)(s,u) = \begin{cases} 0 & \text{se } s = u \\ 1 & \text{se } s < u. \end{cases}$$

[4] Laddove non ci siano ambiguità, spesso nel seguito scriveremo 1 per indicare la funzione δ e analogamente, per $n \in \mathbb{K}$, la funzione $n\delta$ sarà indicata semplicemente con n.

Possiamo interpretare $\zeta - 1$ come la funzione che conta il numero di catene di lunghezza 1 tra s ed u. Quest'intuizione è riscontrata per $(\zeta-1)^2$, che in effetti vale

$$(\zeta-1)^2(s,u) = \sum_{s \leqslant t \leqslant u} (\zeta-1)(s,t)(\zeta-1)(t,u)$$

che è diversa da 0 solo per i t che verificano $s < t < u$. Anche in questo caso, per induzione si verifica che $(\zeta-1)^k$ conta le catene di lunghezza k di estremi s ed u.

Consideriamo infine $2-\zeta$. Per definizione,

$$(2-\zeta)(s,t) = \begin{cases} 1 & \text{se } s = t \\ -1 & \text{se } s < t \end{cases}$$

e per quanto visto prima $2-\zeta$ è invertibile.

Proposizione 2.19. $(2-\zeta)^{-1}(s,t)$ *conta il numero totale di catene con estremi* s *ed* t*, di qualsiasi lunghezza.*

Prima dimostrazione. Sia ℓ la lunghezza dell'intervallo $[s,t]$, cioè la lunghezza di una catena massimale in $[s,t]$. Quindi $(\zeta-1)^{\ell+1}(u,v) = 0$ per ogni u, v tali che $s \leqslant u \leqslant v \leqslant t$ ($(\zeta-1)^{\ell+1}$ conta le catene di lunghezza $\ell+1$ tra u e v, ma essi sono compresi tra s e t e la lunghezza massima di una catena in $[s,t]$ è ℓ). Ora, $2-\zeta = 1-(\zeta-1)$, dunque

$$(2-\zeta)\big(1+(\zeta-1)+\cdots+(\zeta-1)^{\ell}\big)(u,v) = \big(1-(\zeta-1)^{\ell+1}\big)(u,v) = 1(u,v)$$

(osserviamo che tutti gli addendi sono potenze di $(\zeta-1)$, quindi commutano tra loro). In altre parole, l'inversa di $2-\zeta$ è

$$1+(\zeta-1)+\cdots+(\zeta-1)^{\ell}$$

e per ogni $i = 0,\dots,\ell$ l'addendo $(\zeta-1)^i$ conta le catene di lunghezza i. □

Seconda dimostrazione. Questa dimostrazione è essenzialmente equivalente alla prima, ma vorremmo migliorare la notazione introducendo una topologia su $\mathcal{I}(P)$. In effetti, abbiamo dovuto fissare un intervallo $[s,t]$ e valutare il comportamento di $2-\zeta$ su quell'intervallo. Tornerebbe comodo poter scrivere direttamente ▹ *25/03/2015*

$$(2-\zeta)^{-1} = \sum_{k=0}^{\infty} (\zeta-1)^k$$

ma la serie a destra *non* è formale, quindi questa scrittura non ha senso, a meno che non si definisca una nozione di convergenza su $\mathcal{I}(P)$. In questo modo, possiamo dire che la serie converge se e solo se la successione delle somme parziali converge.

Osserviamo che $\mathcal{I}(P)$, in quanto spazio di funzioni, è naturalmente realizzato come spazio prodotto: possiamo identificare una $f : \mathcal{I}nt(P) \to \mathbb{K}$ con la successione generalizzata $(f(s,t) \mid [s,t] \in \mathcal{I}nt(P))$ e quindi considerare $\mathcal{I}(P) = \mathbb{K}^{\mathcal{I}nt(P)}$. Mettiamo allora su $\mathbb{K}$ la topologia discreta e su $\mathbb{K}^{\mathcal{I}nt(P)}$ la topologia prodotto. In particolare, una base di aperti è data dagli insiemi della forma[5]

$$\mathbb{K} \times \cdots \times \{s\} \times \cdots \times \mathbb{K}$$

al variare di $s \in \mathbb{K}$ e del fattore diverso da $\mathbb{K}$.

In questa topologia la nozione di convergenza diventa: una successione $(f_n)_{n\in\mathbb{N}}$ converge a f se e solo se per ogni $s \leqslant t$ esiste $n_0 \in \mathbb{N}$ (che dipende da s e t) tale che per ogni $n \geqslant n_0$ si ha $f_n(s,t) = f(s,t)$.

A questo punto possiamo effettivamente scrivere

$$(2-\zeta)^{-1} = (1-(\zeta-1))^{-1} = \sum_{k=0}^{\infty} (\zeta-1)^k$$

e la serie di destra è ben definita perché le somme parziali convergono (fissato un intervallo $s \leqslant t$, le lunghezze delle catene in $[s,t]$ sono limitate da $\ell(s,t)$). □

Proposizione 2.20. *Definendo*

$$\eta(s,t) := \begin{cases} 1 & \text{se } s \lessdot t \\ 0 & \text{altrimenti,} \end{cases}$$

si ha che $(1-\eta)^{-1}(s,t)$ *è il numero di catene massimali di estremi* s *e* t.

Dimostrazione. Innanzitutto osserviamo che $(1-\eta)(s,s) = 1$ per ogni s, quindi $1-\eta$ è invertibile. Possiamo in effetti scrivere

$$(1-\eta)^{-1} = \sum_{k=0}^{\infty} \eta^k$$

e la serie converge perché $\eta^k(s,t)$ conta in effetti il numero di catene massimali di lunghezza k di estremi s e t: più in dettaglio

$$\eta^k(s,t) = \sum_{s\leqslant t_1 \leqslant \cdots \leqslant t_{k-1} \leqslant t} \eta(s,t_1)\cdots\eta(t_{k-1},t)$$

e nel prodotto a destra c'è un fattore 1 solo quando $t_i \lessdot t_{i+1}$, quindi nella somma si salvano solo i termini

$$s \lessdot t_1 \lessdot \cdots \lessdot t_{k-1} \lessdot t.$$ □

[5] Ricordiamo che per uno spazio prodotto $\prod X_i$ su un insieme arbitrario di indici $i \in I$, una base di aperti è data da insiemi del tipo $\prod U_i$ dove $U_i \subseteq X_i$ è aperto in X_i e $U_i \neq X_i$ solo per un numero finito di indici $i \in I$.

2.3 La funzione di Möbius

Nella Sezione 1.5 abbiamo introdotto la funzione di Möbius aritmetica come l'inversa della ζ di Riemann rispetto al prodotto di convoluzione. Nel contesto più generale dei poset abbiamo definito una funzione ζ, che è invertibile. Ci sarà qualche analogia?

Definizione 2.21. Sia P un poset localmente finito e $\zeta \in \mathcal{I}(P)$ definita come sopra. Chiamiamo *funzione di Möbius* di P l'inversa della funzione ζ e la indichiamo con $\mu := \zeta^{-1}$.

Dalla relazione $\mu\zeta = \delta$ ricaviamo

$$\begin{cases} \mu(s,s)\zeta(s,s) = 1 \\ (\mu\zeta)(s,t) = 0 \qquad \text{se } s < t, \end{cases}$$

cioè si ha che $\mu(s,s) = 1$ per ogni $s \in P$ e

$$\mu(s,t) = -\sum_{s \leqslant u < t} \mu(s,u). \tag{2.4}$$

Per la funzione di Möbius aritmetica vale la formula di inversione di Möbius (Proposizione 1.12). Anche per la funzione di Möbius di un poset vale un risultato analogo, ma prima dobbiamo premettere una definizione.

Definizione 2.22. Sia P un poset. Un sottoinsieme $I \subseteq P$ è detto *ideale d'ordine* di P se per ogni $s, t \in P$ vale che $(t \in I) \wedge (s \leqslant t) \to s \in I$. Un ideale d'ordine è detto *principale* se è generato da un solo elemento, cioè se è della forma $\Lambda_t := \{\gamma \in P \mid \gamma \leqslant t\}$.

Teorema 2.23 (Formula di inversione di Möbius)**.** *Sia P un poset (localmente finito) tale che ogni ideale d'ordine principale sia finito. Siano inoltre $f, g \colon P \to \mathbb{K}$. Allora per ogni $t \in P$ si ha*

$$g(t) = \sum_{s \leqslant t} f(s) \quad \textit{se e solo se} \quad f(t) = \sum_{s \leqslant t} g(s)\mu(s,t).$$

Dimostrazione. Vogliamo definire un'azione destra di $\mathcal{I}(P)$ sul $\mathbb{K}$-spazio vettoriale $\mathbb{K}^P := \{f \colon P \to \mathbb{K}\}$, cioè un omomorfismo di $\mathbb{K}$-algebre da $\mathcal{I}(P)$ in $\mathcal{E}nd(\mathbb{K}^P)$.[6] Per $f \in \mathbb{K}^P$ e $\xi \in \mathcal{I}(P)$ definiamo $f \cdot \xi \in \mathbb{K}^P$ come

$$(f \cdot \xi)(t) := \sum_{s \leqslant t} f(s)\xi(s,t)$$

[6] Ricordiamo che il prodotto nella struttura di $\mathbb{K}$-algebra su $\mathcal{E}nd(\mathbb{K}^P)$ è dato dalla composizione.

e quindi l'omomorfismo

$$\begin{array}{rcl} \Phi : \mathcal{I}(P) & \longrightarrow & \mathcal{E}nd(\mathbb{K}^P) \\ \xi & \longmapsto & (f \mapsto f \cdot \xi). \end{array}$$

Ci sono delle verifiche tecniche da fare...

- Per $\alpha, \beta \in \mathbb{K}$ e $\xi_1, \xi_2 \in \mathcal{I}(P)$ abbiamo

$$\begin{aligned} \big(f \cdot (\alpha\xi_1 + \beta\xi_2)\big)(t) &= \sum_{s \leqslant t} f(s)(\alpha\xi_1 + \beta\xi_2)(s,t) = \\ &= \alpha\Big(\sum_{s \leqslant t} f(s)\xi_1(s,t)\Big) + \beta\Big(\sum_{s \leqslant t} f(s)\xi_2(s,t)\Big) = \\ &= \big(\alpha(f \cdot \xi_1) + \beta(f \cdot \xi_2)\big)(t). \end{aligned}$$

- Per $\xi_1, \xi_2 \in \mathcal{I}(P)$ abbiamo

$$\begin{aligned} \big(f \cdot (\xi_1\xi_2)\big)(t) &= \sum_{s \leqslant t} f(s)(\xi_1\xi_2)(s,t) = \\ &= \sum_{s \leqslant t} f(s)\Big(\sum_{s \leqslant u \leqslant t} \xi_1(s,u)\xi_2(u,t)\Big) = \\ &= \sum_{s \leqslant u \leqslant t} f(s)\xi_1(s,u)\xi_2(u,t) = \\ &= \sum_{u \leqslant t} \Big(\sum_{s \leqslant u} f(s)\xi_1(s,u)\Big)\xi_2(u,t) = \\ &= \sum_{u \leqslant t} (f \cdot \xi_1)(u)\xi_2(u,t) = \big((f \cdot \xi_1) \cdot \xi_2\big)(t). \end{aligned}$$

Una volta verificata la buona definizione dell'azione, il resto della dimostrazione occupa un paio di righe. Infatti in termini dell'azione la tesi diventa

$$g = f \cdot \zeta \Leftrightarrow f = g \cdot \mu.$$

$\boxed{\Rightarrow}$ Facendo agire μ a destra

$$g \cdot \mu = (f \cdot \zeta) \cdot \mu = f \cdot (\zeta\mu) = f \cdot \delta = f.$$

$\boxed{\Leftarrow}$ Facendo agire ζ a destra

$$f \cdot \zeta = (g \cdot \mu) \cdot \zeta = g \cdot (\mu\zeta) = g \cdot \delta = g. \qquad \square$$

Vale anche una versione duale della formula di inversione di Möbius, in cui si rovesciano i segni di ordine, si considerano gli *ideali d'ordine duali principali* $V_t := \{\gamma \in P \mid \gamma \geqslant t\}$ e la dimostrazione passa attraverso la definizione di un'azione sinistra di $\mathcal{I}(P)$ su $\mathbb{K}^P$.

Teorema 2.23* (Formula duale di inversione di Möbius)**.** *Sia* P *un poset (localmente finito) tale che ogni ideale d'ordine duale principale sia finito. Siano inoltre* $f, g\colon P \to \mathbb{K}$*. Allora per ogni* $s \in P$ *si ha*

$$g(s) = \sum_{t \geqslant s} f(t) \quad \textit{se e solo se} \quad f(s) = \sum_{t \geqslant s} \mu(s,t)g(t).$$

Esempio 2.3. Proviamo a calcolare la funzione di Möbius di un semplice poset, di cui viene dato il diagramma di Hasse in Figura 2.4. Ovviamente $\mu(X,X) = 1$

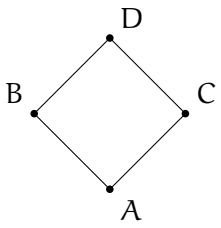


Figura 2.4: Diagramma di Hasse per l'Esempio 2.3.

per ogni $X \in \{A, B, C, D\}$. Dobbiamo calcolare i cinque valori $\mu(A,B)$, $\mu(A,C)$, $\mu(A,D)$, $\mu(B,D)$ e $\mu(C,D)$: per fare ciò useremo la formula ricorsiva definita in (2.4).

Dal momento che $A \lessdot B$, $A \lessdot C$, $B \lessdot D$ e $C \lessdot D$, calcolare i valori assunti da μ su questi intervalli è facile: per esempio

$$\mu(A,B) = -\sum_{A \leqslant X < B} \mu(A,X) = -\mu(A,A) = -1$$

e analogamente $\mu(A,C) = \mu(B,D) = \mu(C,D) = -1$. Invece

$$\mu(A,D) = -\sum_{A \leqslant X < D} \mu(A,X) = -(\mu(A,A)+\mu(A,B)+\mu(A,C)) = -(1-1-1) = 1.$$

Vediamo ora come la funzione di Möbius, se applicata a opportuni poset, generalizzi il *principio di inclusione/esclusione*. Iniziamo da un caso semplice: siano A, B e C tre insiemi tali che $A \cap B = A \cap C = B \cap C = A \cap B \cap C$ e consideriamo il loro *poset delle intersezioni*, ovvero il poset i cui elementi sono tutte le possibili intersezioni di k insiemi scelti tra A, B e C, per $k = 0, \ldots, 3$ (per $k = 0$, l'intersezione è data convenzionalmente da $A \cup B \cup C$), ordinate parzialmente per inclusione.

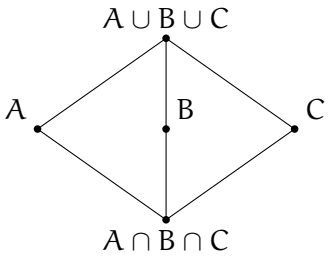


Figura 2.5: Diagramma di Hasse del poset delle intersezioni tra A, B, C con $A \cap B = A \cap C = B \cap C = A \cap B \cap C$.

La Figura 2.5 mostra il diagramma di Hasse del poset delle intersezioni. Da questo è facile ricavare la funzione di Möbius:

$$\mu(A \cap B \cap C, X) = \begin{cases} 1 & \text{per } X = A \cap B \cap C \\ -1 & \text{per } X = A, B, C \\ 2 & \text{per } X = A \cup B \cup C. \end{cases}$$

Ora, se applichiamo il principio di inclusione/esclusione ad A, B e C, otteniamo

$$\#(A \cup B \cup C) - \#(A) - \#(B) - \#(C) + 2\#(A \cap B \cap C) = 0,$$

ma questa è proprio l'espressione, vera per le proprietà generali della funzione di Möbius,

$$\sum_{X \in P} \mu(A \cap B \cap C, X) = 0.$$

dove P è il poset delle intersezioni (in questo caso X può variare su tutto P perché $A \cap B \cap C$ è sempre confrontabile). In altre parole, la funzione di Möbius può essere vista come generalizzazione del principio di inclusione/esclusione a poset generici (e il "vero" principio di inclusione/esclusione si ricava da essa nel caso dei poset di intersezione).

Generalizzando l'esempio precedente, siano $A_1, \ldots, A_n$ insiemi e sia P il poset delle intersezioni di $A_1, \ldots, A_n$. In particolare, prendiamo tutte le intersezioni di k insiemi scelti in $A_1, \ldots, A_n$ per $k = 1, \ldots, n$ e aggiungiamo "artificialmente" l'intersezione per $k = 0$, cioè l'unione di $A_1, \ldots, A_n$, che chiameremo $\hat{1}$ (questa notazione sarà giustificata a breve).[7] Per $T \in P$, sia $f(T)$ il numero di elementi di

[7] Questa sottile differenza rispetto all'esempio precedente serve per far sì che il poset con $n = 1$ abbia *due* elementi: A_1, ottenuto come intersezione del solo insieme A_1, e $\hat{1} = A_1$ ottenuto come intersezione vuota.

T che non appartengono a nessun T' con $T' < T$, cioè

$$f(T) := \#\left(T \setminus \bigcup_{T' < T} T'\right),$$

e sia $g(T) := \#(T)$. Vale naturalmente

$$g(T) = \sum_{T' \leqslant T} f(T')$$

perché in pratica stiamo sommando gli elementi che stanno solo in T con quelli che stanno nelle intersezioni che coinvolgono T, iterativamente sulle intersezioni. Per la formula di inversione di Möbius

$$f(\hat{1}) = \sum_{T \in P} g(T)\mu(T, \hat{1}).$$

Ma ora $f(\hat{1}) = 0$, perché non ci sono elementi che stanno in $A_1 \cup \cdots \cup A_n$ ma non in $A_1, \ldots, A_n$, da cui otteniamo

$$g(\hat{1}) = -\sum_{T < \hat{1}} g(T)\mu(T, \hat{1}) = -\sum_{T < \hat{1}} \#(T)\mu(T, \hat{1})$$

con $g(\hat{1}) = \#(A_1 \cup \cdots \cup A_n)$. Abbiamo ottenuto una versione "contratta" del principio di inclusione/esclusione, con i pesi delle intersezioni dati dai valori assunti dalla μ.

Finora abbiamo calcolato la funzione di Möbius sfruttando la formula ricorsiva (2.4). Fortunatamente ci sono anche altri modi.

Definizione 2.24. Siano $(P, \leqslant)$ e $(Q, \preccurlyeq)$ due poset. Definiamo *prodotto (diretto)* di P e Q il poset $(P \times Q, \trianglelefteq)$ dove $P \times Q$ è il prodotto cartesiano e

$$(s, t) \trianglelefteq (s', t') \Leftrightarrow (s \leqslant s') \wedge (t \preccurlyeq t').$$

Proposizione 2.25. *Siano P e Q due poset localmente finiti. Indichiamo con μ_P, μ_Q e $\mu_{P\times Q}$ le funzioni di Möbius di P, Q e $P \times Q$ rispettivamente. Allora per ogni $s \leqslant s' \in P$ e $t \leqslant t' \in Q$*

$$\mu_{P\times Q}((s, t), (s', t')) = \mu_P(s, s')\mu_Q(t, t').$$

Dimostrazione. È un conto. In effetti, per $(s, t) \leqslant (s', t')$

$$\sum_{(s,t) \leqslant (u,v) \leqslant (s',t')} \mu_P(s, u)\mu_Q(t, v) = \left(\sum_{s \leqslant u \leqslant s'} \mu_P(s, u)\right)\left(\sum_{t \leqslant v \leqslant t'} \mu_Q(t, v)\right),$$

ma per la proprietà della funzione di Möbius i due fattori a destra valgono 1 se $s = s'$ (rispettivamente $t = t'$) e 0 se $s < s'$ (rispettivamente $t < t'$), dunque

$$\sum_{(s,t)\leqslant(u,v)\leqslant(s',t')} \mu_P(s,u)\mu_Q(t,v) = \delta_{s,s'}\delta_{t,t'}$$

dove $\delta_{i,j}$ è la delta di Dirac. D'altra parte, per definizione

$$\sum_{(s,t)\leqslant(u,v)\leqslant(s',t')} \mu_{P\times Q}((s,t),(u,v)) = \delta_{(s,s'),(t,t')}$$

da cui abbiamo la tesi. □

Vediamo subito un esempio: calcoliamo la funzione di Möbius per l'algebra booleana standard $B_n = \wp(\{1,\dots,n\})$. Essa è isomorfa come poset a $\{0,1\}^n$, con l'ovvio isomorfismo che ad $A \subseteq \{1,\dots,n\}$ associa l'n-upla $(a_1,\dots,a_n)$ tale che $a_i = 1$ se $i \in A$ e $a_i = 0$ se $i \notin A$. Sul poset $\{0,1\}$[8] la funzione di Möbius è data da $\mu(0,0) = \mu(1,1) = 1$ e $\mu(0,1) = -1$. Per la Proposizione 2.25 allora si ha che per $S, T \in B_n$ con $T \subseteq S$ vale

$$\mu_{B_n}(T,S) = (-1)^{\#(S\smallsetminus T)}.$$

Infatti se $(s_1,\dots,s_n)$ e $(t_1,\dots,t_n)$ sono le n-uple che identificano rispettivamente S e T, abbiamo

$$\mu_{B_n}(T,S) = \prod_{i=1}^{n} \mu_{\{0,1\}}(t_i,s_i).$$

Dato che $T \subseteq S$ abbiamo $t_i \leqslant s_i$ per ogni $i = 1,\dots,n$; ma $\mu_{\{0,1\}}(t_i,s_i) = 1$ ogni volta che $t_i = s_i$, cioè se i sta in T (e quindi anche in S) oppure i non sta in S (e quindi neanche in T), e $\mu_{\{0,1\}}(t_i,s_i) = -1$ quando $t_i < s_i$, cioè se i sta in $S \smallsetminus T$. Ricordando infine che $\#(S \smallsetminus T) = \ell(T,S)$ (si ottiene una catena massimale aggiungendo ogni volta un elemento a T fino ad arrivare a S), arriviamo a

$$\mu_{B_n}(T,S) = (-1)^{\ell(T,S)}.$$

Concludiamo questa sezione mostrando finalmente il legame tra la funzione di Möbius di un poset e la funzione di Möbius aritmetica introdotta nella Sezione 1.5. In effetti ci possiamo aspettare che ci sia una qualche relazione considerando, per un numero fissato, l'insieme dei suoi divisori parzialmente ordinato dalla divisibilità.

Siano $n_1,\dots,n_k \in \mathbb{N}$ e consideriamo il poset prodotto

$$P := \{0,\dots,n_1\} \times \cdots \times \{0,\dots,n_k\}$$

[8] L'ordine è $0 < 1$, naturalmente...

dove sui singoli fattori c'è il consueto ordinamento sui naturali. P può essere identificato con il poset dei divisori di un certo numero (se $p_1, \dots, p_k \in \mathbb{N}$ sono numeri primi distinti, P è il poset dei divisori di $p_1^{n_1} \cdots p_k^{n_k}$). Ora, se $\mathbf{a} = (a_1, \dots, a_k)$ e $\mathbf{b} = (b_1, \dots, b_k)$ sono elementi di P con $\mathbf{a} \leqslant \mathbf{b}$, l'intervallo chiuso $[\mathbf{a}, \mathbf{b}]$ è isomorfo al prodotto di catene

$$\{0, \dots, b_1 - a_1\} \times \cdots \times \{0, \dots, b_k - a_k\}$$

(in effetti è isomorfo a $[a_1, b_1] \times \cdots \times [a_k, b_k]$, dopodiché basta traslare). La funzione di Möbius di una catena C è facile da calcolare:

$$\mu_C(i, j) = \begin{cases} 1 & \text{se } i = j \\ -1 & \text{se } i \lessdot j \\ 0 & \text{altrimenti,} \end{cases}$$

dunque possiamo dire

$$\mu_P(\mathbf{a}, \mathbf{b}) = \begin{cases} (-1)^{\sum (b_i - a_i)} & \text{se } b_i - a_i \in \{0, 1\} \text{ per ogni } i = 1, \dots, k \\ 0 & \text{altrimenti.} \end{cases}$$

Detti $r = p_1^{a_1} \cdots p_k^{a_k}$ e $s = p_1^{b_1} \cdots p_k^{b_k}$, abbiamo allora che $\mu(r, s) \neq 0$ solo se s/r è *square-free* (un primo in s/r può comparire solo con esponente 0 oppure 1) e in tal caso $\mu(r, s) = (-1)^t$ se s/r è il prodotto di esattamente t primi distinti. Confrontando questo risultato con quanto visto nella Sezione 1.5 otteniamo che *la funzione di Möbius del poset P valutata in $[r, s]$ coincide con la funzione di Möbius aritmetica valutata in s/r.*

2.4 Complessi simpliciali astratti

Abbiamo visto che la funzione di Möbius è uno strumento molto versatile: quando applicata al poset delle parti, ci permette di ricavare il principio di inclusione/esclusione; quando applicata al poset dei divisori, ricade nella funzione di Möbius aritmetica. Un altro campo della matematica legato a questa funzione è la *topologia algebrica*. In questa sezione richiameremo alcuni risultati di topologia algebrica, senza dimostrarli; saranno indicati con il simbolo †. Per chi fosse interessato a questo settore della matematica, rimandiamo al libro di Hatcher [5].

Sia P un poset. Indichiamo con $\hat{P}$ il poset ottenuto aggiungendo due elementi distinti $\hat{0}$, $\hat{1}$ all'insieme supporto di P, con le relazioni $\hat{0} < t$, $t < \hat{1}$ per ogni $t \in P$ (e $\hat{0} < \hat{1}$).

Teorema 2.26 (Philip Hall)**.** *Sia* P *un poset finito e* $\hat{P}$ *il poset definito sopra. Sia* c_i *il numero di catene tra* $\hat{0}$ *e* $\hat{1}$ *in* $\hat{P}$ *di lunghezza* i*, cioè il numero di catene*

$$\hat{0} = t_0 < t_1 < \cdots < t_i = \hat{1}.$$

Allora

$$\mu_{\hat{P}}(\hat{0}, \hat{1}) = \sum_{i \geqslant 0} (-1)^i c_i$$

(in cui $c_0 = 0$ *perché* $\hat{0} \neq \hat{1}$ *e* $c_1 = 1$ *per l'unica catena* $\hat{0} < \hat{1}$*).*

Dimostrazione. Abbiamo che

$$\mu_{\hat{P}} = (\zeta_{\hat{P}})^{-1} = (1 + (\zeta_{\hat{P}} - 1))^{-1} = \sum_{i \geqslant 0} (-1)^i (\zeta_{\hat{P}} - 1)^i.$$

Ma abbiamo visto nella Sezione 2.2 che $(\zeta_{\hat{P}} - 1)^i$ conta le catene di lunghezza i, quindi

$$\mu_{\hat{P}}(\hat{0}, \hat{1}) = \sum_{i \geqslant 0} (-1)^i (\zeta_{\hat{P}} - 1)^i (\hat{0}, \hat{1}) = \sum_{i \geqslant 0} (-1)^i c_i. \qquad \square$$

Dunque $\mu_{\hat{P}}(\hat{0}, \hat{1})$ è data da una somma a segni alterni. C'è un'altra famosa somma alternata in matematica, che è la caratteristica di Eulero. Forse c'è una qualche analogia? La risposta è sì e per vederlo definiamo un concetto che introduce i poset in topologia algebrica.

Definizione 2.27. Un *complesso simpliciale astratto* su un insieme finito di vertici V è una collezione Δ di sottoinsiemi di V tale che

1. se $t \in V$, allora $\{t\} \in \Delta$;
2. se $F \in \Delta$ e $G \subseteq F$, allora $G \in \Delta$.

In altre parole, Δ è un ideale d'ordine sul poset $(\wp(V), \subseteq)$ che contiene tutti i singoletti. Tradizionalmente un insieme $F \in \Delta$ è detto *faccia* e la sua *dimensione* è $\dim(F) = \#(F) - 1$.

C'è un caso antipatico: su $V = \varnothing$ sono possibili ben due complessi simpliciali, nella fattispecie

- $\Delta = \varnothing$ è un complesso simpliciale che non ha facce;
- $\Delta = \{\varnothing\}$ rispetta entrambe le condizioni della definizione; è un complesso simpliciale con una sola faccia di dimensione -1.

Nel seguito indicheremo con f_i il numero di facce i-dimensionali di un complesso simpliciale Δ. Osserviamo che se $V \neq \varnothing$ la proprietà 2. della definizione di complesso simpliciale fa sì che $\varnothing \in \Delta$, quindi $f_{-1} = 1$.

Definizione 2.28. Dato un complesso simpliciale Δ, definiamo la sua *caratteristica di Eulero ridotta* come ▹ *30/03/2015*

$$\tilde{\chi}(\Delta) := \sum_{i \geqslant -1} (-1)^i f_i.$$

A questo punto, dato un generico poset P, costruiamo un complesso simpliciale a partire da P che contenga le informazioni sull'ordine.

Definizione 2.29. Sia P un poset (finito). Il *complesso d'ordine* (*order complex*) di P, indicato da $\Delta(P)$, è il complesso simpliciale i cui vertici sono gli elementi di P dato da

$$\Delta(P) := \{C \subseteq P \mid C \text{ è una catena di } P\}.$$

$\Delta(P)$ è in effetti un complesso simpliciale: tutti i vertici di P sono catene (di lunghezza 0) e un sottoinsieme di una catena è ovviamente una catena.

Esempio 2.4. Riprendiamo il poset dell'Esempio 2.3. In questo caso $\Delta(P)$ è l'insieme

$$\{\varnothing, \{A\}, \{B\}, \{C\}, \{D\}, \{A, B\}, \{A, C\}, \{A, D\}, \{B, D\}, \{C, D\}, \{A, B, D\}, \{A, C, D\}\}.$$

Con il concetto di complesso d'ordine in mano, possiamo riscrivere la tesi del Teorema 2.26.

Teorema 2.30 (Philip Hall, seconda versione)**.** *Nelle stesse ipotesi del Teorema 2.26, si ha*

$$\mu_{\hat{P}}(\hat{0}, \hat{1}) = \tilde{\chi}(\Delta(P)).$$

Dimostrazione. È sufficiente provare che $f_k = c_{k+2}$ per ogni $k \geqslant -1$ (perché tanto $c_0 = 0$). Intanto $f_{-1} = c_1 = 1$; ora, una faccia di dimensione 0 è un singoletto $\{t\}$ con $t \in P$ e ad essa corrisponde la catena $\hat{0} < t < \hat{1}$, e viceversa: quindi $f_0 = c_2$. In generale la faccia k-dimensionale $\{t_0, \ldots, t_k\}$ è in corrispondenza con la catena $\hat{0} < t_0 < \cdots < t_k < \hat{1}$ di lunghezza $k + 2$. □

In topologia c'è un procedimento standard per associare a un complesso simpliciale astratto Δ uno spazio topologico $|\Delta|$ (la sua *realizzazione*). Ad esempio, se V è finito (come nel nostro caso), è sufficiente immergere V in un opportuno spazio euclideo $\mathbb{R}^m$ in modo che per ogni faccia $\{v_1, \ldots, v_k\}$ i vertici $v_1, \ldots, v_k$ siano affinemente indipendenti e poi definire

$$|\Delta| = \bigcup_{F \in \Delta} \operatorname{conv}(F)$$

dove $\operatorname{conv}(F)$ è l'inviluppo convesso dei vertici della faccia F.

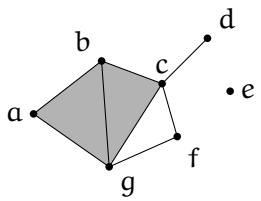


Figura 2.6: Esempio di realizzazione. In questo caso $V = \{a, b, c, d, e, f, g\}$ e le facce massimali (cioè non contenute in nessun'altra faccia) sono $\{a, b, g\}$, $\{b, c, g\}$, $\{c, d\}$, $\{c, f\}$, $\{f, g\}$ ed $\{e\}$. Osserviamo che la faccia $\{c, f, g\}$ *non* fa parte di Δ e quindi nemmeno di $|\Delta|$.

In generale, la caratteristica di Eulero (ridotta) di uno spazio topologico X è definita da

$$\tilde{\chi}_{\text{top}}(X) := \sum_{i \geqslant 0} (-1)^i \operatorname{rk}(\tilde{H}_i(X; \mathbb{Z}))$$

dove $\tilde{H}_i(X; \mathbb{Z})$ è l'i-esimo gruppo di omologia ridotta di X a coefficienti in $\mathbb{Z}$.

†**Teorema 2.31.** *Per un complesso simpliciale Δ vale che $\tilde{\chi}_{\text{top}}(|\Delta|) = \tilde{\chi}(\Delta)$.*

Notiamo che quindi $\mu_{\hat{P}}(\hat{0}, \hat{1})$ dipende solo dalla realizzazione geometrica di $\Delta(P)$.

Definizione 2.32. Un *complesso di celle finito regolare* è un insieme finito $\{\sigma_i \mid i \in I\}$, con I insieme di indici e $\sigma_i \subseteq \mathbb{R}^m$, non vuoti e disgiunti a due a due tali che

1. $(\overline{\sigma}_i, \overline{\sigma}_i \smallsetminus \sigma_i) \simeq (D^n, S^{n-1})$ per un qualche $n \in \mathbb{N}$ che dipende da i;[9]
2. $\overline{\sigma}_i \smallsetminus \sigma_i$ è unione di altri σ_j del complesso.

(Richiamiamo alcuni concetti di topologia usati nella definizione precedente. Una *coppia di spazi* è, per l'appunto, una coppia di spazi topologici (X, A) con $A \subseteq X$. Una *funzione continua tra coppie* $f\colon (X, A) \to (Y, B)$ è una funzione continua $f\colon X \to Y$ tale che $f(A) \subseteq B$. Un *omeomorfismo tra coppie* è una funzione continua tra coppie $f\colon (X, A) \to (Y, B)$ tale che $f\colon X \to Y$ sia un omeomorfismo e $f|_A : A \to B$ sia un omeomorfismo. Infine D^n e S^n sono rispettivamente il disco chiuso e la sfera n-dimensionali.)

A un complesso di celle finito regolare Γ è associato uno spazio topologico (la sua *realizzazione*)

$$\|\Gamma\| := \bigcup_{i \in I} \sigma_i \subseteq \mathbb{R}^m.$$

[9] Se $\sigma_i = \{p\}$, allora $(\overline{\sigma}_i, \overline{\sigma}_i \smallsetminus \sigma_i) \simeq (\{0\}, \varnothing)$: infatti per convenzione D^0 è un punto e $S^{-1} = \varnothing$ (invece S^0 è formata da *due* punti).

Definizione 2.33. Dato un complesso di celle finito regolare Γ, la sua *(prima) suddivisione baricentrica* $\mathrm{sd}(\Gamma)$ è il complesso simpliciale astratto in cui i vertici sono dati dalle celle chiuse $\{\overline{\sigma}_i \mid i \in I\}$ e le cui facce sono gli insiemi $\{\overline{\sigma}_{i_1}, \dots, \overline{\sigma}_{i_k}\}$ tali che $\overline{\sigma}_{i_1} \subset \cdots \subset \overline{\sigma}_{i_k}$ (le inclusioni sono strette).

†**Teorema 2.34.** *I due spazi* $|\mathrm{sd}(\Gamma)|$ *e* $\|\Gamma\|$ *sono omeomorfi.*

Dato un complesso di celle finito regolare Γ possiamo definire un poset $P(\Gamma)$ i cui elementi sono le celle di Γ e vale che $\sigma_i \leqslant \sigma_j$ se e solo se $\overline{\sigma}_i \subseteq \overline{\sigma}_j$. Dunque abbiamo due modi per ottenere un complesso simpliciale a partire da Γ: la suddivisione baricentrica $\mathrm{sd}(\Gamma)$ e il complesso d'ordine $\Delta(P(\Gamma))$ costruito da $P(\Gamma)$.

Proposizione 2.35. *I due complessi simpliciali* $\mathrm{sd}(\Gamma)$ *e* $\Delta(P(\Gamma))$ *sono isomorfi.*

Ma in effetti non abbiamo mai detto quando due complessi simpliciali sono isomorfi (anche se potremmo immaginarcelo...).

Definizione 2.36. Due complessi simpliciali astratti Δ e Δ' sui vertici rispettivamente V e V' sono *isomorfi* se esiste una biiezione $f\colon V \to V'$ tale che $\{v_1, \dots, v_k\} \in \Delta$ se e solo se $\{f(v_1), \dots, f(v_k)\} \in \Delta'$.

Dimostrazione della Proposizione 2.35. In realtà basta ripercorrere le definizioni dei due oggetti: $\mathrm{sd}(\Gamma)$ è un complesso simpliciale sui $\{\overline{\sigma}_i \mid i \in I\}$, mentre i vertici di $\Delta(P(\Gamma))$ sono $\{\sigma_i \mid i \in I\}$, ma in entrambi i casi una faccia è data da $\{\overline{\sigma}_{i_1}, \dots, \overline{\sigma}_{i_k}\}$ (rispettivamente $\{\sigma_{i_1}, \dots, \sigma_{i_k}\}$) se e solo se $\overline{\sigma}_{i_1} \subset \cdots \subset \overline{\sigma}_{i_k}$. Quindi la biiezione $\sigma_i \mapsto \overline{\sigma}_i$ induce un isomorfismo di complessi simpliciali tra $\mathrm{sd}(\Gamma)$ e $\Delta(P(\Gamma))$. □

Proposizione 2.37. *Per un complesso di celle finito regolare* Γ *vale*

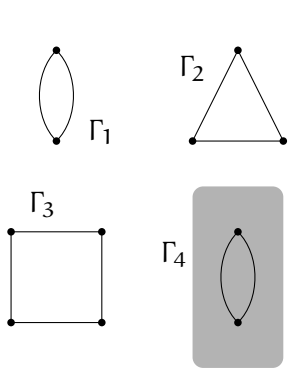
$$\mu_{\widehat{P(\Gamma)}}(\hat{0}, \hat{1}) = \tilde{\chi}_{\mathrm{top}}(\|\Gamma\|).$$

Dimostrazione. Applicando in ordine il Teorema 2.34, la Proposizione 2.35, il Teorema 2.31 e il Teorema 2.30 abbiamo

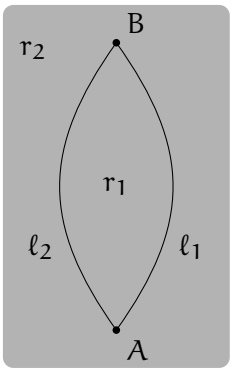
$$\tilde{\chi}_{\mathrm{top}}(\|\Gamma\|) = \tilde{\chi}_{\mathrm{top}}(|\mathrm{sd}(\Gamma)|) = \tilde{\chi}_{\mathrm{top}}(|\Delta(P(\Gamma))|) = \tilde{\chi}(\Delta(P(\Gamma))) = \mu_{\widehat{P(\Gamma)}}(\hat{0}, \hat{1}). \qquad \square$$

Nella Figura 2.7 sono disegnati alcuni complessi di celle finiti regolari in $\mathbb{R}^2$. Soffermiamoci particolarmente su Γ_4: come si vede in Figura 2.7b, ci sono due 0-celle A e B, due 1-celle ℓ_1 ed ℓ_2 e due 2-celle r_1 e r_2. È noto che $\|\Gamma_4\| \simeq S^2$; dal diagramma di Hasse di $\widehat{P(\Gamma_4)}$, disegnato in Figura 2.8, otteniamo

$$\mu_{\widehat{P(\Gamma_4)}}(\hat{0}, x) = \begin{cases} 1 & \text{per } x \in \{\hat{0}, \ell_1, \ell_2\} \\ -1 & \text{per } x \in \{A, B, r_1, r_2\} \end{cases}$$



(a) In Γ_1, Γ_2 e Γ_3 ci sono solo 0-celle e 1-celle; Γ_4 invece comprende anche le due 2-celle colorate in grigio.



(b) Dettaglio di Γ_4 con i nomi assegnati alle celle.

Figura 2.7: Esempi di complessi di celle regolari.

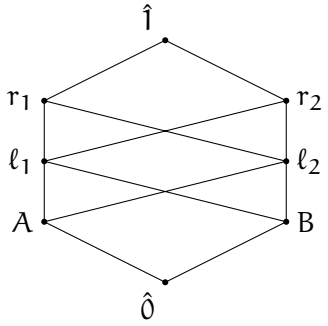


Figura 2.8: Diagramma di Hasse di $\widehat{P(\Gamma_4)}$.

e quindi $\mu_{\widehat{P(\Gamma_4)}}(\hat{0}, \hat{1}) = 1$.

Per quanto visto allora possiamo calcolare la caratteristica di Eulero ridotta di S^2:

$$\tilde{\chi}_{\text{top}}(S^2) = \mu_{\widehat{P(\Gamma_4)}}(\hat{0}, \hat{1}) = 1$$

che è in accordo con il valore già noto.[10]

Definizione 2.38. Un poset finito graduato Q in cui esistono due elementi $\hat{0}$ e $\hat{1}$ si dice *semi-euleriano* se vale che

$$\mu_Q(s,t) = (-1)^{\ell(s,t)} \tag{2.5}$$

[10] La caratteristica di Eulero di S^2 è 2; in generale vale $\tilde{\chi} = \chi - 1$.

per ogni $(s,t) \neq (\hat{0},\hat{1})$; si dice *euleriano* se (2.5) vale anche per $(s,t) = (\hat{0},\hat{1})$.

È un semplice conto verificare che tutti i $\widehat{P(\Gamma_i)}$ per $i = 1,\dots,4$ della Figura 2.7 sono euleriani. In realtà si può dimostrare che se $\|\Gamma\|$ è omeomorfo a una sfera S^n per qualche n, allora $\widehat{P(\Gamma)}$ è euleriano.

Esempio 2.5. Consideriamo di nuovo $B_n = \mathcal{P}(\{1,\dots,n\})$, per $n \geqslant 2$. Avendo già calcolato la funzione di Möbius di B_n, sappiamo che esso è un poset euleriano; vediamolo qui in un altro modo.

Sia $\mathring{B}_n$ la *parte propria* di B_n, cioè $\mathring{B}_n := B_n \setminus \{\{1,\dots,n\},\varnothing\}$. Naturalmente il poset $\widehat{\mathring{B}_n}$ è isomorfo a B_n (abbiamo tolto e poi riaggiunto gli elementi massimo e minimo). Cerchiamo dunque un complesso di celle finito regolare Γ tale che $P(\Gamma) = \mathring{B}_n$.

Apriamo qui una parentesi. Un m-*simplesso* è l'inviluppo convesso di un insieme di $m+1$ punti $\{v_0,\dots,v_m\}$ affinemente indipendenti. È noto che un m-simplesso è omeomorfo al disco m-dimensionale D^m. Un qualsiasi sottoinsieme di $k+1$ vertici del simplesso forma un k-simplesso (detto k-faccia), dunque c'è una struttura di complesso di celle sull'm-simplesso. Sia Γ tale complesso di celle, a cui però togliamo la cella vuota e la cella m-dimensionale: anche in questo caso è noto che $\|\Gamma\| \simeq S^{m-1}$.

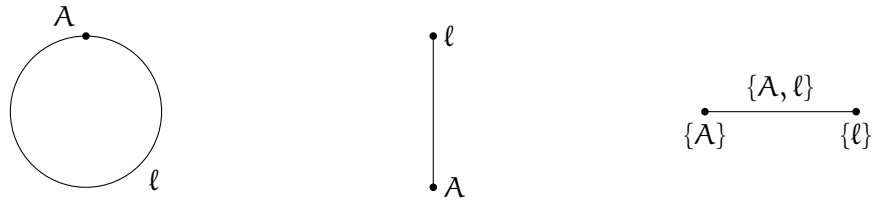
Torniamo a $\mathring{B}_n$. Prendiamo un $(n-1)$-simplesso generato da $\{v_1,\dots,v_n\}$ e costruiamo Γ come nel paragrafo precedente. Chi è $P(\Gamma)$? Gli elementi sono le celle di Γ e un qualsiasi sottoinsieme di $\{v_1,\dots,v_n\}$ (a parte $\{v_1,\dots,v_n\}$ stesso e $\varnothing$) dà origine a una cella; quindi il supporto di $P(\Gamma)$ è $\mathcal{P}(\{v_1,\dots,v_n\}) \setminus \{\{v_1,\dots,v_n\},\varnothing\}$, che è in corrispondenza biunivoca con $\mathcal{P}(\{1,\dots,n\}) \setminus \{\{1,\dots,n\},\varnothing\}$. Inoltre la relazione di contenimento tra facce di $P(\Gamma)$ coincide con la relazione di contenimento in B_n. Possiamo concludere allora che $P(\Gamma)$ e $\mathring{B}_n$ sono isomorfi come poset. Dal fatto che $\|\Gamma\| \simeq S^{n-2}$ deduciamo dunque che B_n è un poset euleriano.

Esempio 2.6. Vorremmo sottolineare a questo punto che tutti i risultati di questa sezione valgono per complessi di celle regolari. Vediamo come prendendo un complesso non regolare i teoremi precedenti non siano più validi.

Sia Γ il complesso di celle ottenuto incollando entrambi gli estremi di una 1-cella ℓ a una 0-cella A, come in Figura 2.9a. Questo complesso non è regolare: infatti $(\overline{\ell}, \overline{\ell} \setminus \ell) \not\simeq (D^1, S^0)$, dato che $\overline{\ell} \setminus \ell$ è il singolo punto A mentre S^0 è composta da due punti. Il diagramma di Hasse di $P(\Gamma)$ è rappresentato in Figura 2.9b. Da questo possiamo ricavare il complesso d'ordine sui vertici $\{A,\ell\}$

$$\Delta(P(\Gamma)) = \{\{A\},\{\ell\},\{A,\ell\}\}$$

la cui realizzazione geometrica è un segmento (vedi Figura 2.9c). D'altra parte $\|\Gamma\| \simeq S^1$, contraddicendo la tesi del Teorema 2.34. Tra parentesi, notiamo che $\widehat{P(\Gamma)}$ *non* è euleriano nonostante $\|\Gamma\|$ sia omeomorfo a una sfera.

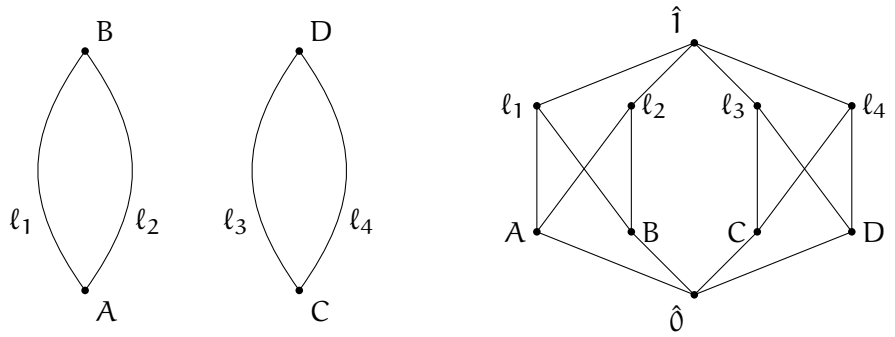


(a) Il complesso Γ, formato da una 0-cella A e una 1-cella ℓ.

(b) Diagramma di Hasse per $P(\Gamma)$.

(c) Realizzazione geometrica di $\Delta(P(\Gamma))$.

Figura 2.9: Un complesso di celle non regolare.



(a) Il complesso è formato da quattro 0-celle e quattro 1-celle.

(b) Diagramma di Hasse per $\widehat{P(\Gamma)}$.

Figura 2.10: Un complesso di celle Γ con $\|\Gamma\| \not\simeq S^n$ ma $\widehat{P(\Gamma)}$ euleriano.

Esempio 2.7. Terminiamo la lunga sezione sulla topologia algebrica mostrando che la condizione $\|\Gamma\| \simeq S^n$ è sufficiente ma non necessaria perché $\widehat{P(\Gamma)}$ sia euleriano. Consideriamo il complesso di celle indicato in Figura 2.10a. Il conto sul diagramma di Hasse (Figura 2.10b) mostra che in effetti $\widehat{P(\Gamma)}$ è euleriano, ma $\|\Gamma\| \simeq S^1 \sqcup S^1 \not\simeq S^n$ per ogni n.

2.5 Reticoli

Proseguiamo nello studio dei nostri poset aggiungendo qualcosa alla struttura.

Definizione 2.39. Siano P un poset e $s, t \in P$. Un *maggiorante* (*upper bound*) di s e t è un elemento $u \in P$ tale che $s \leqslant u$ e $t \leqslant u$. L'*estremo superiore*, o *join*, di s e t è

un maggiorante u di s e t tale che per ogni altro maggiorante v si abbia $u \leqslant v$; in altre parole, è il minimo dei maggioranti di s e t. Il *join* di s e t è indicato con $s \vee t$.

Definizione 2.40. Siano P un poset e $s, t \in P$. Un *minorante* (*lower bound*) di s e t è un elemento $u \in P$ tale che $u \leqslant s$ e $u \leqslant t$. L'*estremo inferiore*, o *meet*, di s e t è un minorante u di s e t tale che per ogni altro minorante v si abbia $v \leqslant u$; in altre parole, è il massimo dei minoranti di s e t. Il *meet* di s e t è indicato con $s \wedge t$.

Non è detto che esistano sempre il *join* e il *meet* di due elementi. Inoltre non necessariamente un maggiorante di s e t li ricopre (né un minorante è necessariamente ricoperto da essi).

Definizione 2.41. Un *reticolo* (*lattice*) L è un poset in cui ogni coppia di elementi possiede un *join* e un *meet*.

Osserviamo *en passant* che ogni reticolo finito ammette massimo e minimo (se $L = \{v_1, \ldots, v_k\}$, allora $1 := \max L = v_1 \vee \cdots \vee v_k$ e $0 := \min L = v_1 \wedge \cdots \wedge v_k$;[11] sono ben definiti perché si può dimostrare che $\vee$ e $\wedge$ sono associative.)

Spesso è più facile verificare che esiste sempre il *meet* di due elementi (oppure il *join*), ma non viceversa. Definiamo *join-semireticolo* (rispettivamente *meet-semireticolo*) un poset in cui ogni coppia di elementi ha un *join* (rispettivamente *meet*).

Proposizione 2.42. *Sia* L *un* meet*-semireticolo finito e dotato di elemento massimo* 1. *Allora* L *è un reticolo.*

Dimostrazione. Siano $s, t \in P$ e sia $M := \{u \in P \mid u \geqslant s \text{ e } u \geqslant t\}$ l'insieme dei maggioranti. Sicuramente M non è vuoto, perché $1 \in M$, e finito perché P è finito. Come abbiamo visto sopra, dunque, ha senso il *meet*

$$m := \bigwedge_{u \in M} u.$$

Poniamo dunque $s \vee t := m$. □

Come ci aspettiamo, vale anche la proposizione duale per i *join*-semireticoli.

Proposizione 2.42*. *Sia* L *un* join*-semireticolo finito e dotato di elemento minimo* 0. *Allora* L *è un reticolo.*

[11] Nel resto della sezione useremo i simboli 0 e 1 per indicare rispettivamente il minimo e il massimo di un reticolo.

In generale, in un reticolo quindi possiamo definire il *join* e il *meet* di un insieme finito non vuoto di elementi. Questo non è più vero nel caso di insiemi infiniti di elementi. In effetti, un reticolo per cui esistono il *join* e il *meet* di un qualsiasi sottoinsieme è detto *completo*. Chiaramente, generalizzando quanto visto prima, possiamo concludere che in un reticolo completo esistono sempre il massimo e il minimo.

Cosa c'è di più bello di un reticolo? Ad esempio, ci sono i reticoli graduati (quando il poset di partenza è graduato). Ma c'è una struttura ancora migliore.

Definizione 2.43. Sia L un reticolo finito graduato con funzione rango ρ. Se per ogni $s, t \in L$ vale che

$$\rho(s) + \rho(t) \geqslant \rho(s \vee t) + \rho(s \wedge t)$$

allora il reticolo è detto *semimodulare*.

Esempio 2.8. Prendiamo in $\mathbb{R}^3$ quattro piani (sottospazi vettoriali) H_1, H_2, H_3 ed H_4 tali che $H_1 \cap H_2 = H_2 \cap H_3 = H_1 \cap H_3 = r$, dove r è una retta, mentre $H_3 \cap H_4 = s$ dove s è un'altra retta ($r \cap s = \{0\}$).

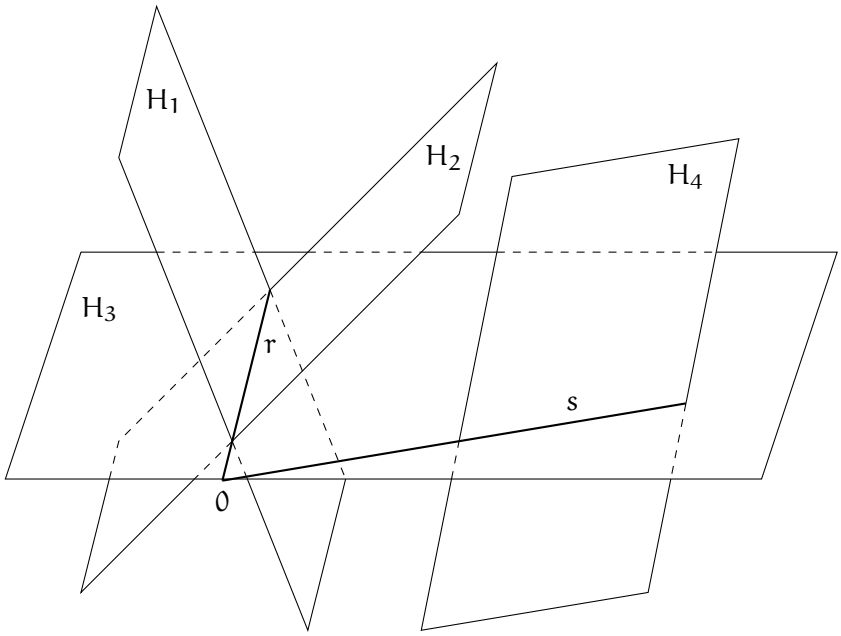


Figura 2.11: La situazione geometrica dell'Esempio 2.8.

Chiamiamo r_1 ed r_2 le due rette date rispettivamente da $H_1 \cap H_4$ e $H_2 \cap H_4$ e consideriamo il poset delle intersezioni, a cui aggiungiamo l'intersezione vuota

(data da tutto lo spazio $\mathbb{R}^3$), ordinato per inclusione al contrario: l'insieme dei vertici è

$$L = \{\{0\}, r, s, r_1, r_2, H_1, H_2, H_3, H_4, \mathbb{R}^3\}$$

e si ha $V \leqslant W$ se e solo se $V \supseteq W$. Il diagramma di Hasse di questo poset è raffigurato in Figura 2.12.

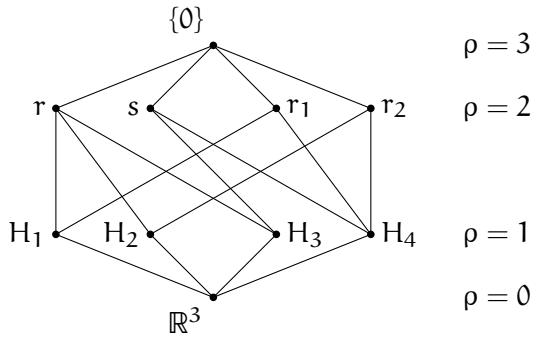


Figura 2.12: Diagramma di Hasse per il poset dell'Esempio 2.8.

Il reticolo L è graduato dalla codimensione: per ogni $W \in L$, definiamo $\rho(W) := \operatorname{codim}(W) = 3 - \dim(W)$. Concentrandoci su r ed s, abbiamo che $r \vee s = \{0\}$ e $r \wedge s = H_3$, quindi

$$\begin{array}{ccccccc} \rho(r) & + & \rho(s) & \geqslant & \rho(r \vee s) & + & \rho(r \wedge s) \\ 2 & + & 2 & \geqslant & 3 & + & 1. \end{array}$$

In realtà provando tutte le coppie si scopre che L è effettivamente semimodulare.

Esempio 2.9. Nell'esempio precedente, la disuguaglianza di semimodularità per le due rette è risultata casualmente un'uguaglianza. Vediamo che non è sempre così... ▷ *01/04/2015*

Supponiamo di prendere quattro piani $H_1, H_2, H_3, H_4 \subset \mathbb{R}^3$ in modo tale che le sei rette $r_{ij} := H_i \cap H_j$ ($i = 1, \ldots, 4$; $i < j$) siano tutte distinte ed anche in questo caso costruiamo il reticolo delle intersezioni con l'ordinamento di inclusione inversa.

Per le rette r_{12} e r_{34} abbiamo che $r_{12} \wedge r_{34} = \mathbb{R}^3$ mentre $r_{12} \vee r_{34} = \{0\}$, dunque

$$\begin{array}{ccccccc} \rho(r_{12}) & + & \rho(r_{34}) & \geqslant & \rho(r_{12} \vee r_{34}) & + & \rho(r_{12} \wedge r_{34}) \\ 2 & + & 2 & \geqslant & 0 & + & 3 \end{array}$$

e in questo caso la disuguaglianza è stretta. Comunque si può verificare che anche questo reticolo è semimodulare.

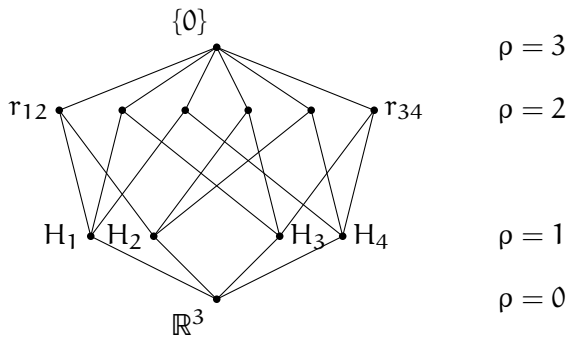


Figura 2.13: Diagramma di Hasse per il poset dell'Esempio 2.9.

In questi ultimi esempi la relazione di semimodularità aveva una forte somiglianza con la formula di Grassmann, anche se come è noto in tale formula vale sempre l'uguaglianza. Il fatto è che con i sottospazi ordinati per inclusione inversa, mentre $s \vee t = s \cap t$, in generale $s \wedge t \neq s + t$ (somma di sottospazi): potrebbe essere più grande. (Come nell'Esempio 2.9: abbiamo visto che $r_{12} \wedge r_{34} = \mathbb{R}^3$, a differenza di $r_{12} + r_{34}$ che è un piano.)

Dal momento che un reticolo è un particolare poset, ne possiamo studiare la funzione di Möbius. Introduciamo intanto un'altra algebra.

Definizione 2.44. Siano L un reticolo[12] e $\mathbb{K}$ un campo. L'*algebra di Möbius* di L, indicata con $\mathcal{A}(L)$, è la $\mathbb{K}$-algebra data dal $\mathbb{K}$-spazio vettoriale libero generato da L (combinazioni $\mathbb{K}$-lineari formali di elementi di L) con il prodotto dato da

$$st := s \wedge t$$

per ogni $s, t \in L$ ed esteso per linearità. Analogamente si definisce l'*algebra di Möbius duale* $\mathcal{A}'(L)$, in cui il prodotto è dato da $s \vee t$.

Se esiste l'elemento massimo 1 (e nel nostro caso esiste, perché consideriamo solo reticoli finiti), esso è l'unità del prodotto. Vedremo tra breve che in realtà $\mathcal{A}(L)$ è un'algebra molto semplice: è isomorfa a $\mathbb{K}^{\#(L)}$ (in cui la struttura di algebra è data dal prodotto componente per componente).

Una base di $\mathcal{A}(L)$ come $\mathbb{K}$-spazio vettoriale è data per definizione da $\{t \mid t \in L\}$. Ora, se μ è la funzione di Möbius del poset L, definiamo

$$\delta_t := \sum_{s \leqslant t} \mu(s,t)s \in \mathcal{A}(L)$$

[12] La definizione non richiede che L sia finito; comunque nel resto della sezione supporremmo sempre di lavorare con un reticolo finito.

al variare di $t \in L$. L'insieme $\{\delta_t \mid t \in L\}$ ha cardinalità $\#(L)$[13] e genera $\mathcal{A}(L)$ perché, applicando la formula di inversione di Möbius,[14]

$$t = \sum_{s \leqslant t} \delta_s$$

per ogni $t \in L$. Dunque anche $\{\delta_t \mid t \in L\}$ è una base per $\mathcal{A}(L)$ come $\mathbb{K}$-spazio vettoriale.

Teorema 2.45. *Scriviamo* $\mathbb{K}^{\#(L)} = \prod_{t \in L} \mathbb{K}_t$, *dove* $\mathbb{K}_t = \mathbb{K}$ *per ogni* $t \in L$. *Sia inoltre* $\boldsymbol{e}_t \in \mathbb{K}^{\#(L)}$ *il vettore che vale* 1 *sulla* t*-esima componente e* 0 *altrove. La mappa*

$$\begin{array}{rcl} \theta : \mathcal{A}(L) & \longrightarrow & \mathbb{K}^{\#(L)} \\ \delta_t & \longmapsto & \boldsymbol{e}_t \end{array}$$

estesa per linearità è un isomorfismo di $\mathbb{K}$*-algebre.*

Dimostrazione. Ovviamente la mappa θ è un isomorfismo di $\mathbb{K}$-spazi vettoriali (manda una base in una base). Ora, per $t \in L$, abbiamo

$$\theta(t) = \sum_{s \leqslant t} \boldsymbol{e}_s.$$

Di conseguenza

$$\theta(s)\theta(t) = \Big(\sum_{v \leqslant s} \boldsymbol{e}_v\Big)\Big(\sum_{u \leqslant t} \boldsymbol{e}_u\Big) = \sum_{(w \leqslant s) \wedge (w \leqslant t)} \boldsymbol{e}_w = \sum_{w \leqslant s \wedge t} \boldsymbol{e}_w = \theta(st). \qquad \square$$

Corollario 2.46. *Per ogni* $s, t \in L$ *vale che* $\delta_s \delta_t = \delta_{st}$ *(delta di Dirac; in questo caso* 1 *è l'identità di* $\mathcal{A}(L)$*).*

I prossimi corollari sono risultati tecnici, la cui dimostrazione è magari un po' noiosa, ma ci serviranno in seguito.

Corollario 2.47 (Teorema di Weisner)**.** *Sia* L *un reticolo finito con* $\#(L) \geqslant 2$ *e sia* $a \in L$, $a \neq 1$. *Allora*

$$\sum_{t \wedge a = 0} \mu(t, 1) = 0.$$

In altre parole, nella formula ricorsiva per il calcolo della funzione di Möbius di L possiamo tralasciare i $t \in L$ per i quali esiste un $a \in L$ che non sia 1 per cui $t \wedge a = 0$.

[13] Infatti per un poset P qualsiasi $\{u \in P \mid u \leqslant s\} = \{u \in P \mid u \leqslant t\}$ se e solo se $s = t$, quindi $\delta_s = \delta_t$ se e solo se $s = t$.

[14] Tecnicamente, abbiamo dimostrato la formula di inversione di Möbius solo per funzioni $L \to \mathbb{K}$; in questo caso, con abuso di notazione, confondiamo l'elemento $t \in L$ con la sua "funzione caratteristica" $\chi_t \colon L \to \mathbb{K}$ tale che $\chi_t(t) = 1$ e $\chi_t(s) = 0$ per $s \neq t$.

Dimostrazione. Calcoliamo $a\delta_1$ in $\mathcal{A}(L)$. Da un lato

$$a\delta_1 = \Big(\sum_{b \leqslant a} \delta_b\Big)\delta_1 = 0 \tag{2.6}$$

perché $a \neq 1$; dall'altro

$$a\delta_1 \overset{\blacktriangleright 15}{=} a\Big(\sum_{t \in L} \mu(t,1)t\Big) = \sum_{t \in L} \mu(t,1)at = \sum_{t \in L} \mu(t,1)(a \wedge t). \tag{2.7}$$

Ora, scrivendo $a\delta_1 = \sum c_t t$ in termini della base $\{t \mid t \in L\}$, abbiamo $c_0 = 0$ dall'Equazione (2.6) e

$$c_0 = \sum_{\substack{t \in L \\ a \wedge t = 0}} \mu(t,1)$$

dall'Equazione (2.7). □

Passando dall'algebra di Möbius duale si ottiene la versione duale del teorema di Weisner.

Corollario 2.47* (Teorema di Weisner duale)**.** *Sia* L *un reticolo finito con* $\#(L) \geqslant 2$ *e sia* $a \in L$, $a \neq 0$. *Allora*

$$\sum_{t \vee a = 1} \mu(0,t) = 0.$$

Corollario 2.48 (Teorema *crosscut*)**.** *Sia* L *un reticolo finito e sia* $X \subseteq L$ *tale che*

1. $1 \notin X$;
2. *se* $s \in L$, $s \neq 1$, *allora esiste* $t \in X$ *tale che* $s \leqslant t$ *(in altre parole,* X *contiene tutti gli elementi massimali di* L *ma non il massimo).*

Allora

$$\mu(0,1) = \sum_{k \geqslant 0} (-1)^k N_k,$$

dove N_k *è il numero di sottoinsiemi di* X *di cardinalità* k *il cui* meet *è* 0*, cioè*

$$N_k := \#\{Y = \{t_1, \ldots, t_k\} \subseteq X \mid t_1 \wedge \cdots \wedge t_k = 0\}.$$

Dimostrazione. In $\mathcal{A}(L)$, per $t \in L$ vale che

$$1 - t = \sum_{s \in L} \delta_s - \sum_{s \leqslant t} \delta_s = \sum_{s \not\leqslant t} \delta_s.$$

[15] La somma è estesa a tutti i $t \in L$ perché naturalmente $t \leqslant 1$ vale sempre in L.

Dunque

$$\prod_{t\in X}(1-t)=\prod_{t\in X}\sum_{s\not\leqslant t}\delta_s=\delta_1.$$

Infatti nel prodotto sopravvivono solo gli $s\in L$ tali che $s\not\leqslant t$ per ogni $t\in X$, ma per definizione di X l'unico elemento di L con tali caratteristiche è 1.

Scriviamo, come nel corollario precedente,

$$\prod_{t\in X}(1-t)=\sum_{s\in L}c_s s$$

e vediamo chi è c_0. Quando valutiamo il prodotto $\prod(1-t)$, scegliamo per ogni $t\in X$ se il fattore $(1-t)$ contribuisca con 1 oppure con $-t$ e poi sommiamo tutte le possibili scelte. Dato che $t\wedge 1=t$ e $t\wedge t=t$ per ogni $t\in L$, il prodotto $\prod(1-t)$ dà un contributo a c_0 ogni volta che scegliamo $\{t_1,\dots,t_k\}\subseteq X$ tali che $t_1\wedge\cdots\wedge t_k=0$ e questo contributo è $(-1)^k$. Dall'altra parte

$$\delta_1=\sum_{s\leqslant 1}\mu(s,1)s$$

e dunque $c_0=\mu(0,1)$. □

Corollario 2.48* (Teorema *crosscut* duale)**.** *Sia* L *un reticolo finito e sia* $X\subseteq L$ *tale che*

1. $0\notin X$*;*
2. *se* $s\in L$, $s\neq 0$*, allora esiste* $t\in X$ *tale che* $t\leqslant s$ *(in altre parole,* X *contiene tutti gli elementi minimali di* L *ma non il minimo).*

Allora

$$\mu(0,1)=\sum_{k\geqslant 0}(-1)^k N'_k,$$

dove N'_k *è il numero di sottoinsiemi di* X *di cardinalità* k *il cui* join *è* 1*, cioè*

$$N'_k:=\#\{Y=\{t_1,\dots,t_k\}\subseteq X\mid t_1\vee\cdots\vee t_k=1\}.$$

Dunque abbiamo un'algebra $\mathcal{A}(L)$ con due basi, $\{t\mid t\in L\}$ e $\{\delta_t\mid t\in L\}$, e l'abbiamo studiata vedendo cosa succedeva alternando queste due basi. Applichiamo il tutto al caso di un reticolo semimodulare, tenendo in mente che il nostro esempio cardine sarà il reticolo delle intersezioni di iperpiani. Ma prima ci serve un'altra definizione importante.

Definizione 2.49. Sia L un reticolo (finito). Un *atomo* di L è un elemento che copre 0. Il reticolo è detto *atomico* se ogni suo elemento è esprimibile come *join* di atomi (per convenzione 0 è *join* di zero atomi). Dualmente, un *coatomo* di L è un elemento ricoperto da 1. Il reticolo è detto *coatomico* se ogni suo elemento è esprimibile come *meet* di coatomi (per convenzione 1 è *meet* di zero coatomi).

Ad esempio, il reticolo delle intersezioni di iperpiani (sempre con l'inclusione inversa) è atomico, in cui gli iperpiani sono gli atomi. (In effetti, ogni altro elemento è per definizione *join*, ovvero intersezione, di iperpiani.)

Sia ora L un reticolo finito semimodulare con funzione rango ρ, in cui il rango massimo è n. Sia a un atomo di L. Nel Corollario 2.47*, duale del teorema di Weisner, siamo interessati agli elementi t tali che $a \vee t = 1$. Se a è un atomo, quali sono questi t?

- Se $a \leqslant t$, allora $t = (a \vee t) = 1$.
- Se $a \nleqslant t$, allora $t \wedge a = 0$ (perché $a \nleqslant t$ implica che $t \wedge a < a$ ed a è un atomo).

Di conseguenza, la relazione di semimodularità $\rho(t) + \rho(a) \geqslant \rho(t \wedge a) + \rho(t \vee a)$ ci dice:

- nel caso $t = 1$, $n + 1 \geqslant 1 + n$ senza informazioni aggiuntive;
- nel caso $t \wedge a = 0$, $\rho(t) + 1 \geqslant 0 + n$ cioè $\rho(t) \geqslant n - 1$.

In altre parole, se a è un atomo $a \vee t = 1$ solo se $t = 1$ oppure t è un coatomo. La tesi del Corollario 2.47*, isolando il termine $t = 1$, diventa

$$\mu(0,1) = -\sum_{\substack{t \text{ coatomo} \\ t \not\geqslant a}} \mu(0,t). \tag{2.8}$$

Teorema 2.50. *La funzione di Möbius di un reticolo semimodulare "alterna i segni", cioè vale che per ogni* $s, t \in L$ *con* $s \leqslant t$

$$(-1)^{\ell(s,t)}\mu(s,t) \geqslant 0.$$

Dimostrazione. Per induzione su n, rango massimo di L.
$\boxed{n = 1}$ L'unico reticolo con $n = 1$ è $\{0,1\}$ con $0 < 1$ e per tale reticolo la tesi è vera.
$\boxed{1, \ldots, n-1 \Rightarrow n}$ Innanzitutto è facile verificare che un qualsiasi segmento di un reticolo semimodulare è ancora un reticolo semimodulare.[16] Ora, moltiplicando

[16] Discende dal fatto che la semimodularità è equivalente al fatto che per ogni $s, t \in L$ vale l'implicazione "se sia s che t ricoprono $s \wedge t$, allora $s \vee t$ ricopre sia s che t". Per una dimostrazione, si veda [8].

ambo i membri della relazione (2.8) per $(-1)^{\ell(0,1)}$ otteniamo

$$\begin{aligned}(-1)^{\ell(0,1)}\mu(0,1) &= (-1)^{\ell(0,1)+1} \sum_{\substack{t \text{ coatomo} \\ t \not\geqslant a}} \mu(0,t) \\ &= (-1)(-1) \sum_{\substack{t \text{ coatomo} \\ t \not\geqslant a}} (-1)^{\ell(0,1)-1}\mu(0,t),\end{aligned}$$

ma $\ell(0,1) - 1 = \ell(0,t)$ perché t è un coatomo; per ipotesi induttiva dunque $(-1)^{\ell(0,t)}\mu(0,t) \geqslant 0$ e infine

$$(-1)^{\ell(0,1)}\mu(0,1) = (-1)(-1) \sum_{\substack{t \text{ coatomo} \\ t \not\geqslant a}} (-1)^{\ell(0,t)}\mu(0,t) \geqslant 0. \qquad \square$$

Abbiamo ottenuto una quantità, $(-1)^{\ell(s,t)}\mu(s,t)$, che è sempre positiva o nulla. Il primo pensiero di un matematico che studia combinatoria è: "Forse sta contando qualcosa!". In effetti, vedremo a breve il significato combinatorio di questo risultato.

2.6 Arrangiamenti di iperpiani

Sia $V = \mathbb{K}^n$ un $\mathbb{K}$-spazio vettoriale n-dimensionale. Un insieme finito di iperpiani affini $\mathcal{A}$ è detto *arrangiamento di iperpiani (affini)*.

Sappiamo che a un iperpiano affine è associata un'equazione lineare della forma

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = a \quad \text{oppure} \quad \langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle = a$$

dove $\langle \cdot, \cdot \rangle$ è il prodotto scalare standard su V. Di conseguenza, possiamo identificare un iperpiano con una coppia $(\boldsymbol{\alpha}, a) \in (V \smallsetminus \{\mathbf{0}\}) \times \mathbb{K}$ in modo che[17]

$$H_{(\boldsymbol{\alpha}, a)} := \{\boldsymbol{x} \in V \mid \langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle = a\}.$$

Il vettore $\boldsymbol{\alpha}$ è detto *vettore normale* all'iperpiano H.

Definiamo $L(\mathcal{A})$ come l'insieme di tutte le intersezioni non vuote di iperpiani in $\mathcal{A}$, a cui aggiungiamo come al solito V che è l'intersezione di nessun iperpiano. $L(\mathcal{A})$ è un poset ordinato dall'inclusione inversa.

Definizione 2.51. Un arrangiamento di iperpiani $\mathcal{A}$ è *centrale* se

$$\bigcap_{H \in \mathcal{A}} H \neq \varnothing.$$

[17] In realtà tutte le coppie della forma $(k\boldsymbol{\alpha}, ka)$ al variare di $k \in \mathbb{K} \smallsetminus \{0\}$ definiscono lo stesso iperpiano. Per i nostri scopi questo non creerà problemi.

Proposizione 2.52. *Se $\mathcal{A}$ è centrale, allora $L(\mathcal{A})$ è un reticolo.*

Dimostrazione. Per $H, K \in \mathcal{A}$ esiste il *join* $H \vee K$ che è dato dall'intersezione $H \cap K$, la quale non è vuota per centralità di $\mathcal{A}$. Inoltre esiste l'elemento minimo 0, che è V. Dunque, per la Proposizione 2.42*, $L(\mathcal{A})$ è un reticolo. □

Ora, le catene massimali di $L(\mathcal{A})$ hanno tutte la stessa lunghezza, quindi $L(\mathcal{A})$ è un reticolo graduato (dalla codimensione). Inoltre la formula di Grassmann per spazi affini garantisce la semimodularità. Infine, è immediato verificare che gli $H \in \mathcal{A}$ sono atomi per $L(\mathcal{A})$ ed ogni elemento di $L(\mathcal{A})$ è *join*, in questo caso intersezione, di atomi (proprio per definizione di $L(\mathcal{A})$): dunque $L(\mathcal{A})$ è atomico.

Definizione 2.53. Un reticolo finito semimodulare atomico è detto *reticolo geometrico*.

Il concetto di reticolo geometrico è stato introdotto proprio perché i reticoli che nascono dagli arrangiamenti di iperpiani sono stati i primi ad essere studiati e a manifestare queste caratteristiche di semimodularità e atomicità. Inoltre, "reticolo finito semimodulare atomico" è davvero troppo lungo da dire.

Notiamo che, anche se $\mathcal{A}$ non è centrale, ogni intervallo $[s, t]$ di $L(\mathcal{A})$ è un reticolo geometrico (perché l'intersezione di tutti gli elementi di $[s, t]$ è proprio $t \neq \varnothing$).

2.6.1 Il polinomio caratteristico

Introduciamo ora uno dei protagonisti di questa sezione sugli arrangiamenti di iperpiani.

Definizione 2.54. Sia $\mathcal{A}$ un arrangiamento di iperpiani. Il *polinomio caratteristico* di $\mathcal{A}$ è

$$\chi_{\mathcal{A}}(X) := \sum_{t \in L(\mathcal{A})} \mu(0, t) X^{\dim t} \in \mathbb{K}[X].$$

Vedremo che $\chi_{\mathcal{A}}$ ha un sacco di significati. Ecco qui una veloce anticipazione.

1. Il polinomio caratteristico si può adattare al polinomio cromatico di un grafo. (Lo vedremo più avanti.)

2. Se $\mathcal{A}$ è un arrangiamento di iperpiani in $\mathbb{K}^n$, definiamo

$$M(\mathcal{A}) := \mathbb{K}^n \setminus \bigcup_{H \in \mathcal{A}} H.$$

   Per $\mathbb{K} = \mathbb{R}$, questa varietà è poco significativa (tutte le componenti connesse sono contrattili...), mentre è più interessante su $\mathbb{K} = \mathbb{C}$. Infatti, detto

$$\pi_{\mathcal{A}}(X) := (-1)^{\ell} X^{\ell} \chi_{\mathcal{A}}\left(-\frac{1}{X}\right)$$

il *polinomio di Poincaré* (che è sostanzialmente il polinomio caratteristico con i coefficienti un po' rigirati; $\ell = \deg(\chi_{\mathcal{A}})$), si ha

$$\pi_{\mathcal{A}}(X) = \sum_{i \geqslant 0} \dim(H^i(\mathcal{M}(\mathcal{A}); \mathbb{Z}))X^i$$

dove $H^i(M; \mathbb{Z})$ è l'i-esimo gruppo di coomologia di M a coefficienti in $\mathbb{Z}$.

3. Ci sono arrangiamenti di iperpiani $\mathcal{A}$ per i quali, detta σ_H la riflessione per l'iperpiano $H \in \mathcal{A}$, l'insieme $\{\sigma_H \mid H \in \mathcal{A}\}$ genera un gruppo (con l'operazione di composizione) finito. L'esempio più semplice è dato dagli iperpiani $\{X_i - X_j = 0 \mid 1 \leqslant i < j \leqslant n\}$ in $\mathbb{R}^n$, le cui riflessioni generano il gruppo simmetrico $\mathcal{S}_n$. Il Teorema di Chevalley-Shepherd-Todd afferma che se G è un gruppo finito generato da riflessioni che agisce su $\mathbb{K}[X_1, \ldots, X_n]$, allora gli invarianti $\mathbb{K}[X_1, \ldots, X_n]^G$ sono generati da polinomi $f_1, \ldots, f_n$ *non* unici, ma con i gradi unici.[18] I numeri $d_i := \deg(f_i) - 1$ sono detti *esponenti* del gruppo G. Ora, se $\mathcal{A}$ è l'arrangiamento di iperpiani le cui riflessioni generano G, si ha

$$\pi_{\mathcal{A}}(X) = (1 + d_1X) \cdots (1 + d_nX).$$

Dato che $\chi_{\mathcal{A}}$ è così importante, cerchiamo un modo per calcolarlo. Iniziamo con un altro paio di definizioni. ▹ *13/04/2015*

Definizione 2.55. La *dimensione* di un arrangiamento $\mathcal{A}$ è $\dim(\mathcal{A}) := \dim(V)$.

Osserviamo che, nel caso in cui $\mathcal{A}$ sia formato da un solo iperpiano H, $\dim(\mathcal{A})$ *non* è la dimensione di H come sottospazio affine (che sarebbe $\dim(V) - 1$).

Definizione 2.56. Il *rango* di un arrangiamento $\mathcal{A}$ è la dimensione dello spazio vettoriale generato dai vettori normali agli iperpiani di $\mathcal{A}$, cioè

$$\operatorname{rk}(\mathcal{A}) := \dim\left\langle \boldsymbol{\alpha} \;\middle|\; H_{(\boldsymbol{\alpha}, a)} \in \mathcal{A} \right\rangle.$$

L'arrangiamento è detto *essenziale* se $\dim(\mathcal{A}) = \operatorname{rk}(\mathcal{A})$.

È sempre possibile *essenzializzare* un arrangiamento $\mathcal{A}$, cioè costruire un arrangiamento essenziale $\operatorname{ess}(\mathcal{A})$ che mantenga in un certo senso le principali proprietà di $\mathcal{A}$ (ad esempio tale che $L(\operatorname{ess}(\mathcal{A})) \simeq L(\mathcal{A})$), eliminando la "ridondanza" presente in un arrangiamento non essenziale. Vediamo brevemente come.

1. Dato un arrangiamento $\mathcal{A}$ in $\mathbb{K}^n$, sia $U := \left\langle \boldsymbol{\alpha} \;\middle|\; H_{(\boldsymbol{\alpha}, a)} \in \mathcal{A} \right\rangle$.

[18] Come abbiamo visto nella Sezione 1.8, sia i polinomi simmetrici elementari che quelli completi che quelli di Newton generano gli invarianti rispetto all'azione di $\mathcal{S}_n$; in ogni caso si ha $\deg(f_i) = i$.

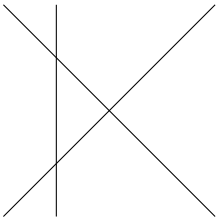
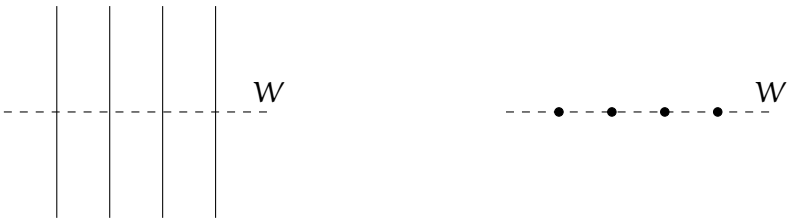


Figura 2.14: Esempio di arrangiamento essenziale in $\mathbb{R}^2$. In questo caso $\dim(\mathcal{A}) = \mathrm{rk}(\mathcal{A}) = 2$.

2. Sia Y un sottospazio complementare di U, cioè tale che $U \oplus Y = \mathbb{K}^n$.
3. Sia $W := Y^\perp = \{\boldsymbol{w} \in \mathbb{K}^n \mid \langle \boldsymbol{v}, \boldsymbol{w} \rangle = 0 \text{ per ogni } \boldsymbol{v} \in Y\}$.[19]
4. Definiamo $\mathcal{A}_W := \{H \cap W \mid H \in \mathcal{A}\}$. La dimostrazione del fatto che $\mathcal{A}_W$ è un arrangiamento essenziale in W può essere trovata nell'Appendice A.



(a) Le quattro rette parallele *non* sono un arrangiamento essenziale: lo spazio dei vettori normali ha dimensione 1.

(b) L'essenzializzazione $\mathrm{ess}(\mathcal{A})$ è formata da quattro punti. *Nota:* la retta tratteggiata è W e *non* fa parte di $\mathrm{ess}(\mathcal{A})$.

Figura 2.15: Esempio di essenzializzazione di un arrangiamento $\mathcal{A}$ in $\mathbb{R}^2$.

Torniamo al polinomio caratteristico. La seguente proposizione mostra un primo modo per calcolarlo.

Proposizione 2.57. *Sia $\mathcal{A}$ un arrangiamento di iperpiani in V con $\dim(V) = n$. Allora*

$$\chi_{\mathcal{A}}(X) = \sum_{\substack{\mathcal{B} \subseteq \mathcal{A} \\ \mathcal{B} \text{ centrale}}} (-1)^{\#(\mathcal{B})} X^{n - \mathrm{rk}(\mathcal{B})}$$

dove la somma è estesa a tutti i sottoarrangiamenti centrali di $\mathcal{A}$.

[19] Se $\mathrm{char}(\mathbb{K}) = 0$, possiamo prendere direttamente $W = U$; questo non si può fare in caratteristica positiva, perché è possibile che $\dim(Y \cap Y^\perp) > 0$.

Esempio 2.10. Consideriamo l'arrangiamento $\mathcal{A} := \{a, b, c, d\}$ in $\mathbb{R}^2$ mostrato in Figura 2.16.

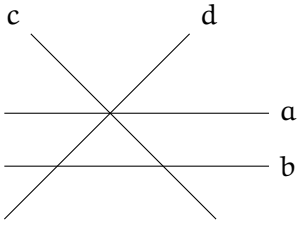


Figura 2.16: L'arrangiamento per l'Esempio 2.10.

$\mathcal{B}$	$\#(\mathcal{B})$	$\mathrm{rk}(\mathcal{B})$
$\varnothing$	0	0
$\{a\}$	1	1
$\{b\}$	1	1
$\{c\}$	1	1
$\{d\}$	1	1
$\{a, c\}$	2	2
$\{a, d\}$	2	2
$\{b, c\}$	2	2
$\{b, d\}$	2	2
$\{c, d\}$	2	2
$\{a, c, d\}$	3	2

Tabella 2.1: I possibili sottoarrangiamenti centrali dell'arrangiamento in Figura 2.16.

La Tabella 2.1 elenca i possibili sottoarrangiamenti centrali $\mathcal{B}$ di $\mathcal{A}$. In base alla Proposizione 2.57, il polinomio caratteristico di $\mathcal{A}$ è

$$\chi_{\mathcal{A}}(X) = X^2 - 4X + 5 - 1 = X^2 - 4X + 4.$$

Osserviamo *en passant* che

- $\chi_{\mathcal{A}}(-1) = 9$ e il piano $\mathbb{R}^2$ è diviso in nove regioni dagli iperpiani di $\mathcal{A}$;
- $\chi_{\mathcal{A}}(1) = 1$ e una sola delle nove regioni è limitata.

Non è un caso... Lo vedremo in seguito. In effetti avevamo già anticipato che il polinomio caratteristico "conta" qualcosa.

Dimostrazione della Proposizione 2.57. Sia $t \in L(\mathcal{A})$. Definiamo

$$\mathcal{A}_t := \{H \in \mathcal{A} \mid H \leqslant t\},$$

cioè $\mathcal{A}_t$ è l'insieme degli iperpiani di $\mathcal{A}$ che includono t. Ora, $[0, t]$ è un reticolo e $\mathcal{A}_t \subseteq [0, t]$ soddisfa le ipotesi del Teorema *crosscut* duale (Corollario 2.48*). Dunque

$$\mu(0, t) = \sum_{k \geqslant 0} (-1)^k N_k(t)$$

in cui $N_k(t)$ è il numero di sottoinsiemi di $\mathcal{A}_t$ di cardinalità k il cui *join* è t. Detto altrimenti,

$$\mu(0, t) = \sum_{\mathcal{B} \in \mathfrak{B}} (-1)^{\#(\mathcal{B})}$$

dove si è posto per comodità di scrittura

$$\mathfrak{B} := \left\{ \mathcal{B} \subseteq \mathcal{A}_t \;\middle|\; \bigcap_{H \in \mathcal{B}} H = t \right\},$$

ricordando che in questo contesto il *join* è dato dall'intersezione. Moltiplicando ora per $X^{\dim t}$ e sommando su tutti i $t \in L(\mathcal{A})$ si arriva a

$$\chi_{\mathcal{A}}(X) = \sum_{t \in L(\mathcal{A})} \left(\sum_{\mathcal{B} \in \mathfrak{B}} (-1)^{\#(\mathcal{B})} \right) X^{\dim t}.$$

Su quali addendi scorre questa doppia sommatoria? Riflettendoci un po' ci accorgiamo che stiamo sommando su tutti i $\mathcal{B} \subseteq \mathcal{A}$ sottoarrangiamenti per i quali esiste $t \in L(\mathcal{A})$ tale che $\bigcap_{H \in \mathcal{B}} H = t$, ossia sui sottoarrangiamenti *centrali* di $\mathcal{A}$. Da questa osservazione e dal fatto che $\dim t = n - \mathrm{rk}(\mathcal{B})$ (si veda il Lemma A.2 nell'Appendice A) si ha la tesi. □

Presentiamo ora una formula ricorsiva per il calcolo del polinomio caratteristico. Per $t \in L(\mathcal{A})$, definiamo

$$\mathcal{A}^t := \{t \cap H \mid t \cap H \neq \varnothing,\ H \in \mathcal{A} \setminus \mathcal{A}_t\}$$

cioè $\mathcal{A}^t$ è l'insieme di tutte le intersezioni non vuote $t \cap H$ al variare degli iperpiani $H \in \mathcal{A}$ che non contengono t. Notiamo che $\mathcal{A}^t$ è un arrangiamento di iperpiani nello spazio affine t.

Dato che $\mathcal{A}_t$ e $\mathcal{A}^t$ sono arrangiamenti, possiamo chiederci chi siano i poset associati ad essi; risulta che

- $L(\mathcal{A}_t) \simeq \Lambda_t$, dove Λ_t è l'ideale d'ordine principale in $L(\mathcal{A})$ generato da t, cioè $\{s \in L(\mathcal{A}) \mid s \leqslant t\}$;

- $L(\mathcal{A}^t) \simeq V_t$, dove V_t è l'ideale d'ordine duale principale in $L(\mathcal{A})$ generato da t, cioè $\{s \in L(\mathcal{A}) \mid s \geqslant t\}$.

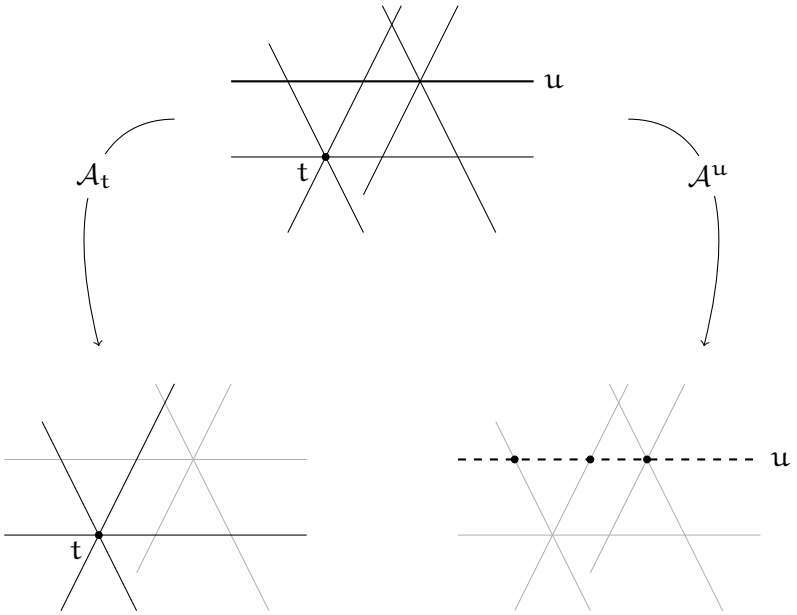


Figura 2.17: Esempio di $\mathcal{A}_t$ e $\mathcal{A}^u$ per un arrangiamento $\mathcal{A}$ in $\mathbb{R}^2$. Ricordiamo che $u \notin \mathcal{A}^u$.

Definizione 2.58. Siano $\mathcal{A}$ un arrangiamento di iperpiani e $H_0 \in \mathcal{A}$. Definiamo *tripla* (o *terna*) *di arrangiamenti con iperpiano scelto* H_0 la tripla ordinata $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ dove

$$\mathcal{A}' := \mathcal{A} \setminus \{H_0\} \qquad \text{e} \qquad \mathcal{A}'' := \mathcal{A}^{H_0}.$$

Teorema 2.59 (*Deletion-Restriction*)**.** *Sia $\mathcal{A}$ un arrangiamento in $\mathbb{K}^n$ e sia $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ una tripla di arrangiamenti. Allora*

$$\chi_{\mathcal{A}}(X) = \chi_{\mathcal{A}'}(X) - \chi_{\mathcal{A}''}(X).$$

Dimostrazione. Sia H_0 l'iperpiano scelto per la tripla. Per la Proposizione 2.57 possiamo scrivere

$$\begin{aligned}\chi_{\mathcal{A}}(X) &= \sum_{\substack{\mathcal{B}\subseteq\mathcal{A}\\ \mathcal{B}\text{ centrale}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})} \\ &= \sum_{\substack{\mathcal{B}\subseteq\mathcal{A}\\ \mathcal{B}\text{ centrale}\\ H_0\notin\mathcal{B}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})} + \sum_{\substack{\mathcal{B}\subseteq\mathcal{A}\\ \mathcal{B}\text{ centrale}\\ H_0\in\mathcal{B}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})}.\end{aligned}$$

Dal momento che $\mathcal{A}'$ vive nello stesso spazio di $\mathcal{A}$ e $H_0 \notin \mathcal{A}'$ per definizione, la prima sommatoria si riduce a

$$\sum_{\substack{\mathcal{B}\subseteq\mathcal{A}\\ \mathcal{B}\text{ centrale}\\ H_0\notin\mathcal{B}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})} = \sum_{\substack{\mathcal{B}\subseteq\mathcal{A}'\\ \mathcal{B}\text{ centrale}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})} = \chi_{\mathcal{A}'}(X).$$

Vediamo ora la seconda sommatoria. Se $\mathcal{B}$ è un sottoarrangiamento centrale di $\mathcal{A}$ con $H_0 \in \mathcal{B}$, definiamo $\mathcal{B}_1 := \mathcal{B}^{H_0}$, il quale è un arrangiamento centrale in H_0 (che è uno spazio di dimensione $n-1$), anzi è un sottoarrangiamento di $\mathcal{A}'' = \mathcal{A}^{H_0}$.

Risulta che $\mathrm{rk}(\mathcal{B}_1) = \mathrm{rk}(\mathcal{B}) - 1$. Infatti dal Lemma A.2 sappiamo che

$$(n-1) - \mathrm{rk}(\mathcal{B}_1) = \dim\left(\bigcap_{H'\in\mathcal{B}_1} H'\right) \qquad \text{e} \qquad n - \mathrm{rk}(\mathcal{B}) = \dim\left(\bigcap_{H\in\mathcal{B}} H\right).$$

Ma per definizione $H' \in \mathcal{B}_1$ è dato da $H \cap H_0$ al variare di $H \in \mathcal{B} \smallsetminus \{H_0\}$,[20] quindi

$$\bigcap_{H'\in\mathcal{B}_1} H' = \bigcap_{H\in\mathcal{B}\smallsetminus\{H_0\}} H \cap H_0 = \left(\bigcap_{H\in\mathcal{B}\smallsetminus\{H_0\}} H\right) \cap H_0 = \bigcap_{H\in\mathcal{B}} H$$

da cui $(n-1) - \mathrm{rk}(\mathcal{B}_1) = n - \mathrm{rk}(\mathcal{B})$.

Se ora fosse $\#(\mathcal{B}_1) = \#(\mathcal{B}) - 1$, avremmo la tesi; purtroppo non è così, perché può capitare che per due iperpiani $H_1, H_2 \in \mathcal{B}$ distinti si abbia $H_1 \cap H_0 = H_2 \cap H_0$; questo tuttavia non è un problema. Infatti per un qualsiasi insieme S con $\#(S) = r$ vale che

$$\sum_{\substack{T\subseteq S\\ T\neq\varnothing}} (-1)^{\#(T)} = \sum_{k=1}^{r} (-1)^k \binom{r}{k} = -1;$$

è sufficiente scrivere $0 = (1-1)^r$ e sviluppare il binomio.

Nella costruzione di $\mathcal{B}_1$ a partire da $\mathcal{B}$, se $S = \{H_1, \dots, H_r\} \subseteq \mathcal{B} \smallsetminus \{H_0\}$ è tale che $H_i \cap H_0 = H_j \cap H_0 = t$ per ogni $H_i, H_j \in S$, allora basta prendere un qualsiasi sottoinsieme non vuoto $T \subseteq S$ affinché ci sia l'elemento t in $\mathcal{B}_1$. Di conseguenza, se $\mathcal{B}_1 = \{t_1, \dots, t_k\}$, possiamo partizionare $\mathcal{B} \smallsetminus \{H_0\}$ in $\{S_1, \dots, S_k\}$ in modo che t_j provenga (nel senso descritto prima) da S_j. Dunque i possibili arrangiamenti $\mathcal{B}$ che danno origine a $\mathcal{B}_1$[21] sono della forma $\{H_0\} \cup T_1 \cup \cdots \cup T_k$ al variare di tutti i possibili sottoinsiemi non vuoti $T_j \subseteq S_j$, quindi

$$\sum_{\mathcal{B}\rightsquigarrow\mathcal{B}_1} (-1)^{\#(\mathcal{B})} = (-1)\left(\sum_{\substack{T_1\subseteq S_1\\ T_1\neq\varnothing}} (-1)^{\#(T_1)}\right)\cdots\left(\sum_{\substack{T_k\subseteq S_k\\ T_k\neq\varnothing}} (-1)^{\#(T_k)}\right) = (-1)^{\#(\mathcal{B}_1)+1}.$$

[20] In effetti se $H_0 \in \mathcal{B}$ si ha $\mathcal{B}_{H_0} = \{H_0\}$.

[21] Useremo la notazione $\mathcal{B} \rightsquigarrow \mathcal{B}_1$ per denotarli più sotto.

In conclusione

$$\sum_{\substack{\mathcal{B}\subseteq\mathcal{A}\\ \mathcal{B}\text{ centrale}\\ H_0\in\mathcal{B}}} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})} = \sum_{\mathcal{B}_1\subseteq\mathcal{A}''} \sum_{\mathcal{B}\rightsquigarrow\mathcal{B}_1} (-1)^{\#(\mathcal{B})} X^{n-\mathrm{rk}(\mathcal{B})}$$

$$= \sum_{\mathcal{B}_1\subseteq\mathcal{A}''} (-1)^{\#(\mathcal{B}_1)+1} X^{(n-1)-\mathrm{rk}(\mathcal{B}_1)} = -\chi_{\mathcal{A}''}(X). \quad \square$$

2.6.2 Regioni

Ci concentriamo ora sul caso $\mathbb{K} = \mathbb{R}$. In particolare vediamo come il polinomio caratteristico ci permette di contare le regioni in cui lo spazio resta diviso dagli iperpiani di un arrangiamento.

Definizione 2.60. Una *regione* dell'arrangiamento $\mathcal{A}$ in $\mathbb{R}^n$ è una componente connessa della varietà

$$\mathcal{M}(\mathcal{A}) := \mathbb{R}^n \setminus \bigcup_{H\in\mathcal{A}} H.$$

Denotiamo con $\mathcal{R}(\mathcal{A})$ l'insieme delle regioni di $\mathcal{A}$.

Se W è lo spazio generato dai vettori normali agli iperpiani di $\mathcal{A}$, ricordiamo che $\mathcal{A}_W := \{H \cap W \mid H \in \mathcal{A}\}$ è un arrangiamento essenziale (in W). Il numero di regioni di $\mathcal{A}$ e $\mathcal{A}_W$ è lo stesso (si veda l'Appendice A per una dimostrazione).

Definizione 2.61. Una regione $R \in \mathcal{R}(\mathcal{A})$ è *relativamente limitata* se $R \cap W$ è limitata. Indichiamo con $\mathcal{B}(\mathcal{A})$ l'insieme delle regioni relativamente limitate di $\mathcal{A}$.

Naturalmente se $\mathcal{A}$ è essenziale una regione è limitata se e solo se è relativamente limitata, poiché $W = \mathbb{R}^n$. Viceversa, se l'arrangiamento non è essenziale non esistono regioni limitate:[22] infatti in questo caso $W^\perp \neq \{0\}$ e se $\mathbf{p} \in R$, allora anche $\mathbf{p} + \boldsymbol{w} \in R$ per ogni $\boldsymbol{w} \in W^\perp$. In altre parole, ogni regione R contiene un sottospazio affine di dimensione non nulla.

Proposizione 2.62. *Sia $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ una tripla di arrangiamenti. Allora*

$$\#(\mathcal{R}(\mathcal{A})) = \#\big(\mathcal{R}(\mathcal{A}')\big) + \#\big(\mathcal{R}(\mathcal{A}'')\big)$$

$$\#(\mathcal{B}(\mathcal{A})) = \begin{cases} \#(\mathcal{B}(\mathcal{A}')) + \#(\mathcal{B}(\mathcal{A}'')) & \text{se } \mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}') \\ 0 & \text{se } \mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}') + 1. \end{cases}$$

Dimostrazione. Consideriamo le regioni in $\mathcal{R}(\mathcal{A}')$. Quando "tagliamo" con l'iperpiano H_0, ci sono regioni $R_1 \in \mathcal{R}(\mathcal{A}')$ tali che $R_1 \cap H_0 = \varnothing$ e regioni $R_2 \in \mathcal{R}(\mathcal{A}')$

[22] Ma possono esistere regioni relativamente limitate.

tali che $R_2 \cap H_0 \neq \varnothing$. Le prime si ritrovano anche in $\mathcal{R}(\mathcal{A})$, mentre ciascuna delle seconde è divisa in due da H_0 (vedi anche Figura 2.18). Quindi

$$\begin{aligned}\#(\mathcal{R}(\mathcal{A})) &= \#\{R_1 \in \mathcal{R}(\mathcal{A}') \mid R_1 \cap H_0 = \varnothing\} + 2 \cdot \#\{R_2 \in \mathcal{R}(\mathcal{A}') \mid R_2 \cap H_0 \neq \varnothing\} \\ &= \#\big(\mathcal{R}(\mathcal{A}')\big) + \#\{\text{regioni divise in due da } H_0\}.\end{aligned}$$

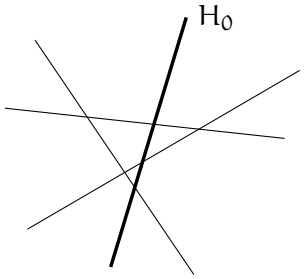


Figura 2.18: Delle sette regioni di $\mathcal{R}(\mathcal{A}')$, quattro sono tagliate in due da H_0. Quindi $\#(\mathcal{R}(\mathcal{A})) = 3 + 2 \cdot 4 = 7 + 4 = 11$.

Ora, c'è una biiezione tra le regioni divise in due da H_0 e $\mathcal{R}(\mathcal{A}'')$. Infatti, se R' è una regione di $\mathcal{R}(\mathcal{A}')$ tagliata in due da H_0 allora $R' \cap H_0 \in \mathcal{R}(\mathcal{A}'')$; viceversa, se $R'' \in \mathcal{R}(\mathcal{A}'')$, sia $\mathbf{p} \in R''$ e sia $d > 0$ un numero reale minore del minimo delle distanze di $\mathbf{p}$ dagli iperpiani di $\mathcal{A}$ diversi da H_0. Detto $\boldsymbol{\alpha}_0$ il vettore normale ad H_0 di norma unitaria, consideriamo i due punti $\mathbf{p}^+ := \mathbf{p} + d\boldsymbol{\alpha}_0$ e $\mathbf{p}^- := \mathbf{p} - d\boldsymbol{\alpha}_0$ (vedi Figura 2.19): supponiamo che esista un iperpiano $H \in \mathcal{A}$ diverso da H_0 che li separi e siano $(\boldsymbol{\beta}, b)$ con $\|\boldsymbol{\beta}\| = 1$ tali che $H = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x}, \boldsymbol{\beta} \rangle = b\}$. È noto che in tal caso la distanza (con segno) di un punto $\mathbf{q}$ da H è data da

$$d(\mathbf{q}, H) := \langle \mathbf{q}, \boldsymbol{\beta} \rangle - b.$$

Ora, la distanza tra $\mathbf{p}^+$ e $\mathbf{p}^-$ è $2d$ e per il Teorema di Pitagora (multidimensionale)

$$2d \geqslant d(\mathbf{p}^+, H) + d(\mathbf{p}^-, H) = \langle \mathbf{p}^+, \boldsymbol{\beta} \rangle - b + \langle \mathbf{p}^-, \boldsymbol{\beta} \rangle - b = 2(\langle \mathbf{p}, \boldsymbol{\beta} \rangle - b) > 2d$$

e questo non può verificarsi. Di conseguenza i punti $\mathbf{p}^+$ e $\mathbf{p}^-$ devono appartenere a una stessa regione $R' \in \mathcal{R}(\mathcal{A}')$, che viene tagliata in due da H_0. In conclusione $\#\{\text{regioni divise in due da } H_0\} = \#(\mathcal{R}(\mathcal{A}''))$ e la prima formula è dimostrata.

Passiamo alla seconda formula e consideriamo dapprima il caso $\operatorname{rk}(\mathcal{A}') = \operatorname{rk}(\mathcal{A})$. Dato che $\big\langle \boldsymbol{\alpha} \;\big|\; H_{(\boldsymbol{\alpha},a)} \in \mathcal{A} \big\rangle = \big\langle \boldsymbol{\alpha} \;\big|\; H_{(\boldsymbol{\alpha},a)} \in \mathcal{A} \smallsetminus \{H_0\} \big\rangle$, possiamo passare alle essenzializzazioni intersecando con $W := \big\langle \boldsymbol{\alpha} \;\big|\; H_{(\boldsymbol{\alpha},a)} \in \mathcal{A} \big\rangle$ e contare le regioni limitate anziché quelle relativamente limitate.

La Figura 2.20 elenca tutti i possibili casi in cui sono coinvolte le regioni limitate di $\mathcal{A}$, $\mathcal{A}'$ e $\mathcal{A}''$: analizziamoli singolarmente.

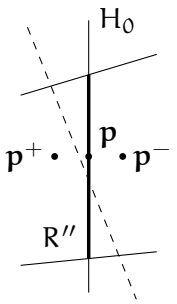
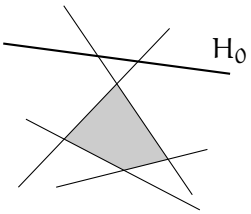
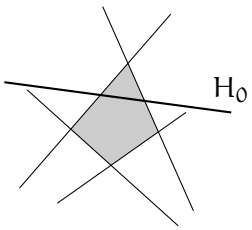


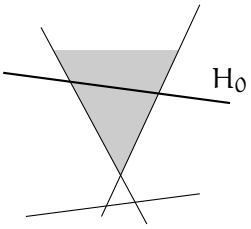
Figura 2.19: Due punti "sufficientemente vicini" a R'' devono appartenere a una stessa regione di $\mathcal{A}'$, perché un eventuale iperpiano (tratteggiato in figura) che li separasse taglierebbe anche R''.



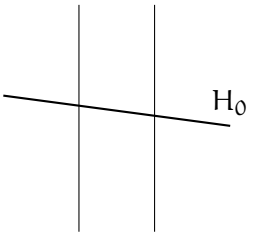
(a) Una regione limitata di $\mathcal{A}'$ non tagliata da H_0.



(b) Una regione limitata di $\mathcal{A}'$ tagliata da H_0 in due regioni limitate di $\mathcal{A}$.



(c) H_0 dà luogo a una regione limitata di $\mathcal{A}$ a partire da una illimitata di $\mathcal{A}'$.



(d) H_0 dà luogo a una regione limitata di $\mathcal{A}''$, ma non di $\mathcal{A}$.

Figura 2.20: Possibili relazioni tra le regioni limitate di $\mathcal{A}$, $\mathcal{A}'$ e $\mathcal{A}''$.

- Nel caso in Figura 2.20a, abbiamo una regione limitata di $\mathcal{A}'$ che ritroviamo anche tra le regioni limitate di $\mathcal{A}$, perché non è interessata dall'intersezione con H_0, e nessuna regione limitata di $\mathcal{A}''$. Quindi vale che $\#(\mathcal{B}(\mathcal{A})) = \#(\mathcal{B}(\mathcal{A}')) + \#(\mathcal{B}(\mathcal{A}''))$, poiché $1 = 1 + 0$.

- Nel caso in Figura 2.20b, una regione limitata di $\mathcal{A}'$ è tagliata in due regioni limitate di $\mathcal{A}$ e nel mezzo viene creata una regione limitata di $\mathcal{A}''$. Anche qui vale $\#(\mathcal{B}(\mathcal{A})) = \#(\mathcal{B}(\mathcal{A}')) + \#(\mathcal{B}(\mathcal{A}''))$, poiché $2 = 1 + 1$.
- Nel caso in Figura 2.20c, è presente una sola regione limitata di $\mathcal{A}$ nata da una regione illimitata di $\mathcal{A}'$; inoltre l'intersezione con H_0 dà origine a una regione limitata di $\mathcal{A}''$. Dunque anche in questo caso $\#(\mathcal{B}(\mathcal{A})) = \#(\mathcal{B}(\mathcal{A}')) + \#(\mathcal{B}(\mathcal{A}''))$, poiché $1 = 0 + 1$.
- Infine, il caso in Figura 2.20d non può verificarsi se $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}')$.

Dato che i casi precedenti esauriscono tutte le possibili situazioni, alla fine possiamo dedurne che la formula

$$\#(\mathcal{B}(\mathcal{A})) = \#\big(\mathcal{B}(\mathcal{A}')\big) + \#\big(\mathcal{B}(\mathcal{A}'')\big)$$

è vera.

Cosa succede se invece $\mathrm{rk}(\mathcal{A}') = \mathrm{rk}(\mathcal{A}) - 1$? Siano $W := \langle \boldsymbol{\alpha} \mid H_{(\boldsymbol{\alpha},a)} \in \mathcal{A} \rangle$ e $W' := \langle \boldsymbol{\alpha} \mid H_{(\boldsymbol{\alpha},a)} \in \mathcal{A}' \rangle$. Ancora una volta intersechiamo con W e cerchiamo le regioni limitate. Dato che $W' \subsetneq W$, l'arrangiamento $\mathcal{A}'$ non è essenziale in W: per quanto visto prima, dunque, $\mathcal{A}'$ non ha regioni limitate in W, anzi ogni regione di $\mathcal{A}'$ contiene certamente una retta. Intersecando con H_0, tutt'al più questa retta è spezzata in due semirette, che sono comunque sottoinsiemi illimitati della regione. Quindi in $\mathcal{A}$ non ci sono regioni relativamente limitate. □

Teorema 2.63. *Sia $\mathcal{A}$ un arrangiamento di iperpiani in $\mathbb{R}^n$. Allora*

$$\#(\mathcal{R}(\mathcal{A})) = (-1)^n \chi_{\mathcal{A}}(-1) \qquad e \qquad \#(\mathcal{B}(\mathcal{A})) = (-1)^{\mathrm{rk}(\mathcal{A})} \chi_{\mathcal{A}}(1).$$

Esempio 2.11. Consideriamo l'arrangiamento in $\mathbb{R}^2$ disegnato in Figura 2.21. Calcoliamone il polinomio caratteristico a partire dai possibili sottoarrangiamenti centrali, elencati nella Tabella 2.2.

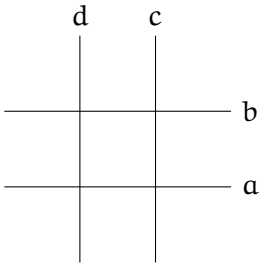


Figura 2.21: L'arrangiamento per l'Esempio 2.11.

$\mathcal{B}$	$\#(\mathcal{B})$	$\mathrm{rk}(\mathcal{B})$
$\varnothing$	0	0
$\{a\}$	1	1
$\{b\}$	1	1
$\{c\}$	1	1
$\{d\}$	1	1
$\{a, c\}$	2	2
$\{a, d\}$	2	2
$\{b, c\}$	2	2
$\{b, d\}$	2	2

Tabella 2.2: I possibili sottoarrangiamenti centrali dell'arrangiamento in Figura 2.21.

Dalla Proposizione 2.57 otteniamo che

$$\chi_{\mathcal{A}}(X) = X^2 - 4X + 4.$$

In questo caso $\mathrm{rk}(\mathcal{A}) = n = 2$, quindi

$$\begin{aligned}\#(\mathcal{R}(\mathcal{A})) &= (-1)^2\chi_{\mathcal{A}}(-1) = 1 + 4 + 4 = 9\\ \#(\mathcal{B}(\mathcal{A})) &= (-1)^2\chi_{\mathcal{A}}(1) = 1 - 4 + 4 = 1.\end{aligned}$$

Dimostrazione del Teorema 2.63. Dimostriamo le due relazioni con un ragionamento induttivo. Per prima cosa, le funzioni $\#(\mathcal{R}(\mathcal{A}))$ e $(-1)^n\chi_{\mathcal{A}}(-1)$ coincidono sull'arrangiamento vuoto: infatti $\#(\mathcal{R}(\varnothing)) = 1$ e $\chi_{\varnothing}(X) = X^n$, dunque $(-1)^n\chi_{\varnothing}(-1) = (-1)^{2n} = 1$. Inoltre soddisfano la stessa regola ricorsiva sulle terne: da un lato la Proposizione 2.62 ci dice che ▷ *15/04/2015*

$$\#(\mathcal{R}(\mathcal{A})) = \#\big(\mathcal{R}(\mathcal{A}')\big) + \#\big(\mathcal{R}(\mathcal{A}'')\big)$$

e dall'altro il Teorema 2.59 afferma che

$$\chi_{\mathcal{A}}(X) = \chi_{\mathcal{A}'}(X) - \chi_{\mathcal{A}''}(X).$$

Moltiplicando quest'ultima relazione per $(-1)^n$ abbiamo

$$\begin{aligned}(-1)^n\chi_{\mathcal{A}}(X) &= (-1)^n\chi_{\mathcal{A}'}(X) - (-1)^n\chi_{\mathcal{A}''}(X) =\\ &= (-1)^n\chi_{\mathcal{A}'}(X) + (-1)^{n-1}\chi_{\mathcal{A}''}(X).\end{aligned}$$

che è proprio la stessa formula ricorsiva (ricordiamo che $\dim(\mathcal{A}'') = n - 1$). Dunque le due funzioni devono coincidere su ogni arrangiamento.

Passiamo alla seconda formula. Osserviamo che $\mathcal{B}(\varnothing) = 1$: infatti lo spazio generato dai vettori normali è $W = \langle \varnothing \rangle = \{0\}$, dunque l'unica regione dell'arrangiamento vuoto (che è $\mathbb{R}^n$) è relativamente limitata ($\mathbb{R}^n \cap \{0\} = \{0\}$). D'altra parte $\operatorname{rk}(\varnothing) = 0$, quindi la formula è verificata. Per il passo induttivo, separiamo i due casi della Proposizione 2.62.

Se $\operatorname{rk}(\mathcal{A}) = \operatorname{rk}(\mathcal{A}')$, notiamo che $\operatorname{rk}(\mathcal{A}'') = \operatorname{rk}(\mathcal{A}') - 1$. Questo perché, detti $W_{\mathcal{A}}$, $W_{\mathcal{A}'}$ e $W_{\mathcal{A}''}$ gli spazi generati dai vettori normali,[23] l'algebra lineare ci dice che $H_0 \cap W_{\mathcal{A}'} = W_{\mathcal{A}''}$. Ora, $\operatorname{rk}(\mathcal{A}) = \operatorname{rk}(\mathcal{A}')$ implica che $\alpha_{H_0} \in W_{\mathcal{A}'}$ e quindi che $\dim(H_0 + W_{\mathcal{A}'}) = n$.[24] Dalla formula di Grassmann segue allora facilmente che $\dim(W_{\mathcal{A}''}) = \dim(W_{\mathcal{A}'}) - 1$. Non resta che verificare la relazione ricorsiva per $(-1)^{\operatorname{rk}(\mathcal{A})}\chi_{\mathcal{A}}(1)$: dal Teorema 2.59 moltiplicando per $(-1)^{\operatorname{rk}(\mathcal{A})}$ abbiamo

$$\begin{aligned}(-1)^{\operatorname{rk}(\mathcal{A})}\chi_{\mathcal{A}}(1) &= (-1)^{\operatorname{rk}(\mathcal{A})}\chi_{\mathcal{A}'}(1) - (-1)^{\operatorname{rk}(\mathcal{A})}\chi_{\mathcal{A}''}(1) = \\ &= (-1)^{\operatorname{rk}(\mathcal{A}')}\chi_{\mathcal{A}'}(1) + (-1)^{\operatorname{rk}(\mathcal{A}'')}\chi_{\mathcal{A}''}(1).\end{aligned}$$

Se invece $\operatorname{rk}(\mathcal{A}) = \operatorname{rk}(\mathcal{A}') + 1$, allora $\#(\mathcal{B}(\mathcal{A})) = 0$. È sufficiente mostrare che in questo caso $L(\mathcal{A}') \simeq L(\mathcal{A}'')$ (come poset): dal momento che il polinomio caratteristico dipende solo dalla funzione di Möbius di $L(\mathcal{A})$, ne deduciamo che $\chi_{\mathcal{A}'}(X) = \chi_{\mathcal{A}''}(X)$, da cui $\chi_{\mathcal{A}}(X) = 0$ per il Teorema 2.59.

Dimostriamo allora che l'intersezione con H_0 manda $t' \in L(\mathcal{A}')$ in un elemento $t'' \in L(\mathcal{A}'')$ e viceversa. Supponiamo che $t = H_1 \cap \cdots \cap H_k$, le cui equazioni siano $\langle \alpha_i, x \rangle = a_i$ per ogni $i = 1, \dots, k$. Per il Teorema di Rouché-Capelli

$$\operatorname{rk}\begin{pmatrix} — & \alpha_1 & — \\ & \vdots & \\ — & \alpha_k & — \end{pmatrix} = \operatorname{rk}\left(\begin{array}{ccc|c} — & \alpha_1 & — & a_1 \\ & \vdots & & \vdots \\ — & \alpha_k & — & a_k \end{array}\right). \tag{2.9}$$

Ora, se H_0 è dato dall'equazione $\langle \alpha, x \rangle = a$, il fatto che $\operatorname{rk}(\mathcal{A}) = \operatorname{rk}(\mathcal{A}') + 1$ implica che $\{\alpha_1, \dots, \alpha_k, \alpha\}$ è un insieme di vettori linearmente indipendenti per ogni scelta di $\alpha_1, \dots, \alpha_k$, quindi $t'' := t' \cap H_0 \in L(\mathcal{A}'')$ è non vuoto, in quanto il sistema che lo definisce verifica

$$\operatorname{rk}\begin{pmatrix} — & \alpha_1 & — \\ & \vdots & \\ — & \alpha_k & — \\ — & \alpha & — \end{pmatrix} = \operatorname{rk}\left(\begin{array}{ccc|c} — & \alpha_1 & — & a_1 \\ & \vdots & & \vdots \\ — & \alpha_k & — & a_k \\ — & \alpha & — & a \end{array}\right)$$

perché in entrambi i casi il rango è aumentato di 1 rispetto all'Equazione (2.9). Viceversa, se $t'' \in L(\mathcal{A}'')$ è dato da $H_1 \cap \cdots \cap H_k \cap H_0$, allora $t' := H_1 \cap \cdots \cap H_k$ è non vuoto ed è un elemento di $L(\mathcal{A}')$. □

[23] I primi due sono sottospazi vettoriali di $\mathbb{R}^n$, il terzo di H_0.

[24] $W_{\mathcal{A}'}$ contiene α_{H_0} e per definizione di vettore normale $H_0 + \langle \alpha_{H_0} \rangle = \mathbb{R}^n$.

Come esempio di applicazione del teorema precedente, ci chiediamo: in quante parti si può tagliare al massimo una torta con m tagli rettilinei? In altre parole, qual è il massimo numero di regioni in cui resta diviso il piano $\mathbb{R}^2$ da un arrangiamento di rette di cardinalità m?

Definizione 2.64. Un arrangiamento $\mathcal{A}$ in $\mathbb{K}^n$ è *in posizione generica* se per ogni scelta di p iperpiani $\{H_1, \dots, H_p\} \subseteq \mathcal{A}$ si ha

$$\begin{cases} \dim(H_1 \cap \cdots \cap H_p) = n - p & \text{se } p \leqslant n \\ H_1 \cap \cdots \cap H_p = \varnothing & \text{se } p > n. \end{cases}$$

Ad esempio, nel piano un arrangiamento di rette è in posizione generica se e solo se non ci sono due rette parallele né tre rette che si intersecano in un punto solo.

Nell'Appendice A si dimostra che il massimo numero di regioni si ha per arrangiamenti in posizione generica.

Proposizione 2.65. *Se $\mathcal{A}$ è un arrangiamento in posizione generica in $\mathbb{K}^n$ con $\#(\mathcal{A}) = m$, allora*

$$\chi_{\mathcal{A}}(X) = X^n - mX^{n-1} + \binom{m}{2} X^{n-2} - \cdots + (-1)^n \binom{m}{n}.$$

In particolare, se $\mathbb{K} = \mathbb{R}$,

$$\begin{aligned} \#(\mathcal{R}(\mathcal{A})) &= 1 + m + \binom{m}{2} + \cdots + \binom{m}{n}, \\ \#(\mathcal{B}(\mathcal{A})) &= (-1)^n \left(1 - m + \binom{m}{2} - \cdots + (-1)^n \binom{m}{n}\right) = \binom{m-1}{n}. \end{aligned}$$

Osserviamo che, in base a quanto dice il Teorema 2.63, la seconda formula dovrebbe essere

$$\#(\mathcal{B}(\mathcal{A})) = (-1)^{\mathrm{rk}(\mathcal{A})} \left(1 - m + \binom{m}{2} - \cdots + (-1)^n \binom{m}{n}\right). \tag{2.10}$$

Notiamo però che, se $\mathcal{A}$ è un arrangiamento di m iperpiani in uno spazio di dimensione n in posizione generica, allora $\mathcal{A}$ è essenziale se e solo se $m \geqslant n$: infatti se $\mathcal{A} = \{H_1, \dots, H_m\}$ è essenziale e supponendo per assurdo $m < n$, si ha $\mathrm{rk}(\mathcal{A}) = n - \dim(H_1 \cap \cdots \cap H_m) = n - (n - m) = m$ in contraddizione con l'essenzialità di $\mathcal{A}$ ($\mathrm{rk}(\mathcal{A}) = n$); d'altra parte se $m \geqslant n$ distinguiamo due casi:

1. se $m = n$, concludiamo direttamente con $\mathrm{rk}(\mathcal{A}) = n - \dim(H_1 \cap \cdots \cap H_m) = n - (n - m) = m = n$;

2. se $m > n$, scegliamo n iperpiani $H_{i_1}, \dots, H_{i_n}$ e osserviamo che $\operatorname{rk}(\mathcal{A}) \geqslant n - \dim(H_{i_1} \cap \cdots \cap H_{i_n}) = n$.

Quindi

- se $\mathcal{A}$ è essenziale, allora $\operatorname{rk}(\mathcal{A}) = n$ e ritroviamo l'enunciato della Proposizione 2.65;
- se $\mathcal{A}$ non è essenziale, allora dalla posizione generica discende che per un qualsiasi $\mathcal{A}' = \mathcal{A} \smallsetminus \{H_0\}$ vale che

$$\begin{aligned}\operatorname{rk}(\mathcal{A}') &= n - \dim\left(\bigcap_{H \in \mathcal{A}'} H\right) = \\ &= n - \left(1 + \dim\left(H_0 \cap \bigcap_{H \in \mathcal{A}'} H\right)\right) = \operatorname{rk}(\mathcal{A}) - 1,\end{aligned}$$

  dunque $\#(\mathcal{B}(\mathcal{A})) = 0$ e anche l'espressione a destra nell'Equazione (2.10) è nulla, quindi la formula resta valida.

Dimostrazione della Proposizione 2.65. Ogni $\Gamma \subseteq \mathcal{A}$ con $\#(\Gamma) \leqslant n$ definisce un elemento di $L(\mathcal{A})$, precisamente $\bigcap_{H \in \Gamma} H$. Dunque si ha

$$L(\mathcal{A}) \simeq \{S \subseteq \{1, \dots, m\} \mid \#(S) \leqslant n\},$$

che è un poset ordinato per inclusione (è la cosiddetta *algebra booleana troncata*) di cui sappiamo calcolare la funzione di Möbius: infatti per un qualsiasi elemento $t \in L(\mathcal{A})$ con $\operatorname{codim}(t) = k$, abbiamo che $[0, t] \simeq B_k$ (algebra booleana standard), dunque $\mu(0, t) = (-1)^k$. Per definizione di polinomio caratteristico

$$\chi_{\mathcal{A}}(X) = \sum_{\substack{S \subseteq \{1, \dots, m\} \\ \#(S) \leqslant n}} (-1)^{\#(S)} X^{n - \#(S)}.$$

La tesi segue facilmente dal fatto che il coefficiente di X^{n-k} è il numero di sottoinsiemi di cardinalità k (moltiplicato per $(-1)^k$). □

2.6.3 Combinatoria "quantizzata"

Sia $\mathcal{A}$ un arrangiamento di iperpiani in $\mathbb{Q}^n$. Possiamo scrivere le equazioni che li definiscono usando coefficienti di $\mathbb{Z}$ (dopo aver raccolto opportuni GCD), anzi possiamo anche supporre che tali coefficienti siano primi tra loro.

L'idea è leggere i coefficienti modulo un primo p. In questo modo essi possono essere interpretati come elementi di un campo finito di caratteristica

p, diciamo $\mathbb{F}_q$ ($q = p^r$). Chiameremo $\mathcal{A}_q$ l'arrangiamento in $(\mathbb{F}_q)^n$ ottenuto riducendo i coefficienti modulo p. Il problema è che non sempre si può ridurre impunemente.

Esempio 2.12. Consideriamo l'arrangiamento 1-dimensionale $\mathcal{A} = \{\{0\}, \{2\}\}$ definito dalle equazioni $X = 0$ e $X = 2$. In questo caso ridurre modulo 2 porta a $\mathcal{A}_2 = \{\{0\}\}$. In particolare $L(\mathcal{A})$ e $L(\mathcal{A}_2)$ non solo sono diversi, ma non possono essere neppure isomorfi (il primo ha tre elementi, il secondo due).

Definizione 2.66. Un arrangiamento $\mathcal{A}$ definito su $\mathbb{Z}$ ha una *buona riduzione modulo* p se $L(\mathcal{A}_q) \simeq L(\mathcal{A})$.

Proposizione 2.67. *Un arrangiamento $\mathcal{A}$ ha una buona riduzione modulo p per ogni primo p, tranne al più un numero finito.*

Dimostrazione. Supponiamo di avere $H_1, \dots, H_j$ iperpiani definiti dalle equazioni $\langle \boldsymbol{\alpha}_i, \mathbf{x} \rangle = a_i$ per ogni $i = 1, \dots, j$. Sappiamo che $H_1 \cap \cdots \cap H_j \neq \varnothing$ se e solo se

$$\operatorname{rk} \left(\begin{array}{ccc|c} — & \boldsymbol{\alpha}_1 & — & a_1 \\ & \vdots & & \vdots \\ — & \boldsymbol{\alpha}_j & — & a_j \end{array}\right) = \operatorname{rk} \begin{pmatrix} — & \boldsymbol{\alpha}_1 & — \\ & \vdots & \\ — & \boldsymbol{\alpha}_j & — \end{pmatrix}.$$

Quindi non si ha una buona riduzione modulo p quando esiste una matrice A (data dai vettori normali) che abbia rango diverso dalla matrice completa, se letta modulo p. Supponendo che $\operatorname{rk}(A) = k$, questo si può verificare se tutti i minori $k \times k$ di A hanno determinante nullo modulo p (cioè p divide il loro GCD). Ma ora le matrici A date dai vettori normali sono in numero finito e ciascuna ha un numero finito di minori; quindi i primi p per cui si abbia cattiva riduzione possono essere scelti solamente in un insieme finito di primi. □

Teorema 2.68. *Sia $\mathcal{A}$ un arrangiamento a coefficienti in $\mathbb{Z}$ di dimensione n e sia $q = p^r$, con p primo, tale che $L(\mathcal{A}) \simeq L(\mathcal{A}_q)$. Allora*

$$\chi_{\mathcal{A}}(q) = \#\left((\mathbb{F}_q)^n \setminus \bigcup_{H \in \mathcal{A}_q} H\right) = q^n - \#\left(\bigcup_{H \in \mathcal{A}_q} H\right).$$

Dimostrazione. Sia $t \in L(\mathcal{A}_q)$. Dato che t è un sottospazio (affine) di $(\mathbb{F}_q)^n$, vale che $\#(t) = q^{\dim t}$.

Useremo una strategia simile a quella per la dimostrazione del principio di inclusione/esclusione generalizzato. Per $t \in L(\mathcal{A})$, siano $f(t) := \#(t)$ e

$$g(t) := \#\left(t \setminus \bigcup_{u > t} u\right).$$

Osserviamo che

$$f(t) = \sum_{u \geqslant t} g(u),$$

dunque per la Formula duale di inversione di Möbius (Teorema 2.23*)

$$g(t) = \sum_{u \geqslant t} \mu(t,u) f(u) = \sum_{u \geqslant t} \mu(t,u) q^{\dim u}.$$

In particolare, per $t = 0$ (cioè $t = (\mathbb{F}_q)^n$) si ha

$$g(0) = \sum_{u \geqslant 0} \mu(0,u) q^{\dim u} = \chi_{\mathcal{A}}(q)$$

e d'altra parte per definizione di g

$$g(0) = \#\left((\mathbb{F}_q)^n \smallsetminus \bigcup_{u>0} u \right),$$

ma $\bigcup_{u>0} u$ è l'insieme dei punti di $(\mathbb{F}_q)^n$ che appartengono a un qualche iperpiano $H \in \mathcal{A}_q$. La tesi è così dimostrata. □

Esempio 2.13 (Arrangiamento delle trecce). Definiamo $\mathcal{B}r_n$ come l'arrangiamento in $\mathbb{Q}^n$ di rango $n-1$ i cui iperpiani sono dati da $H_{ij} := \{x \in \mathbb{Q}^n \mid x_i - x_j = 0\}$ per ogni $i < j$. (Notiamo che ha rango $n-1$ perché lo spazio $\langle (1,\dots,1) \rangle$ è contenuto in ogni iperpiano di $\mathcal{B}r_n$.) Chi è $\chi_{\mathcal{B}r_n}$?

Per definizione, un punto $x \in \mathbb{Q}^n$ appartiene all'iperpiano H_{ij} se e solo se $x_i = x_j$. Quindi i punti che non stanno in nessun iperpiano sono quelli con tutte le coordinate diverse tra loro. Alla luce del teorema precedente,

$$\chi_{\mathcal{B}r_n}(q) = \#\{(x_1,\dots,x_n) \in (\mathbb{F}_q)^n \mid x_i \neq x_j \ \forall i \neq j\}.$$

Il numero di elementi di questo insieme si conta facilmente: abbiamo q scelte per la prima coordinata, $q-1$ per la seconda e così via fino a $q-n+1$ per l'ultima. Dunque

$$\chi_{\mathcal{B}r_n}(q) = q(q-1)\cdots(q-n+1).$$

Questo vale per infiniti valori di q per la Proposizione 2.67, o in altri termini il polinomio

$$\chi_{\mathcal{B}r_n}(X) - X(X-1)\cdots(X-n+1)$$

ha infinite radici, quindi dev'essere il polinomio nullo. Possiamo allora concludere che

$$\chi_{\mathcal{B}r_n}(X) = X(X-1)\cdots(X-n+1).$$

2.6.4 Arrangiamenti e grafi

Abbiamo già visto qualcosa sui grafi nel Capitolo 1. In quest'ultima sezione esploreremo un legame (che avevamo anticipato dopo aver definito il polinomio caratteristico) tra gli arrangiamenti di iperpiani e i grafi.

Definizione 2.69. Un *grafo semplice non orientato finito*[25] è una coppia ordinata $G = (V, E)$ di insiemi (V è detto *insieme dei vertici*, E *insieme degli archi*) tali che

1. V è finito;
2. E è costituito da sottoinsiemi di V di cardinalità esattamente 2.

È possibile associare un arrangiamento a un grafo G. Supponiamo che $V = \{1, \dots, n\}$ e definiamo l'arrangiamento $\mathcal{A}(G)$ in $\mathbb{K}^n$ come

$$\mathcal{A}(G) := \{\ker(x_i - x_j) \mid \{i, j\} \in E\}.$$

Nella scrittura precedente abbiamo usato l'espressione "$\ker(x_i - x_j)$" considerando x_i e x_j come appartenenti al duale $(\mathbb{K}^n)^*$ (cioè x_i è la proiezione sull'i-esima coordinata). È solo un altro modo, magari un po' contorto ma più compatto, per dire $\{\mathbf{x} \in \mathbb{K}^n \mid x_i - x_j = 0\}$.

Ad esempio, se G è il grafo completo su n vertici (cioè per ogni $i \neq j$ si ha $\{i, j\} \in E$), allora $\mathcal{A}(G) = \mathcal{B}r_n$.

Definizione 2.70. Sia C un insieme finito, che chiameremo *insieme dei colori*. Sia inoltre $G = (V, E)$ un grafo. Una *colorazione* di G tramite C è una mappa $\varphi\colon V \to C$ tale che $\varphi(i) \neq \varphi(j)$ se $\{i, j\} \in E$.

Definizione 2.71 (Birkhoff, 1913)**.** Sia G un grafo. La sua *funzione cromatica* è definita come

$$\chi(G; t) := \#\{\text{colorazioni di } G \text{ usando } t \text{ colori}\}.$$

Ad esempio, in termini della funzione cromatica il famoso Teorema dei Quattro colori può essere riformulato come segue: "Sia G un grafo planare.[26] Allora $\chi(G; 4) > 0$."

Esempio 2.14. Sia G il grafo su ℓ vertici privo di archi. Possiamo colorare i vertici arbitrariamente, quindi $\chi(G; t) = t^\ell$.

[25] Nel resto della sezione diremo semplicemente "grafo" per indicare un grafo semplice non orientato finito, se non diversamente specificato.

[26] Non definiremo qui il termine "planare", questa è solo una nota di colore...

Esempio 2.15. Torniamo al grafo completo su n vertici. Possiamo calcolare la sua funzione cromatica facilmente: abbiamo t colori tra cui scegliere per il primo vertice, $t-1$ per il secondo e così via, da cui

$$\chi(G;t) = t(t-1)\cdots(t-n+1).$$

Un momento, dove abbiamo già visto quest'espressione? In effetti è la stessa del polinomio caratteristico dell'arrangiamento delle trecce $\mathcal{B}r_n$. D'altra parte $\mathcal{B}r_n$ è proprio $\mathcal{A}(G)$: i due fatti devono essere collegati in qualche modo...

Definizione 2.72. Siano $G = (V, E)$ un grafo e $\{i,j\} \in E$ un suo arco. Definiamo un nuovo grafo $G' := (V', E')$ dove

- $V' = V$;
- $E' = E \setminus \{\{i,j\}\}$, cioè G' ha gli stessi archi di G tranne $\{i,j\}$.

Il grafo G' è ottenuto *per cancellazione dell'arco* $\{i,j\}$ da G.

Definizione 2.73. Siano $G = (V, E)$ un grafo e $\{i,j\} \in E$ un suo arco. Definiamo un nuovo grafo $G'' := (V'', E'')$ dove

- $V'' := (V \setminus \{i,j\}) \cup \{(ij)\}$, dove (ij) è un nuovo vertice (in particolare $\#(V'') = \#(V) - 1$);
- E'' contiene tutti gli archi di E che non coinvolgono né i né j e contiene l'arco $\{(ij), k\}$ se e solo se $\{i,k\} \in E$ oppure $\{j,k\} \in E$.

Il grafo G'' è ottenuto *per contrazione dell'arco* $\{i,j\}$ da G.

Teorema 2.74. *Siano G un grafo e G', G'' i grafi ottenuti da G rispettivamente per cancellazione e contrazione di un arco fissato. Allora*

$$\chi(G';t) = \chi(G;t) + \chi(G'';t).$$

Dimostrazione. Ogni colorazione φ di G può essere applicata ai vertici di G' (che sono gli stessi) e rimane una colorazione, poiché $E' \subset E$. Quindi abbiamo una mappa iniettiva tra le colorazioni di G e quelle di G'.

Quali sono le colorazioni di G' che non abbiamo contato? Per costruzione di G', se $\{i,j\}$ è l'arco eliminato, le uniche colorazioni aggiuntive di G' sono le φ tali che $\varphi(i) = \varphi(j)$ (che sono lecite in G' ma non in G). Ma queste sono proprio le colorazioni di G'', dal momento che in G'' i vertici i e j sono identificati. In particolare, in G' ai vertici i e j è assegnato il colore $\varphi((ij))$. □

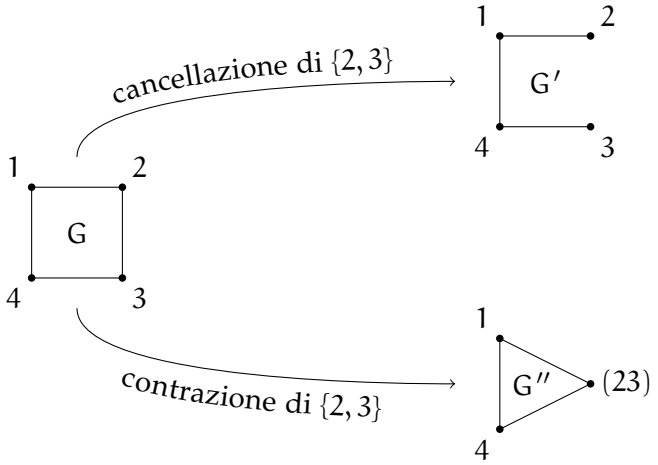


Figura 2.22: Esempio di cancellazione e contrazione di un arco.

Corollario 2.75. *La funzione* $\chi(G;t)$ *è un polinomio in* t *(e d'ora in avanti lo chiameremo* polinomio cromatico*), monico di grado* $\#(V)$*.*

Dimostrazione. Sia $\ell := \#(V)$ e procediamo per induzione sul numero di archi di G.

$\boxed{\#(E) = 0}$ Abbiamo visto nell'Esempio 2.14 che la funzione cromatica del grafo senza archi è t^ℓ.

$\boxed{\#(E) > 0}$ Sia $\{i,j\} \in E$ e consideriamo i grafi G' e G'' ottenuti rispettivamente per cancellazione e contrazione di $\{i,j\}$ da G. Dal Teorema 2.74 abbiamo che

$$\chi(G;t) = \chi(G';t) - \chi(G'';t).$$

Dato che sia G' che G'' hanno meno archi di G, possiamo applicare l'ipotesi induttiva e dedurre che $\chi(G';t)$ è un polinomio in t il cui *leading term* è t^ℓ, mentre $\chi(G'';t)$ è un polinomio in t il cui *leading term* è $t^{\ell-1}$. In particolare $\chi(G;t)$ è un polinomio e il *leading term* di $\chi(G'';t)$ non può cancellare quello di $\chi(G';t)$ perché ha grado inferiore. □

Proposizione 2.76. *Sia* G *un grafo su* ℓ *vertici con almeno un arco* e_0*. Siano* G' *e* G'' *i grafi ottenuti per cancellazione e contrazione di* e_0*. Sia* H_0 *l'iperpiano di* $\mathcal{A}(G)$ *corrispondente a* e_0*. Allora* $\mathcal{A}(G)' = \mathcal{A}(G')$ *e* $\mathcal{A}(G)'' = \mathcal{A}(G'')$*.*

Dimostrazione. Per definizione

$$\mathcal{A}(G') = \{\ker(x_i - x_j) \mid \{i,j\} \in E \smallsetminus \{e_0\}\}$$
$$\mathcal{A}(G)' = \{\ker(x_i - x_j) \mid \{i,j\} \in E\} \smallsetminus \{H_0\}$$

e i due insiemi sono uguali.

Per quanto riguarda la seconda uguaglianza, occorre prestare un minimo di attenzione in più, in quanto $\mathcal{A}(G)''$ e $\mathcal{A}(G'')$ vivono in ambienti diversi (il primo in H_0, il secondo in un $\mathbb{K}^{\ell-1}$ astratto). Possiamo supporre senza perdita di generalità che $e_0 = \{1, 2\}$ e $H_0 = \{x \in \mathbb{K}^\ell \mid x_1 = x_2\}$. H_0 è isomorfo a $\mathbb{K}^{\ell-1}$ ad esempio tramite la mappa

$$\begin{array}{rccc} \psi: & H_0 & \longrightarrow & \mathbb{K}^{\ell-1} \\ & (x_1, \dots, x_\ell) & \longmapsto & (x_2, \dots, x_\ell) \end{array}$$

in cui su H_0 ci sono le coordinate dello spazio ambiente $\mathbb{K}^\ell$. Vogliamo mostrare che ψ induce un isomorfismo tra gli arrangiamenti $\mathcal{A}(G)''$ e $\mathcal{A}(G'')$.[27] Sia $H_{ij} := \ker(x_i - x_j) \in \mathcal{A}(G)$ diverso da H_0 e consideriamo $H_{ij} \cap H_0 \in \mathcal{A}(G)''$.

1. Se sia i che j sono diversi da 1 e 2, allora $\psi(H_{ij} \cap H_0) = \ker(x_i - x_j)$ in $\mathbb{K}^{\ell-1}$, che è un elemento di $\mathcal{A}(G'')$.

2. Se uno solo tra i e j è diverso da 1 e 2 (supponiamo che sia i), allora $\psi(H_{i1} \cap H_0) = \psi(H_{i2} \cap H_0)$ perché entrambi uguali a $\ker(x_i - x_2)$ in $\mathbb{K}^{\ell-1}$.

La mappa inversa è naturalmente quella che associa a un iperpiano $\ker(x_i - x_j) \subseteq \mathbb{K}^{\ell-1}$ l'iperpiano $\ker(x_i - x_j) \cap H_0$ (stavolta x_i e x_j sono coordinate di $\mathbb{K}^\ell$). □

Teorema 2.77. *Per un grafo* G *vale* $\chi_{\mathcal{A}(G)}(t) = \chi(G; t)$.

Dimostrazione. Per induzione sul numero di archi di G.
$\boxed{\#(E) = 0}$ Se G è il grafo senza archi, allora $\mathcal{A}(G) = \varnothing$ e in entrambi i casi il polinomio è t^ℓ.
$\boxed{\#(E) > 0}$ Applicando, in ordine, il Teorema 2.74, l'ipotesi induttiva, la Proposizione 2.76 e il Teorema 2.59 si ottiene

$$\begin{aligned} \chi(G; t) &= \chi(G'; t) - \chi(G''; t) = \\ &= \chi_{\mathcal{A}(G')}(t) - \chi_{\mathcal{A}(G'')}(t) = \\ &= \chi_{\mathcal{A}(G)'}(t) - \chi_{\mathcal{A}(G)''}(t) = \chi_{\mathcal{A}(G)}(t). \end{aligned}$$ □

A prima vista si direbbe che il teorema precedente sia solo una traduzione tra il linguaggio degli arrangiamenti di iperpiani e quello dei grafi; in fondo, i due polinomi sono stati definiti in contesti diversi. Vediamo per concludere un'applicazione più profonda.

[27] Diciamo che due arrangiamenti $\mathcal{A}$ e $\mathcal{B}$, che vivono rispettivamente negli spazi V e W, sono isomorfi se esiste un isomorfismo lineare $f: V \to W$ che mappa gli iperpiani di $\mathcal{A}$ negli iperpiani di $\mathcal{B}$.

Definizione 2.78. Sia G un grafo. Un'*orientazione* di G è un assegnamento[28] $i \to j$ oppure $j \to i$ ad ogni arco $\{i, j\}$. Un *ciclo orientato* è un insieme di vertici $\{v_1, \dots, v_k\} \subseteq V$ per cui esistono gli archi $v_1 \to v_2, v_2 \to v_3, \dots, v_{k-1} \to v_k, v_k \to v_1$. Un'orientazione è detta *aciclica* se non ha cicli orientati.

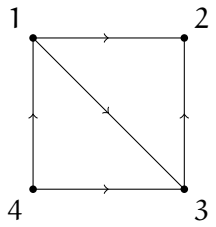


Figura 2.23: Esempio di orientazione aciclica.

Teorema 2.79. *Sia $\mathcal{AO}(G)$ l'insieme di tutte le orientazioni acicliche su G (dall'inglese* acyclic orientation*). Esiste una corrispondenza biunivoca tra $\mathcal{AO}(G)$ e l'insieme delle regioni $\mathcal{R}(\mathcal{A}(G))$ (l'arrangiamento è costruito in $\mathbb{R}^\ell$).*

Dimostrazione. Sia ω un'orientazione aciclica. Chiamiamo $G = (\{1, \dots, \ell\}, E)$ e sia $p_i(\omega)$ il numero di vertici raggiungibili da i seguendo l'orientazione, cioè il numero di vertici j per cui esistono $v_1, \dots, v_k$ tali che $v_1 = i$, $v_k = j$ e ci sono gli archi $v_1 \to v_2, v_2 \to v_3, \dots, v_{k-1} \to v_k$; conveniamo che $p_i(\omega) \geqslant 1$ perché includiamo i stesso tra i vertici raggiungibili (stando fermi). Ad esempio, nel grafo della Figura 2.23 $p_1(\omega) = 3$ e $p_4(\omega) = 4$. Definiamo inoltre il vettore

$$\mathbf{p}(\omega) := (p_1(\omega), \dots, p_\ell(\omega)) \in \mathbb{R}^\ell.$$

Osserviamo che se esiste l'arco $i \to j$, allora $p_i(\omega) > p_j(\omega)$, perché tutti i vertici raggiungibili da j lo sono anche da i, mentre i non è raggiungibile da j per aciclicità. È vero anche il viceversa, poiché se $\{i, j\}$ è un arco allora l'orientazione deve assegnargli uno tra $i \to j$ e $j \to i$.

Sia H_{ij} l'iperpiano definito da $x_i - x_j = 0$ e H_{ij}^+ il semispazio $x_i - x_j > 0$. Per quanto visto sopra l'arco $\{i, j\}$ è orientato $i \to j$ se e solo se $p_i(\omega) > p_j(\omega)$ e questo può avvenire se e solo se $\mathbf{p}(\omega) \in H_{ij}^+$. Dunque al variare di i, j scopriamo che $\mathbf{p}(\omega)$ non può stare su nessun iperpiano di $\mathcal{A}(G)$: deve appartenere a una qualche regione.

Resta solo da mostrare che la mappa $\mathcal{AO}(G) \to \mathcal{R}(\mathcal{A}(G))$ che associa a ω la regione a cui appartiene $\mathbf{p}(\omega)$ è biiettiva.

[28] Non ci soffermeremo su come questo assegnamento sia effettivamente realizzato (ad esempio, ridefinire l'insieme degli archi come insieme di coppie ordinate).

- La mappa è iniettiva perché se η è un'orientazione diversa da ω allora esiste almeno un arco diversamente orientato; supponendo che ω assegni $i \to j$ mentre η dia $j \to i$, abbiamo che $\mathbf{p}(\omega)$ e $\mathbf{p}(\eta)$ giacciono da parti diverse rispetto a H_{ij}, quindi appartengono a regioni diverse.
- Sia $(p_1, \ldots, p_\ell)$ un punto in una qualsiasi regione. Per ogni coppia $\{i, j\}$ si ha $p_i \neq p_j$, quindi possiamo definire un'orientazione ω che assegni $i \to j$ se $p_i > p_j$ e $j \to i$ in caso contrario. Questo prova la suriettività della mappa. □

Corollario 2.80 (Stanley, 1973)**.** *Il numero di orientazioni acicliche di un grafo è* $(-1)^{\#(V)}\chi(G; -1)$.

In altre parole, scopriamo che il polinomio cromatico di un grafo, che era stato definito per contare il numero di possibili colorazioni, contiene al suo interno le informazioni per contare anche il numero di orientazioni acicliche definibili sul grafo.

Capitolo 3

Teoria di Pólya-Redfield

Iniziamo con un esempio. Supponiamo di avere una griglia di 2×2 caselle e di volerla colorare con i colori bianco e nero. Chiaramente il numero totale di possibili colorazioni è $2^4 = 16$. Ma cosa succede se al posto di una griglia astratta avessimo una scacchiera delle medesime dimensioni? Scopriamo che in realtà abbiamo solo *sei* modi diversi per colorarla, che sono visualizzati in Figura 3.1. Questo perché una scacchiera è un oggetto fisico dello spazio e può essere *ruotata*: in effetti ciascuna delle 16 colorazioni si ottiene a partire da uno dei sei "modelli" tramite rotazione. In questo capitolo vedremo come si possono contare oggetti a meno di opportune relazioni di equivalenza. ▷ *20/04/2015*

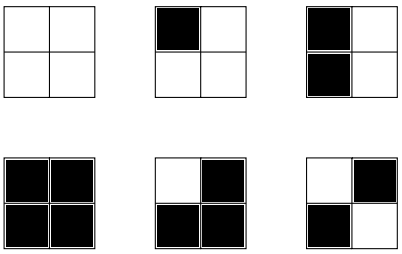


Figura 3.1: I sei modi possibili di colorare in bianco/nero una scacchiera 2×2 a meno di rotazioni.

3.1 Il Teorema di Pólya-Redfield

Proviamo a formalizzare il tutto. Siano D un insieme finito di "oggetti" e C un insieme finito di "colori". Consideriamo l'insieme $C^D := \{f\colon D \to C\}$ (colorazioni di D tramite C). Sia G un gruppo finito che agisce su D. Mettiamo su C^D la

relazione di equivalenza

$$f \sim g \quad \text{se e solo se} \quad \exists\, \sigma \in G \text{ tale che } \forall\, x \in D\ f(\sigma(x)) = g(x). \tag{3.1}$$

Un *modello* per una $f \in C^D$ è la sua classe di equivalenza.

Nell'esempio precedente, $D = \{\text{caselle della scacchiera}\}$, $C = \{\text{nero, bianco}\}$ e G è il gruppo delle rotazioni di $0°$, $90°$, $180°$ e $270°$.

Definizione 3.1. Sia A un dominio di integrità. Una *funzione peso* per C è una mappa $w\colon C \to A$.

Normalmente si prende come A l'anello dei polinomi in $\#(C)$ variabili e per ogni $c_i \in C$ si definisce $w(c_i) = X_i$.

La funzione peso si estende a C^D ponendo

$$w(f) := \prod_{d \in D} w(f(d)).$$

Esempio 3.1. Per $C = \{\text{nero, bianco}\}$ scegliamo $A = \mathbb{K}[X, Y]$ e definiamo $w(\text{nero}) = X$ e $w(\text{bianco}) = Y$. Una colorazione con tre caselle bianche e una nera avrà peso XY^3.

Osserviamo che banalmente se $f \sim g$, allora $w(f) = w(g)$; è dunque ben definito il peso di un modello come peso comune di ogni elemento della classe di equivalenza.

Definizione 3.2. L'*enumeratore* di C[1] è definito come

$$g(C) := \sum_{y \in C} w(y) \in A.$$

Osservazione. Scegliendo $A = \mathbb{K}[\![T]\!]$, potremmo anche prendere insiemi di colori C infiniti: assegnando a un colore c_i il peso T^i, otteniamo $g(C) := \sum k_i T^i$, dove k_i è il numero di colori di peso T^i. Se si vuole, è una sorta di funzione generatrice per i colori.

Lemma 3.3. *Vale che* $g(C^D) = g(C)^{\#(D)}$.

Dimostrazione. Procediamo per induzione su $n = \#(D)$.
$\boxed{n = 1}$ Se $D = \{*\}$, ovviamente c'è una corrispondenza biunivoca tra C e l'insieme $C^D = \{f\colon \{*\} \to C\}$ rispetto alla quale si ha $w(f) = w(c)$ se $f(*) = c$. Dunque

$$g(C^D) = \sum_{f \in C^D} w(f) = \sum_{c \in C} w(c) = g(C).$$

[1] Qui C non è necessariamente l'insieme dei colori: può essere un qualsiasi insieme (finito) su cui è definita una funzione peso.

$\boxed{n \Rightarrow n+1}$ Scriviamo $D = D_0 \cup \{d\}$ e iniziamo a calcolare:

$$g(C^D) = \sum_{f \in C^D} \prod_{x \in D} w(f(x)) =$$
$$= \sum_{f \in C^D} w(f(d)) \prod_{x \in D_0} w(f(x)) = (\star)$$

Raccogliamo gli addendi a seconda del valore $f(d)$:

$$(\star) = \sum_{y \in C} \sum_{\substack{f \in C^D \\ f(d)=y}} w(y) \prod_{x \in D_0} w(f(x)) =$$
$$= \sum_{y \in C} w(y) \sum_{\substack{f \in C^D \\ f(d)=y}} \prod_{x \in D_0} w(f(x)) = (\star\star)$$

Ora notiamo che c'è corrispondenza biunivoca tra $\{f \in C^D \mid f(d) = y\}$ e C^{D_0} e che nella produttoria contano solo i valori assunti da f su D_0; quindi possiamo applicare l'ipotesi induttiva scrivendo

$$(\star\star) = \sum_{y \in C} w(y) \sum_{f \in C^{D_0}} \prod_{x \in D_0} w(f(x)) =$$
$$= g(C) g(C)^{\#(D_0)} = g(C)^{\#(D)}. \qquad \square$$

Lemma 3.4. *Sia* $\{X_1, \ldots, X_r\}$ *una partizione di* D *e sia*

$$Q := \{f \colon D \to C \mid f \text{ } \textit{è costante su ciascuno degli } X_i\}.$$

Allora

$$g(Q) = \prod_{i=1}^{r} \sum_{y \in C} w(y)^{\#(X_i)}.$$

Dimostrazione. Iniziamo dal caso in cui si abbia la partizione banale con $r = 1$ e $X_1 = D$. Vogliamo calcolare l'enumeratore dell'insieme delle funzioni costanti su tutto D, che indicheremo con Q_D. Ora, dalla definizione di enumeratore è ovvio che, se $\{Y_1, \ldots, Y_m\}$ è una partizione di C, allora $g(C) = g(Y_1) + \cdots + g(Y_m)$. Posto $C = \{y_1, \ldots, y_m\}$, scrivendo

$$Q_D = \{f \in Q_D \mid f(d) = y_1\} \cup \cdots \cup \{f \in Q_D \mid f(d) = y_m\}$$

ricaviamo

$$g(Q_D) = \sum_{j=1}^{m} w(y_j)^{\#(D)}$$

che è la tesi in questo caso.

Passiamo ora al caso generale. C'è un'ovvia corrispondenza biunivoca tra Q e $\prod_{i=1}^{r} Q_{X_i}$ (in cui, analogamente a sopra, Q_{X_i} indica l'insieme delle funzioni costanti definite su X_i), che associa a una $f \in Q$ l'r-upla $(f_1, \dots, f_r)$ dove $f_i := f|_{X_i}$. Dalla definizione di peso è chiaro che

$$w(f) = \prod_{i=1}^{r} w(f_i).$$

Dunque

$$\begin{aligned} g(Q) = \sum_{f \in Q} w(f) &= \sum_{(f_1,\dots,f_r) \in \prod Q_{X_i}} w(f_1) \cdots w(f_r) = \\ &= \left(\sum_{f_1 \in Q_{X_1}} w(f_1) \right) \cdots \left(\sum_{f_r \in Q_{X_r}} w(f_r) \right) = \\ &= g(Q_{X_1}) \cdots g(Q_{X_r}) = \prod_{i=1}^{r} \sum_{j=1}^{m} w(y_j)^{\#(X_i)}. \end{aligned}$$ □

Esempio 3.2. Prendiamo $D = \{a, b, c, d, e, f, g\}$ partizionato in $\{a, b, c\}$, $\{d, e\}$, $\{f\}$ e $\{g\}$. Ad esempio, D potrebbe essere un insieme di sette persone e ciascun elemento della partizione una famiglia. Prendiamo poi $C = \{c_1, c_2, c_3\}$ che interpretiamo come insieme di città. È ragionevole pensare che l'intera famiglia viva nella stessa città. Se scegliamo i pesi in $\mathbb{K}[X, Y, Z]$ assegnando $w(c_1) = X$, $w(c_2) = Y$ e $w(c_3) = Z$, l'enumeratore dei possibili accoppiamenti persone-città è dato da

$$g(Q) = (X^3 + Y^3 + Z^3)(X^2 + Y^2 + Z^2)(X + Y + Z)^2.$$

Ricordiamo a questo punto un po' di terminologia sulle azioni di gruppo. Se G è un gruppo che agisce sull'insieme D con l'azione

$$\begin{array}{ccc} G \times D & \longrightarrow & D \\ (g, x) & \longmapsto & g \cdot x, \end{array}$$

si definisce *orbita* di un punto $x \in D$ l'insieme

$$\mathcal{O}rb(x) := \{g \cdot x \mid g \in G\} \subseteq D$$

e *stabilizzatore* di un punto $x \in D$ l'insieme

$$\mathcal{S}tab(x) := \{g \in G \mid g \cdot x = x\} < G.^{\blacktriangleright 2}$$

Assumiamo come noto che l'insieme delle orbite $\mathcal{O} = \{\mathcal{O}rb(x) \mid x \in D\}$ sia una partizione di D e che per ogni $x \in D$ si abbia

$$\#(\mathcal{S}tab(x)) \cdot \#(\mathcal{O}rb(x)) = \#(G). \tag{3.2}$$

Assumiamo per evitare complicazioni che l'azione di G sia *fedele*, cioè che ogni elemento di G diverso dall'identità sposti almeno un punto di D (cioè per ogni $g \in G \setminus \{e\}$ esiste $x \in D$ tale che $g \cdot x \neq x$): in questo modo G è isomorfo a un sottogruppo di permutazioni di D.[3]

Teorema 3.5 (Burnside)**.** *Sia* G *un gruppo di permutazioni di* D *e sia* $\mathcal{O}$ *l'insieme delle orbite. Supponiamo che* $\#(D) = n$ *e* $G < \mathcal{S}_n$*. Per ogni* $\sigma \in G$ *sia* $c_1(\sigma)$ *il numero di punti fissi di* σ*, cioè*

$$c_1(\sigma) := \#\{x \in D \mid \sigma \cdot x = x\}.$$

Allora

$$\#(\mathcal{O}) = \frac{1}{\#(G)} \sum_{\sigma \in G} c_1(\sigma).$$

Dimostrazione. Consideriamo l'insieme $A := \{(\sigma, a) \in G \times D \mid \sigma \cdot a = a\}$. Possiamo calcolare $\#(A)$ in due modi:

1. fissiamo σ, contiamo gli a tali che $\sigma \cdot a = a$ e sommiamo su tutte le $\sigma \in G$;
2. fissiamo a, contiamo le σ tali che $\sigma \cdot a = a$ e sommiamo su tutti gli $a \in D$.

Nel primo modo risulta

$$\#(A) = \sum_{\sigma \in G} c_1(\sigma),$$

nel secondo

$$\#(A) = \sum_{a \in D} \#(\mathcal{S}tab(a)) = (\star)$$

Ora, sia $\mathcal{O} = \{\mathcal{O}_1, \ldots, \mathcal{O}_m\}$ l'insieme delle orbite. Se a e b appartengono alla stessa orbita, cioè $\mathcal{O}rb(a) = \mathcal{O}rb(b)$, dall'Equazione (3.2) deduciamo che $\#(\mathcal{S}tab(a)) = \#(\mathcal{S}tab(b))$.[4] Dunque

$$(\star) = \sum_{i=1}^{m} \sum_{a \in \mathcal{O}_i} \#(\mathcal{S}tab(a)) = \sum_{i=1}^{m} \#(\mathcal{O}_i)\,\#(\mathcal{S}tab(a)) = (\star\star)$$

[2] La notazione $H < G$ indica che H è sottogruppo di G.

[3] D'ora in avanti diremo che G è un gruppo di permutazioni di D se G agisce fedelmente su D.

[4] Non possiamo dedurre invece che $\mathcal{S}tab(a) = \mathcal{S}tab(b)$: gli stabilizzatori sono solamente coniugati tra loro.

in cui nell'ultima uguaglianza a è un qualsiasi elemento di $\mathcal{O}_i$. Usando ancora l'Equazione (3.2) ricaviamo

$$(\star\star) = \sum_{i=1}^{m} \#(G) = m \cdot \#(G). \qquad \square$$

Esempio 3.3. Sia $G := \langle (123), (45) \rangle < \mathcal{S}_5$ che agisce sull'insieme $\{1, \ldots, 5\}$. Chiaramente $\#(G) = 6$; la Tabella 3.1 elenca il numero di punti fissi per ogni $\sigma \in G$.

σ	$c_1(\sigma)$
Id	5
(123)	2
(132)	2
(45)	3
(123)(45)	0
(132)(45)	0

Tabella 3.1: Numero di punti fissi per le $\sigma \in G$ dell'Esempio 3.3.

Quindi il numero di orbite è

$$\#(\mathcal{O}) = \frac{1}{\#(G)} \sum_{\sigma \in G} c_1(\sigma) = \frac{1}{6} 12 = 2.$$

In effetti, si vedeva quasi ad occhio che $\mathcal{O} = \{\{1, 2, 3\}, \{4, 5\}\}$.

Teorema 3.6 (Pólya-Redfield)**.** *Siano* $C = \{y_1, \ldots, y_m\}$ *l'insieme dei colori e* D *un insieme con* $\#(D) = n$*. Sia* w *una funzione peso su* C *e indichiamo con* $w_i := w(y_i)$*. Sia inoltre* G *un gruppo di permutazioni di* D *e sia* $\mathcal{M}$ *l'insieme dei modelli per* C^D *rispetto all'equivalenza data dall'azione di* G*. Allora*

$$g(\mathcal{M}) = \frac{1}{\#(G)} \sum_{\sigma \in G} \prod_{k=1}^{n} (w_1^k + \cdots + w_m^k)^{c_k(\sigma)}$$

dove $c_k(\sigma)$ *è il numero di* k*-cicli di* σ*.*[5]

Osservazione. Il peso di una $f : D \to C$ tale che $\#\{x \in D \mid f(x) = y_i\} = k_i$ è il monomio $w_1^{k_1} \cdots w_m^{k_m}$. Di conseguenza, per definizione di $g(\mathcal{M})$, il coefficiente di $w_1^{k_1} \cdots w_m^{k_m}$ è il numero di modelli rappresentati da una tale f.

[5] Coerentemente con la notazione del Teorema 3.5: $c_1(\sigma)$ è il numero di 1-cicli di σ, cioè di punti fissi di σ.

Dimostrazione del Teorema 3.6. Iniziamo definendo gli ingredienti principali di questa dimostrazione. Innanzitutto dividiamo le funzioni rispetto al loro peso: dato un peso p, consideriamo la famiglia

$$\mathcal{F}_p := \{f\colon D \to C \mid w(f) = p\}.$$

Dopodiché definiamo un'azione di G su C^D data da

$$\begin{array}{ccc} G \times C^D & \longrightarrow & C^D \\ (\sigma, f) & \longmapsto & f \circ \sigma^{-1}. \end{array}$$

Questa naturalmente dà un omomorfismo di gruppi $G \to \mathcal{S}(C^D)$, dove $\mathcal{S}(C^D)$ indica le permutazioni di C^D. Siano $\tilde{\sigma} \in \mathcal{S}(C^D)$ l'immagine di σ tramite quest'omomorfismo e $\tilde{G} := \{\tilde{\sigma} \mid \sigma \in G\}$. Osserviamo che, poiché l'azione di G su D è fedele, per ogni $\sigma \neq \mathrm{Id}$ in G esiste $x \in D$ tale che $\sigma^{-1}(x) \neq x$, quindi esiste $f \in C^D$ tale che $f(\sigma^{-1}(x)) \neq f(x)$.[6] Dunque anche l'azione di G su C^D è fedele e ne deduciamo che $\tilde{G} \simeq G$.

Per definizione, $f \sim g$ se e solo se esiste $\sigma \in G$ tale che $g = f \circ \sigma$, o equivalentemente $f = g \circ \sigma^{-1}$; in altre parole, se esiste $\tilde{\sigma} \in \tilde{G}$ tale che $f = \tilde{\sigma}(g)$. Quindi un modello di C^D corrisponde a un'orbita dell'azione di G su C^D.

Ora osserviamo che se $f \sim g$ allora $f \in \mathcal{F}_p$ se e solo se $g \in \mathcal{F}_p$: dunque un'orbita dell'azione di G su C^D è tutta contenuta in uno degli $\mathcal{F}_p$. Per calcolare $g(\mathcal{M})$, allora, sarà sufficiente contare il numero di orbite contenute in $\mathcal{F}_p$, moltiplicare tale numero per il peso p e sommare su tutti i possibili pesi.

Per il Teorema 3.5, le orbite di $\mathcal{F}_p$ rispetto all'azione di G su $\mathcal{F}_p$ sono[7]

$$\frac{1}{\#(\tilde{G})} \sum_{\tilde{\sigma} \in \tilde{G}} c_1(\tilde{\sigma}) = \frac{1}{\#(G)} \sum_{\sigma \in G} \nu_p(\sigma)$$

dove $\nu_p(\sigma) := \#\{f \in \mathcal{F}_p \mid f \circ \sigma^{-1} = f\}$ (che è uguale a $c_1(\tilde{\sigma}) = \#\{f \in \mathcal{F}_p \mid \tilde{\sigma}(f) = f\}$). Di conseguenza

$$g(\mathcal{M}) = \sum_p \left(\frac{1}{\#(G)} \sum_{\sigma \in G} \nu_p(\sigma) \right) p = \frac{1}{\#(G)} \sum_{\sigma \in G} \sum_p \nu_p(\sigma) p.$$

Ma ora vediamo che

$$\sum_p \nu_p(\sigma) p = \sum_{\{f \mid f = f \circ \sigma^{-1}\}} w(f)$$

[6] Stiamo implicitamente supponendo che $\#(C) \geqslant 2$...

[7] Nell'equazione che segue usiamo $\tilde{G}$ anziché G perché abbiamo formulato il Teorema 3.5 in termini di un sottogruppo di permutazioni. Naturalmente, dato che $G \simeq \tilde{G}$, questo è solo un formalismo.

(per definizione di peso di f: abbiamo contato quante hanno peso p, moltiplicato per p e sommato su tutti i pesi). Dunque

$$g(\mathcal{M}) = \frac{1}{\#(G)} \sum_{\sigma \in G} \sum_{\{f | f = f \circ \sigma^{-1}\}} w(f).$$

D'altra parte, abbiamo che $f = f \circ \sigma^{-1}$ se e solo se, partizionando $D = X_1 \cup \cdots \cup X_r$ tramite la struttura in cicli di σ, si ha $f|_{X_i}$ costante per ogni $i = 1, \ldots, r$. Per il Lemma 3.4

$$\sum_{\{f | f = f \circ \sigma^{-1}\}} w(f) = \prod_{i=1}^{r} \sum_{y \in C} w(y)^{\#(X_i)}.$$

Se quindi σ ha $c_1(\sigma)$ cicli di lunghezza 1, $c_2(\sigma)$ cicli di lunghezza 2, e così via fino a $c_n(\sigma)$ cicli di lunghezza n, associando il prodotto in base alla cardinalità dei cicli si ottiene

$$\sum_{\{f | f = f \circ \sigma^{-1}\}} w(f) = \prod_{k=1}^{n} \left(\sum_{y \in C} w(y)^k \right)^{c_k(\sigma)}.$$

Rimettendo insieme i pezzi si giunge alla tesi. □

Esempio 3.4. Riprendiamo l'esempio iniziale della scacchiera 2×2. L'insieme D è dato dalle 4 caselle e i colori sono {bianco, nero}. Il gruppo G che agisce è il gruppo ciclico di ordine 4 dato dalle rotazioni; visto come sottogruppo di $\mathcal{S}_4$ è dato da

$$\{\mathrm{Id}, (1234), (1234)^{-1}, (13)(24)\}.$$

Supponiamo di assegnare ai due colori i pesi X e Y. Ora,

- l'identità ha quattro cicli di lunghezza 1, quindi il suo contributo è $(X+Y)^4$;
- i due 4-cicli danno ciascuno un termine $(X^4 + Y^4)$;
- $(13)(24)$ ha due 2-cicli, quindi il suo contributo è $(X^2 + Y^2)^2$.

Di conseguenza

$$\begin{aligned} g(\mathcal{M}) &= \frac{1}{4}\left((X+Y)^4 + 2(X^4 + Y^4) + (X^2 + Y^2)^2\right) = \\ &= X^4 + X^3Y + 2X^2Y^2 + XY^3 + Y^4 \end{aligned}$$

che è proprio il risultato ottenuto a mano (il coefficiente di X^iY^j dà il numero di modelli con i caselle colorate del colore X e j colorate con Y). Ora, questo era un conto facile e sembra che la teoria ce lo abbia complicato; ma se ci chiedessimo in quanti modi si possono colorare con k colori le facce di un icosaedro regolare a meno di rotazioni?

3.2 Il polinomio indice dei cicli

Per poter applicare il Teorema 3.6 dobbiamo conoscere la decomposizione in cicli di ogni elemento di G. Introduciamo un polinomio che ci aiuti in questa direzione. ▹ *22/04/2015*

Definizione 3.7. Siano G un sottogruppo di $\mathfrak{S}_n$ e $X_1, \dots, X_n$ indeterminate. Il polinomio di $\mathbb{Q}[X_1, \dots, X_n]$ definito da

$$Z(G; X_1, \dots, X_n) := \frac{1}{\#(G)} \sum_{\sigma \in G} \prod_{k=1}^{n} X_k^{c_k(\sigma)}$$

è detto *polinomio indice dei cicli* di G.

Osserviamo che $g(\mathcal{M})$ si ottiene valutando $Z(G; X_1, \dots, X_n)$ in $X_k = w_1^k + \cdots + w_m^k$. D'altra parte, poiché il coefficiente di $w_1^{k_1} \cdots w_m^{k_m}$ in $g(\mathcal{M})$ è il numero di modelli di peso $w_1^{k_1} \cdots w_m^{k_m}$, supponendo che i w_i siano indeterminate polinomiali e valutando $g(\mathcal{M})$ per $w_i = 1$ si ottiene il numero totale di modelli. Dal fatto che

$$g(\mathcal{M}) = Z(G; w_1 + \cdots + w_m, \dots, w_1^n + \cdots + w_m^n)$$

ricaviamo

$$\#(\mathcal{M}) = Z(G; m, \dots, m).$$

Esempio 3.5. Vogliamo sapere in quanti modi è possibile colorare le facce di un cubo con due colori a meno di rotazioni.

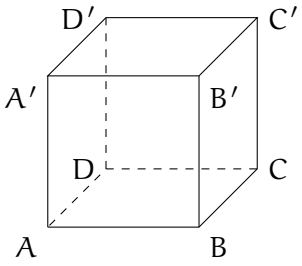


Figura 3.2: Il cubo di riferimento per l'Esempio 3.5.

Per prima cosa identifichiamo il gruppo delle rotazioni del cubo, usando la Figura 3.2 come riferimento. Sia A un vertice del cubo. Ci sono esattamente tre rotazioni che lasciano fisso A: l'identità e le due rotazioni intorno alla diagonale AC' che mandano B rispettivamente in A' e D. D'altra parte esiste almeno una rotazione che manda A in un qualsiasi altro vertice, cioè tutti i vertici sono raggiungibili da A con una rotazione. Per l'Equazione (3.2) allora

$$\#(G) = \#(\mathcal{S}tab(A)) \cdot \#(\mathcal{O}rb(A)) = 3 \cdot 8 = 24. \tag{3.3}$$

Ora osserviamo che una rotazione del cubo determina una permutazione delle quattro diagonali AC', BD', CA' e DB', quindi si ha una mappa $G \to \mathcal{S}_4$. Supponiamo che esista una rotazione σ diversa dall'identità che lasci fisse tutte le diagonali; tale rotazione scambia tra loro almeno una coppia di vertici opposti sulla stessa diagonale (se non lo facesse, sarebbe l'identità): supponiamo che scambi A e C'. Si vede facilmente che in tal caso dovrebbe scambiare tra loro anche tutte le altre coppie di vertici B e D', C e A', D e B'. Un veloce calcolo mostra che σ è un'isometria con determinante -1, che *non* è una rotazione. Ne deduciamo che la mappa $G \to \mathcal{S}_4$ è iniettiva e da (3.3) concludiamo che $G \simeq \mathcal{S}_4$.

A questo punto dobbiamo studiare la struttura in cicli di G visto come sottogruppo di $\mathcal{S}_6$, perché ci interessa l'azione di G sulle facce del cubo. La Tabella 3.2 riassume questo lavoro di classificazione.

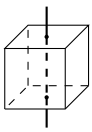
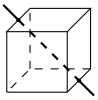
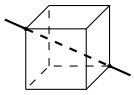
Asse di rotazione	Numero di assi nel cubo	Numero e tipo di rotazioni per asse	Monomio in Z
Identità	–	1 di tipo $(*)(*)(*)(*)(*)(*)$	X_1^6
	3	2 di tipo $(****)(*)(*)$ 1 di tipo $(**)(**)(*)(*)$	$6X_1^2X_4$ $3X_1^2X_2^2$
	6	1 di tipo $(**)(**)(**)$	$6X_2^3$
	4	2 di tipo $(***)(***)$	$8X_3^2$

Tabella 3.2: Strutture in cicli degli elementi di G, visto come sottogruppo di $\mathcal{S}_6$.

Di conseguenza, il polinomio indice dei cicli è

$$Z(G; X_1, \ldots, X_6) = \frac{1}{24}(X_1^6 + 3X_1^2X_2^2 + 6X_1^2X_4 + 6X_2^3 + 8X_3^2)$$

Assegnando per esempio i pesi $w_1 = X$ e $w_2 = Y$ ricaviamo che

$$g(\mathcal{M}) = X^6 + X^5Y + 2X^4Y^2 + 2X^3Y^3 + 2X^2Y^4 + XY^5 + Y^6$$

mentre il numero di modelli con due colori è

$$\#(\mathcal{M}) = Z(G; 2, \dots, 2) = 10.$$

Generalizzare a m colori a questo punto è immediato: il numero di modelli è

$$\#(\mathcal{M}) = Z(G; m, \dots, m) = \frac{1}{24}(m^6 + 3m^4 + 12m^3 + 8m^2).$$

Esempio 3.6. Proviamo stavolta a colorare gli spigoli di un cubo. Il gruppo G delle rotazioni non cambia, ma dobbiamo vederlo come sottogruppo di $\mathcal{S}_{12}$ e calcolare dunque $Z(G; X_1, \dots, X_{12})$. Occorre ripetere l'analisi delle strutture cicliche degli elementi di G; ad esempio, le rotazioni intorno ad un asse che passa per i punti medi di facce opposte hanno struttura $(****)(****)(****)$ e $(**)(**)(**)(**)(**)(**)$. Il risultato finale è

$$Z(G; X_1, \dots, X_{12}) = \frac{1}{24}(X_1^{12} + 3X_2^6 + 6X_4^3 + 6X_1^2X_2^5 + 8X_3^4).$$

Con due colori (diciamo bianco e nero), ci sono 218 modelli ripartiti come in Tabella 3.3, mentre con m colori il risultato è

$$\#(\mathcal{M}) = \frac{1}{24}(m^{12} + 6m^7 + 3m^6 + 8m^4 + 6m^3).$$

Spigoli neri	0	1	2	3	4	5	6	7	8	9	10	11	12
Numero modelli	1	1	5	13	27	38	48	38	27	13	5	1	1

Tabella 3.3: Numero di colorazioni degli spigoli di un cubo con i colori bianco e nero, a meno di rotazioni (#{spigoli bianchi} = 12 − #{spigoli neri}).

Proposizione 3.8. *Per* $G = \mathcal{S}_n$ *visto come sottogruppo di sé stesso si ha*

$$Z(\mathcal{S}_n; X_1, \dots, X_n) = \sum_{\mathbf{c} \in \mathcal{C}} \prod_{k=1}^{n} \frac{1}{c_k!} \left(\frac{X_k}{k}\right)^{c_k}$$

dove $\mathcal{C} := \{(c_1, \dots, c_n) \in \mathbb{N}^n \mid c_1 + 2c_2 + \cdots + nc_n = n\}$.

Dimostrazione. L'insieme $\mathcal{C}$ contiene tutte le possibili strutture cicliche degli elementi di $\mathcal{S}_n$, cioè vale che $\sigma \in \mathcal{S}_n$ ha c_k cicli di lunghezza k per ogni $k = 1, \dots, n$ se e solo se $(c_1, \dots, c_n) \in \mathcal{C}$.

Fissiamo allora una possibile scelta $(c_1, \dots, c_n) \in \mathcal{C}$ e chiediamoci: quante sono le $\sigma \in \mathcal{S}_n$ che hanno questa struttura ciclica? Scopriamo che

$$\#\{\sigma \in \mathcal{S}_n \mid \#\{\text{i-cicli di } \sigma\} = c_i\} = \frac{n!}{1^{c_1} \cdots n^{c_n} \cdot c_1! \cdots c_n!}. \tag{3.4}$$

Mostriamo come si ottiene la formula precedente. Iniziamo scegliendo gli 1-cicli: il primo può essere scelto in $\binom{n}{1}$ modi, il secondo in $\binom{n-1}{1}$ e così via fino al c_1-esimo per cui si hanno $\binom{n-c_1+1}{1}$ posibilità. L'ordine con cui compaiono questi cicli non conta, quindi occorre dividere per $c_1!$. I possibili modi per fissare gli 1-cicli sono dunque

$$\frac{n \cdot (n-1) \cdots (n-c_1+1)}{c_1!}.$$

Passiamo ai 2-cicli. Sono rimasti $n - c_1$ elementi e ne dobbiamo scegliere due: abbiamo $\binom{n-c_1}{2}$ possibilità. I successivi due possono essere scelti in $\binom{n-c_1-2}{2}$ modi e così via fino al c_2-esimo. Dunque il numero totale di modi per i 2-cicli è

$$\frac{\binom{n-c_1}{2} \cdots \binom{n-c_1-2c_2+2}{2}}{c_2!} = \frac{(n-c_1)(n-c_1-1)\cdots(n-c_1-2c_2+1)}{(2!)^{c_2}c_2!}.$$

In generale per il primo k-ciclo sono rimasti $n - \sum_{i=1}^{k-1}(ic_i)$ elementi tra cui scegliere e proseguendo si scopre che gli elementi rimasti a disposizione per l'ultimo k-ciclo sono $n - \sum_{i=1}^{k}(ic_i) + k$. Occorre fare attenzione ora: si divide per $c_k!$ poiché l'ordine con cui compaiono i k-cicli non conta, ma bisogna anche moltiplicare per $((k-1)!)^{c_k}$ perché in realtà finora abbiamo scelto solo gli elementi che compongono i cicli, ma ogni insieme di k elementi dà origine a $(k-1)!$ cicli distinti (abbiamo $k-1$ scelte per il primo elemento del ciclo, $k-2$ per il secondo e così via fino all'ultimo che è obbligato). Per gli 1-cicli e i 2-cicli non ne abbiamo tenuto conto dato che $(1-1)! = 1$ e $(2-1)! = 1$. In definitiva, il numero di modi per scegliere i k-cicli è

$$\binom{n-\sum_{i=1}^{k-1}(ic_i)}{k}\binom{n-\sum_{i=1}^{k-1}(ic_i)-k}{k}\cdots\binom{n-\sum_{i=1}^{k}(ic_i)+k}{k} \cdot \frac{((k-1)!)^{c_k}}{c_k!} =$$

$$= \frac{\left(n-\sum_{i=1}^{k-1}(ic_i)\right)\left(n-\sum_{i=1}^{k-1}(ic_i)-1\right)\cdots\left(n-\sum_{i=1}^{k}(ic_i)+1\right)}{k^{c_k}c_k!}.$$

Moltiplicando tra loro tutti i risultati per $k = 1, \ldots, n$ si ottiene l'Equazione (3.4). Dunque

$$Z(\mathcal{S}_n; X_1, \ldots, X_n) = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\prod_{k=1}^{n} X_k^{c_k(\sigma)} =$$

$$= \sum_{c \in \mathcal{C}} \frac{1}{n!} \cdot \frac{n!}{1^{c_1} \cdots n^{c_n} \cdot c_1! \cdots c_n!} X_1^{c_1} \cdots X_n^{c_n} =$$
$$= \sum_{c \in \mathcal{C}} \prod_{k=1}^{n} \frac{1}{c_k!} \left(\frac{X_k}{k} \right)^{c_k}. \qquad \square$$

Vediamo per esempio quali sono i polinomi indici dei cicli per $\mathcal{S}_3$ e $\mathcal{S}_4$ (senza riportare i calcoli):

$$Z(\mathcal{S}_3; X_1, X_2, X_3) = \frac{1}{6}(X_1^3 + 3X_1X_2 + 2X_3),$$
$$Z(\mathcal{S}_4; X_1, X_2, X_3, X_4) = \frac{1}{24}(X_1^4 + 6X_1^2X_2 + 3X_2^2 + 8X_1X_3 + 6X_4).$$

Proviamo a racchiudere queste informazioni in una funzione generatrice. Per ogni $n \in \mathbb{N}$, sia

$$\varphi_n(X_1, \ldots, X_n) := Z(\mathcal{S}_n; X_1, \ldots, X_n) = \sum_{c \in \mathcal{C}} \frac{X_1^{c_1} \cdots X_n^{c_n}}{1^{c_1} \cdots n^{c_n} \cdot c_1! \cdots c_n!}$$

dove $\mathcal{C}$ è lo stesso della proposizione precedente e sia

$$F(\mathbf{X}, T) := \sum_{n=0}^{\infty} \varphi_n(X_1, \ldots, X_n) T^n \in \mathbb{Q}[\mathbf{X}, T] \tag{3.5}$$

in cui $\mathbf{X} = \{X_1, X_2, \ldots\}$ sono infinite variabili. Sia ora n fissato; l'n-upla $(c_1, \ldots, c_n) \in \mathbb{N}^n$ compare nel coefficiente di T^k in cui $c_1 + 2c_2 + \cdots + nc_n = k$, quindi al variare di n e delle n-uple di $\mathbb{N}^n$ si ottengono tutti e soli i termini di $F(\mathbf{X}, T)$. In altre parole, distribuendo il prodotto, vale che

$$F(\mathbf{X}, T) = \left(\sum_{c_1=0}^{\infty} \frac{(TX_1)^{c_1}}{1^{c_1} c_1!} \right) \left(\sum_{c_2=0}^{\infty} \frac{(T^2X_2)^{c_2}}{2^{c_2} c_2!} \right) \cdots \left(\sum_{c_n=0}^{\infty} \frac{(T^nX_n)^{c_n}}{n^{c_n} c_n!} \right) \cdots$$
$$= \prod_{j=1}^{\infty} \exp\left(\frac{T^j X_j}{j} \right) =$$
$$= \exp\left(\sum_{j=1}^{\infty} \frac{T^j X_j}{j} \right). \tag{3.6}$$

Ora, possiamo ricavare la funzione generatrice per il numero dei modelli: se per ogni $n \in \mathbb{N}$ definiamo $\#(\mathcal{M})_n := Z(\mathcal{S}_n; m, \ldots, m)$, cioè il numero di modelli sotto l'azione di $\mathcal{S}_n$, e $F_{\mathcal{M}}(T) := \sum \#(\mathcal{M})_n T^n$, allora

$$F_{\mathcal{M}}(T) = F(\mathbf{m}, T) = \exp\left(\sum_{j=1}^{\infty} \frac{T^j m}{j} \right) = \exp(-m \ln(1 - T)) = (1 - T)^{-m}.$$

Il numero di modelli è il coefficiente di T^n, quindi

$$\#(\mathcal{M})_n = \binom{m+n-1}{n}.$$

In effetti, a questo risultato si può arrivare in un modo più diretto, senza passare per le funzioni generatrici: si rimanda all'Appendice A per i dettagli.

3.3 Altri esempi di applicazione del Teorema di Pólya-Redfield

In questa sezione mostreremo come il Teorema di Pólya-Redfield sia applicabile in numerosi contesti, anche valicando i confini della matematica.

Definizione 3.9. Sia $G < \mathcal{S}_n$. Due sottoinsiemi $A, B \subseteq \{1, \dots, n\}$ si dicono *equivalenti* rispetto a G se esiste $\sigma \in G$ tale che $\sigma(A) = B$.

Quella appena definita è chiaramente una relazione di equivalenza. Possiamo ricondurci al caso precedente passando alle funzioni caratteristiche: per $A \subseteq \{1, \dots, n\}$ definiamo

$$\begin{aligned} \chi_A : \{1, \dots, n\} &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A. \end{cases} \end{aligned}$$

Osserviamo che, prendendo come insieme degli oggetti $D = \{1, \dots, n\}$ e come colori $C = \{0, 1\}$, abbiamo che A e B sono equivalenti se e solo se $\chi_A \sim \chi_B$ nel senso della relazione di equivalenza definita in (3.1).

Diamo ora un peso agli elementi di $\{0, 1\}$. Scegliamo come dominio $\mathbb{K}[X]$ e definiamo $w(0) = 1$ e $w(1) = X$. In questo modo $w(\chi_A) = X^{\#(A)}$.

Per quanto visto prima, il numero di modelli di cardinalità k[8] è il coefficiente di X^k del polinomio

$$Z(G; 1 + X, 1 + X^2, \dots, 1 + X^n)$$

mentre il totale dei modelli è dato dal valore

$$Z(G; 2, \dots, 2) = \frac{1}{\#(G)} \sum_{\sigma \in G} 2^{c(\sigma)}$$

in cui $c(\sigma)$ è il numero totale dei cicli di σ. Vediamo due casi particolari.

[8] La cardinalità di un modello è ben definita, in quanto se A e B sono equivalenti allora $\#(A) = \#(B)$. Quindi "il numero di modelli di cardinalità k" è il numero di modelli rappresentati da un sottoinsieme di cardinalità k.

- $G = \{\mathrm{Id}\}$. In questo caso ciascun sottoinsieme è un modello, quindi ci aspettiamo $\binom{n}{k}$ modelli di cardinalità k e 2^n modelli totali. In effetti Id ha n cicli di lunghezza 1, quindi $Z(\{\mathrm{Id}\}; X_1, \ldots, X_n) = X_1^n$ da cui

$$Z(\{\mathrm{Id}\}; 1+X, 1+X^2, \ldots, 1+X^n) = (1+X)^n$$

  e lo sviluppo del binomio conferma le nostre aspettative.

- $G = \mathcal{S}_n$. In questo caso tutti i sottoinsiemi di cardinalità k sono equivalenti tra loro, quindi dovrebbe risultare che c'è un solo modello di cardinalità k per ogni $k = 0, \ldots, n$ (dunque $n+1$ modelli totali). In effetti, svolgendo i conti, si trova che

$$Z(\mathcal{S}_n; 1+X, 1+X^2, \ldots, 1+X^n) = 1 + X + \cdots + X^n.$$

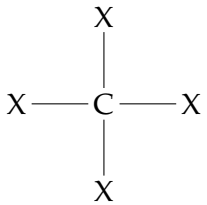
  Per dimostrarlo, riprendiamo la funzione generatrice $F(\mathbf{X}, T)$ definita in (3.5). Il polinomio $Z(\mathcal{S}_n; 1+X, 1+X^2, \ldots, 1+X^n)$ si ottiene valutando $F(\mathbf{X}, T)$ in $X_j = 1 + X^j$ e prendendo poi il coefficiente di T^n. Dall'Equazione (3.6) si ricava

$$\begin{aligned}
\exp\left(\sum_{j=1}^{\infty} \frac{T^j(1+X^j)}{j}\right) &= \exp\left(\sum_{j=1}^{\infty} \frac{T^j}{j}\right) \cdot \exp\left(\sum_{j=1}^{\infty} \frac{(TX)^j}{j}\right) = \\
&= \exp(-\ln(1-T)) \cdot \exp(-\ln(1-TX)) = \\
&= \frac{1}{1-T} \cdot \frac{1}{1-TX} = \left(\sum_{n=0}^{\infty} T^n\right) \cdot \left(\sum_{n=0}^{\infty} (TX)^n\right) = \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} T^k (TX)^{n-k}\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} X^{n-k}\right) T^n
\end{aligned}$$

  e possiamo concludere che

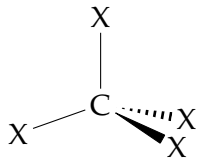
$$Z(\mathcal{S}_n; 1+X, 1+X^2, \ldots, 1+X^n) = \sum_{k=0}^{n} X^{n-k} = 1 + X + \cdots + X^n.$$

Il Teorema di Pólya-Redfield è stato sviluppato a partire da una richiesta dei chimici: contare il numero di molecole possibili con una determinata struttura, a meno di isometrie dello spazio. Ad esempio, supponiamo di voler classificare tutte le molecole organiche con la struttura



(3.7)

dove X può essere scelto in $\{H, CH_3, C_2H_5, Cl\}$. Ora, i chimici ci dicono che una molecola con la struttura (3.7) non è planare, ma i quattro gruppi X si dispongono ai vertici di un tetraedro più o meno regolare con l'atomo di carbonio al centro:



Il gruppo delle rotazioni di un tetraedro regolare è isomorfo al gruppo alterno $\mathcal{A}_4$ e in questo caso agisce sui quattro vertici del tetraedro; risulta che

$$Z(\mathcal{A}_4; X_1, X_2, X_3, X_4) = \frac{1}{12}(X_1^4 + 3X_2^2 + 8X_1X_3).$$

Avendo a disposizione quattro tipi diversi di gruppi atomici da assegnare, il numero totale di modelli è

$$\#(\mathcal{M}) = Z(\mathcal{A}_4; 4, 4, 4, 4) = 36.$$

Possiamo contare anche il numero di modelli $\mathcal{M}_H$ in cui è presente k volte un gruppo fissato, per esempio $-H$. In tal caso, l'assegnamento del peso potrebbe essere

$$\begin{aligned} w(H) &= X, \\ w(CH_3) &= Y, \\ w(C_2H_5) &= Z, \\ w(Cl) &= T, \end{aligned}$$

per ottenere $g(\mathcal{M})$ come polinomio nelle indeterminate X, Y, Z e T. Ricordiamo che il coefficiente di $X^iY^jZ^kT^\ell$ conta i modelli che contengono i volte H, j volte CH_3 e così via: basta allora porre $Y = Z = T = 1$ per far sì che i coefficienti si sommino e concludere che

$$\#(\mathcal{M}_H) = 15 + 11X + 6X^2 + 3X^3 + X^4,$$

cioè che ci sono 15 modelli senza il gruppo H, 11 con un solo H e così via fino all'unico con tutti e quattro H (il metano, CH_4).

Proviamo ora a calcolare il polinomio indice dei cicli del gruppo ciclico di n elementi (che agisce su $\{1, \dots, n\}$). Vediamo il gruppo come $\mathbb{Z}_n := \mathbb{Z}/(n)$.

Proposizione 3.10. *Il polinomio indice dei cicli del gruppo ciclico su n elementi è*

$$Z(\mathbb{Z}_n; X_1, \dots, X_n) = \frac{1}{n} \sum_{d|n} \varphi(d) X_d^{n/d}$$

dove φ è la funzione di Eulero.

Dimostrazione. Immergiamo $\mathbb{Z}_n$ in $\mathcal{S}_n$ con la mappa data dal Teorema di Cayley: per $g \in \mathbb{Z}_n$ definiamo

$$\begin{array}{rcl} \sigma_g : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ x & \longmapsto & g + x. \end{array}$$

È noto che se g ha ordine d, allora σ_g ha n/d cicli di lunghezza d. La tesi segue ricordando che ci sono $\varphi(d)$ elementi di ordine d in $\mathbb{Z}_n$ per ogni d che divide n. □

Corollario 3.11. *Il numero di modi di colorare i vertici di un n-agono regolare con m colori, a meno di rotazioni del piano, è*

$$C_{n,m} := \frac{1}{n} \sum_{d|n} \varphi(d) m^{n/d}.$$

Esempio 3.7. Quanti grafi non etichettati su n vertici esistono? Abbiamo già visto nel Capitolo 1 che i grafi etichettati sono $2^{\binom{n}{2}}$. Il problema è che i grafi non etichettati sono le classi di isomorfismo dei grafi etichettati.[9] ▷ *29/04/2015*

Vediamo più in dettaglio. Se indichiamo con $\mathcal{P}_2(V) := \{A \subseteq V \mid \#(A) = 2\}$ l'insieme delle coppie (non ordinate) di vertici, abbiamo che i grafi etichettati sono in corrispondenza biunivoca con le funzioni $F\colon \mathcal{P}_2(V) \to \{0,1\}$, in cui $F(\{i,j\}) = 1$ se l'arco $\{i,j\}$ è presente nel grafo e $F(\{i,j\}) = 0$ altrimenti.

Dobbiamo ora scegliere un sottogruppo $G < \mathcal{S}_{\binom{n}{2}}$ che agisca su $\mathcal{P}_2(V)$ in modo che due grafi G_1 e G_2 siano isomorfi se e solo se le rispettive $F_1, F_2\colon \mathcal{P}_2(V) \to \{0,1\}$ appartengono alla stessa classe di equivalenza rispetto all'azione di G.

Sicuramente una permutazione $\sigma \in \mathcal{S}_n$ che agisce su V induce una permutazione $\sigma^{(2)} \in \mathcal{S}_{\binom{n}{2}}$ definita da $\sigma^{(2)}(\{i,j\}) = \{\sigma(i), \sigma(j)\}$. Ora, la mappa

$$\begin{array}{rcl} \mathcal{S}_n & \longrightarrow & \mathcal{S}_{\binom{n}{2}} \\ \sigma & \longmapsto & \sigma^{(2)} \end{array}$$

è un omomorfismo di gruppi, iniettivo per $n \geqslant 3$ (vedi l'Appendice A). Il nostro candidato è dunque $\mathcal{S}_n^{(2)} := \{\sigma^{(2)} \mid \sigma \in \mathcal{S}_n\}$, che è un sottogruppo di $\mathcal{S}_{\binom{n}{2}}$ di cardinalità $n!$.

Per poter contare i grafi definiamo un opportuno peso su $\{0,1\}$: scegliendo $w(0) = 1$ e $w(1) = X$, con X indeterminata, otterremo che $g(\mathcal{M})$ è un polinomio in X in cui il coefficiente di X^k è il numero di grafi non etichettati su n vertici con esattamente k archi. Per quanto visto, è sufficiente calcolare il polinomio indice dei cicli

$$Z(\mathcal{S}_n^{(2)}; X_1, \ldots, X_{\binom{n}{2}})$$

[9] Ricordiamo che due grafi $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ sono isomorfi se esiste una mappa $f\colon V_1 \to V_2$ biiettiva tale che per ogni $i, j \in V_1$ si ha $\{i,j\} \in E_1$ se e solo se $\{f(i), f(j)\} \in E_2$.

per poi ricavare

$$g(\mathcal{M}) = Z(\mathcal{S}_n^{(2)}; 1+X, \dots, 1+X^{\binom{n}{2}}),$$
$$\#(\mathcal{M}) = Z(\mathcal{S}_n^{(2)}; 2, \dots, 2).$$

A titolo d'esempio, calcoliamo questi valori per $n = 2, 3, 4$.
$\boxed{n=2}$ Abbiamo solo una possibile coppia di vertici, che possono essere uniti da un arco oppure no. I grafi etichettati sono tanti quanti quelli non etichettati, cioè due. In effetti $\mathcal{S}_2^{(2)} = \{\mathrm{Id}\} < \mathcal{S}_1$, quindi $Z(\mathcal{S}_2^{(2)}; X_1) = X_1$, $g(\mathcal{M}) = 1 + X$ (come ci aspettiamo: un modello con zero archi e uno con un arco) e $\#(\mathcal{M}) = 2$.
$\boxed{n=3}$ In questo caso le permutazioni degli archi sono $\mathcal{S}_{\binom{3}{2}} = \mathcal{S}_3$ e la mappa $\sigma \mapsto \sigma^{(2)}$ è in realtà un isomorfismo di gruppi; ricordando che

$$Z(\mathcal{S}_3^{(2)}; X_1, X_2, X_3) = Z(\mathcal{S}_3; X_1, X_2, X_3) = \frac{1}{6}(X_1^3 + 3X_1X_2 + 2X_3),$$

otteniamo $g(\mathcal{M}) = 1 + X + X^2 + X^3$ e $\#(\mathcal{M}) = 4$.
$\boxed{n=4}$ Qui occorre fare qualche conto in più: dobbiamo vedere la struttura in cicli degli elementi di $\mathcal{S}_4^{(2)}$ visti all'interno di $\mathcal{S}_6$. Innanzitutto osserviamo che se $\sigma, \tau \in \mathcal{S}_4$ hanno la stessa struttura in cicli, allora ciò vale anche per $\sigma^{(2)}$ e $\tau^{(2)}$, quindi possiamo limitarci ad analizzare una sola permutazione per ogni possibile struttura in cicli. I risultati sono esposti nella Tabella 3.4.

Numero di permutazioni	Struttura in $\mathcal{S}_4$	Struttura in $\mathcal{S}_4^{(2)} < \mathcal{S}_6$
1 (Id)	$(*)(*)(*)(*)$	$(*)(*)(*)(*)(*)(*)$
6	$(**)(*)(*)$	$(**)(**)(*)(*)$
3	$(**)(**)$	$(**)(**)(*)(*)$
8	$(***)(*)$	$(***)(***)$
6	$(****)$	$(****)(**)$

Tabella 3.4: Le strutture in cicli degli elementi di $\mathcal{S}_4^{(2)}$ in $\mathcal{S}_6$.

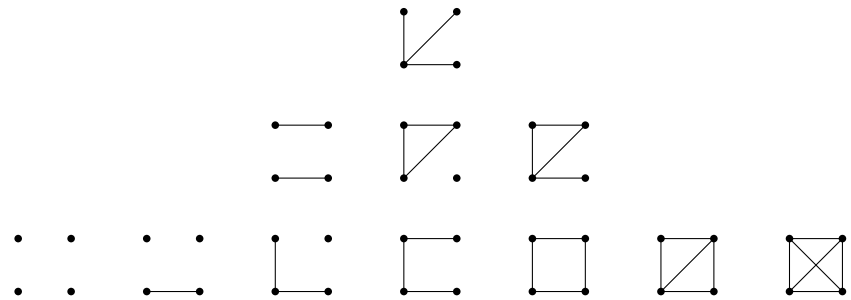
Di conseguenza abbiamo che

$$Z(\mathcal{S}_4^{(2)}; X_1, \dots, X_6) = \frac{1}{24}(X_1^6 + 9X_1^2X_2^2 + 8X_3^2 + 6X_2X_4),$$

da cui ricaviamo $g(\mathcal{M}) = 1 + X + 2X^2 + 3X^3 + 2X^4 + X^5 + X^6$ e $\#(\mathcal{M}) = 11$.

3.4 Una versione più sottile del Teorema di Pólya-Redfield

Finora abbiamo trattato i modelli dati dalle colorazioni di un insieme di oggetti, a meno di un'equivalenza data dall'azione di un gruppo sugli oggetti. Ma cosa



Numero di archi	0	1	2	3	4	5	6

Figura 3.3: Gli undici possibili grafi non etichettati su quattro vertici, ordinati per numero di archi.

succede se facciamo agire un gruppo anche sull'insieme dei colori? In altre parole, cosa succede se vogliamo rendere due modelli equivalenti anche a meno di una permutazione dei colori?

Facciamo subito un esempio. Abbiamo 10 oggetti su cui agisce un gruppo di permutazioni e li coloriamo con due colori. Vogliamo contare i modelli in cui 7 oggetti sono colorati con un colore, *non importa quale*, e 3 con l'altro. Quindi contiamo una sola volta due modelli se è possibile ottenere uno dall'altro scambiando tra loro i colori, cioè lasciando agire $\mathcal{S}_2$ sull'insieme dei colori.

Formalizziamo il tutto. Siano D un insieme (finito) di oggetti e C un insieme (finito) di colori. Siano G e H due gruppi di permutazioni rispettivamente di D e C. Sull'insieme $C^D = \{f\colon D \to C\}$ definiamo un'azione di $G \times H$ come

$$(\sigma, \tau) \cdot f = \tau \circ f \circ \sigma^{-1}$$

per ogni $(\sigma, \tau) \in G \times H$ e $f \in C^D$. La relazione di equivalenza indotta da questa azione è

$$f \sim g \quad \text{se e solo se} \quad \exists\, (\sigma, \tau) \in G \times H \text{ tale che } \forall\, x \in D\ \tau(f(x)) = g(\sigma(x)). \tag{3.8}$$

Esempio 3.8. Torniamo alla scacchiera 2×2. Supponiamo sempre che sulle caselle agisca il gruppo delle rotazioni, mentre ammettiamo una permutazione qualsiasi dei colori (in questo caso il gruppo che agisce è $\mathcal{S}_2$, quindi possiamo solo scambiare i due colori). Il totale dei modelli si riduce a quattro: infatti se scambiamo tra loro bianco e nero, la configurazione  diventa  , quindi questi due modelli appartengono alla stessa classe di equivalenza; discorso analogo per  e  . Tuttavia, la configurazione con i colori scambiati è e le due

colorazioni già appartenevano alla stessa classe di equivalenza; lo stesso discorso vale per  e  . In altre parole, i due modelli  e non diventano equivalenti neppure a meno di permutare i colori.

Teorema 3.12. *Siano* D *e* C *insiemi finiti con* $\#(D) = n$ *e siano* G, H *gruppi di permutazioni di* D *e* C *rispettivamente. Il numero di classi di equivalenza della relazione* (3.8)*, cioè il numero di orbite sotto l'azione di* $G \times H$ *su* C^D*, è*

$$\#(\mathcal{M}) = \frac{1}{\#(H)} \sum_{\tau \in H} Z(G; m_1(\tau), \dots, m_n(\tau))$$

dove $m_i(\tau) := \sum_{j|i} j c_j(\tau)$*, in cui* $c_j(\tau)$ *è il numero di cicli di lunghezza* j *in* τ*.*

Dimostrazione. Per il Teorema 3.5,

$$\#(\mathcal{M}) = \frac{1}{\#(G)\,\#(H)} \sum_{(\sigma,\tau) \in G \times H} c_1(\sigma, \tau)$$

con $c_1(\sigma,\tau) = \#\{f \in C^D \mid (\sigma,\tau) \cdot f = f\} = \#\{f \in C^D \mid \tau \circ f = f \circ \sigma\}$. Abbiamo allora la tesi se dimostriamo che per ogni $\tau \in H$

$$Z(G; m_1(\tau), \dots, m_n(\tau)) = \frac{1}{\#(G)} \sum_{\sigma \in G} c_1(\sigma, \tau).$$

Siano σ e τ fissate e sia $D = X_1 \cup \cdots \cup X_k$ la partizione di D indotta dalla struttura in cicli di σ (dunque $k = c_1(\sigma) + \cdots + c_n(\sigma)$). Osserviamo che $f \in C^D$ è lasciata fissa da (σ,τ) se e solo se lo sono tutte le sue restrizioni ai cicli $f_i := f|_{X_i} : X_i \to C$. Di conseguenza

$$\#\{f \in C^D \mid \tau \circ f = f \circ \sigma\} = \prod_{i=1}^{k} \#\{f_i : X_i \to C \mid \tau \circ f_i = f_i \circ \sigma\}.$$

Fissiamo dunque un ciclo X_i e chiediamoci quante sono le f_i tali che $f_i(\sigma(d)) = \tau(f_i(d))$ per ogni $d \in X_i$. Supponiamo che la lunghezza del ciclo X_i sia $\#(X_i) = \ell$, scegliamo $d_0 \in X_i$ e sia $c := f_i(d_0)$. Allora f_i è completamente determinata. Infatti $X_i = \{\sigma^t(d_0) \mid t = 0, \dots, \ell-1\}$ e vale che $f_i(\sigma^t(d_0)) = \tau^t(c)$; dimostriamolo velocemente per induzione su t: per $t = 0$ è l'ipotesi, mentre supponendo che $f_i(\sigma^{t-1}(d_0)) = \tau^{t-1}(c)$ otteniamo

$$f_i(\sigma^t(d_0)) = (f_i \circ \sigma)(\sigma^{t-1}(d_0)) = (\tau \circ f_i)(\sigma^{t-1}(d_0)) = \tau \circ \tau^{t-1}(c) = \tau^t(c).$$

Dal fatto che $\sigma^\ell(d_0) = d_0$ deduciamo che $\tau^\ell(c) = c$, dunque il ciclo di τ che contiene c ha lunghezza ℓ' che divide ℓ.

Viceversa, sia $c \in C$ che appartiene a un ciclo di τ di lunghezza ℓ' che divide ℓ; possiamo definire una mappa $f_i \colon X_i \to C$ ponendo $f_i(\sigma^t(d_0)) := \tau^t(c)$. Tale mappa è ben definita perché $\sigma^s(d_0) = \sigma^t(d_0)$ se e solo se $s \equiv t \pmod{\ell}$ e in tal caso

$$\tau^s(c) = \tau^{t+m\ell}(c) = \tau^{t+md\ell'}(c) = \tau^t(c);$$

infine $f_i \circ \sigma = \tau \circ f_i$ per costruzione. Dunque

$$\begin{aligned}\#\{f_i \mid \tau \circ f_i = f_i \circ \sigma\} &= \#\{c \in C \mid c \in \text{ ciclo di } \tau \text{ di lunghezza che divide } \ell\} \\ &\overset{\blacktriangleright 10}{=} \sum_{j \mid \ell} j c_j(\tau) = m_\ell(\tau)\end{aligned}$$

e infine

$$\#\{f \in C^D \mid \tau \circ f = f \circ \sigma\} = \prod_{i=1}^{k} m_{\#(X_i)}(\tau) = \prod_{r=1}^{n} m_r(\tau)^{c_r(\sigma)}. \qquad \square$$

Esempio 3.9. Vediamo una prima applicazione banale: la nostra scacchiera 2×2. Effettivamente in questo esempio è molto più veloce contare i modelli a mano...

Il gruppo $G \simeq \mathbb{Z}_4$ è il gruppo delle rotazioni che agisce su quattro elementi: per la Proposizione 3.10

$$Z(\mathbb{Z}_4; X_1, X_2, X_3, X_4) = \frac{1}{4}(X_1^4 + X_2^2 + 2X_4).$$

Il gruppo H è invece il gruppo di ordine due $\mathcal{S}_2 = \{\mathrm{Id}, (12)\}$. Dobbiamo calcolare i valori $m_1(\tau) = c_1(\tau)$, $m_2(\tau) = c_1(\tau) + 2c_2(\tau)$ e $m_4(\tau) = c_1(\tau) + 2c_2(\tau) + 4c_4(\tau)$ per $\tau \in \mathcal{S}_2$: il risultato è riportato nella Tabella 3.5.

Id	
$c_1 = 2$	$m_1 = 2$
$c_2 = 0$	$m_2 = 2$
$c_4 = 0$	$m_4 = 2$

(a) $\tau = \mathrm{Id}$.

(12)	
$c_1 = 0$	$m_1 = 0$
$c_2 = 1$	$m_2 = 2$
$c_4 = 0$	$m_4 = 2$

(b) $\tau = (12)$.

Tabella 3.5: Valori di c_i e m_i per $\tau \in \mathcal{S}_2$.

Possiamo allora calcolare

$$Z(\mathbb{Z}_4; m_1(\mathrm{Id}), \dots, m_4(\mathrm{Id})) = \frac{1}{4}(2^4 + 2^2 + 2 \cdot 2) = 6$$
$$Z(\mathbb{Z}_4; m_1(12), \dots, m_4(12)) = \frac{1}{4}(2^2 + 2 \cdot 2) = 2$$

[10] Ci sono j elementi in un ciclo di lunghezza j e $c_j(\tau)$ cicli di lunghezza j in τ.

e concludere

$$\#(\mathcal{M}) = \frac{1}{2}(6+2) = 4$$

che è il risultato ottenuto *by inspection*.

Esempio 3.10. In quanti modi possono essere distribuite 2 palline rosse, 2 gialle e 4 verdi in 4 scatole di cui una rotonda e 3 quadrate? Indichiamo con $D := \{r_1, r_2, g_1, g_2, v_1, v_2, v_3, v_4\}$ le otto palline e con $C := \{R, Q_1, Q_2, Q_3\}$ le quattro scatole. Chiaramente le palline con lo stesso colore e le scatole con la stessa forma sono indistinguibili, quindi i gruppi che agiscono sono rispettivamente $G = \mathcal{S}_2 \times \mathcal{S}_2 \times \mathcal{S}_4$ e $H = \mathcal{S}_1 \times \mathcal{S}_3$. Per il Lemma A.9 nell'Appendice A abbiamo

$$\begin{aligned} Z(G; X_1, \dots, X_8) &= Z(\mathcal{S}_2; X_1, X_2)^2 Z(\mathcal{S}_4; X_1, \dots, X_4) = \\ &= \frac{1}{2!2!4!}(X_1^2 + X_2)^2 (X_1^4 + 6X_1^2X_2 + 3X_2^2 + 8X_1X_3 + 6X_4). \end{aligned} \tag{3.9}$$

Dobbiamo ora calcolare i valori m_i degli elementi di H come sottogruppo di $\mathcal{S}_4$. Osserviamo che nel polinomio (3.9) compaiono le indeterminate X_1, X_2, X_3 e X_4, quindi è necessario conoscere m_1, m_2, m_3 ed m_4. Il conto è facile ma noioso e il risultato è esposto nella Tabella 3.6.

$(*) \times (*)(*)(*)$	
$c_1 = 4$	$m_1 = 4$
$c_2 = 0$	$m_2 = 4$
$c_3 = 0$	$m_3 = 4$
$c_4 = 0$	$m_4 = 4$

(a) τ è l'identità di H (numero di elementi in H con questa struttura: 1).

$(*) \times (**)(*)$	
$c_1 = 2$	$m_1 = 2$
$c_2 = 1$	$m_2 = 4$
$c_3 = 0$	$m_3 = 2$
$c_4 = 0$	$m_4 = 4$

(b) τ è una trasposizione in $\mathcal{S}_3$ (numero di elementi in H con questa struttura: 3).

$(*) \times (***)$	
$c_1 = 1$	$m_1 = 1$
$c_2 = 0$	$m_2 = 1$
$c_3 = 1$	$m_3 = 4$
$c_4 = 0$	$m_4 = 1$

(c) τ è un 3-ciclo di $\mathcal{S}_3$ (numero di elementi in H con questa struttura: 2).

Tabella 3.6: Valori di c_i e m_i per $\tau \in \mathcal{S}_1 \times \mathcal{S}_3$, al variare della struttura in cicli. Ricordiamo che $m_1 = c_1$, $m_2 = c_1 + 2c_2$, $m_3 = c_1 + 3c_3$, $m_4 = c_1 + 2c_2 + 4c_4$.

Abbiamo ora tutti gli ingredienti: iniziamo con valutare il polinomio (3.9) negli m_i (il tipo di permutazione è definito nella Tabella 3.6). Risulta

- τ di tipo (a): $Z(G; m_1(\tau), \dots, m_4(\tau)) = 3500$;
- τ di tipo (b): $Z(G; m_1(\tau), \dots, m_4(\tau)) = 144$;
- τ di tipo (c): $Z(G; m_1(\tau), \dots, m_4(\tau)) = 2$.

In conclusione

$$\#(\mathcal{M}) = \frac{1}{3!}(3500 + 3 \cdot 144 + 2 \cdot 2) = 656.$$

Capitolo 4

q-analoghi e *cyclic sieving phenomenon*

In questo capitolo introduciamo i q-*analoghi*, cioè generalizzazioni tramite un parametro q di quantità o teoremi combinatori, che si riconducono alla quantità o teorema originale considerando il limite per $q \to 1$. I q-analoghi emergono naturalmente nella costruzione dei *gruppi quantici* "deformando" opportunamente alcune strutture algebriche "rigide" (ad esempio, algebre di Lie semisemplici). Comunque, non tratteremo qui questi argomenti, concentrandoci più sugli aspetti combinatori: osserveremo infatti che a volte un q-analogo permette di contare le orbite e i punti fissi dell'azione di un gruppo ciclico. ▹ *04/05/2015*

4.1 q-numero e q-fattoriale

Definiamo innanzitutto il q-analogo più basilare: quello di un numero naturale.

Definizione 4.1. Sia q un parametro (*a priori* complesso). Per $n \in \mathbb{N}$, definiamo *numero* q-*analogo* (o q-*numero*) di n la quantità

$$(n)_q := \frac{1-q^n}{1-q} = 1 + q + \cdots + q^{n-1};$$

per convenzione $(0)_q = 0$.

Definizione 4.2. Definiamo il q-analogo del fattoriale, o q-*fattoriale*, la quantità

$$(n)_q! := (n)_q (n-1)_q \cdots (1)_q.$$

Come vedremo a breve, il q-analogo non è semplicemente un polinomio che restituisce una vecchia funzione combinatoria per $q \to 1$, ma ha anche un significato combinatorio intrinseco.

Esempio 4.1. Consideriamo l'insieme $\{1,\dots,n\}$. Una *bandiera massimale* di sottoinsiemi è una catena

$$\varnothing = S_0 \subsetneq S_1 \subsetneq \cdots \subsetneq S_n = \{1,\dots,n\}.$$

Le bandiere massimali in $\{1,\dots,n\}$ sono $n!$: infatti abbiamo n scelte per S_1, per ciascuna delle quali $n-1$ per completarlo a S_2 e così via fino ad esaurire tutti gli n elementi.

Analogamente, il numero di bandiere massimali

$$\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = (\mathbb{F}_q)^n$$

di sottospazi lineari di $(\mathbb{F}_q)^n$ è $(n)_q!$. In effetti, vediamo in quanti modi possiamo scegliere in successione i sottospazi $V_1,\dots,V_n$.

1. Per V_1 basta prendere un qualsiasi vettore non nullo $\boldsymbol{v}_1$ di $(\mathbb{F}_q)^n$ e definire $V_1 := \langle \boldsymbol{v}_1 \rangle$; ci sono $q^n - 1$ possibili scelte per $\boldsymbol{v}_1$, ma dato che $\langle \boldsymbol{v}_1 \rangle = \langle \lambda \boldsymbol{v}_1 \rangle$ per ogni $\lambda \in \mathbb{F}_q \setminus \{0\}$ restano solo
$$\frac{q^n - 1}{q - 1} = (n)_q$$
scelte per V_1.

2. Ora vorremmo estendere V_1 a $V_2 := \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$. Possiamo scegliere $\boldsymbol{v}_2 \in (\mathbb{F}_q)^n \setminus V_1$, in $q^n - q$ modi; ma $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \langle \boldsymbol{v}_1, \lambda \boldsymbol{v}_2 + \boldsymbol{w} \rangle$ per ogni $\lambda \in \mathbb{F}_q \setminus \{0\}$ e per ogni $\boldsymbol{w} \in V_1$, dunque abbiamo
$$\frac{q^n - q}{q(q-1)} = (n-1)_q$$
scelte per V_2.

3. In generale, se $V_k = \langle \boldsymbol{v}_1, \dots, \boldsymbol{v}_k \rangle$, ci sono $q^n - q^k$ modi per scegliere $\boldsymbol{v}_{k+1} \in (\mathbb{F}_q)^n \setminus V_k$ e, osservando che $\langle \boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \boldsymbol{v}_{k+1} \rangle = \langle \boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \lambda \boldsymbol{v}_{k+1} + \boldsymbol{w} \rangle$ per ogni $\lambda \in \mathbb{F}_q \setminus \{0\}$ e per ogni $\boldsymbol{w} \in V_k$, restano
$$\frac{q^n - q^k}{q^k(q-1)} = (n-k+1)_q$$
possibili sottospazi V_{k+1}.

Ricomponendo il tutto abbiamo $(n)_q!$ bandiere massimali in $(\mathbb{F}_q)^n$.

Definizione 4.3. Il q-analogo del coefficiente binomiale, o q-*binomiale*, è definito da

$$\binom{n}{k}_q := \frac{(n)_q!}{(k)_q!(n-k)_q!}.$$

Il coefficiente binomiale conta i possibili sottoinsiemi di k elementi di un insieme di n elementi; alla luce dell'esempio precedente, ci aspettiamo un risultato analogo per i sottospazi vettoriali di $(\mathbb{F}_q)^n$.

Proposizione 4.4. *Il numero di sottospazi* k*-dimensionali in* $(\mathbb{F}_q)^n$ *è* $\binom{n}{k}_q$.

Dimostrazione. Contiamo le k-uple ordinate di vettori in $(\mathbb{F}_q)^n$ linearmente indipendenti. Abbiamo $q^n - 1$ scelte per il primo vettore v; per il secondo dobbiamo togliere l'intera retta $\langle v \rangle$, quindi restano $q^n - q$ vettori. Proseguendo così si ha che il numero di k-uple di vettori linearmente indipendenti è

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}). \tag{4.1}$$

D'altra parte, i sottospazi di dimensione k partizionano le k-uple ordinate, quindi possiamo contare il numero di k-uple presenti in un sottospazio e poi moltiplicare per il numero totale dei sottospazi (che sarà indicato con $G(n,k)$): con un ragionamento analogo al precedente si ottiene

$$G(n,k) \cdot (q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}). \tag{4.2}$$

Uguagliando le espressioni (4.1) e (4.2) si ricava

$$G(n,k) = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \frac{(n)_q!}{(k)_q!(n-k)_q!} = \binom{n}{k}_q. \qquad \square$$

4.2 Ancora partizioni di interi

Dopo averne parlato in termini di funzioni generatrici nella Sezione 1.7.1, torniamo ad occuparci delle partizioni di interi. Ricordiamo che, se $n \in \mathbb{N}$, una partizione di n è una successione

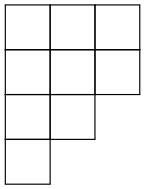
$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_i, \dots)$$

con $\lambda_i \in \mathbb{N}$, $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant 0$ e $\sum \lambda_i = n$. Osserviamo che quest'ultima condizione implica che la successione λ è definitivamente nulla: possiamo dunque trascurare gli zeri e scrivere direttamente, per esempio,

$$(3,3,2,1) \text{ invece di } (3,3,2,1,0,0,0,\dots).$$

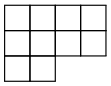
Per rappresentare una partizione è comodo utilizzare i *diagrammi di Young*: se $\lambda = (\lambda_1, \dots, \lambda_m)$ con $\sum \lambda_i = n$, si disegnano m righe di celle quadrate allineate

a sinistra, in cui la prima riga contiene λ_1 celle, la seconda λ_2 e così via. Ad esempio, la partizione precedente può essere descritta con



Notazione 4.5. Nel seguito indicheremo con

- $p(n)$ il numero totale delle partizioni di n;
- $p_k(n)$ il numero delle partizioni di n con esattamente k termini non nulli;
- $p(j,k,n)$ il numero delle partizioni di n con al più k termini non nulli e $\lambda_1 \leqslant j$.

Ad esempio,  è un diagramma di Young contato in $p(4,3,10)$.

Proposizione 4.6. *Siano* $j,k \in \mathbb{N}$. *Allora*

$$\sum_{n \geqslant 0} p(j,k,n)q^n = \binom{j+k}{k}_q.^{\blacktriangleright 1}$$

Prima di dimostrare la proposizione, richiamiamo una definizione di algebra lineare.

Definizione 4.7. Sia $A \in \mathcal{M}_{k\times m}(\mathbb{K})$. La matrice A è *a scalini* se il primo elemento non nullo di una riga ha un indice di colonna maggiore (strettamente) rispetto al primo elemento non nullo della riga precedente; in altre parole, se p_i è il primo elemento non nullo della riga i-esima ed è in posizione (i,j), allora tutti gli elementi in posizione (s,t) con $s > i$ e $t \leqslant j$ sono nulli. L'elemento p_i è detto *pivot* i-esimo. Una matrice A a scalini è *ridotta per righe* se i suoi pivot sono uguali a 1 e sono gli unici elementi non nulli della loro colonna.

Ad esempio, la seguente matrice è a scalini ridotta per righe (in breve SRR):

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 4 & 0 & 8 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 8 \end{pmatrix}.$$

Ogni matrice può essere portata in forma SRR tramite mosse di Gauss per righe.

[▸1] Osserviamo che, fissati j e k, la somma a sinistra è finita: nessun numero maggiore di $j \cdot k$ può essere partizionato in al più k parti, ciascuna minore di j.

Dimostrazione della Proposizione 4.6. Sia $m := j + k$. Osserviamo che ogni sottospazio k-dimensionale di $(\mathbb{F}_q)^m$ ha un'unica base $(v_1, \dots, v_k)$ tale che la matrice

$$\begin{pmatrix} — & v_1 & — \\ & \vdots & \\ — & v_k & — \end{pmatrix}$$

sia SRR. Infatti, se $(v'_1, \dots, v'_k)$ fosse un'altra base con la stessa proprietà, scrivendo $v_1 = \mu_1 v'_1 + \cdots + \mu_k v'_k$ e imponendo la forma SRR si ricava $v_1 = v'_1$ e analogamente per gli altri vettori.

Dunque abbiamo ricondotto il problema di contare i sottospazi a contare le matrici SRR. Ora, supponiamo di avere una successione di interi

$$1 \leqslant a_1 < \cdots < a_k \leqslant m$$

e consideriamo tutte le matrici SRR in cui il pivot della riga i-esima appartiene alla a_i-esima colonna. Il numero di elementi "liberi" nella riga i-esima, in cui può esserci un qualsiasi elemento di $\mathbb{F}_q$, è $j - a_i + i$: infatti dal numero totale di elementi sulla riga $m = j + k$ vanno tolti i posti obbligati, cioè gli $a_i - 1$ zeri che precedono il pivot, l'uno del pivot stesso e i $k - i$ zeri dovuti ai pivot delle righe successive.

Sia ora $\lambda_i := j - a_i + i$. La k-upla $(\lambda_1, \dots, \lambda_k)$ è una partizione di un certo intero $n := \sum \lambda_i$, in al più k parti con $\lambda_1 \leqslant j$. Infatti

- $\lambda_1 = j - a_1 + 1$ e $a_1 \geqslant 1$, quindi $\lambda_1 \leqslant j$;
- da $a_1 \leqslant a_2 - 1$ ricaviamo che $\lambda_2 = j - a_2 + 2 \leqslant j - (a_1 + 1) + 2 = \lambda_1$;
- analogamente si ottiene che $\lambda_i \leqslant \lambda_{i+1}$ per ogni $i = 1, \dots, k - 1$.

Dunque il numero totale di matrici SRR con $a_1, \dots, a_k$ fissati è

$$q^{|\lambda|} = q^{\lambda_1} \cdots q^{\lambda_k}, \quad |\lambda| := \sum_{i=1}^{k} \lambda_i,$$

perché ogni casella libera può essere riempita con un qualsiasi elemento di $\mathbb{F}_q$.

Viceversa, data una partizione λ in al più k parti con $\lambda_1 \leqslant j$, definiamo $a_i := j - \lambda_i + i$. È immediato verificare che $1 \leqslant a_1 < \cdots < a_k \leqslant m$. Di conseguenza, indicando con $\mathcal{A} := \{a = (a_1, \dots, a_m) \in \mathbb{N}^m \mid 1 \leqslant a_1 < \cdots < a_k \leqslant m\}$ e con $\mathcal{L} := \{\lambda = (\lambda_1, \dots, \lambda_k) \mid \lambda \text{ partizione con al più k parti e } \lambda_1 \leqslant j\}$ per brevità di scrittura, abbiamo che il numero di matrici SRR è

$$\sum_{a \in \mathcal{A}} q^{|\lambda|} = \sum_{\lambda \in \mathcal{L}} q^{|\lambda|} = \sum_{n \geqslant 0} p(j, k, n) q^n$$

in cui nell'ultimo passaggio si sono raccolte le partizioni λ tali che $|\lambda| = n$. D'altra parte, tale numero è uguale al numero di sottospazi k-dimensionali di $(\mathbb{F}_q)^m$, che è

$$\binom{m}{k}_q = \binom{j+k}{k}_q. \qquad \square$$

Ricordiamo che per i coefficienti binomiali vale la regola di Tartaglia

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{4.3}$$

Anche per i q-binomiali vale un risultato simile (che si riconduce all'Equazione (4.3) per $q \to 1$): si ha infatti

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q.$$

È possibile trovare una dimostrazione nell'Appendice A.

Teorema 4.8 (Teorema q-binomiale)**.** *Per ogni* $j \geqslant 1$ *vale che*

$$\prod_{i=0}^{j-1}(1+q^iX) = \sum_{k=0}^{j} q^{\binom{k}{2}} \binom{j}{k}_q X^k. \tag{4.4}$$

Dimostrazione. Vediamo chi è il coefficiente di X^k nel prodotto a sinistra. Calcolando

$$(1+q^0X)(1+q^1X)\cdots(1+q^{j-1}X)$$

per ogni fattore scegliamo 1 oppure q^iX e poi sommiamo su tutte le possibili scelte. Focalizziamoci su un singolo addendo: ogni volta che scegliamo q^iX creiamo un vettore in $(\mathbb{F}_q)^j$ del tipo

$$\gamma_i := \begin{pmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * \end{pmatrix}$$

in cui il pivot 1 è nella $(j-i)$-esima colonna e $*$ è un qualsiasi elemento di $\mathbb{F}_q$; abbiamo q^i possibili scelte di un vettore siffatto. Supponiamo di aver scelto k volte q^iX e siano $\gamma_{i_1}, \ldots, \gamma_{i_k}$ i vettori creati come sopra e

$$M := \begin{pmatrix} — & \gamma_{i_1} & — \\ & \vdots & \\ — & \gamma_{i_k} & — \end{pmatrix}.$$

La matrice M è a scalini, ma non per righe ridotte; definiamo allora una nuova matrice $\tilde{M}$ sostituendo gli elementi sopra ai pivot con 0. Quante sostituzioni abbiamo fatto? Sopra al primo pivot non ci sono elementi, sopra al secondo ce

n'è uno e così via fino al k-esimo pivot che ha $k-1$ elementi sopra di sé, per un totale di

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

Quindi $q^{\binom{k}{2}}$ delle possibili matrici M costruite sopra danno la stessa $\tilde{M}$, che essendo in forma SRR corrisponde biunivocamente a un sottospazio k-dimensionale di $(\mathbb{F}_q)^j$.

Riassumendo, il coefficiente di X^k nel prodotto a sinistra in (4.4) è

$$\sum_{0\leqslant i_1<\cdots<i_k\leqslant j-1} q^{i_1+\cdots+i_k}$$

che è il numero di possibili scelte dei vettori γ_i. D'altra parte questo numero è

$$q^{\binom{k}{2}}\cdot \#\{\text{possibili matrici } \tilde{M}\}=q^{\binom{k}{2}}\binom{j}{k}_q$$

che è proprio il coefficiente di X^k nell'espressione a destra in (4.4). □

4.3 Introduzione al *cyclic sieving phenomenon*

Sia X un insieme qualsiasi. Non c'è una definizione univoca di "q-analogo per X"; diremo che un'espressione parametrica $X(q)$ è un q-analogo per X se

$$\lim_{q\to 1} X(q)=\#(X).$$

In quest'introduzione al *cyclic sieving phenomenon* considereremo un esempio specifico: siano $[n]:=\{1,\dots,n\}$ e $X:=\wp_k([n])$ l'insieme delle parti di $[n]$ di cardinalità k. Per quanto visto precedentemente,

$$X(q):=\binom{n}{k}_q$$

è un q-analogo per X. Quello che ci chiediamo è: il q-analogo ha anche un significato combinatorio? In altre parole, ritornando per un momento a un insieme X generico, è possibile scrivere

$$X(q)=\sum_{x\in X} q^{s(x)}$$

dove $s\colon X\to\mathbb{N}$ è una qualsiasi funzione che assegna un numero naturale agli elementi di X, in modo che lo stesso valore venga assunto da elementi che

condividono determinate proprietà combinatorie?[2] In tal caso il coefficiente di q^n in $X(q)$ restituisce $\#\{x \in X \mid s(x) = n\}$.

Per $X = \wp_k([n])$ la risposta è affermativa, come vediamo nella seguente proposizione.

Proposizione 4.9. *Sia*

$$\begin{array}{rccc} s : \wp_k([n]) & \longrightarrow & \mathbb{N} \\ A & \longmapsto & \mathrm{sum}(A) - \binom{k+1}{2} \end{array}$$

dove $\mathrm{sum}(A)$ *è la somma di tutti gli elementi di* A.[3] *Allora*

$$\binom{n}{k}_q = \sum_{A \in \wp_k([n])} q^{s(A)}.$$

Dimostrazione. Come abbiamo visto nella dimostrazione del Teorema 4.8,

$$q^{\binom{k}{2}} \binom{n}{k}_q = \sum_{0 \leqslant i_1 < \cdots < i_k \leqslant n-1} q^{i_1 + \cdots + i_k} = (*)$$

e la somma a destra è estesa su tutti i sottoinsiemi di cardinalità k in $\{0, \ldots, n-1\}$. Aggiungere 1 a ogni elemento dà una corrispondenza biunivoca con i sottoinsiemi $A \in \wp_k([n])$, dunque

$$(*) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} q^{(i_1 - 1) + \cdots + (i_k - 1)} = \left(\sum_{A \in \wp_k([n])} q^{\mathrm{sum}(A)} \right) q^{-k}.$$

Portando a destra il fattore $q^{\binom{k}{2}}$ si ha la tesi. □

Possiamo allora concludere che $X(q)$ è un polinomio di $\mathbb{Z}[q]$ con coefficienti positivi.[4] Vediamo un esempio concreto: scegliamo $n = 4$ e $k = 2$, cioè $X = \wp_2(\{1, 2, 3, 4\})$. In questo caso

$$X(q) = \binom{4}{2}_q = \frac{(4)_q (3)_q}{(2)_q (1)_q} = \frac{(q^3 + q^2 + q + 1)(q^2 + q + 1)}{q + 1} = q^4 + q^3 + 2q^2 + q + 1.$$

Questo q-analogo in realtà contiene molte più informazioni di quanto sembri. Sia ζ una radice quarta primitiva dell'unità (per esempio, $\zeta = i$) e valutiamo $X(q)$ in ζ^j per $j = 0, 1, 2, 3$:

[2] In questo contesto la funzione s prende il nome di *statistica* su X.

[3] Osserviamo che $\binom{k+1}{2}$ è il minimo valore che può assumere la funzione sum, ottenuto per $A = \{1, \ldots, k\}$.

[4] In realtà questo fatto discende direttamente dalla Proposizione 4.6.

- $X(i^0) = X(1) = 6$;
- $X(i^1) = X(i) = 0$;
- $X(i^2) = X(-1) = 2$;
- $X(i^3) = X(-i) = 0$.

Avendo ottenuto numeri interi positivi (o nulli), è naturale chiedersi se anche questa valutazione abbia un significato combinatorio.

Consideriamo il 4-ciclo $c := (1234) \in \mathcal{S}_4$ e il gruppo ciclico da esso generato $C := \langle c \rangle$. Il gruppo C agisce naturalmente su $X = \wp_2(\{1,2,3,4\})$.

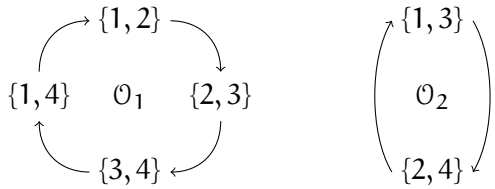


Figura 4.1: Orbite dell'azione dell'elemento c su X.

A partire dalla Figura 4.1, possiamo contare il numero di elementi di X che sono lasciati fissi da c^i, per $i = 0, 1, 2, 3$:

- l'identità c^0 lascia fissi tutti e sei gli elementi;
- c^1 non fissa alcun elemento;
- c^2 fissa i due elementi dell'orbita $\mathcal{O}_2$ in Figura 4.1;
- infine, c^3 sposta tutti gli elementi di X.

Osserviamo che il numero di elementi fissati da c^i è uguale al valore di $X(\zeta^i)$. Questo fenomeno si manifesta in situazioni anche molto diverse tra loro, tanto da meritare un nome: diciamo che in tal caso la terna $(X, X(q), C)$ manifesta il *cyclic sieving phenomenon* (CSP).

In presenza di CSP dal q-analogo $X(q)$ possiamo ricavare ulteriori informazioni. Consideriamo infatti gli stabilizzatori delle orbite[5] $\mathcal{O}_1$ e $\mathcal{O}_2$, che sono

[5] Per una generica azione $G \times X \to X$, lo stabilizzatore di un'orbita $\mathcal{O}$ è il sottogruppo $\mathcal{S}tab(\mathcal{O}) := \{g \in G \mid g \cdot x = x \text{ per ogni } x \in \mathcal{O}\}$, cioè è l'intersezione di tutti gli stabilizzatori degli elementi dell'orbita. Notiamo che se G è abeliano $\mathcal{S}tab(x) = \mathcal{S}tab(y)$ per ogni x, y che appartengano alla stessa orbita, quindi in questo caso $\mathcal{S}tab(\mathcal{O}) = \mathcal{S}tab(x)$ per un qualsiasi $x \in \mathcal{O}$.

rispettivamente $\mathcal{S}\mathrm{tab}(\mathcal{O}_1) = \{\mathrm{Id}\}$ e $\mathcal{S}\mathrm{tab}(\mathcal{O}_2) = \{\mathrm{Id}, (13)(24)\}$. Riduciamo $X(q)$ modulo $q^4 - 1$: si ha

$$X(q) \equiv 2 + q + 2q^2 + q^3 \pmod{q^4 - 1}.$$

Anche i coefficienti di questo nuovo polinomio hanno un significato combinatorio:

- il termine noto (coefficiente di q^0) conta il numero di orbite il cui stabilizzatore ha ordine che divide 0 (tutte le orbite);
- il coefficiente di q^1 conta il numero di orbite il cui stabilizzatore ha ordine che divide 1 (che è solo $\mathcal{O}_1$);
- il coefficiente di q^2 conta il numero di orbite il cui stabilizzatore ha ordine che divide 2 (entrambe le orbite);
- il coefficiente di q^3 conta il numero di orbite il cui stabilizzatore ha ordine che divide 3 (anche in questo caso solo $\mathcal{O}_1$).

Per poter dare una spiegazione più profonda al *cyclic sieving phenomenon*, dobbiamo dare qualche nozione di teoria delle rappresentazioni di un gruppo finito.

4.4 Cenni di teoria delle rappresentazioni

06/05/2015 ◃ Nella sezione precedente abbiamo dato un nome alla strana relazione tra il q-analogo di un insieme X e l'azione di un gruppo ciclico su X. Questo fenomeno può sembrare una coincidenza; vediamo qui che la teoria delle rappresentazioni permette di dare una *buona dimostrazione* della comparsa del CSP. In alcuni casi, tuttavia, è dimostrato che si manifesta il CSP ma ancora non è nota questa "buona dimostrazione".

4.4.1 Definizione e primi risultati

Iniziamo proprio con la definizione di rappresentazione di un gruppo. Laddove non diversamente specificato, supporremo sempre che G sia un gruppo *finito*.

Definizione 4.10. Sia G un gruppo (finito). Una *rappresentazione (finita)* di G è una coppia (V, ρ) dove V è un $\mathbb{C}$-spazio vettoriale di dimensione finita e $\rho\colon G \to \mathsf{GL}(V)$ è un omomorfismo di gruppi.

Spesso, quando la mappa ρ è implicita nel contesto, si dice che V stesso è una rappresentazione di G, o G-rappresentazione; inoltre, è ben definita un'azione di G su V, indicata con $g \cdot \boldsymbol{v}$, data da

$$\begin{array}{ccc} G \times V & \longrightarrow & V \\ (g, \boldsymbol{v}) & \longmapsto & \rho(g)(\boldsymbol{v}) \end{array}$$

e per questo si dice anche che V è un G-*modulo*.

Definizione 4.11. Date V e W rappresentazioni di G, un *omomorfismo di rappresentazioni* è una mappa lineare $\varphi\colon V \to W$ tale che $\varphi(g \cdot \boldsymbol{v}) = g \cdot \varphi(\boldsymbol{v})$ per ogni $\boldsymbol{v} \in V$ e per ogni $g \in G$. Indichiamo con $\mathcal{H}om_G(V, W)$ l'insieme degli omomorfismi di G-rappresentazioni.

Definizione 4.12. Una G-*sottorappresentazione* (o G-*sottomodulo*) di una G-rappresentazione V è un sottospazio lineare $U \subseteq V$ tale che $g \cdot U \subseteq U$ per ogni $g \in G$.

Definizione 4.13. Data una G-rappresentazione V, esistono sempre le *sottorappresentazioni banali* $\{0\}$ e V; $V \neq \{0\}$ si dice *rappresentazione irriducibile* se non ha sottorappresentazioni non banali.

Esempio 4.2. L'azione di $\mathcal{S}_3$ su $\mathbb{C}^3$ data dalla permutazione delle coordinate induce una rappresentazione non irriducibile di $\mathcal{S}_3$: la retta $\langle (1,1,1) \rangle$ è una sottorappresentazione non banale.

Teorema 4.14. *Ogni* G*-rappresentazione* V *si decompone come somma diretta di rappresentazioni irriducibili.*

Dimostrazione. Sia $W \subseteq V$ una sottorappresentazione; abbiamo concluso se riusciamo a trovare un sottospazio W' tale che $W \oplus W' = V$ e che sia anch'esso una sottorappresentazione, cioè tale che $g \cdot W' \subseteq W'$ per ogni $g \in G$. In tal caso avremmo concluso procedendo per induzione sulla dimensione di V.

Sia $H_0(\cdot, \cdot)$ un qualsiasi prodotto hermitiano su V e sia

$$H(\boldsymbol{v}, \boldsymbol{w}) := \frac{1}{\#(G)} \sum_{g \in G} H_0(g \cdot \boldsymbol{v}, g \cdot \boldsymbol{w}).$$

Poiché G è un gruppo finito, anche $H(\cdot, \cdot)$ è un prodotto hermitiano. Inoltre H è G-*invariante*, cioè per ogni $g \in G$ vale che $H(g \cdot \boldsymbol{v}, g \cdot \boldsymbol{w}) = H(\boldsymbol{v}, \boldsymbol{w})$. Di conseguenza, ponendo

$$W' := W^{\perp} = \{\boldsymbol{v} \in V \mid H(\boldsymbol{v}, \boldsymbol{w}) = 0 \text{ per ogni } \boldsymbol{w} \in W\},$$

si ha che $W \oplus W' = V$ e W' è una sottorappresentazione, in quanto per ogni $\mathbf{u} \in W'$, $\boldsymbol{w} \in W$ e $g \in G$ si ha che

$$H(\boldsymbol{w}, g \cdot \mathbf{u}) = H(g^{-1} \cdot \boldsymbol{w}, \mathbf{u}) = 0$$

dato che $g^{-1} \cdot \boldsymbol{w} \in W$. □

Nel teorema precedente è necessario che G sia un gruppo finito. Come controesempio, consideriamo la rappresentazione del gruppo additivo

$$\begin{array}{rcl} \rho : \mathbb{R} & \longrightarrow & GL_2(\mathbb{C}) \\ r & \longmapsto & \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}. \end{array}$$

La rappresentazione *non* è irriducibile, in quanto $W := \langle (1, 0) \rangle$ è una sottorappresentazione non banale. D'altra parte, se esistesse U sottorappresentazione di dimensione 1 tale che $W \oplus U = \mathbb{C}^2$, per ogni r essa sarebbe un autospazio per $\rho(r)$ (che dunque risulterebbe sempre diagonalizzabile), ma $\rho(1)$ è in forma di Jordan e non è diagonalizzabile.

Vediamo com'è la situazione nel caso che ci interessa, cioè le rappresentazioni dei gruppi ciclici. Sia C_n un gruppo ciclico di ordine n generato da c. Naturalmente $\rho(c)^n = \mathrm{Id}$, quindi il polinomio minimo di $\rho(c)$ divide $T^n - 1$ che ha radici distinte; dunque $\rho(c)$ è diagonalizzabile ed ha radici n-esime dell'unità come autovalori.

Ora, C_n è abeliano e finito, quindi tutti i suoi elementi $\rho(c^i)$ sono simultaneamente diagonalizzabili. Scegliendo questa base comune di autovettori per la rappresentazione V, deduciamo che

$$V = \bigoplus_{\substack{W \text{ autospazio} \\ \text{per } \rho(c)}} W,$$

i quali autospazi hanno dimensione 1 e sono irriducibili.[6] Dunque abbiamo trovato almeno n rappresentazioni irriducibili (di dimensione 1) per C_n, della forma $(\mathbb{C}, \rho^{(\ell)})$ in cui

$$\rho^{(\ell)} \colon c \mapsto \zeta^\ell \, \mathrm{Id}$$

dove ζ è una radice primitiva n-esima dell'unità. Vedremo a breve che queste sono tutte e sole le rappresentazioni irriducibili di C_n.

[6] Questo ragionamento si può generalizzare a un qualunque gruppo abeliano finito.

4.4.2 Costruire nuove rappresentazioni

A partire da G-rappresentazioni se ne possono costruire altre usando le comuni operazioni sugli spazi vettoriali. Le verifiche di buona definizione di tutte queste costruzioni saranno omesse.

- Se V e W sono G-rappresentazioni, allora anche $V \oplus W$ è una G-rappresentazione con l'azione $g \cdot (\boldsymbol{v}, \boldsymbol{w}) := (g \cdot \boldsymbol{v}, g \cdot \boldsymbol{w})$.
- Analogamente, $V \otimes W$ è una G-rappresentazione in cui l'azione su un elemento della base è $g \cdot (\boldsymbol{v} \otimes \boldsymbol{w}) := (g \cdot \boldsymbol{v}) \otimes (g \cdot \boldsymbol{w})$.
- Se V è una rappresentazione, il duale V^* è una rappresentazione con la mappa $(g \cdot \varphi)\colon \boldsymbol{v} \mapsto \varphi(g^{-1} \cdot \boldsymbol{v})$. Il motivo per cui compare g^{-1} anziché g è che in questo modo il *pairing*

$$\begin{array}{rcl} \langle \cdot, \cdot \rangle : V^* \times V & \longrightarrow & \mathbb{C} \\ (\varphi, \boldsymbol{v}) & \longmapsto & \langle \varphi, \boldsymbol{v} \rangle = \varphi(\boldsymbol{v}) \end{array}$$

  è G-invariante, cioè $\langle g \cdot \varphi, g \cdot \boldsymbol{v} \rangle = \langle \varphi, \boldsymbol{v} \rangle$. Osserviamo che se $\rho\colon G \to \mathsf{GL}(V)$ è la G-rappresentazione di partenza e $\rho^*\colon G \to \mathsf{GL}(V^*)$ è quella appena costruita, allora $\rho^*(g) = (\rho(g^{-1}))^T$.
- L'algebra simmetrica $S^k V$ e l'algebra esterna $\Lambda^k V$ sono G-rappresentazioni con le rispettive azioni (definite sulle basi) $g \cdot (\boldsymbol{v}_1 \odot \cdots \odot \boldsymbol{v}_k) = (g \cdot \boldsymbol{v}_1) \odot \cdots \odot (g \cdot \boldsymbol{v}_k)$ e $g \cdot (\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_k) = (g \cdot \boldsymbol{v}_1) \wedge \cdots \wedge (g \cdot \boldsymbol{v}_k)$.
- Dal momento che la mappa

$$\begin{array}{rcl} V^* \otimes W & \longrightarrow & \mathcal{H}om(V, W) \\ f \otimes \boldsymbol{w} & \longmapsto & (\boldsymbol{v} \mapsto f(\boldsymbol{v})\boldsymbol{w}) \end{array}$$

  è un isomorfismo di $\mathbb{C}$-spazi vettoriali, se V e W sono G-rappresentazioni, anche $\mathcal{H}om(V, W)$ lo è, con l'azione

$$(g \cdot \varphi)\colon \boldsymbol{v} \mapsto g \cdot \varphi(g^{-1} \cdot \boldsymbol{v})$$

  coerentemente con i punti precedenti.
- Se $\varphi\colon V \to W$ è un omomorfismo di rappresentazioni, allora $\ker(\varphi)$, $\mathrm{Im}(\varphi)$ e $\mathrm{coker}(\varphi)$ sono rappresentazioni; in particolare $\ker(\varphi)$ è una sottorappresentazione di V e $\mathrm{Im}(\varphi)$ è una sottorappresentazione di W.

Un'altra rappresentazione di G che useremo in seguito può essere definita a partire da un'azione di G su un certo insieme X.

Definizione 4.15. Supponiamo che G agisca su un insieme finito X. Il $\mathbb{C}$-spazio vettoriale libero generato dagli elementi di X è una G-rappresentazione, detta *rappresentazione di permutazione* ed indicata con $\mathbb{C}X$, con l'azione definita sugli elementi della base $g \cdot \boldsymbol{v}_x := \boldsymbol{v}_{g\cdot x}$ per ogni $x \in X$.

4.4.3 Il Lemma di Schur

Abbiamo visto che ogni rappresentazione di un gruppo finito si decompone in somma diretta di sottorappresentazioni irriducibili. Cosa possiamo dire sull'unicità di questa decomposizione?

Lemma 4.16 (Schur)**.** *Sia $\varphi\colon V \to W$ un omomorfismo di G-rappresentazioni irriducibili. Allora*

1. *$\varphi = 0$ oppure φ è un isomorfismo;*
2. *se $V = W$, allora $\varphi = \lambda\,\mathrm{Id}$ per un opportuno $\lambda \in \mathbb{C}$.*

Dimostrazione. Il nucleo $\ker(\varphi)$ è una sottorappresentazione di V, quindi per irriducibilità si ha $\ker(\varphi) = V$ (cioè φ è la mappa nulla) oppure $\ker(\varphi) = \{0\}$, cioè φ è iniettiva. In questo secondo caso $\mathrm{Im}(\varphi) \neq \{0\}$, dunque, sempre per irriducibilità, $\mathrm{Im}(\varphi) = W$, cioè φ è anche suriettiva.

Per il secondo punto, sia $\lambda \in \mathbb{C}$ un autovalore per φ. Allora la mappa $\varphi - \lambda\,\mathrm{Id}\colon V \to V$ non può essere un isomorfismo, perché l'autovettore relativo a λ viene mandato in 0. Per il punto precedente $\varphi - \lambda\,\mathrm{Id} = 0$. □

Corollario 4.17. *Sia V una G-rappresentazione tale che*

$$V = V_1^{\oplus k_1} \oplus \cdots \oplus V_r^{\oplus k_r}$$

in cui ciascun V_i è irriducibile e $V_i^{\oplus k_i} := V_i \oplus \cdots \oplus V_i$ ripetuto k_i volte. Allora sono univocamente determinati i fattori V_i, i numeri k_i e i sottospazi $V_i^{\oplus k_i}$.

Per una dimostrazione del corollario, si veda [3]. Nel caso del gruppo ciclico C_n, non è necessario scomodare il Lemma di Schur per ottenere il corollario: sappiamo già che V si spezza negli autospazi del generatore del gruppo.

4.4.4 Caratteri

Per studiare le rappresentazioni è comodo definire il concetto di carattere di una rappresentazione.

Definizione 4.18. Sia (V, ρ) una rappresentazione di G. Si definisce *carattere* di V la funzione

$$\begin{aligned} \chi_V : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \mathrm{tr}(\rho(g)). \end{aligned}$$

Come vedremo tra poco, anche se a prima vista sembra che nel carattere di una rappresentazione ci siano meno informazioni (abbiamo solamente le tracce delle immagini degli elementi di G), esso determina completamente una rappresentazione.

Proposizione 4.19. *Siano V e W* G*-rappresentazioni. Allora*

1. $\chi_{V\oplus W} = \chi_V + \chi_W$;
2. $\chi_{V\otimes W} = \chi_V\chi_W$;
3. $\chi_{V^*} = \overline{\chi_V}$ *(complesso coniugato).*

Dimostrazione. Supponiamo che la mappa associata a V sia ρ_1 e quella associata a W sia ρ_2. Inoltre chiamiamo le mappe associate a $V \oplus W$, $V \otimes W$ e V^* rispettivamente $\rho_\oplus$, $\rho_\otimes$ e ρ^*.

1. È possibile scegliere una base di $V \oplus W$ in modo che la matrice $\rho_\oplus(g)$ sia diagonale a blocchi della forma
$$\begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$
Segue facilmente che
$$\chi_{V\oplus W}(g) = \operatorname{tr}(\rho_\oplus(g)) = \operatorname{tr}(\rho_1(g)) + \operatorname{tr}(\rho_2(g)) = \chi_V(g) + \chi_W(g).$$

2. Analogamente al punto precedente, possiamo scegliere una base di $V \otimes W$ in modo che la matrice $\rho_\otimes(g)$ sia il prodotto di Kronecker di $\rho_1(g)$ e $\rho_2(g)$, ed è noto che per due generiche matrici A e B vale $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$.[7]

3. Sappiamo che $\rho^*(g) = (\rho_1(g^{-1}))^T$. Osserviamo inoltre che se $g \in G$ ha ordine n, allora $\rho_1(g)^n = \rho_1(g^n) = \mathrm{Id}$; dunque gli autovalori di $\rho_1(g)$ sono radici n-esime dell'unità.[8] Ora, $\operatorname{sp}(\rho^*(g)) = \operatorname{sp}(\rho_1(g^{-1})) = \{\lambda^{-1} \mid \lambda \in \operatorname{sp}(\rho_1(g))\}$ e $\lambda^{-1} = \overline{\lambda}$ perché radice dell'unità; in conclusione
$$\chi_{V^*}(g) = \operatorname{tr}((\rho_1(g^{-1}))^T) = \sum_{\lambda\in\operatorname{sp}(\rho_1(g))} \lambda^{-1} =$$
$$= \sum_{\lambda\in\operatorname{sp}(\rho_1(g))} \overline{\lambda} = \overline{\sum_{\lambda\in\operatorname{sp}(\rho_1(g))} \lambda} = \overline{\chi_V(g)}. \qquad \square$$

[7] In effetti si può dimostrare che $\operatorname{sp}(A \otimes B) = \{\lambda\mu \mid \lambda \in \operatorname{sp}(A),\ \mu \in \operatorname{sp}(B)\}$.
[8] In generale è vero che se $A \in \mathcal{M}_n(\mathbb{K})$ e $p(X) \in \mathbb{K}[X]$, allora $\operatorname{sp}(p(A)) = \{p(\lambda) \mid \lambda \in \operatorname{sp}(A)\}$.

Proposizione 4.20. *Sia* V *la* G*-rappresentazione di permutazione per un insieme* X*. Allora*

$$\chi_V(g) = \#\{x \in X \mid g \cdot x = x\}.$$

Dimostrazione. La matrice che rappresenta $\rho(g)$ rispetto alla base $(\boldsymbol{v}_x \mid x \in X)$ è una matrice di permutazione, cioè una matrice in cui in ogni riga e in ogni colonna è presente esattamente un 1 (e 0 altrove).[9] La traccia di questa matrice è allora il numero di 1 presenti sulla diagonale, cioè il numero di $x \in X$ tali che $\boldsymbol{v}_{g\cdot x} = \boldsymbol{v}_x$. □

Sia V una G-rappresentazione. Seguendo una notazione standard, denoteremo con V^G i vettori fissi rispetto all'azione di G su V, cioè

$$V^G := \{\boldsymbol{v} \in V \mid g \cdot \boldsymbol{v} = \boldsymbol{v} \text{ per ogni } g \in G\}.$$

Teorema 4.21. *Sia* V *una* G*-rappresentazione e sia* $\varphi \in \mathsf{GL}(V)$ *definito da*

$$\varphi := \frac{1}{\#(G)} \sum_{g \in G} \rho(g). \tag{4.5}$$

È immediato verificare che $\varphi \colon V \to V$ *è un omomorfismo di rappresentazioni. In realtà* φ *è la proiezione di* V *su* V^G*, cioè vale che*

- $\varphi(\boldsymbol{v}) \in V^G$ *per ogni* $\boldsymbol{v} \in V$*;*
- $\varphi(\boldsymbol{w}) = \boldsymbol{w}$ *per ogni* $\boldsymbol{w} \in V^G$*.*

Dimostrazione. Sia $\varphi(\boldsymbol{v}) \in \mathrm{Im}(\varphi)$ e verifichiamo che $h \cdot \varphi(\boldsymbol{v}) = \varphi(\boldsymbol{v})$ per ogni $h \in G$. Il conto è presto fatto:

$$h \cdot \varphi(\boldsymbol{v}) = h \cdot \left(\frac{1}{\#(G)} \sum_{g \in G} g \cdot \boldsymbol{v} \right) = \frac{1}{\#(G)} \sum_{g \in G} (hg) \cdot \boldsymbol{v} = \varphi(\boldsymbol{v})$$

in cui l'ultima uguaglianza segue dal fatto che $\{hg \mid g \in G\} = G$ per ogni $h \in G$.

D'altra parte, se $g \cdot \boldsymbol{w} = \boldsymbol{w}$ per ogni $g \in G$, si ha

$$\varphi(\boldsymbol{w}) = \frac{1}{\#(G)} \sum_{g \in G} g \cdot \boldsymbol{w} = \frac{1}{\#(G)} \sum_{g \in G} \boldsymbol{w} = \frac{\#(G)}{\#(G)} \boldsymbol{w} = \boldsymbol{w}.$$ □

Corollario 4.22. *Si ha che* $\dim(V^G) = \mathrm{tr}(\varphi)$.

[9] Più precisamente, data una permutazione σ, la matrice Π_σ ha un 1 nel posto (i, j) se e solo se $\sigma(i) = j$ (e 0 altrove).

Dimostrazione. In una base opportuna di V ottenuta estendendo una base di V^G possiamo scrivere la matrice associata a φ come una matrice di proiezione

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

da cui la tesi segue immediatamente. □

Se a questo punto applichiamo l'operatore traccia ad ambo i membri dell'Equazione (4.5), ricordando che la traccia è lineare, otteniamo la *formula di proiezione*

$$\operatorname{tr}(\varphi) = \frac{1}{\#(G)} \sum_{g \in G} \chi_V(g).$$

Applichiamo quanto visto finora alla rappresentazione $\mathcal{H}om(V, W)$. Per prima cosa chiediamoci: chi sono i punti fissi $\mathcal{H}om(V, W)^G$?

Proposizione 4.23. *Si ha che $\mathcal{H}om(V, W)^G$ sono gli omomorfismi lineari da V in W che sono anche omomorfismi di rappresentazioni; in altre parole*

$$\mathcal{H}om(V, W)^G = \mathcal{H}om_G(V, W).$$

Dimostrazione. Ricordiamo che l'azione di G su $\mathcal{H}om(V, W)$ è data da

$$(g \cdot \varphi) \colon \boldsymbol{v} \mapsto g \cdot \varphi(g^{-1} \cdot \boldsymbol{v})$$

Sia $\varphi \in \mathcal{H}om(V, W)^G$. Allora $g \cdot \varphi = \varphi$ per ogni $g \in G$, cioè per ogni $\boldsymbol{v} \in V$

$$g \cdot \varphi(g^{-1} \cdot \boldsymbol{v}) = \varphi(\boldsymbol{v}).$$

Applicando g^{-1} da ambo le parti si ottiene

$$\varphi(g^{-1} \cdot \boldsymbol{v}) = g^{-1} \cdot \varphi(\boldsymbol{v})$$

questo vale per ogni $g \in G$, quindi $\varphi \in \mathcal{H}om_G(V, W)$. Rileggendo il tutto al contrario si ottiene il contenimento inverso. □

Dunque, per il Corollario 4.22, la formula di proiezione e la Proposizione 4.19 si ha

$$\dim(\mathcal{H}om_G(V, W)) = \dim(\mathcal{H}om(V, W)^G) = \frac{1}{\#(G)} \sum_{g \in G} \chi_{\mathcal{H}om(V,W)}(g) =$$

$$= \frac{1}{\#(G)} \sum_{g \in G} \chi_{V^* \otimes W}(g) = \frac{1}{\#(G)} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g).$$

Definizione 4.24. Definiamo lo spazio delle *funzioni di classe* come

$$\begin{aligned}\mathbb{C}_{cl}(G) &:= \{f\colon G \to \mathbb{C} \mid f \text{ è costante sulle classi di coniugio di } G\}\\ &= \{f\colon G \to \mathbb{C} \mid f(h^{-1}gh) = f(g) \text{ per ogni } g, h \in G\}.\end{aligned}$$

Ad esempio, i caratteri sono funzioni di classe, in quanto la traccia è invariante per similitudine e

$$\chi_V(h^{-1}gh) = \mathrm{tr}(\rho(h^{-1})\rho(g)\rho(h)) = \mathrm{tr}(\rho(h)^{-1}\rho(g)\rho(h)) = \mathrm{tr}(\rho(g)) = \chi_V(g).$$

Sullo spazio delle funzioni di classe mettiamo il prodotto hermitiano

$$\langle \alpha, \beta \rangle_G := \frac{1}{\#(G)} \sum_{g \in G} \overline{\alpha(g)}\beta(g).$$

Proposizione 4.25. *I caratteri delle rappresentazioni irriducibili sono ortonormali rispetto a* $\langle \cdot, \cdot \rangle_G$ *(a meno di isomorfismo).*

Dimostrazione. Siano V e W due rappresentazioni irriducibili. Per il Lemma di Schur si ha in alternativa

- se $V \simeq W$, allora $\dim(\mathcal{H}om_G(V, W)) = 1$, in quanto $\mathcal{H}om_G(V, W) = \{\lambda \mathrm{Id} \circ \psi \mid \lambda \in \mathbb{C}\}$ (se $\psi\colon V \to W$ è l'isomorfismo tra V e W);
- se $V \not\simeq W$, allora $\mathcal{H}om_G(V, W) = \{0\}$ e $\dim(\mathcal{H}om_G(V, W)) = 0$.

Per quanto visto sopra

$$\langle \chi_V, \chi_W \rangle_G = \dim(\mathcal{H}om_G(V, W)) = \begin{cases} 1 & \text{se } V \simeq W \\ 0 & \text{se } V \not\simeq W, \end{cases}$$

cioè χ_V e χ_W sono ortonormali. □

Corollario 4.26. *I caratteri delle rappresentazioni irriducibili sono linearmente indipendenti.*

Dimostrazione. Segue direttamente dall'ortonormalità: se $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k$ sono ortonormali e $a_1\boldsymbol{w}_1 + \cdots + a_k\boldsymbol{w}_k = 0$, allora

$$0 = \langle a_1\boldsymbol{w}_1 + \cdots + a_k\boldsymbol{w}_k, \boldsymbol{w}_i \rangle = a_i \langle \boldsymbol{w}_i, \boldsymbol{w}_i \rangle = a_i.$$ □

Corollario 4.27. *Il numero di* G*-rappresentazioni irriducibili è minore o uguale al numero di classi di coniugio in* G*.*

Dimostrazione. Osserviamo che $\dim(\mathbb{C}_{cl}(G)) = \#\{\text{classi di coniugio in } G\}$, perché una base è data dalle funzioni che valgono 1 su una fissata classe e 0 altrove. La tesi segue allora dal Corollario 4.26. □

In particolare, essendo il gruppo ciclico C_n abeliano, ci sono n classi di coniugio (ciascun elemento ne determina una) e all'inizio di questa sezione abbiamo trovato n rappresentazioni irriducibili (quelle della forma $(\mathbb{C}, \rho^{(\ell)})$ per $\ell = 0, \dots, n-1$), le quali dunque sono tutte e sole le rappresentazioni irriducibili di C_n.

In realtà si può dimostrare che il numero di rappresentazioni irriducibili è sempre uguale al numero di classi di coniugio, ma noi non lo faremo.

Corollario 4.28. *Ogni* G*-rappresentazione è univocamente determinata dal suo carattere.*

Dimostrazione. In base al Teorema 4.14, ogni rappresentazione V si spezza in somma diretta di rappresentazioni irriducibili, quindi ogni carattere χ_V si scrive come somma di caratteri di rappresentazioni irriducibili. Siano $W_1, \dots, W_r$ le rappresentazioni irriducibili di G e supponiamo che U, V siano due G-rappresentazioni tali che $\chi_U = \chi_V$. Possiamo allora scrivere

$$U = \bigoplus_{i=1}^{r} W_i^{\oplus h_i} \qquad \text{e} \qquad V = \bigoplus_{i=1}^{r} W_i^{\oplus k_i}$$

in cui alcuni degli h_i o dei k_i possono essere nulli. Dunque

$$\chi_U = \sum_{i=1}^{r} h_i \chi_{W_i} \qquad \text{e} \qquad \chi_V = \sum_{i=1}^{r} k_i \chi_{W_i}.$$

Ma per il Corollario 4.26 $\chi_U = \chi_V$ implica $h_i = k_i$ per ogni $i = 1, \dots, r$ e quindi $U \simeq V$. □

4.5 Il *cyclic sieving phenomenon*

Ora che abbiamo visto le prime nozioni di teoria delle rappresentazioni, possiamo dedicarci al *cyclic sieving phenomenon* e alla buona dimostrazione della sua presenza.

Sia X un insieme e supponiamo che il gruppo ciclico di ordine n C_n agisca su X. Sia $X(q)$ un q-analogo per X (nel senso visto nella Sezione 4.3). Sia inoltre $\omega \colon C_n \to \mu_n$ un isomorfismo fissato, dove μ_n è il sottogruppo moltiplicativo di $\mathbb{C}$ delle radici n-esime dell'unità.

Teorema 4.29 (Buona dimostrazione del CSP)**.** *Supponiamo di avere una* C_n*-rappresentazione* (A_X, ρ) *tale che* A_X *sia un* $\mathbb{C}$*-spazio vettoriale* graduato*, cioè per il quale esista una decomposizione in somma diretta*

$$A_X = \bigoplus_{i \in \mathbb{N}} A_{X,i}$$

con un numero finito di addendi. Siano inoltre X*,* $X(q)$ *e* ω *come sopra. Supponiamo che*

(a) $X(q) = \sum_{i \geqslant 0} \dim(A_{X,i}) q^i$;

(b) se $c \in C_n$ *è un generatore fissato,* $\rho(c)\big|_{A_{X,i}} = \omega(c)^i \,\mathrm{Id}$.

Sia infine $\mathbb{C}X$ *la* C_n*-rappresentazione di permutazione indotta dall'azione di* C_n *su* X. *Allora sono equivalenti:*

1. *per ogni* $\gamma \in C_n$, $X(\omega(\gamma)) = \#\{x \in X \mid \gamma \cdot x = x\}$;
2. *se* $X(q) \equiv a_0 + a_1 q + \cdots + a_{n-1} q^{n-1} \pmod{q^n - 1}$, *allora* a_ℓ *è il numero di orbite dell'azione di* C_n *su* X *il cui stabilizzatore ha ordine che divide* ℓ;
3. $A_X \simeq \mathbb{C}X$ *come* C_n*-rappresentazioni.*

Definizione 4.30. Diciamo che la terna $(X, X(q), C_n)$ esibisce il *cyclic sieving phenomenon* se vale una (e quindi tutte) delle condizioni precedenti.

Notiamo che il punto 1. era quello che avevamo definito *cyclic sieving phenomenon* nella Sezione 4.3; inoltre avevamo osservato il verificarsi del punto 2. nel caso di $X = \wp_2([4])$.

Il Teorema 4.29 vale in tutti i contesti in cui si manifesta il CSP e permette di dare una *buona dimostrazione* del singolo caso: se riusciamo a trovare uno spazio vettoriale A_X per cui valgano le ipotesi del teorema, abbiamo una dimostrazione della presenza del CSP garantita dalla teoria delle rappresentazioni. In altri casi abbiamo una "cattiva dimostrazione" del CSP, cioè riusciamo a dimostrarne la presenza per altre vie, senza trovare la rappresentazione A_X.

Dimostrazione del Teorema 4.29. $\boxed{1. \Leftrightarrow 3.}$ Sia $\gamma \in C_n$. Allora $X(\omega(\gamma))$ è il carattere $\chi_{A_X}(\gamma)$: infatti per il punto (b) si ha

$$\chi_{A_X}(\gamma) = \mathrm{tr}(\rho(\gamma)) = \sum_{i \geqslant 0} \mathrm{tr}\Big(\rho(\gamma)\big|_{A_{X,i}}\Big) = \sum_{i \geqslant 0} \dim(A_{X,i}) \omega(\gamma)^i$$

che per il punto (a) è uguale a $X(\omega(\gamma))$. D'altra parte per la Proposizione 4.20

$$\chi_{\mathbb{C}X}(\gamma) = \#\{x \in X \mid \gamma \cdot x = x\}.$$

La tesi segue dal Corollario 4.28, poiché $A_X \simeq \mathbb{C}X$ se e solo se $\chi_{A_X} = \chi_{\mathbb{C}X}$.
$\boxed{2. \Leftrightarrow 3.}$ Indichiamo con $\chi_{(\ell)}$ il carattere della rappresentazione irriducibile $\rho^{(\ell)}$ di C_n. Osserviamo che, per ortonormalità, se V è una C_n-rappresentazione qualsiasi, $\langle \chi_{(\ell)}, \chi_V \rangle_{C_n}$ è il numero di copie isomorfe a $\rho^{(\ell)}$ presente della decomposizione in rappresentazioni irriducibili di V. Dunque abbiamo che $A_X \simeq \mathbb{C}X$ se e solo se

$$\langle \chi_{(\ell)}, \chi_{A_X} \rangle_{C_n} = \langle \chi_{(\ell)}, \chi_{\mathbb{C}X} \rangle_{C_n} \quad \text{per ogni } \ell = 0, \ldots, n-1. \tag{4.6}$$

Siano ora a_ℓ come nel punto 2. Un semplice conto mostra che

$$a_\ell = \frac{1}{n} \sum_{\theta \in \mu_n} \theta^{-\ell} \chi(\theta).$$

Infatti ricordiamo che se ζ è una radice primitiva n-esima dell'unità, allora

$$\sum_{j=0}^{n-1} \zeta^{ij} = \begin{cases} n & \text{se } i = 0 \\ 0 & \text{altrimenti,} \end{cases}$$

dunque

$$\sum_{\theta \in \mu_n} \theta^{-\ell} \chi(\theta) = \sum_{j=0}^{n-1} \zeta^{-j\ell} \chi(\zeta^j) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \zeta^{-j\ell} a_i \zeta^{ij} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \zeta^{j(i-\ell)} = n a_\ell.$$

Ora osserviamo che $a_\ell = \langle \chi_{(\ell)}, \chi_{A_X} \rangle_{C_n}$, in quanto

$$\langle \chi_{(\ell)}, \chi_{A_X} \rangle_{C_n} = \frac{1}{n} \sum_{\gamma \in C_n} \overline{\chi_{(\ell)}(\gamma)} \chi_{A_X}(\gamma) = \frac{1}{n} \sum_{\gamma \in C_n} \omega(\gamma)^{-\ell} \chi(\omega(\gamma))$$

($\chi_{(\ell)}(\gamma) = \omega(\gamma)^\ell$, $\overline{\omega(\gamma)} = \omega(\gamma)^{-1}$ poiché radice dell'unità e $\chi_{A_X}(\gamma) = \chi(\omega(\gamma))$ per la prima parte della dimostrazione). D'altra parte, un'orbita $\mathcal{O}$ dell'azione di C_n su X dà origine a una sottorappresentazione di $\mathbb{C}X$, anzi

$$\mathbb{C}X = \bigoplus_{\mathcal{O} \text{ orbita}} \mathbb{C}\mathcal{O},$$

quindi

$$\langle \chi_{(\ell)}, \chi_{\mathbb{C}X} \rangle_{C_n} = \sum_{\mathcal{O} \text{ orbita}} \langle \chi_{(\ell)}, \chi_{\mathbb{C}\mathcal{O}} \rangle_{C_n}$$

e l'azione di c su un'orbita $\mathcal{O}$ con $\#(\mathcal{O}) = m$ è rappresentata dalla matrice di permutazione ciclica

$$\begin{pmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$$

(c manda il primo elemento nel secondo, il secondo nel terzo e così via). Riconoscendo in tale matrice la *companion* del polinomio $T^m - 1$, possiamo dedurre che c ha m autovalori distinti: tutte e sole le radici m-esime dell'unità, che in μ_n[10] sono

$$(\zeta^{n/m})^0, (\zeta^{n/m})^1, \ldots, (\zeta^{n/m})^{m-1}.$$

[10] Ricordiamo che comunque $\mathrm{sp}(c) \subseteq \mu_n \ldots$

Ma per la Formula (3.2) $n/m = \#(\mathcal{S}\mathrm{tab}\,\mathcal{O})$ e ne deduciamo che le sottorappresentazioni irriducibili presenti in $\mathbb{C}\mathcal{O}$ sono le $\rho^{(k)}$ tali che $\#(\mathcal{S}\mathrm{tab}\,\mathcal{O})$ divide k, cioè

$$\mathbb{C}\mathcal{O} = \bigoplus_{\#(\mathcal{S}\mathrm{tab}\,\mathcal{O})|k} \rho^{(k)}$$

e quindi

$$\langle \chi_{(\ell)}, \chi_{\mathbb{C}\mathcal{O}} \rangle_{C_n} = \begin{cases} 1 & \text{se } \#(\mathcal{S}\mathrm{tab}\,\mathcal{O}) \mid \ell \\ 0 & \text{altrimenti,} \end{cases}$$

da cui possiamo concludere che

$$\langle \chi_{(\ell)}, \chi_{\mathbb{C}X} \rangle_{C_n} = \#\{\mathcal{O} \text{ orbite di } X \text{ il cui stabilizzatore ha ordine che divide } \ell\}.$$

Dunque abbiamo dimostrato che vale il punto 2. se e solo se vale (4.6) e questo conclude la dimostrazione. □

11/05/2015 ◁ Vediamo un'applicazione concreta del Teorema 4.29. Sia C_n il gruppo ciclico di ordine n e supponiamo che agisca fedelmente su $[N] := \{1, \dots, N\}$. Quest'azione induce un omomorfismo iniettivo

$$\iota \colon C_n \hookrightarrow \mathsf{GL}_N(\mathbb{C})$$

dato dalla permutazione delle coordinate su $\mathbb{C}^N$. Ora, nella Sezione 4.4 abbiamo visto solamente rappresentazioni di gruppi finiti, ma non è difficile immaginarsi cosa sia una rappresentazione di un gruppo G qualunque; pertanto consideriamo una rappresentazione (V, ρ) di $\mathsf{GL}_N(\mathbb{C})$, o se si preferisce un omomorfismo

$$\rho \colon \mathsf{GL}_N(\mathbb{C}) \to \mathsf{GL}(V)$$

dove V è un $\mathbb{C}$-spazio vettoriale. Chiamiamo $\chi_\rho(x_1, \dots, x_N)$ il carattere di un qualsiasi elemento di $\mathsf{GL}_N(\mathbb{C})$ diagonalizzabile che abbia come autovalori (anche ripetuti) $x_1, \dots, x_N$. Tale carattere è ben definito in quanto la traccia è invariante per similitudine.

Osserviamo che, fissato ρ, abbiamo una C_n-rappresentazione data dalla composizione $\rho \circ \iota$:

$$C_n \hookrightarrow \mathsf{GL}_N(\mathbb{C}) \to \mathsf{GL}(V).$$

Definizione 4.31. Il gruppo ciclico C_n agisce *quasi liberamente* su $[N]$ se, vedendo $C_n < \mathcal{S}_N$, un generatore $c \in C_n$ ha una struttura in cicli alternativamente del tipo:

- a cicli di lunghezza n (quindi $N = an$ e C_n agisce liberamente su $\{1, \dots, N\}$);
- a cicli di lunghezza n e uno di lunghezza 1 (quindi $N = an + 1$).

Ad esempio, $c = (1\ 3\ 5\ 7\ 9)(2\ 4\ 6\ 8\ 10)$ genera un C_5 che agisce liberamente su $\{1,\dots,10\}$ e quasi liberamente su $\{1,\dots,11\}$ (lascia fisso 11).

Teorema 4.32. *Sia* C_n *un gruppo ciclico di ordine* n *che agisce quasi liberamente su* $[N]$. *Sia* $X := \wp_k([N])$. *Allora*

$$\left(X, \binom{N}{k}_q, C_n\right)$$

esibisce il CSP.

La dimostrazione di questo teorema sarà una *buona dimostrazione*, cioè costruiremo esplicitamente una rappresentazione A_X che verifichi le ipotesi del Teorema 4.29. Osserviamo che questo risultato è leggermente più generale dell'esempio considerato nella Sezione 4.3: in quel caso $N = n$ e $c = (1\ \cdots\ n)$. Il teorema precedente afferma che lo stesso risultato vale anche se C_n agisce su un insieme più grande, basta che lo faccia quasi liberamente.

Prima di dimostrare il Teorema 4.32, dobbiamo collegarci alla teoria delle rappresentazioni. Supponiamo che C_n agisca quasi liberamente su $[N]$ e, come sopra, consideriamo l'omomorfismo $\iota\colon C_n \to \mathsf{GL}_N(\mathbb{C})$. Sia (V,ρ) una $\mathsf{GL}_N(\mathbb{C})$-rappresentazione fissata e, sempre come sopra, consideriamo la C_n-rappresentazione $(V,\tilde{\rho})$ con $\tilde{\rho} = \rho \circ \iota$. Supponiamo che V abbia una base della forma $(\boldsymbol{v}_x \mid x \in X)$ con X insieme qualsiasi e supponiamo anche che C_n agisca su X con un'azione quasi libera tale che

$$\tilde{\rho}(\gamma)\colon \boldsymbol{v}_x \mapsto \omega(\gamma)^m \boldsymbol{v}_{\gamma\cdot x} \tag{4.7}$$

con $m \in \mathbb{Z}$ fissato (*indipendente da* γ *e* x), per ogni $\gamma \in C_n$ e per ogni $x \in X$. (Al solito, $\omega\colon C_n \to \mu_n$ è un isomorfismo fissato di C_n con le radici n-esime dell'unità.)

Consideriamo la C_n-rappresentazione $\rho^{(-m)} \otimes V$. Dato che $\rho^{(-m)}(\gamma)$ è la mappa che agisce come $\omega(\gamma)^{-m}\,\mathrm{Id}$, abbiamo che per costruzione $\rho^{(-m)} \otimes V$ è isomorfa alla rappresentazione di permutazione $\mathbb{C}X$. D'altra parte, essendo una rappresentazione di C_n, $\rho^{(-m)} \otimes V$ ammette una decomposizione della forma

$$\bigoplus_{i=0}^{n-1} (\rho^{(i)})^{\oplus k_i}.$$

Di conseguenza possiamo definire

$$A_X := \rho^{(-m)} \otimes V, \quad A_{X,i} := (\rho^{(i)})^{\oplus k_i} \quad \text{e} \quad X(q) := \sum_{i \geqslant 0} \dim(A_{X,i})\, q^i.$$

Per costruzione sono verificate le ipotesi del Teorema 4.29, quindi concludiamo che $(X, X(q), C_n)$ esibisce il CSP.

Proposizione 4.33. *Nelle stesse ipotesi e notazioni usate finora, abbiamo che*

$$X(\omega(\gamma)) = \chi_\rho(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1})\chi_{\rho^{(-m)}}(\gamma)$$

per ogni $\gamma \in C_n$.

Dimostrazione. Se C_n agisce quasi liberamente su $[N]$ (supponendo $N = an$ oppure $N = an + 1$), allora gli autovalori di $\iota(\gamma) \in \mathsf{GL}_N(\mathbb{C})$ sono

$$1, \omega(\gamma), \dots, \omega(\gamma)^{N-1}$$

non necessariamente tutti distinti. Infatti esiste una base di $\mathbb{C}^N$ rispetto alla quale $\iota(\gamma)$ è una matrice diagonale a blocchi formata da a blocchi $n \times n$ del tipo

$$\begin{pmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$$

ed eventualmente un piccolo "blocco" 1×1 con un 1 (se l'azione è quasi libera ma non libera). Di conseguenza il polinomio caratteristico $p(T)$ di $\iota(\gamma)$ è

$$(T^n - 1)^a \quad \text{oppure} \quad (T^n - 1)^a(T - 1).$$

Ma ora osserviamo che, poiché le radici di $T^n - 1$ sono $\omega(\gamma)^i$ per $i = 0, \dots, n-1$ e per ogni $j \in \mathbb{N}$ si ha che $\omega(\gamma)^j = \omega(\gamma)^{n+j}$, i due multiinsiemi

$$[\lambda \in \mathbb{C} \mid p(\lambda) = 0] \quad \text{e} \quad [\omega(\gamma)^i \mid i = 0, \dots, N-1]$$

sono uguali.

Dal momento che $A_X = \rho^{(-m)} \otimes V$, i loro caratteri devono essere uguali; quindi

$$\chi_{\rho^{(-m)} \otimes V}(\gamma) = \chi_{\rho^{(-m)}}(\gamma)\chi_\rho(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1})$$

dev'essere uguale a $\chi_{A_X}(\gamma)$, che, come abbiamo visto nella dimostrazione del Teorema 4.29, è uguale a $X(\omega(\gamma))$. □

Dimostrazione del Teorema 4.32. Sia $U := \mathbb{C}^N$ vista come rappresentazione (U, Id) di $\mathsf{GL}_N(\mathbb{C})$. Con le notazioni introdotte precedentemente $(U, \tilde{\rho})$ è una C_n-rappresentazione (con $\tilde{\rho} = \mathrm{Id} \circ \iota$). Sia $V := \Lambda^k U$ l'algebra esterna, che è una C_n-rappresentazione come abbiamo visto nella Sezione 4.4.2: se $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_N)$ è la base standard di $\mathbb{C}^N$, una base per V è data da

$$\boldsymbol{v}_S := \bigwedge_{i \in S} \boldsymbol{e}_i$$

al variare di $S \in \wp_k([N])$ e l'azione di C_n su V è data da

$$\rho(\gamma)\colon \boldsymbol{v}_S \mapsto \bigwedge_{i\in S} \tilde{\rho}(\gamma)(\boldsymbol{e}_i) = \bigwedge_{i\in S} \boldsymbol{e}_{\gamma\cdot i}.$$

Ovviamente C_n agisce anche su $X = \wp_k([N])$. Dimostreremo che l'azione indotta di C_n sui vettori $\boldsymbol{v}_S$ verifica

$$\gamma \cdot \boldsymbol{v}_S = \omega(\gamma)^{\binom{k}{2}} \boldsymbol{v}_{\gamma\cdot S} \tag{4.8}$$

cioè l'Equazione (4.7) con $m = \binom{k}{2}$. In tal caso, $X(q)$ costruito come sopra verifica

$$X(\omega(\gamma)) = \chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1})\omega(\gamma)^{-\binom{k}{2}}.$$

D'altra parte, per la Proposizione 4.9

$$\binom{N}{k}_q = q^{-\binom{k}{2}} \left(\sum_{S\in X} \frac{q^{\mathrm{sum}(S)}}{q^k} \right)$$

e quindi

$$\binom{N}{k}_{\omega(\gamma)} = \omega(\gamma)^{-\binom{k}{2}} \chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1}).$$

Per dimostrare quest'ultima uguaglianza ricordiamo che, se $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_N)$ è una base di U fatta da autovettori per $\iota(\gamma)$ (in cui $\boldsymbol{w}_i$ ha autovalore $\omega(\gamma)^{i-1}$), allora

$$\left(\bigwedge_{i\in S} \boldsymbol{w}_i \;\middle|\; S \in \wp_k([N]) \right)$$

è una base di V fatta da autovettori per $\rho(\gamma)$: infatti

$$\rho(\gamma)\left(\bigwedge_{i\in S} \boldsymbol{w}_i \right) = \bigwedge_{i\in S} \iota(\gamma)\boldsymbol{w}_i = \bigwedge_{i\in S} \omega(\gamma)^{i-1}\boldsymbol{w}_i = \left(\prod_{i\in S} \omega(\gamma)^{i-1} \right) \bigwedge_{i\in S} \boldsymbol{w}_i$$

dunque[11]

$$\chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1}) = \mathrm{tr}(\rho(\gamma)) = \sum_{S\in X} \prod_{i\in S} \omega(\gamma)^{i-1} = \sum_{S\in X} \omega(\gamma)^{\mathrm{sum}(S)-k}.$$

Da quello che abbiamo visto prima, allora, $(X, X(q), C_n)$ esibisce il CSP ed abbiamo appena mostrato che $\binom{N}{k}_q$ e $X(q)$ assumono gli stessi valori valutati in $\omega(\gamma)$. Ne deduciamo che $\left(X, \binom{N}{k}_q, C_n\right)$ esibisce il CSP.

[11] Osserviamo che il carattere $\chi_V(\gamma)$, vedendo (V, ρ) come C_n-rappresentazione, per quanto detto nella dimostrazione della Proposizione 4.33 è uguale a $\chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1})$.

Resta solo da dimostrare che vale l'Equazione (4.8). L'azione di C_n su V si spezza in sottorappresentazioni indotte dalle orbite dell'azione di C_n su X:

$$V = \bigoplus_{\mathcal{O} \text{ orbita in } X} V_{\mathcal{O}}$$

dove $V_{\mathcal{O}} = \langle \boldsymbol{v}_S \mid S \in \mathcal{O} \rangle$. Supponiamo che un'orbita $\mathcal{O}$ abbia stabilizzatore $\mathcal{S}tab(\mathcal{O}) = \langle c^{n/d} \rangle$ (ove $C_n = \langle c \rangle$): dato che $c^{n/d} \cdot S = S$ per ogni $S \in \mathcal{O}$, abbiamo che ogni vettore $\boldsymbol{v}_S$ è un autovettore per l'azione di $c^{n/d}$ e, dal momento che $\langle c^{n/d} \rangle \simeq C_d$, il rispettivo autovalore sarà una radice d-esima dell'unità. In altre parole, per ogni $S \in \mathcal{O}$ vale che

$$c^{n/d} \cdot \boldsymbol{v}_S = \omega(c^{n/d})^{m(S)} \boldsymbol{v}_S$$

con $m(S) \in \mathbb{Z}$ che dipende dall'elemento S. Abbiamo concluso se dimostriamo che per ogni orbita $\mathcal{O}$ e per ogni $S \in \mathcal{O}$ possiamo scegliere $m(S) = \binom{k}{2}$.

E qui arriva il conto. Scriviamo $S \in X = \wp_k([N])$ come $S = S_0 \sqcup S_1 \sqcup \cdots \sqcup S_b$ in cui $S_1, \ldots, S_b$ sono le intersezioni non vuote di S con i d-cicli[12] di $c^{n/d}$ e $S_0 = \varnothing$ oppure l'eventuale singoletto lasciato fisso da c. A seconda dei casi abbiamo $k = bd$ oppure $k = bd + 1$: infatti se $c^{n/d} \cdot S = S$, un d-ciclo di $c^{n/d}$ non disgiunto da S dev'esserne interamente contenuto. Ora, l'azione di $c^{n/d}$ su $\boldsymbol{v}_S$ è data da

$$c^{n/d} \cdot \boldsymbol{v}_S = c^{n/d} \cdot \left(\bigwedge_{i \in S} \boldsymbol{e}_i \right) = \bigwedge_{i \in S} \boldsymbol{e}_{c^{n/d} \cdot i} = \operatorname{sgn}(c^{n/d}|_S) \bigwedge_{i \in S} \boldsymbol{e}_i = (-1)^{b(d-1)} \boldsymbol{v}_S;$$

abbiamo finito se, detta $\zeta = \omega(c)$ una radice n-esima primitiva dell'unità, vale che

$$(\zeta^{n/d})^{\binom{k}{2}} = (-1)^{b(d-1)}.$$

Sicuramente $(\zeta^{n/d})^{\binom{k}{2}} = (\zeta^{n/d})^{\binom{bd}{2}}$: è ovvio se $k = bd$ e d'altra parte, se $k = bd + 1$,

$$\binom{k}{2} = \binom{bd+1}{2} = \binom{bd}{2} + \binom{bd}{1} = \binom{bd}{2} + bd$$

da cui

$$(\zeta^{n/d})^{\binom{k}{2}} = (\zeta^{n/d})^{\binom{bd}{2}} (\zeta^{n/d})^{bd} = (\zeta^{n/d})^{\binom{bd}{2}}.$$

Fattorizzando il polinomio $(T^d - 1)^b$ come

$$\prod_{i=0}^{bd-1} (T - (\zeta^{n/d})^i)$$

[12] Ovviamente, se c è formato da a n-cicli, allora $c^{n/d}$ è formato da an/d d-cicli...

ed uguagliando i termini noti di questa fattorizzazione, risulta

$$(-1)^{bd}(\zeta^{n/d})^{\binom{bd}{2}} = (-1)^b$$

e la tesi si ottiene moltiplicando ambo i membri per $(-1)^{bd}$ (notiamo che $(-1)^b(-1)^{bd} = (-1)^{b(d+1)} = (-1)^{b(d-1)}$). □

Esercizio. Siano C_n come sopra e X l'insieme dei multiinsiemi di $\{1, \dots, N\}$ di cardinalità k. Sia

$$X(q) := \binom{N+k-1}{k}_q.$$

Allora $(X, X(q), C_n)$ manifesta il CSP.

(Suggerimento. Procedendo in modo analogo al teorema precedente, scegliamo $U := \mathbb{C}^N$ e $V := S^k U$, l'algebra simmetrica. Risulterà

$$X(\omega(\gamma)) = \chi_V(1, \dots, \omega(\gamma)^{N-1}) = \binom{N+k-1}{k}_{\omega(\gamma)}$$

in cui quest'ultima uguaglianza è dovuta al fatto che, se $i \boldsymbol{v}_i \in \mathbb{C}^N$ sono gli autovettori rispetto all'azione del generatore c di C_n, allora un elemento $\gamma \in C_n$ agisce su un vettore $\boldsymbol{v}_{i_1} \odot \cdots \odot \boldsymbol{v}_{i_k}$ della base di $S^k U$ come

$$\gamma \cdot (\boldsymbol{v}_{i_1} \odot \cdots \odot \boldsymbol{v}_{i_k}) = \omega(\gamma)^{(i_1-1)+\cdots+(i_k-1)} \boldsymbol{v}_{i_1} \odot \cdots \odot \boldsymbol{v}_{i_k};$$

ma $(i_1 - 1) + \cdots + (i_k - 1)$ è una partizione in k parti in cui il massimo addendo può essere $N - 1$: per la Proposizione 4.6

$$\sum_{t \geqslant 0} p(N-1, k, t) q^t = \binom{N+k-1}{k}_q. \qquad \blacksquare)$$

4.6 Altri esempi di *cyclic sieving phenomenon*

Per concludere presentiamo, a titolo puramente informativo e senza dimostrazioni, qualche altra situazione in cui si manifesta il CSP.

4.6.1 CSP e poligoni

Questo è un caso in cui si manifesta il CSP, ma non è ancora nota una *buona dimostrazione* che passi per la teoria delle rappresentazioni.

Definizione 4.34. Una k-*dissezione* di un n-agono convesso (con i lati etichettati) è un modo di disegnare k diagonali senza intersecarle.

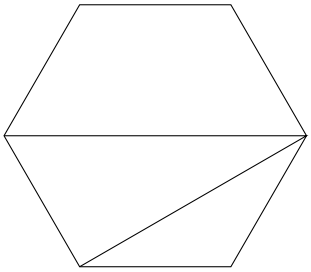


Figura 4.2: Esempio di 2-dissezione di un esagono.

Teorema 4.35. *Il numero di* k*-dissezioni di un* n*-agono è*

$$D_{n,k} := \frac{1}{k+1}\binom{n-3}{k}\binom{n+k-1}{k}.$$

I numeri $D_{n,k}$ prendono il nome di *numeri di Kirkman-Cayley*. In effetti la formula è stata congetturata da Kirkman nel 1857 e dimostrata da Cayley nel 1890 con tecniche basate sulle funzioni generatrici. È sorprendente che una dimostrazione diretta per biiezione si sia trovata solamente oltre un secolo dopo la congettura di Kirkman. Nell'Appendice B è possibile trovare i passaggi salienti di una dimostrazione per biiezione.

Osserviamo che se $k = n-3$, che è il massimo numero di diagonali tracciabili per un n-agono rispettando la regola di non intersezione,[13]

$$\begin{aligned} D_{n,n-3} &= \frac{1}{n-2}\binom{2n-4}{n-3} = \frac{1}{n-2}\frac{(2n-4)!}{(n-3)!(n-1)!} = \frac{(2n-4)!}{(n-2)!(n-1)!} = \\ &= \frac{1}{n-1}\frac{(2n-4)!}{(n-2)!(n-2)!} = \frac{1}{n-1}\binom{2n-4}{n-2} = c_{n-1} \end{aligned}$$

in cui i c_n sono i numeri di Catalan, in accordo con i risultati della Sezione 1.1.3.

Teorema 4.36. *Sia* X *l'insieme delle* k*-dissezioni di un* n*-agono convesso. Sia* $X(q)$ *il* q*-analogo di* $D_{n,k}$*, cioè*

$$X(q) := \frac{1}{(k+1)_q}\binom{n-3}{k}_q\binom{n+k-1}{k}_q.$$

Il gruppo ciclico C_n *agisce su* X *tramite rotazione dell'*n*-agono. Allora la terna* $(X, X(q), C_n)$ *manifesta il CSP.*

In [7], gli autori danno una dimostrazione per verifica diretta di questo teorema; ad oggi non si conosce una *buona dimostrazione*.

[13] Questo fatto è dimostrato nell'Appendice A.

4.6.2 Permutazioni regolari

Nel caso del nostro primo esempio, con $X = \wp_k([N])$ e $X(q) = \binom{N}{k}_q$, possiamo dare un'ulteriore interpretazione (e, in un certo senso, una *dimostrazione migliore* rispetto alla *buona dimostrazione*), considerando i gruppi finiti generati da riflessioni (ne abbiamo già parlato nella Sezione 2.6.1, a proposito del polinomio caratteristico di un arrangiamento di iperpiani). In effetti, il CSP è un fenomeno intrinseco nella struttura di $\mathcal{S}_N$, che è un gruppo generato dalle riflessioni rispetto agli iperpiani $H_{ij} := \{\mathbf{x} \in \mathbb{C}^N \mid x_i - x_j = 0\}$.

Definizione 4.37. Un elemento $\sigma \in \mathcal{S}_N$ è *regolare* se, visto come operatore lineare $\mathbb{C}^N \to \mathbb{C}^N$ che permuta le coordinate, ha un autovettore che non appartiene a nessuno degli iperpiani H_{ij}.

Ad esempio, $(1 \ \cdots \ N)$ è regolare in $\mathcal{S}_N$: il vettore

$$\begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{N-1} \end{pmatrix} \in \mathbb{C}^N,$$

dove ζ è una radice primitiva N-esima dell'unità, è un autovettore con ζ^{-1} come autovalore ed ha tutte le componenti distinte (quindi non appartiene ad alcun H_{ij}). Anche $(1 \ \cdots \ N-1)(N)$ è un elemento regolare, in quanto, se θ è una radice $(N-1)$-esima dell'unità,

$$\begin{pmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{N-2} \\ 0 \end{pmatrix} = \theta^{-1} \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{N-2} \\ 0 \end{pmatrix}.$$

Ora, come abbiamo visto nella Sezione 1.8, $\mathcal{S}_N$ agisce su $\mathbb{C}[X_1, \ldots, X_N]$ permutando le indeterminate e $\mathbb{C}[X_1, \ldots, X_N]^{\mathcal{S}_N}$ è generato da funzioni simmetriche. Sia $\{f_1, \ldots, f_N\}$ un tale insieme di generatori e consideriamo l'anello quoziente

$$A := \mathbb{C}[X_1, \ldots, X_N] / (f_1, \ldots, f_N).$$

Teorema 4.38 (Springer; Reiner, Stanton, White)**.** *Sia $c \in \mathcal{S}_N$ regolare di ordine n e sia $C = \langle c \rangle$ il gruppo ciclico generato da c. Sia $W < \mathcal{S}_N$ un sottogruppo qualunque. L'azione di permutazione di W su $\mathbb{C}[X_1, \ldots, X_N]$ si estende naturalmente al quoziente A (perché le f_i sono funzioni simmetriche), quindi possiamo considerare i punti fissi A^W. Siano ora $X := \mathcal{S}_N / W$ (come insieme di classi laterali: non ha struttura di gruppo)*

e $X(q)$ *il polinomio di Hilbert associato a* A^W *(la struttura graduata di* $\mathbb{C}[X_1, \dots, X_N]$ *si mantiene sia in* A *che in* A^W*). Allora la terna* $(X, X(q), C)$ *esibisce il CSP.*

Questo teorema è una *dimostrazione migliore* perché fa sì uso della *buona dimostrazione*, ma a differenza di quest'ultima (che si applica caso per caso) definisce un modo "automatico" per costruire lo spazio vettoriale richiesto dalla *buona dimostrazione* a partire da ipotesi più generali.

Vediamo come ricondurre il nostro $\mathscr{P}_k([N])$ in questo contesto. A un generico sottoinsieme $Y = \{y_1, \dots, y_k\} \in \mathscr{P}_k([N])$, $y_1 < \cdots < y_k$, è possibile associare una permutazione definita da

$$\left(\begin{array}{ccc|ccc} 1 & \cdots & k & k+1 & \cdots & N \\ y_1 & \cdots & y_k & x_1 & \cdots & x_{N-k} \end{array}\right),$$

in cui $\{x_1, \dots, x_{N-k}\} = [N] \setminus Y$, $x_1 < \cdots < x_{N-k}$, che è ben definita come rappresentante di una classe laterale di

$$\mathfrak{S}_N / (\mathfrak{S}_k \times \mathfrak{S}_{N-k})$$

Si ha dunque corrispondenza biunivoca tra questo quoziente e $\mathscr{P}_k([N])$, con le azioni di $\mathfrak{S}_N$ compatibili. Scegliendo $W = \mathfrak{S}_k \times \mathfrak{S}_{N-k}$ si ottiene una dimostrazione della presenza di CSP.

Concludiamo con una curiosità: Springer ha classificato le permutazioni regolari ed è risultato che sono tutte e sole quelle che si scrivono con a cicli di lunghezza n oppure a cicli di lunghezza n e un singoletto...

Capitolo 5

Teoria di Ramsey

Iniziamo con un esempio. In un gruppo di sei persone scelte a caso ce ne sono sempre tre che si conoscono tra loro, oppure tre che non si conoscono tra loro. Può sembrare un fatto strano, ma tra poco formalizzeremo questo enunciato e lo dimostreremo. ▹ *13/05/2015*

La teoria di Ramsey si occupa proprio di studiare problemi di questo tipo: stabilire quanto grande dev'essere una struttura affinché sia garantita l'esistenza di sottostrutture con determinate proprietà. L'esempio più semplice è il *principio dei cassetti*, o *pigeonhole principle*: se si hanno m piccionaie, occorre avere almeno $m+1$ piccioni da disporvi in modo che ci sia almeno una piccionaia che contenga almeno due piccioni.

5.1 I Teoremi di Ramsey

Possiamo rappresentare il problema introduttivo con un grafo completo su sei vertici (che rappresentano le persone) in cui gli archi sono colorati in due modi diversi, per esempio rosso/blu, a seconda che colleghino persone che si conoscono oppure no. La tesi è: per ogni possibile colorazione, esiste sempre un triangolo (cioè un grafo completo su tre vertici) rosso oppure un triangolo blu.

Vediamo la dimostrazione. Sia v un vertice qualsiasi; poiché il grafo è completo, esso è collegato a tutti gli altri 5 vertici. Non è possibile avere solo due archi di ciascun colore per due colori, quindi almeno tre di questi archi devono essere dello stesso colore. Senza perdita di generalità supponiamo che i vertici a, b e c siano collegati a v con un arco rosso. Ora,

- se almeno due tra i vertici a, b e c sono collegati da un arco rosso, questi due vertici e v formano un triangolo tutto rosso;
- altrimenti, i vertici a, b e c formano un triangolo blu.

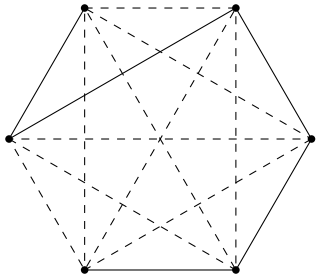


Figura 5.1: Esempio di possibile grafo delle conoscenze di sei persone.

Generalizzando, indichiamo con K_n il grafo completo su n vertici e supponiamo di avere una 2-colorazione degli archi. Ci chiediamo: dato un numero $s \in \mathbb{N}$, esiste un intero $n \in \mathbb{N}$, che dipende da s, tale che ogni grafo completo K_n contenga come sottografo una copia di K_s che sia monocromatica? (Nell'esempio precedente, $n = 6$ funziona per $s = 3$).

Definizione 5.1. Dati due numeri $s, t \in \mathbb{N}$, $s \geqslant 2$ e $t \geqslant 2$, definiamo *numero di Ramsey* relativo a s e t, e lo denotiamo con $R(s,t)$, il minimo $n \in \mathbb{N}$ tale che per ogni 2-colorazione del grafo completo K_n, esso contenga come sottografi un K_s del primo colore oppure un K_t del secondo.

Il nostro esempio dimostra che $R(3,3) \leqslant 6$ e la 2-colorazione in Figura 5.2 mostra che 6 è anche il minimo.

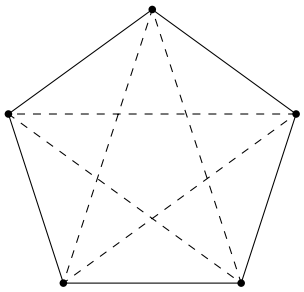


Figura 5.2: Una 2-colorazione di K_5 che non contiene triangoli monocromatici.

Al momento non sappiamo ancora se la definizione di $R(s,t)$ sia buona, cioè se $R(s,t)$ sia effettivamente un numero naturale finito.

Lemma 5.2. *Se esiste* $R(s,t)$*, allora esiste anche* $R(t,s)$ *e* $R(s,t) = R(t,s)$.

Dimostrazione. È sufficiente mostrare che, detta

$$p(n; s, t) := \text{“per ogni 2-colorazione } (K_n \supseteq K_s \text{ rosso}) \vee (K_n \supseteq K_t \text{ blu})\text{”},$$

allora si ha che per ogni s, t

$$\{n \mid p(n; s, t)\} = \{n \mid p(n; t, s)\}.$$

Sia n per cui valga $p(n; s, t)$ e consideriamo una 2-colorazione C di K_n. Sia C' la 2-colorazione che colora un arco di blu se e solo se C lo colora di rosso (e viceversa). Poiché vale $p(n; s, t)$, esiste un K_s *rosso per la colorazione* C' oppure un K_t *blu per la colorazione* C'. Per definizione di C', tali K_s e K_t saranno rispettivamente blu e rosso per la colorazione C. Dato che questo è vero al variare di ogni 2-colorazione C, si può concludere che vale $p(n; t, s)$. Il viceversa è del tutto analogo. □

Lemma 5.3. *Per ogni* $s \geqslant 2$ *vale che* $R(s, 2) = s$.

Dimostrazione. Chiaramente K_2 è semplicemente un arco. Altrettanto chiaramente per ogni s, t dev'essere $R(s, t) \geqslant \max\{s, t\}$:[1] senza perdita di generalità assumiamo $s < t$ e supponiamo per assurdo che $R(s, t) = n < \max\{s, t\} = t$ e che valga $p(n; s, t)$ (definita nella dimostrazione del Lemma 5.2); la 2-colorazione di K_n "tutti gli archi blu" contraddice $p(n; s, t)$ (K_n non può contenere un K_s rosso, perché non esistono archi rossi, e non può contenere un K_t blu perché $n < t$).

Dunque $R(s, 2) \geqslant s$; l'altra disuguaglianza si ottiene osservando che è vera $p(s; 2, s)$: ogni 2-colorazione di K_s contiene almeno un arco (cioè un K_2) rosso, a meno che non sia la colorazione "tutti gli archi blu" e in tal caso l'intero K_s è un sottografo (banale) blu. □

Teorema 5.4. *Siano* $s, t > 2$. *Allora vale*

$$R(s, t) \leqslant R(s - 1, t) + R(s, t - 1). \tag{5.1}$$

In particolare, un semplice ragionamento per induzione (che usa il Lemma 5.3 come passo base e l'Equazione (5.1) *come passo induttivo) mostra che* $R(s, t)$ *è ben definito per ogni* $s, t \geqslant 2$. *Inoltre vale che*

$$R(s, t) \leqslant \binom{s + t - 2}{s - 1}. \tag{5.2}$$

Dimostrazione. Possiamo supporre induttivamente che $n_1 := R(s - 1, t)$ e $n_2 := R(s, t - 1)$ siano finiti. Sia $n := R(s - 1, t) + R(s, t - 1)$ e consideriamo una 2-colorazione di K_n. Abbiamo la tesi se dimostriamo che K_n contiene un K_s rosso oppure un K_t blu. Sia $x \in K_n$ un vertice: sappiamo che è collegato a tutti gli altri $n - 1$ vertici. In particolare è unito ad almeno n_1 vertici con un arco rosso oppure almeno n_2 vertici con un arco blu: se così non fosse, avremmo che

$$n - 1 = \#\{\text{vertici rossi}\} + \#\{\text{vertici blu}\} \leqslant (n_1 - 1) + (n_2 - 1) = n - 2.$$

[1] Supponendo implicitamente che $R(s, t)$ esista...

Senza perdita di generalità supponiamo che x sia unito ad almeno n_1 vertici rossi. Consideriamo il sottografo isomorfo a K_{n_1} formato da questi vertici. Per ipotesi induttiva, al suo interno contiene un K_{s-1} rosso oppure un K_t blu. Nel secondo caso, abbiamo finito; nel primo, unendo i vertici del K_{s-1} con x si ottiene un K_s rosso.

Per quanto riguarda la stima (5.2), procediamo per induzione su $n := s + t$. Per $s = 2$ oppure $t = 2$, per il Lemma 5.3 in realtà si ha un'uguaglianza:

$$R(2,t) = t = \binom{t}{1} = \binom{2+t-2}{2-1}$$

e analogamente per $R(s,2)$. Supponiamo che sia vero allora per ogni $s', t' \geqslant 2$ tali che $s' + t' < n$ e dimostriamo che vale per s, t tali che $s + t = n$: dall'Equazione (5.1)

$$R(s,t) \leqslant R(s-1,t) + R(s,t-1) \leqslant \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1}. \quad \square$$

Possiamo generalizzare i numeri di Ramsey per k-colorazioni con un numero arbitrario (ma finito) di colori.

Definizione 5.5. Definiamo $R(s_1, \ldots, s_k)$ come il minimo $n \in \mathbb{N}$ tale che per ogni k-colorazione del grafo completo K_n, esso contenga, per almeno un $i = 1, \ldots, k$, un sottografo isomorfo a K_{s_i} completamente colorato con l'i-esimo colore.

Teorema 5.6. *$R(s_1, \ldots, s_k)$ è ben definito per ogni k e per ogni $s_1, \ldots, s_k$.*

Dimostrazione. Per induzione sul numero di colori k. La base $k = 2$ è semplicemente il Teorema 5.4. Per il passo induttivo, osserviamo che da una k-colorazione possiamo ottenere una $(k-1)$-colorazione unificando i due colori c_1 e c_2, cioè assegnando un nuovo colore c^* a tutti gli archi che prima erano colorati con c_1 oppure c_2 e lasciando invariati gli altri. Per ipotesi induttiva, esiste $R(\boldsymbol{\nu})$, dove $\boldsymbol{\nu}$ è una qualsiasi $(k-1)$-upla di numeri naturali (maggiori o uguali a 2). In particolare esiste

$$n := R(R(s_1, s_2), s_3, \ldots, s_k),$$

cioè K_n contiene un sottografo K_{s_i} tutto colorato con c_i, per qualche $i = 3, \ldots, k$, oppure contiene un K_m, dove $m = R(s_1, s_2)$, monocromatico con c^*. Ora, spezzando di nuovo c^* nelle due componenti c_1 e c_2, abbiamo una 2-colorazione di K_m e m è proprio il numero di Ramsey relativo a s_1 e s_2: possiamo trovare al suo interno K_{s_1} monocromatico di colore c_1 oppure K_{s_2} di colore c_2. In ogni caso, abbiamo dimostrato che n verifica la condizione della Definizione 5.5; questo prova che $R(s_1, \ldots, s_k)$ esiste (ed è minore o uguale a n). $\square$

Un'altra generalizzazione possibile per i numeri di Ramsey riguarda gli *ipergrafi*, cioè grafi in cui gli archi possono collegare tra loro più di due vertici.

Definizione 5.7. Un *ipergrafo* è una coppia (V, E) in cui V è un insieme arbitrario (i cui elementi sono detti *vertici*) ed $E \subseteq \wp(V) \setminus \{\varnothing\}$ è detto *insieme degli (iper)archi*. Se $E \subseteq \wp_r(V)$, l'ipergrafo è detto r-*uniforme*.

In quest'ottica, un grafo è un ipergrafo 2-uniforme. L'ovvia generalizzazione dei numeri di Ramsey si basa sulle colorazioni degli iperarchi dell'ipergrafo completo su n vertici r-uniforme $K_n^{(r)}$ (cioè l'ipergrafo con $\#(V) = n$ che ha come archi tutti gli elementi di $\wp_r(V)$).

Definizione 5.8. Definiamo $R^{(r)}(s,t)$ il minimo $n \in \mathbb{N}$ per cui, per ogni 2-colorazione di $\wp_r(\{1,\dots,n\})$ esiste $Y_1 \subseteq \{1,\dots,n\}$ con $\#(Y_1) = s$ tale che $\wp_r(Y_1)$ sia colorato di rosso, oppure esiste $Y_2 \subseteq \{1,\dots,n\}$ con $\#(Y_2) = t$ tale che $\wp_r(Y_2)$ sia colorato di blu.

Osserviamo che $R^{(2)}(s,t) = R(s,t)$. Con una dimostrazione analoga a quella del Teorema 5.4 (che qui omettiamo), si può dimostrare l'esistenza di $R^{(r)}(s,t)$ grazie alla relazione

$$R^{(r)}(s,t) \leqslant R^{(r-1)}\big(R^{(r)}(s-1,t), R^{(r)}(s,t-1)\big) + 1.$$

Naturalmente possiamo combinare le generalizzazioni precedenti ed ottenere numeri di Ramsey della forma $R^{(r)}(s_1,\dots,s_k)$. Se tutti gli s_i sono uguali a un certo numero $m \in \mathbb{N}$, otteniamo quello che prende il nome di Teorema di Ramsey, nella sua versione finita.

Teorema 5.9 (Ramsey, versione finita)**.** *Per ogni* $m, r, k \in \mathbb{N} \setminus \{0\}$ *esiste* $n \in \mathbb{N} \setminus \{0\}$ *tale che, per ogni* k*-colorazione di* $\wp_r(\{1,\dots,n\})$ *esiste un insieme* $H \subseteq \{1,\dots,n\}$ *con* $\#(H) = m$ *tale che* $\wp_r(H)$ *sia monocromatico.*

Osservazione. Anche per $r = 2$, non sono noti molti numeri di Ramsey (non banali) "veri", cioè, con la notazione introdotta nel Lemma 5.2, gli n tali che $p(n;s,t)$ sia vera e $p(n-1;s,t)$ sia falsa. Tra i pochi che conosciamo ci sono:[2]

$$\begin{aligned} &R(3,3) = 6 && R(3,4) = 9 && R(3,5) = 14 \\ &R(3,6) = 18 && R(3,7) = 23 && R(4,4) = 18. \end{aligned}$$

Nella maggior parte dei casi sono note semplicemente stime per i numeri di Ramsey.

[2] *NdA:* dall'uscita del nostro libro di riferimento [1] nel 1979, a questo elenco si sono aggiunti $R(3,8) = 28$, $R(3,9) = 36$, $R(4,5) = 25$. Vedi anche `http://oeis.org/A059442`

Finora abbiamo considerato grafi con un numero finito di vertici. In realtà il succo della teoria è la sua generalizzazione ad insiemi infiniti (numerabili), che porta alla versione infinita del Teorema di Ramsey.

Teorema 5.10 (Ramsey, versione infinita)**.** *Siano* A *un insieme infinito (numerabile) e* $c\colon \wp_r(A) \to \{1,\dots,k\}$ *una* k*-colorazione di* $\wp_r(A)$*. Allora esiste* $X \subseteq A$ *infinito tale che* $\wp_r(X)$ *è monocromatico.*

Dimostrazione. Per comodità di scrittura, per un insieme V qualsiasi denoteremo $V^{(r)} := \wp_r(V)$. La dimostrazione procede per induzione su r.
$\boxed{r = 1}$ Il teorema è ovviamente vero, in quanto afferma che in ogni partizione finita di un insieme infinito, almeno una delle parti è infinita.
$\boxed{r - 1 \Rightarrow r}$ Costruiamo l'insieme X induttivamente. Siano $A_0 := A$, $x_1 \in A_0$ qualsiasi e $B_1 := A_0 \setminus \{x_1\}$. Definiamo una k-colorazione

$$c_1\colon B_1^{(r-1)} \to \{1,\dots,k\}$$

ponendo, per ogni $T \in B_1^{(r-1)}$, $c_1(T) = c(T \cup \{x_1\})$ (notiamo che $T \cup \{x_1\} \in A_0^{(r)}$). Per ipotesi induttiva esiste $A_1 \subseteq B_1$, infinito, tale che $A_1^{(r-1)}$ è monocromatico (rispetto alla colorazione c_1), supponiamo del colore $d_1 \in \{1,\dots,k\}$.

Siano ora $x_2 \in A_1$ e $B_2 := A_1 \setminus \{x_2\}$. Analogamente al passo precedente, costruiamo una colorazione

$$c_2\colon B_2^{(r-1)} \to \{1,\dots,k\}$$

definendo $c_2(T) = c(T \cup \{x_2\})$. Sempre per ipotesi induttiva, esiste $A_2 \subseteq B_2$ infinito tale che $A_2^{(r-1)}$ è monocromatico del colore d_2 rispetto alla colorazione c_2.

Procedendo induttivamente otteniamo una catena discendente di sottoinsiemi infiniti

$$A = A_0 \supset A_1 \supset A_2 \supset \cdots$$

e una successione di elementi $x_i \in A_{i-1} \setminus A_i$. Sia $Y = \{x_1, x_2, \dots\}$ e consideriamo $Y^{(r)}$. Qual è il colore assegnato da c a una r-upla $\{x_{i(1)},\dots,x_{i(r)}\} \in Y^{(r)}$ (supponiamo $i(1) < \cdots < i(r)$)? Per costruzione $x_{i(1)} \notin A_{i(1)}$ mentre $\{x_{i(2)},\dots,x_{i(r)}\} \in A_{i(1)}^{(r-1)}$: dunque $c(\{x_{i(1)},\dots,x_{i(r)}\}) = c_{i(1)}(\{x_{i(2)},\dots,x_{i(r)}\}) = d_{i(1)}$. Ma $A_{i(1)}^{(r-1)}$ è monocromatico rispetto alla colorazione $c_{i(1)}$: questo significa che *il colore assegnato a* $\{x_{i(1)},\dots,x_{i(r)}\}$ *dipende solo da* $x_{i(1)}$. Detto in altri termini, per ogni $Z \in Y^{(r)}$ si ha che $c(Z) = d_i$ se $i = \min\{j \mid x_j \in Z\}$, cioè se x_i è l'unico elemento di Z che non appartiene ad A_i.

Ora, i colori sono in numero finito, quindi nella successione $(d_i \mid i \in \mathbb{N} \setminus \{0\})$ esiste un colore che si ripete infinite volte, cioè esiste una sottosuccessione d_{n_i}, con $n_i \to \infty$ per $i \to \infty$, costante. L'insieme $X := \{x_{n_1}, x_{n_2}, \dots\} \subseteq Y$ è l'insieme infinito cercato. □

Vediamo un'ultima generalizzazione. Anziché cercare un sottografo completo K_s monocromatico all'interno di una colorazione di K_n, possiamo considerare un generico grafo G, colorarlo e cercare un sottografo H, magari con una certa struttura (ad esempio, un albero), che sia monocromatico.

Procediamo un passo per volta. Siano H_1 e H_2 grafi arbitrari. Il nostro problema è trovare il minimo $n \in \mathbb{N}$ tale che per ogni 2-colorazione di K_n, esso contenga un sottografo isomorfo ad H_1 rosso oppure un sottografo isomorfo ad H_2 blu. Questo problema ha soluzione, perché ovviamente, se H_1 ha s vertici e H_2 ne ha t, essi sono sottografi dei grafi completi K_s e K_t rispettivamente, quindi, indicando con $r(H_1, H_2)$ l'n che risolve il problema, sicuramente

$$r(H_1, H_2) \leqslant R(s, t).$$

Se al posto del grafo completo K_n cerchiamo sottografi monocromatici in un generico grafo G, dobbiamo stare attenti a problemi di compatibilità dei dati (se gli H_i sono cicli e G è un albero, è abbastanza difficile che il problema abbia soluzione...). In ogni caso, per $G = K_n$, ci sono dei risultati esatti (che non dimostriamo qui; un'interessante lettura a tal proposito è l'articolo di Burr, Erdős e Spencer [2]). Nelle prossime proposizioni, se $s \in \mathbb{N}$ e G è un grafo, indichiamo con sG l'unione disgiunta di s copie del grafo G; ad esempio,

rappresenta il grafo $3K_2$.

Proposizione 5.11. *Sia* T *un albero con* t *vertici. Allora* $r(K_s, T) = (s-1)(t-1)+1$.

Proposizione 5.12. *Se* $s \geqslant t \geqslant 1$, *allora* $r(sK_2, tK_2) = 2s + t - 1$.

Proposizione 5.13. *Se* $s > t \geqslant 1$, *allora* $r(sK_3, tK_3) = 3s + 2t$.

Terminiamo questa sezione con un risultato abbastanza carino, che prende il nome di Teorema di Schur (diverso sia dal Teorema di Schur della Sezione 1.7.2 che dal Lemma di Schur della Sezione 4.4.3).

Teorema 5.14 (Schur)**.** *Sia* c *una* k*-colorazione di* $\mathbb{N}$. *Allora esistono* $x, y \in \mathbb{N}$, *con* $x < y$, *tali che* $\{x, y, x+y\}$ *sia monocromatico.*

Dimostrazione. Sia $n \in \mathbb{N}$ tale che $R(3, \dots, 3) \leqslant n+1$ (numero di Ramsey con k argomenti). In altre parole, sia n sufficientemente grande tale che K_{n+1} contenga un triangolo monocromatico per ogni sua k-colorazione.

Consideriamo $\{0, \dots, n\} \subset \mathbb{N}$ e la colorazione c ristretta a $\{0, \dots, n\}$. Ad essa possiamo associare una k-colorazione c^* di $\wp_2(\{0, \dots, n\})$, cioè degli archi di K_{n+1}, definendo

$$c^*(\{i, j\}) = c(|i - j|).$$

Per costruzione, esiste un triangolo monocromatico per c^* di vertici $\{i, j, k\}$ (supponiamo $i > j > k$). Ma allora $x := i - j$ e $y := j - k$ verificano la tesi. □

5.2 Configurazioni geometriche con la teoria di Ramsey

18/05/2015 ◃ Introduciamo ora una notazione. Se $Z, X_1, \dots, X_k$ sono strutture finite di qualunque tipo, scriveremo

$$Z \to (X_1, \dots, X_k)$$

per indicare la proposizione "per ogni k-colorazione associata alla struttura Z esiste almeno un $i = 1, \dots, k$ tale che Z contenga una sottostruttura isomorfa a X_i monocromatica dell'i-esimo colore". Finora abbiamo visto i casi in cui le strutture sono:

1. grafi, con colorazione degli archi;
2. insiemi, con colorazione dei sottoinsiemi di cardinalità fissata.

Il primo esempio di questo capitolo si può scrivere come $K_6 \to (K_3, K_3)$ e in questi termini potremmo definire

$$R(s, t) := \min\{n \in \mathbb{N} \mid K_n \to (K_s, K_t)\}$$

oppure

$$R(s, t) = n \text{ se e solo se } K_n \to (K_s, K_t) \wedge K_{n-1} \not\to (K_s, K_t).$$

Se $X_1 = \cdots = X_k = X$ scriveremo, in forma più compatta, $Z \to (X)_k$.

Più in generale, useremo la stessa notazione se M è un oggetto geometrico e $\mathcal{P}$ è una famiglia di sottoinsiemi finiti di M: in tal caso $M \to (\mathcal{P})_k$ significa "per ogni k-colorazione di M esistono un colore i e un insieme $P \in \mathcal{P}$ monocromatico dell'i-esimo colore".

Teorema 5.15 (Compattezza combinatoria)**.** *Sia M un insieme infinito. Allora $M \to (\mathcal{P})_k$ se e solo se esiste $X \subset M$ finito tale che $X \to (\mathcal{P})_k$.*

Dimostrazione. $\boxed{\Leftarrow}$ Ovviamente, se $P \subseteq X$ è tale che $P \in \mathcal{P}$ ed è monocromatico, allora P è anche un sottoinsieme di M con le stesse proprietà.
$\boxed{\Rightarrow}$ Una k-colorazione di M è una mappa $c\colon M \to \{1, \dots, k\}$, quindi è un punto dello spazio di funzioni $\mathcal{F} := \{1, \dots, k\}^M$. In particolare, per $x \in M$, la proiezione $\pi_x(c)$ è il colore assegnato a x dalla colorazione c. Mettiamo su $\{1, \dots, k\}$ la topologia discreta e su $\mathcal{F}$ la topologia prodotto. Poiché $\{1, \dots, k\}$ è compatto, anche $\mathcal{F}$ è compatto per il Teorema di Tychonoff.

Ora, per un generico $Y \subset M$ finito, definiamo $N(Y) \subseteq \mathcal{F}$ come l'insieme delle colorazioni di M che ristrette ad Y "vanno male", cioè per le quali *non* esiste $P \in \mathcal{P}$, $P \subseteq Y$ monocromatico. Osserviamo che se $c, d \in \mathcal{F}$ sono tali che $c\big|_Y \equiv d\big|_Y$, allora $c \in N(Y)$ se e solo se $d \in N(Y)$ (lo stesso $P \in \mathcal{P}$ usato per dire che una delle due colorazioni è in $N(Y)$ va bene anche per l'altra). Questo prova che, detti

$$\mathcal{G} := \{f \in \{1, \dots, k\}^Y \mid \text{esiste } P \subseteq Y,\ P \in \mathcal{P} \text{ monocromatico rispetto a } f\}$$
$$\overline{\mathcal{G}} := \{f \in \{1, \dots, k\}^Y \mid \text{non esiste } P \subseteq Y,\ P \in \mathcal{P} \text{ monocromatico rispetto a } f\},$$

si ha che

$$N(Y) = \bigcup_{f \in \overline{\mathcal{G}}} \{c \in \mathcal{F} \mid c\big|_Y = f\}$$
$$\mathcal{F} \setminus N(Y) = \bigcup_{f \in \mathcal{G}} \{c \in \mathcal{F} \mid c\big|_Y = f\}.$$

Notiamo che

$$\{c \in \mathcal{F} \mid c\big|_Y = f\} = \left(\prod_{y \in Y} \{f(y)\}\right) \times \left(\prod_{y \notin Y} \{1, \dots, k\}\right)$$

è un elemento della base di aperti per $\mathcal{F}$ perché Y è finito,[3] dunque $N(Y)$ è un insieme aperto e chiuso in $\mathcal{F}$.

Supponiamo per assurdo che $M \to (\mathcal{P})_k$ ma $X \not\to (\mathcal{P})_k$ per ogni $X \subset M$ finito, cioè che $N(X) \neq \varnothing$ per ogni X finito. Osserviamo che $N(X) \cap N(Z) \supseteq N(X \cup Z)$: infatti, se $c \notin N(X)$, troviamo $P \in \mathcal{P}$ monocromatico e dato che $P \subseteq X \subseteq X \cup Z$ tale P dimostra che $c \notin N(X \cup Z)$; questo prova che $N(X \cup Z) \subseteq N(X)$, e analogamente si dimostra che $N(X \cup Z) \subseteq N(Z)$. Quindi la famiglia di chiusi non vuoti $\{N(X) \mid X \subset M,\ X \text{ finito}\}$ ha la *proprietà dell'intersezione finita* (ogni intersezione finita di elementi della famiglia contiene un altro elemento della famiglia); dato che $\mathcal{F}$ è compatto, ne deduciamo che

$$\bigcap_{\substack{X \subset M \\ X \text{ finito}}} N(X) \neq \varnothing.$$

Ma una qualsiasi colorazione c in questa intersezione porta all'assurdo: per ipotesi esiste $P \subseteq M$, $P \in \mathcal{P}$ monocromatico; poiché P è un insieme finito, $c \in N(P)$ per definizione di c, ma P stesso (essendo monocromatico e in $\mathcal{P}$) dimostra che $c \notin N(P)$. □

Sia $L \subset \mathbb{R}^m$ un insieme finito. Indichiamo con

$$\mathcal{L}_n := \{L' \subset \mathbb{R}^n \mid L' \text{ è congruente a } L\},$$

[3] Vedi nota 5 a pagina 72.

in cui ricordiamo che L è *congruente* a L′ se, dopo aver opportunamente immerso $\mathbb{R}^m$ in $\mathbb{R}^n$, esiste un'isometria[4] di $\mathbb{R}^n$ che manda L in L′. Con abuso di notazione scriveremo $\mathbb{R}^n \to (L)_k$ anziché $\mathbb{R}^n \to (\mathcal{L}_n)_k$ per dire: "per ogni k-colorazione di $\mathbb{R}^n$ esiste un sottoinsieme monocromatico congruente a L".

Definizione 5.16. $L \subset \mathbb{R}^m$ si dice *di Ramsey* se per ogni $k \in \mathbb{N}$ esiste $n \in \mathbb{N}$ tale che $\mathbb{R}^n \to (L)_k$.

Teorema 5.17. *Sia* $L = \{0, 1\} \subset \mathbb{R}$*, cioè un insieme formato da due punti a distanza* 1*. Allora* $\mathbb{R}^2 \to (L)_3$ *ma* $\mathbb{R}^2 \not\to (L)_7$*.*

Dimostrazione. $\boxed{\mathbb{R}^2 \to (L)_3}$ Consideriamo i sette punti $\{x, x_1, x_2, y_1, y_2, z_1, z_2\}$ disegnati in Figura 5.3.

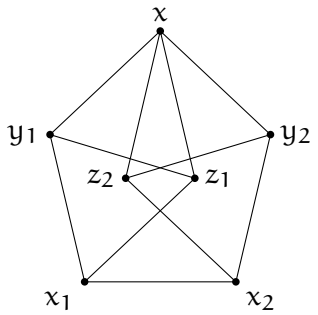


Figura 5.3: Ogni lato tracciato misura esattamente 1.

Supponiamo di avere una 3-colorazione dei sette punti in rosso, verde, blu tale che nessuna coppia di punti a distanza 1 sia monocromatica. Senza perdita di generalità supponiamo x rosso. Di conseguenza y_1 e z_1 devono essere verde e blu (o viceversa), quindi x_1 è costretto ad essere rosso. Lo stesso ragionamento con x_2, y_2 e z_2 porta a dire che anche x_2 è rosso. Ma x_1 e x_2 sono a distanza 1 e non possono essere entrambi rossi.

$\boxed{\mathbb{R}^2 \not\to (L)_7}$ Basta trovare una 7-colorazione del piano in cui coppie di punti monocromatici siano "abbastanza distanti". Tasselliamo il piano con esagoni regolari di lato ℓ (definiremo a breve il valore di ℓ) e li coloriamo con sette colori come mostrato in Figura 5.4. Per essere precisi, la parte del bordo di un esagono che ha lo stesso colore dell'interno è evidenziata da una linea continua nella Figura 5.5.

Vediamo come scegliere ℓ in modo che non ci siano punti a distanza 1 dello stesso colore. Osserviamo in primo luogo che la distanza massima tra due punti

[4] Come spazio affine: le traslazioni sono ammesse.

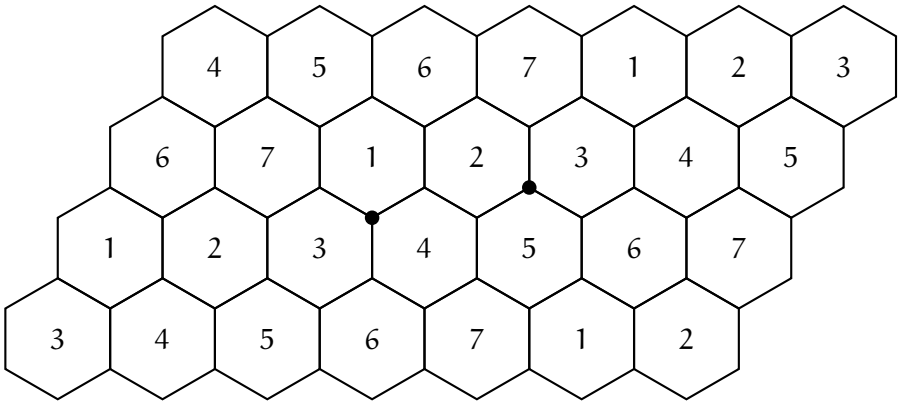


Figura 5.4: A numero uguale corrisponde colore uguale.

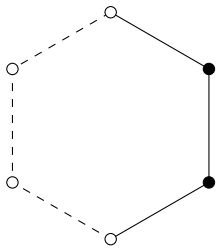


Figura 5.5: Dettaglio della colorazione sul bordo di un esagono.

dello stesso esagono è 2ℓ, quindi la prima condizione da imporre è

$$\ell < \frac{1}{2}.$$

Considerando invece punti che appartengono a esagoni diversi dello stesso colore, la distanza minima è raggiunta per i punti evidenziati in Figura 5.4 e vale, per il Teorema di Pitagora,

$$\sqrt{\left(\frac{3}{2}\sqrt{3}\ell\right)^2 + \left(\frac{1}{2}\ell\right)^2} = \sqrt{7}\ell;$$

dunque basta prendere

$$\ell > \frac{1}{\sqrt{7}}$$

affinché questa distanza sia maggiore di 1. In conclusione, tassellando il piano con esagoni di lato ℓ per il quale si abbia

$$\frac{1}{\sqrt{7}} < \ell < \frac{1}{2}$$

troviamo una 7-colorazione rispetto alla quale non esistono coppie di punti a distanza 1 monocromatici. □

Teorema 5.18. *Sia* Q^2 *l'insieme dei quattro vertici di un quadrato di lato unitario in* $\mathbb{R}^2$ *(ad esempio,* $Q^2 = \{(0,0),(1,0),(0,1),(1,1)\}$*). Allora* $\mathbb{R}^6 \to (Q^2)_2$.

Dimostrazione. Consideriamo i 15 punti di $\mathbb{R}^6$ tali che due coordinate siano uguali a $1/\sqrt{2}$ e le altre siano nulle. (Ci sono $\binom{6}{2} = 15$ modi di scegliere due coordinate su sei.) Sia K_6 il grafo completo sui vertici $\{v_1, \ldots, v_6\}$. Una 2-colorazione di $\mathbb{R}^6$ induce una 2-colorazione degli archi di K_6 in cui $\{v_i, v_j\}$ ha lo stesso colore del punto tale che $x_i = x_j = 1/\sqrt{2}$.

Ora, si ha che $r(C_4, C_4) = 6$, dove $C_4 =$  è un ciclo di lunghezza 4 (lo dimostreremo tra poco), quindi possiamo trovare un 4-ciclo monocromatico in K_6 e senza perdita di generalità supponiamo che tale ciclo sia v_1, v_2, v_3, v_4. Allora i quattro punti associati agli archi $\{v_1, v_2\}$, $\{v_2, v_3\}$, $\{v_3, v_4\}$ e $\{v_4, v_1\}$ sono i vertici di un quadrato di lato unitario monocromatico in $\mathbb{R}^6$. □

Lemma 5.19. *Si ha che* $r(C_4, C_4) = 6$*, cioè che per ogni 2-colorazione di* K_6 *esso contiene un* C_4 *monocromatico.*

Dimostrazione. La 2-colorazione di K_5 mostrata in Figura 5.2 non contiene 4-cicli monocromatici, quindi $r(C_4, C_4) \geqslant 6$; mostriamo che 6 è sufficiente. Consideriamo una 2-colorazione qualsiasi di K_6 e distinguiamo due casi.

Caso 1. Esiste un vertice v collegato ad almeno 4 vertici a, b, c, d con archi dello stesso colore (supponiamo rosso).

(a) Se tra a, b, c e d ci sono almeno due archi adiacenti anch'essi rossi, abbiamo finito. (Ad esempio, supponiamo che $\{a, b\}$ e $\{b, c\}$ siano rossi; allora $\{v, a, b, c\}$ è un C_4 rosso.)

(b) Altrimenti, osservando che se ci fossero tre o più archi rossi ce ne sarebbe una coppia formata da archi adiacenti, restano tre situazioni:

- nessun arco rosso;
- un solo arco rosso (ad esempio, $\{a, c\}$);
- due archi rossi non adiacenti (ad esempio, $\{a, c\}$ e $\{b, d\}$).

In ogni caso, gli archi $\{a, b\}$, $\{b, c\}$, $\{c, d\}$ e $\{d, a\}$ formano un 4-ciclo blu.

Caso 2. Dei cinque archi uscenti da un vertice ce ne sono sempre tre colorati con un colore e due con l'altro. Supponiamo senza perdita di generalità che al vertice v siano collegati a, b e c con archi rossi e d, e con archi blu e consideriamo il (sotto)grafo bipartito $\{\{a, b, c\}, \{d, e\}\}$.

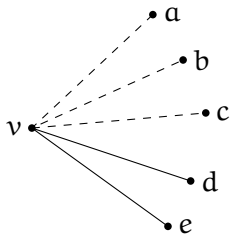
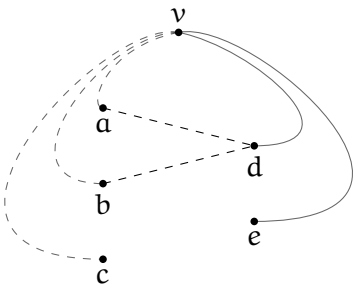


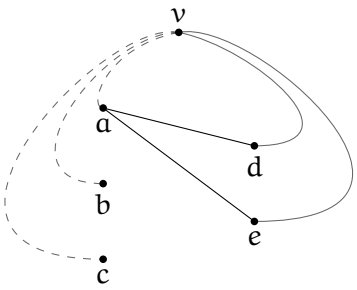
Figura 5.6: Archi uscenti da v nel caso 2.

(a) Se esiste almeno un vertice in $\{d, e\}$ collegato con due vertici in $\{a, b, c\}$ con archi rossi, abbiamo finito (vedi Figura 5.7a).

(b) Se esiste almeno un vertice in $\{a, b, c\}$ collegato sia a d che ad e con archi blu, abbiamo pure finito (vedi Figura 5.7b).



(a) d è collegato ad a e b con archi rossi: $\{v, b, d, a\}$ è un 4-ciclo.



(b) a è collegato a d ed e con archi blu: $\{v, d, a, e\}$ è un 4-ciclo.

Figura 5.7: I due sottocasi del Caso 2. che ci permettono di concludere.

(c) Mostriamo che non possono verificarsi altri casi. Supponiamo per assurdo di non essere né nel sottocaso (a) né nel (b).

  (i) *Se* $\{a, d\}$ *è rosso*, $\{b, d\}$ e $\{c, d\}$ devono essere blu (altrimenti siamo nel caso (a)), quindi $\{b, e\}$ e $\{c, e\}$ devono essere rossi (altrimenti siamo nel caso (b)). Ma in questo modo siamo ricaduti nel caso (a).

  (ii) *Se* $\{a, d\}$ *è blu*, $\{a, e\}$ dev'essere rosso (altrimenti siamo nel caso (b)), quindi $\{b, e\}$ e $\{c, e\}$ devono essere blu (altrimenti siamo nel caso (a)), quindi $\{b, d\}$ e $\{c, d\}$ devono essere rossi (altrimenti siamo nel caso (b)). Ma in questo modo siamo ricaduti nel caso (a).

(a) Assumendo $\{a, d\}$ rosso, ricadiamo nel caso (a).

(b) Assumendo $\{a, d\}$ blu, ricadiamo nel caso (a).

Figura 5.8: Situazioni che mostrano che il sottocaso (c) non può verificarsi.

Avendo esaurito tutti i casi possibili, possiamo finalmente affermare che ogni 2-colorazione di K_6 contiene un 4-ciclo monocromatico. □

Teorema 5.20. *Siano* $L_1 \subset \mathbb{R}^{n_1}$ *e* $L_2 \subset \mathbb{R}^{n_2}$ *di Ramsey. Allora* $L_1 \times L_2 \subset \mathbb{R}^{n_1+n_2}$ *è di Ramsey.*

Dimostrazione. Fissiamo $k \in \mathbb{N}$. Poiché L_1 è di Ramsey, esiste $m \in \mathbb{N}$ tale che $\mathbb{R}^m \to (L_1)_k$. Per il Teorema di Compattezza 5.15 esiste $X \subset \mathbb{R}^m$ finito tale che $X \to (L_1)_k$. Sia $\ell := k^{\#(X)} = \#\{f\colon X \to \{1, \dots, k\}\}$. Dato che L_2 è di Ramsey, esiste $n \in \mathbb{N}$ tale che $\mathbb{R}^n \to (L_2)_\ell$.

Osserviamo che una k-colorazione di $\mathbb{R}^m \times \mathbb{R}^n$ si restringe ovviamente a una k-colorazione c di $X \times \mathbb{R}^n$. Essa induce una ℓ-colorazione $\tilde{c}$ di $\mathbb{R}^n$, in cui i colori sono le funzioni $f\colon X \to \{1, \dots, k\}$, nel modo seguente: per $y \in \mathbb{R}^n$,

$$\begin{array}{rccl} \tilde{c}(y) : X & \longrightarrow & \{1, \dots, k\} \\ x & \longmapsto & c(x, y). \end{array}$$

Ora, $\mathbb{R}^n \to (L_2)_\ell$, quindi esiste un insieme congruo a L_2 monocromatico in $\mathbb{R}^n$ rispetto a $\tilde{c}$, cioè tale che $\tilde{c}(y_1) = \tilde{c}(y_2)$ per ogni $y_1, y_2 \in L_2$. In particolare, per ogni $x \in X$, $y_1, y_2 \in L_2$ si ha che $c(x, y_1) = c(x, y_2)$. È dunque ben definita una k-colorazione c' di X che associa a $x \in X$ il colore $c(x, y)$ con $y \in L_2$ qualsiasi. Ma $X \to (L_1)_k$, quindi esiste un sottoinsieme congruo a L_1 in X monocromatico rispetto a c'. Per costruzione $L_1 \times L_2$ è monocromatico rispetto a c e questo prova che $\mathbb{R}^m \times \mathbb{R}^n \to (L_1 \times L_2)_k$. □

Definizione 5.21. Siano $a_1, \dots, a_n \in \mathbb{R}$, $a_i > 0$. Definiamo *mattoncino* (*brick*) l'insieme

$$B := \{(\varepsilon_1 a_1, \dots, \varepsilon_n a_n) \mid \varepsilon_i \in \{0, 1\}\}.$$

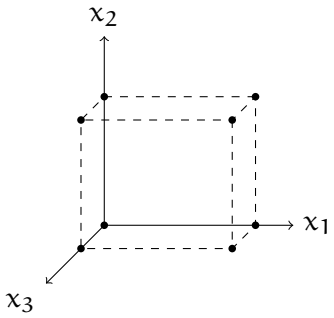


Figura 5.9: Esempio di *brick* in $\mathbb{R}^3$. Le linee tratteggiate *non* ne fanno parte.

Osserviamo che $B = \{0, a_1\} \times \cdots \times \{0, a_n\}$ e che $\{0, a_i\}$ è di Ramsey (si veda l'Appendice A), quindi per il teorema precedente B è di Ramsey. In particolare, dato che se $L' \subseteq L$ e $\mathbb{R}^n \to (L)_k$ si ha ovviamente $\mathbb{R}^n \to (L')_k$, i sottoinsiemi di insiemi di Ramsey sono anch'essi di Ramsey, quindi un qualunque sottoinsieme di B è di Ramsey.

Un altro risultato, che non dimostriamo, sulla classificazione degli insiemi di Ramsey riguarda i cosiddetti insiemi sferici.

Definizione 5.22. Un insieme $Y \subseteq \mathbb{R}^n$ è *sferico* se è immergibile in una sfera $(n-1)$-dimensionale, cioè se esistono $z \in \mathbb{R}^n$ e $r > 0$ tali che $\|z - y\| = r$ per ogni $y \in Y$.

Teorema 5.23. *Un insieme di Ramsey è sferico.*

All'epoca del nostro libro di riferimento [1] ci sono fatti non ancora noti: non si sa se valga il viceversa del teorema precedente, cioè se un insieme sferico sia di Ramsey. In particolare, ci sono insiemi anche semplici (ad esempio, alcuni triangoli ottusangoli) che sono sferici ma non contenuti in un *brick*, dunque non sappiamo se essi siano di Ramsey oppure no.

5.3 Il Teorema di van der Waerden

Come esempio di risultato della Teoria di Ramsey, vediamo un teorema classico: ▹ *20/05/2015*
il Teorema di van der Waerden.

Teorema 5.24 (van der Waerden)**.** *Siano* $p, k \in \mathbb{N}$*. Esiste un numero* $w \in \mathbb{N}$ *che dipende da* p *e* k *tale che per ogni* k*-colorazione di* $\{1, \ldots, w\}$*, esso contiene una progressione aritmetica di* p *termini monocromatica.*

Il minimo w che soddisfa il teorema è detto *numero di van der Waerden* associato a p e k ed è indicato con $W(p, k)$.

Dimostrazione. Siano $\ell, m \in \mathbb{N}$. Definiamo una relazione di equivalenza su $\{0, \dots, \ell\}^m$ in cui poniamo $(x_1, \dots, x_m) \sim (y_1, \dots, y_m)$ se e solo se coincidono fino all'ultima occorrenza di ℓ compresa, cioè se esiste $j \in \{1, \dots, m\}$ tale che

1. $x_i = y_i$ per ogni $i = 1, \dots, j$;
2. $x_j = y_j = \ell$;
3. $x_i \neq \ell$ e $y_i \neq \ell$ per ogni $i = j+1, \dots, m$.

Se ℓ non compare né in $(x_1, \dots, x_m)$ né in $(y_1, \dots, y_m)$, allora le due m-uple sono equivalenti per convenzione.

Sia $S(\ell, m)$ l'enunciato "per ogni $k \in \mathbb{N}$ esiste $w(\ell, m, k) \in \mathbb{N}$ tale che per ogni k-colorazione c di $\{1, \dots, w(\ell, m, k)\}$ esistono $a, d_1, \dots, d_m \in \mathbb{N}$ tali che

(a) $a + \ell \sum_{i=1}^{m} d_i \leqslant w(\ell, k, m)$;

(b) $c\left(a + \sum_{i=1}^{m} x_i d_i\right)$, vista come funzione di $(x_1, \dots, x_m) \in \{0, \dots, \ell\}^m$, è costante sulle classi di equivalenza."

Osservazione. Nel corso della dimostrazione useremo una versione leggermente modificata dell'enunciato, in cui ammettiamo che c sia una k-colorazione di $\{1, \dots, w(\ell, m, k)\}$ a meno di traslazioni, cioè che siano ammesse colorazioni di sottoinsiemi di $w(\ell, k, m)$ elementi consecutivi del tipo

$$\{r+1, \dots, r + w(\ell, k, m)\}.$$

In tal caso, il punto (a) va modificato con

$$r + 1 \leqslant a + \sum_{i=1}^{m} x_i d_i \leqslant r + w(\ell, k, m)$$

per ogni $(x_1, \dots, x_m) \in \{0, \dots, \ell\}^m$, affinché il punto (b) abbia senso.

Notiamo che l'enunciato $S(p, 1)$ è "per ogni $k \in \mathbb{N}$ esiste $w(p, k) \in \mathbb{N}$ tale che per ogni k-colorazione c di $\{1, \dots, w(p, k)\}$ esistono $a, d \in \mathbb{N}$ tali che $a + pd \leqslant w(p, k)$ e $c(a + xd)$ è costante per $0 \leqslant x < p$", che è la tesi del teorema. (Infatti $a + xd$, per $0 \leqslant x < p$, è una progressione aritmetica lunga p; inoltre, se $m = 1$, la relazione di equivalenza su $\{0, \dots, \ell\}$ ha due classi: tutti gli $x < \ell$ sono equivalenti tra loro e ℓ sta in una classe a sé.) Dimostriamo allora l'enunciato $S(\ell, m)$ per doppia induzione su ℓ e m.

$\boxed{S(1,1)}$ L'equivalenza su $\{0,1\}$ è quella banale, in cui ogni classe è formata da un solo elemento, di conseguenza il punto (b) è automaticamente verificato. L'enunciato si riduce a "per ogni $k \in \mathbb{N}$ esiste $w(k) \in \mathbb{N}$ tale che per ogni k-colorazione c di $\{1,\dots,w(k)\}$ esistono $a, d \in \mathbb{N}$ tali che $a + d \leqslant w(k)$", che è evidentemente vero scegliendo opportuni valori per w, a e d (ad esempio, $w = 2$, $a = d = 1$ funzionano).

$\boxed{\big(S(\ell,1) \wedge S(\ell,m)\big) \Rightarrow S(\ell,m+1)}$ Fissiamo k. Per ipotesi induttiva abbiamo $w := w(\ell,m,k)$. Sempre per ipotesi induttiva possiamo definire $w' := w(\ell,1,k^w)$, aumentando il numero di colori.

L'intervallo $\{1,\dots,ww'\}$ può essere suddiviso in w' intervalli

$$W_j := \{(j-1)w+1,\dots,jw\}$$

ciascuno di lunghezza w, per $j = 1,\dots,w'$. Consideriamo una k-colorazione c di $\{1,\dots,ww'\}$; essa induce una k^w-colorazione c' di $\{1,\dots,w'\}$, in cui i colori sono le funzioni $f\colon \{1,\dots,w\} \to \{1,\dots,k\}$, definita per $j = 1,\dots,w'$ da

$$\begin{array}{rccc} c'(j)\colon & \{1,\dots,w\} & \longrightarrow & \{1,\dots,k\} \\ & x & \longmapsto & c((j-1)w+x), \end{array}$$

cioè c' assegna a j la k-colorazione $c\big|_{W_j}$ (opportunamente traslata per riportare W_j in $\{1,\dots,w\}$). Ora, per definizione di w', esistono $a', d' \in \mathbb{N}$ con $a' + \ell d' \leqslant w'$ e $c'(a' + xd')$ è costante per ogni $x = 0,\dots,\ell-1$.

Dato che $a' \leqslant w'$, abbiamo che $Y := \{(a'-1)w+1,\dots,a'w\} \subset \{1,\dots,ww'\}$ ed è un intervallo lungo w; applichiamo dunque l'enunciato $S(\ell,m)$ (nella sua versione "traslata") a Y, k-colorato con $c\big|_Y$: esistono $a, d_1,\dots,d_m \in \mathbb{N}$ tali che

$$(a'-1)w+1 \leqslant a + \sum_{i=1}^{m} x_i d_i \leqslant a'w \tag{5.3}$$

per ogni $(x_1,\dots,x_m) \in \{0,\dots,\ell\}^m$ e $c(a + \sum x_i d_i)$ è costante sulle classi di equivalenza.

Definiamo $d_{m+1} := d'w$ e verifichiamo che $S(\ell,m+1)$ è vero con $w(\ell,m+1,k) := ww'$. Il punto (a) è facile:

$$a + \ell \sum_{i=1}^{m+1} d_i = a + \ell \sum_{i=1}^{m} d_i + \ell d' \leqslant a'w + \ell d'w \leqslant ww'.$$

Il punto (b) è un po' più contorto da verificare: dobbiamo dimostrare che i valori

$$c\left(a + \sum_{i=1}^{m+1} x_i d_i\right) = c\left(a + \sum_{i=1}^{m} x_i d_i + x_{m+1} d'w\right) \tag{5.4}$$

sono costanti sulle classi di equivalenza di $(x_1, \dots, x_{m+1}) \in \{0, \dots, \ell\}^{m+1}$. Scandiremo il ragionamento passo-passo.

1. In primo luogo notiamo che se $(x_1, \dots, x_{m+1}) \in \{0, \dots, \ell\}^{m+1}$ è tale che $x_{m+1} = \ell$, allora esso è l'unico elemento nella sua classe di equivalenza (quindi tale classe verifica il punto (b) banalmente), mentre se per $(x_1, \dots, x_{m+1})$ e $(y_1, \dots, y_{m+1})$ si ha $x_{m+1} \neq \ell$ e $y_{m+1} \neq \ell$, allora sono equivalenti se e solo se $(x_1, \dots, x_m) \sim (y_1, \dots, y_m)$.

2. Osserviamo che, per la stima (5.3), possiamo sempre scrivere

$$a + \sum_{i=1}^{m} x_i d_i = (a' - 1)w + \xi \tag{5.5}$$

   per un opportuno $\xi \in \{1, \dots, w\}$. In particolare, si ha che

$$(a' - 1)w + 1 + x_{m+1} d' w \leqslant a + \sum_{i=1}^{m} x_i d_i + x_{m+1} d' w \leqslant a' w + x_{m+1} d' w$$

   cioè che tale valore appartiene all'intervallo $W_{a' + x_{m+1} d'}$.

3. *Fissato* $x_{m+1} \in \{0, \dots, \ell - 1\}$, per ipotesi induttiva i colori in (5.4) sono costanti sulle classi di equivalenza. Purtroppo non possiamo ancora concludere, perché questo vale solo in un intervallo lungo w (che, per il punto precedente, è $W_{a' + x_{m+1} d'}$): *a priori* deduciamo solamente che all'interno di tale intervallo i colori sono costanti lungo le classi di equivalenza (ma possono essere diversi se $(x_1, \dots, x_{m+1}) \sim (y_1, \dots, y_{m+1})$ ma $x_{m+1} \neq y_{m+1}$).

4. D'altra parte, *fissati* $x_1, \dots, x_m \in \{0, \dots, \ell\}$, i colori in (5.4) sono costanti per ogni $x_{m+1} \in \{0, \dots, \ell - 1\}$. Infatti, se $\xi \in \{1, \dots, w\}$ è tale che valga (5.5), allora

$$\begin{aligned} c\left(a + \sum_{i=1}^{m} x_i d_i + x_{m+1} d' w \right) &= c\big((a' - 1)w + \xi + x_{m+1} d' w\big) = \\ &= c'(a' + x_{m+1} d')(\xi) \end{aligned}$$

   e (dal momento che ξ è fissato) tutti questi valori sono uguali al variare di $x_{m+1} \in \{0, \dots, \ell - 1\}$ per definizione di a' e d'.

$\boxed{\big(\forall\, m\ S(\ell, m)\big) \Rightarrow S(\ell + 1, 1)}$ L'enunciato $S(\ell + 1, 1)$ da dimostrare è: "per ogni k esiste $w(\ell + 1, 1, k)$ tale che per ogni k-colorazione c di $\{1, \dots, w(\ell + 1, 1, k)\}$ esistono a', d' tali che $a' + (\ell + 1)d' \leqslant w(\ell + 1, 1, k)$ e $c(a' + xd')$ è costante per

ogni $x = 0, \dots, \ell''$. Fissiamo k e scegliamo $m = k$; $S(\ell, k)$ afferma che per ogni colorazione $c\colon \{1, \dots, w(\ell, k, k)\} \to \{1, \dots, k\}$ esistono $a, d_1, \dots, d_k$ tali che

$$a + \ell \sum_{i=1}^{k} d_i \leqslant w(\ell, k, k) \tag{5.6}$$

e

$$c\left(a + \sum_{i=1}^{k} x_i d_i\right) \tag{5.7}$$

è costante sulle classi di equivalenza. Vogliamo mostrare che $w(\ell + 1, 1, k) := 2w(\ell, k, k)$ funziona (con a' e d' che sceglieremo tra poco). Una k-colorazione c di $\{1, \dots, 2w(\ell, k, k)\}$ ne induce ovviamente una di $\{1, \dots, w(\ell, k, k)\}$; consideriamo $a, d_1, \dots, d_k$ come sopra per questa colorazione. I numeri

$$a + \ell \sum_{i=1}^{s} d_i$$

per $s = 0, \dots, k$[5] sono colorati da c per (5.6): poiché sono $k+1$, ma abbiamo solo k colori a disposizione, per il *pigeonhole principle* esistono $s, t \in \{0, \dots, k\}$ (senza perdita di generalità $s < t$) tali che

$$c\left(a + \ell \sum_{i=1}^{s} d_i\right) = c\left(a + \ell \sum_{i=1}^{t} d_i\right). \tag{5.8}$$

Definiamo

$$a' := a + \ell \sum_{i=1}^{s} d_i \quad \text{e} \quad d' := \sum_{i=s+1}^{t} d_i$$

e mostriamo che con questi valori $S(\ell + 1, 1)$ è vero. Per il punto (a), osserviamo che

$$\begin{aligned} a' + (\ell + 1)d' &= a + \ell \sum_{i=1}^{s} d_i + (\ell + 1) \sum_{i=s+1}^{t} d_i = \\ &= a + \ell \sum_{i=1}^{t} d_i + \sum_{i=s+1}^{t} d_i \leqslant 2w(\ell, k, k) \end{aligned}$$

in cui l'ultima disuguaglianza è dovuta a (5.6), in quanto

$$a + \ell \sum_{i=1}^{t} d_i \leqslant a + \ell \sum_{i=1}^{k} d_i \leqslant w(\ell, k, k) \quad \text{e} \quad \sum_{i=s+1}^{t} d_i \leqslant a + \ell \sum_{i=1}^{k} d_i \leqslant w(\ell, k, k).$$

[5] Se $s = 0$, la sommatoria è una somma vuota e pertanto vale 0.

Per quanto riguarda il punto (b), calcoliamo

$$c(a' + xd') = c\left(a + \ell \sum_{i=1}^{s} d_i + x \sum_{i=s+1}^{t} d_i\right)$$

e osserviamo che corrisponde a

$$c\left(a + \sum_{i=1}^{k} x_i d_i\right)$$

per $(x_1, \ldots, x_k) \in \{0, \ldots, \ell\}^k$ con

$$x_i = \begin{cases} \ell & \text{per } i = 1, \ldots, s \\ x & \text{per } i = s+1, \ldots, t \\ 0 & \text{per } i = t+1, \ldots, k. \end{cases}$$

Tutte le k-uple con $x = 0, \ldots, \ell - 1$ sono equivalenti tra loro, quindi per ipotesi induttiva hanno lo stesso colore; d'altra parte, se $x = \ell$ si ha che $c(a' + \ell d') = c(a')$ per (5.8), dunque la k-upla con $x = \ell$ ha lo stesso colore della k-upla con $x = 0$. Da questo seguono $S(\ell + 1, 1)$ e, finalmente, la conclusione della dimostrazione. □

5.4 Cenni di ultrafiltri

Per concludere, vediamo un'altra dimostrazione del Teorema di Ramsey (per semplicità solo con $r = 2$, ma si può generalizzare) che fa uso di uno strumento proprio della teoria degli insiemi, gli *ultrafiltri*. Come vedremo, la dimostrazione è più breve, anche se può risultare ostica a chi non sia abituato a questo linguaggio.

Definizione 5.25. Un *filtro* su un insieme X è una famiglia $\mathcal{F} \subseteq \wp(X)$ tale che

1. $\varnothing \notin \mathcal{F}$ e $X \in \mathcal{F}$;
2. se $A, B \in \mathcal{F}$, allora $A \cap B \in \mathcal{F}$;
3. se $A \in \mathcal{F}$ e $A \subseteq C$, allora $C \in \mathcal{F}$.

Ad esempio, sia $A \subseteq X$ non vuoto. La famiglia $\{B \subseteq X \mid A \subseteq B\}$ è un filtro su X (detto *filtro generato da* A).

Definizione 5.26. Un filtro su X è detto *ultrafiltro* se è massimale (rispetto all'inclusione su $\wp(X)$).

Si veda l'Appendice A per alcune definizioni equivalenti di ultrafiltro. Per ogni $x \in X$, la famiglia $\{B \subseteq X \mid x \in B\}$ è un ultrafiltro, detto *ultrafiltro principale* generato da x.

Si può dimostrare che per ogni filtro $\mathcal{F}$ esiste un ultrafiltro $\mathcal{U}$ che lo estende, cioè tale che $\mathcal{F} \subseteq \mathcal{U}$.[6] Questo prova che esistono ultrafiltri non principali: in effetti, se X è un insieme infinito,

$$\mathcal{F}r(X) := \{A \subseteq X \mid A^c \text{ è finito}\}$$

è un filtro su X (*filtro di Fréchet*) e un ultrafiltro $\mathcal{U}$ che lo estenda non è principale (di più: $\mathcal{U}$ non può contenere alcun insieme finito A, perché $A^c \in \mathcal{F}r(X) \subseteq \mathcal{U}$.)

Teorema 5.27. *Sia* $c\colon \mathbb{N}^{(2)} \to \{1, \dots, k\}$ *una* k*-colorazione degli archi del grafo completo infinito che ha* $\mathbb{N}$ *come insieme dei vertici. Allora esiste* $X \subseteq \mathbb{N}$ *infinito tale che* $X^{(2)}$ *sia monocromatico.*

Dimostrazione. Sia $\mathcal{U}$ un ultrafiltro non principale su $\mathbb{N}$. Consideriamo la partizione

$$\mathbb{N}^{(2)} = P_1 \sqcup \cdots \sqcup P_k$$

dove $P_i := \{\{r, s\} \in \mathbb{N}^{(2)} \mid c(\{r, s\}) = i\}$. Per ogni $n \in \mathbb{N}$, per $i = 1, \dots, k$ consideriamo gli insiemi

$$A_i^{(n)} := \{m \in \mathbb{N} \mid \{n, m\} \in P_i\}.$$

Dato che per ogni $m \neq n$ è ben definito $c(\{n, m\})$, si ha che

$$\bigsqcup_{i=1}^{k} A_i^{(n)} = \mathbb{N} \setminus \{n\}.$$

Ora, $\{n\} \notin \mathcal{U}$ per quanto visto sopra ($\mathcal{U}$ non può contenere alcun insieme finito), quindi per le proprietà di ultrafiltro (si veda la Proposizione A.13 nell'Appendice A) $\mathbb{N} \setminus \{n\} \in \mathcal{U}$; dal Corollario A.14, sempre nell'Appendice A, deduciamo che per ogni n esiste un unico $i = 1, \dots, k$ tale che $A_i^{(n)} \in \mathcal{U}$.

Sia dunque $B_i := \{n \in \mathbb{N} \mid A_i^{(n)} \in \mathcal{U}\}$. Da quanto appena visto, $\mathbb{N} = B_1 \sqcup \cdots \sqcup B_k$, quindi esiste un unico j tale che $B_j \in \mathcal{U}$. Scegliamo dunque $x_1 \in B_j$, $x_2 \in B_j \cap A_j^{(x_1)}$, $x_3 \in B_j \cap A_j^{(x_1)} \cap A_j^{(x_2)}$ e così via.[7] L'insieme infinito $X := \{x_1, x_2, \dots\}$ soddisfa la tesi: infatti per ogni r si ha che $x_r \in A_j^{(x_1)} \cap \cdots \cap A_j^{(x_{r-1})}$, cioè che $\{x_r, x_s\} \in P_j$ per ogni $s = 1, \dots, r-1$. Ne deduciamo che $X^{(2)} \subseteq P_j$. □

[6] In effetti la dimostrazione è una semplice applicazione del Lemma di Zorn all'insieme $\{\mathcal{G} \mid \mathcal{G}$ è un filtro su X tale che $\mathcal{F} \subseteq \mathcal{G}\}$, parzialmente ordinato dall'inclusione.

[7] Notiamo che $B_j \neq \varnothing$ perché sta in $\mathcal{U}$; inoltre $x_1 \in B_j$ implica che $A_j^{(x_1)} \in \mathcal{U}$, quindi anche $B_j \cap A_j^{(x_1)} \in \mathcal{U}$ ed è dunque non vuoto (e non contiene x_1 per definizione di $A_j^{(x_1)}$). Il ragionamento si itera per ogni x_r.

Naturalmente questa dimostrazione è completamente ineffettiva: ci dice solo che esiste questo insieme X, ma non ci dà indicazioni su chi siano i suoi elementi né su come trovarli. Le dimostrazioni con ultrafiltri, però, sono sempre più usate nell'ambito della combinatoria infinita.

Appendice A

Ulteriori dimostrazioni

Durante il corso sono stati citati e/o usati alcuni risultati di cui non è stata vista la dimostrazione (e non è stato esplicitamente detto "non vedremo la dimostrazione"). In quest'appendice abbiamo voluto esporre alcune di queste dimostrazioni. Prima del risultato sono richiamate le pagine in cui esso è citato.

Pagina 98 – **Proposizione A.1.** *L'insieme $\mathcal{A}_W$ è un arrangiamento essenziale nello spazio W, che indicheremo con* $\operatorname{ess}(\mathcal{A})$.

Dimostrazione. Innanzitutto occorre dimostrare che $\dim(W \cap H) = \dim W - 1$ per ogni $H \in \mathcal{A}$, cioè che $W \cap H$ è effettivamente un iperpiano di W. Osserviamo che $\dim Y + \dim Y^{\perp} = n$ per costruzione (e questo vale in ogni caratteristica), cioè $\dim W = n - \dim Y$. Siano $(v_1, \dots, v_k)$ una base per Y e (α, a) tali che $H = \{x \in V \mid \langle \alpha, x \rangle = a\}$; allora

$$W \cap H = \left\{ x \in V \;\middle|\; \begin{pmatrix} — & v_1 & — \\ & \vdots & \\ — & v_k & — \\ — & \alpha & — \end{pmatrix} x = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a \end{pmatrix} \right\}. \tag{A.1}$$

Ora, $v_i \in Y$ per ogni $i = 1, \dots, k$ mentre $\alpha \in U$ e i due spazi sono in somma diretta; pertanto $\{v_1, \dots, v_k, \alpha\}$ è un insieme di vettori linearmente indipendenti e di conseguenza

$$\dim(W \cap H) = n - (\dim Y + 1) = \dim W - 1.$$

Supponiamo ora che $\mathcal{A}_W$ non sia essenziale. Per ogni $H \in \mathcal{A}$, siano $(\alpha_H, a_H) \in (V \setminus \{0\}) \times \mathbb{K}$ e $(\beta_H, b_H) \in (W \setminus \{0\}) \times \mathbb{K}$ tali che

$$H = \{x \in V \mid \langle \alpha_H, x \rangle = a_H\},$$
$$H \cap W = \{x \in W \mid \langle \beta_H, x \rangle = b_H\}.$$

Se $\mathcal{A}_W$ non è essenziale, abbiamo che $\langle \boldsymbol{\beta}_H \mid H \in \mathcal{A} \rangle \subsetneq W$, dunque esiste $\boldsymbol{w} \in W$, $\boldsymbol{w} \neq 0$, tale che $\langle \boldsymbol{w}, \boldsymbol{\beta}_H \rangle = 0$ per ogni $H \in \mathcal{A}$. Osserviamo ora che per ogni $\boldsymbol{z} \in W \cap H$ si ha $\boldsymbol{w} + \boldsymbol{z} \in W \cap H$: infatti

$$\langle \boldsymbol{w} + \boldsymbol{z}, \boldsymbol{\beta}_H \rangle = \langle \boldsymbol{w}, \boldsymbol{\beta}_H \rangle + \langle \boldsymbol{z}, \boldsymbol{\beta}_H \rangle = 0 + b_H = b_H.$$

D'altra parte $W \cap H \subseteq H$, quindi

$$\langle \boldsymbol{w} + \boldsymbol{z}, \boldsymbol{\alpha}_H \rangle = a_H \tag{A.2}$$

e anche

$$\langle \boldsymbol{z}, \boldsymbol{\alpha}_H \rangle = a_H; \tag{A.3}$$

sottraendo l'espressione (A.3) da (A.2) otteniamo che $\langle \boldsymbol{w}, \boldsymbol{\alpha}_H \rangle = 0$ per ogni $H \in \mathcal{A}$, cioè che $\langle \boldsymbol{w}, \boldsymbol{u} \rangle = 0$ per ogni $\boldsymbol{u} \in U$. Ricordando ora che $\langle \boldsymbol{w}, \boldsymbol{y} \rangle = 0$ per ogni $\boldsymbol{y} \in Y$ per definizione di W e che $Y \oplus U = \mathbb{K}^n$, possiamo concludere che $\langle \boldsymbol{w}, \boldsymbol{x} \rangle = 0$ per ogni $\boldsymbol{x} \in V$, ma questo è in contraddizione con il fatto che $\langle \cdot, \cdot \rangle$ è un prodotto scalare non degenere. □

Pagine 100 e 102 – **Lemma A.2.** *Sia $\mathcal{A}$ un arrangiamento centrale in $\mathbb{K}^n$. Allora*

$$\dim\left(\bigcap_{H \in \mathcal{A}} H\right) = n - \operatorname{rk}(\mathcal{A}).$$

Dopo aver sviluppato una prima dimostrazione, ci siamo accorti che ce n'è un'altra molto più semplice. Le riportiamo comunque entrambe per non cestinare completamente ciò che si è fatto.

Prima dimostrazione. Se $\mathcal{A} = \{H_1, \dots, H_m\}$, indichiamo con $\mathcal{A}_{(h)} := \{H_1, \dots, H_h\}$ e con $I_{(h)} := \bigcap_{i=1}^{h} H_i$. Procediamo per induzione sul numero di iperpiani da cui è formato $\mathcal{A}$.

$\boxed{h = 1}$ In questo caso $\operatorname{rk}(\mathcal{A}_{(1)}) = 1$ e l'intersezione è formata solo da H_1, che ha dimensione $n - 1$.

$\boxed{h - 1 \Rightarrow h}$ Notiamo che, dal momento che l'arrangiamento è centrale, l'intersezione di un qualunque numero di suoi iperpiani non può essere vuota, quindi possiamo applicare la formula di Grassmann nella versione affine. Sia $\boldsymbol{\alpha}_h$ il vettore normale all'iperpiano H_h e distinguiamo due casi.

- Se $\boldsymbol{\alpha}_h \in \langle \boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_{h-1} \rangle$, allora $\operatorname{rk}(\mathcal{A}_{(h)}) = \operatorname{rk}(\mathcal{A}_{(h-1)})$ e $\dim\langle I_{(h-1)} \cup H_h \rangle = n - 1$, dunque

$$\begin{aligned} \dim I_{(h)} &= \dim I_{(h-1)} + \dim H_h - \dim\langle I_{(h-1)} \cup H_h \rangle = \\ &= n - \operatorname{rk}(\mathcal{A}_{(h-1)}) + n - 1 - (n-1) = n - \operatorname{rk}(\mathcal{A}_{(h)}). \end{aligned}$$

- Se $\alpha_h \notin \langle \alpha_1, \ldots, \alpha_{h-1} \rangle$, allora $\mathrm{rk}(\mathcal{A}_{(h)}) = \mathrm{rk}(\mathcal{A}_{(h-1)}) + 1$ e $\dim\langle I_{(h-1)} \cup H_h \rangle = n$, dunque

$$\begin{aligned}\dim I_{(h)} &= \dim I_{(h-1)} + \dim H_h - \dim\langle I_{(h-1)} \cup H_h \rangle = \\ &= n - \mathrm{rk}(\mathcal{A}_{(h-1)}) + n - 1 - n = n - \mathrm{rk}(\mathcal{A}_{(h)}).\end{aligned}$$

In entrambi i casi si ha la tesi. □

Seconda dimostrazione. L'intersezione $t := \bigcap_{H \in \mathcal{A}} H$ è determinata da un sistema lineare la cui matrice associata A è formata dai vettori normali. È noto dall'algebra lineare che $\dim t = n - \mathrm{rk}(A)$; ma per definizione $\mathrm{rk}(A) = \mathrm{rk}(\mathcal{A})$. □

Pagina 103 – **Proposizione A.3.** *L'intersezione con W manda regioni di $\mathcal{A}$ in regioni di $\mathcal{A}_W$ biiettivamente.*

Dimostrazione. Ricordiamo che $W \oplus W^\perp = \mathbb{R}^n$. Sia $R \in \mathcal{R}(\mathcal{A})$ e sia $\mathbf{p} \in R$. Allora $\mathbf{p}$ soddisfa certe disuguaglianze della forma $\langle \mathbf{p}, \boldsymbol{\alpha} \rangle > a$ dove $\boldsymbol{\alpha} \in W$ è un vettore normale a qualche iperpiano di $\mathcal{A}$. Sia $\pi\colon \mathbb{R}^n \to W$ la proiezione (cioè $\pi(\mathbf{p}) = \boldsymbol{w}$ se $\mathbf{p} = \boldsymbol{w} + \mathbf{p}_0$, con $\boldsymbol{w} \in W$ e $\mathbf{p}_0 \in W^\perp$). Allora

$$\langle \mathbf{p}, \boldsymbol{\alpha} \rangle = \langle \boldsymbol{w} + \mathbf{p}_0, \boldsymbol{\alpha} \rangle = \langle \boldsymbol{w}, \boldsymbol{\alpha} \rangle + \langle \mathbf{p}_0, \boldsymbol{\alpha} \rangle = \langle \boldsymbol{w}, \boldsymbol{\alpha} \rangle$$

quindi $\pi(\mathbf{p})$ verifica le stesse disuguaglianze di $\mathbf{p}$, dunque $\pi(\mathbf{p}) \in R \cap W$. Questo prova che la mappa

$$\begin{array}{ccc} \mathcal{R}(\mathcal{A}) & \longrightarrow & \mathcal{R}(\mathcal{A}_W) \\ R & \longmapsto & R \cap W \end{array}$$

è ben definita ed è una corrispondenza biunivoca. □

Pagina 109 – **Proposizione A.4.** *Sia $\mathcal{A}$ un arrangiamento in $\mathbb{R}^n$ in posizione generica formato da m iperpiani. Allora $\#(\mathcal{R}(\mathcal{A})) \geqslant \#(\mathcal{R}(\mathcal{B}))$ per ogni altro arrangiamento $\mathcal{B}$ in $\mathbb{R}^n$ con m iperpiani.*

Lemma A.5. *Sia $f_n(m)$ il massimo numero di regioni in cui $\mathbb{R}^n$ viene diviso da un arrangiamento $\mathcal{A}$ con m iperpiani. Allora per ogni n si ha $f_n(k) < f_n(m)$ se $k < m$.*

Dimostrazione. È una semplice induzione basata sul fatto che se $\mathcal{A}$ è tale che $\#(\mathcal{R}(\mathcal{A})) = f_n(m)$, allora un qualsiasi iperpiano non appartenente ad $\mathcal{A}$ taglia almeno una regione di $\mathcal{A}$ in due. □

Dimostrazione della Proposizione A.4. Dimostriamo per induzione sul numero di iperpiani di $\mathcal{A}$. Il passo base è ovvio; per il passo induttivo, useremo la formula data dalla Proposizione 2.62. Sia $f_n(m)$ come nel lemma precedente e consideriamo un arrangiamento qualsiasi $\mathcal{B}$ in $\mathbb{R}^n$ con m iperpiani. Per costruzione,

l'arrangiamento $\mathcal{B}'$ ha $m-1$ iperpiani e vive anch'esso in $\mathbb{R}^n$, mentre $\mathcal{B}''$ è un arrangiamento di dimensione $n-1$ formato da k iperpiani, con $k \leqslant m-1$. Dunque

$$\#(\mathcal{R}(\mathcal{B})) = \#\big(\mathcal{R}(\mathcal{B}')\big) + \#\big(\mathcal{R}(\mathcal{B}'')\big) \leqslant f_n(m-1) + f_{n-1}(k).$$

Ora, se $\mathcal{A}$ è un arrangiamento di $\mathbb{R}^n$ con m iperpiani in posizione generica, anche $\mathcal{A}'$ e $\mathcal{A}''$ sono in posizione generica; inoltre $\mathcal{A}''$ ha esattamente $m-1$ iperpiani, poiché se si avesse $H_i \cap H_0 = H_j \cap H_0$ per qualche $H_i, H_j \in \mathcal{A} \smallsetminus \{H_0\}$ allora tale intersezione sarebbe uguale anche a $H_i \cap H_j \cap H_0$, in contraddizione con la posizione generica di $\mathcal{A}$. Applicando l'ipotesi induttiva

$$\#(\mathcal{R}(\mathcal{A})) = f_n(m-1) + f_{n-1}(m-1)$$

e per il lemma precedente

$$\#(\mathcal{R}(\mathcal{A})) = f_n(m-1) + f_{n-1}(m-1) \geqslant f_n(m-1) + f_{n-1}(k) \geqslant \#(\mathcal{R}(\mathcal{B})). \quad \square$$

Pagina 132 – **Proposizione A.6.** *C'è una corrispondenza biunivoca tra $\mathcal{M}_n$, l'insieme dei modelli per le k-colorazioni su cui agisce $\mathcal{S}_n$, e*

$$X := \{F\colon \{1,\dots,k\} \to \{0,\dots,n\} \mid F \textit{ crescente}^{\blacktriangleright 1} \textit{ e } F(k) = n\}.$$

Corollario A.7. *Il numero di modelli in $\mathcal{M}_n$ è $\binom{k+n-1}{n}$.*

Dimostrazione della Proposizione A.6. Per comodità di scrittura indicheremo con $[n] := \{1,\dots,n\}$. Osserviamo che se $A, B \subseteq \{1,\dots,n\}$ con $\#(A) = \#(B)$, allora esiste $\sigma \in \mathcal{S}_n$ tale che $\sigma(A) = B$; in altre parole, se l'intero gruppo $\mathcal{S}_n$ agisce su $\{1,\dots,n\}$, non conta quali elementi siano colorati in un certo modo, ma solo quanti. Quindi la relazione di equivalenza (3.1) si può riscrivere come

$$f \sim g \quad \text{se e solo se} \quad \#\{x \in [n] \mid f(x) = i\} = \#\{x \in [n] \mid g(x) = i\} \tag{A.4}$$

per ogni $i = 1,\dots,k$. Dal fatto che

$$\#\{x \in [n] \mid f(x) \leqslant i\} = \#\{x \in [n] \mid f(x) \leqslant i-1\} + \#\{x \in [n] \mid f(x) = i\}, \tag{A.5}$$

una semplice induzione su i mostra che la relazione (A.4) è equivalente a

$$f \sim g \quad \text{se e solo se} \quad \#\{x \in [n] \mid f(x) \leqslant i\} = \#\{x \in [n] \mid g(x) \leqslant i\}$$

per ogni $i = 1,\dots,k$. Quindi, scelta f per rappresentare un modello $[f] \in \mathcal{M}_n$, è ben definita la mappa $\Psi\colon \mathcal{M}_n \to X$ data da

$$\Psi(f)\colon i \mapsto \#\{x \in [n] \mid f(x) \leqslant i\}.$$

[1] Qui "crescente" è inteso in senso largo, ovvero vale che per ogni $i < j$ si ha $F(i) \leqslant F(j)$.

Dimostriamo ora che la mappa Ψ è biunivoca e la sua inversa $\Phi\colon X \to \mathcal{M}_n$ è data da

$$\Phi(F)\colon x \mapsto i \text{ se } F(i-1) < x \leqslant F(i)$$

in cui conveniamo $F(0) = 0$ per mantenere una scrittura compatta.

In primo luogo dimostriamo che le mappe f e $(\Phi \circ \Psi)(f)$ sono equivalenti sotto l'azione di $\mathcal{S}_n$: infatti per definizione $(\Phi \circ \Psi)(f)\colon x \mapsto i$ se e solo se

$$\Psi(f)(i-1) < x \leqslant \Psi(f)(i)$$

cioè

$$\#\{y \in [n] \mid f(y) \leqslant i-1\} < x \leqslant \#\{y \in [n] \mid f(y) \leqslant i\}$$

e, ricordando l'Equazione (A.5), otteniamo

$$x \leqslant \#\{y \in [n] \mid f(y) = i\}.$$

Di conseguenza

$$\#\{x \in [n] \mid (\Phi \circ \Psi)(f)(x) = i\} = \#\{y \in [n] \mid f(y) = i\}$$

da cui otteniamo $(\Phi \circ \Psi)(f) \sim f$ per la Relazione (A.4).

Terminiamo dimostrando che per ogni $F \in X$ si ha $(\Psi \circ \Phi)(F) = F$. Per definizione di Ψ, abbiamo che

$$(\Psi \circ \Phi)(F)(i) = \#\{x \in [n] \mid \Phi(F)(x) \leqslant i\}$$

ma per definizione di Φ si ha che $\Phi(F)(x) \leqslant i$ se e solo se $x \leqslant F(i)$, dunque

$$\#\{x \in [n] \mid \Phi(F)(x) \leqslant i\} = \#\{x \in [n] \mid x \leqslant F(i)\} = F(i)$$

e la dimostrazione è così conclusa. □

Dimostrazione del Corollario A.7. È noto che il numero di funzioni (debolmente) crescenti da un insieme C con $\#(C) = c$ a un insieme D con $\#(D) = d$ è $\binom{c+d-1}{c}$.[2] Ora, le funzioni crescenti $F\colon \{1, \dots, k\} \to \{0, \dots, n\}$ tali che $F(k) = n$ sono ovviamente in corrispondenza biunivoca con le funzioni crescenti $\tilde{F}\colon \{1, \dots, k-1\} \to \{0, \dots, n\}$, quindi

$$\#(X) = \binom{(n+1)+(k-1)-1}{k-1} = \binom{n+k-1}{k-1} = \binom{n+k-1}{n}. \qquad \square$$

[2] Identificando una funzione con la sua immagine, abbiamo che il numero di tali funzioni è uguale al numero di multiinsiemi di cardinalità c con elementi scelti in D.

Pagina 135 – **Proposizione A.8.** *Se $n \geqslant 3$, la mappa*

$$\begin{array}{ccc} \mathcal{S}_n & \longrightarrow & \mathcal{S}_{\binom{n}{2}} \\ \sigma & \longmapsto & \sigma^{(2)} \end{array}$$

è un omomorfismo iniettivo di gruppi.

Dimostrazione. È immediato verificare che $(\sigma \circ \tau)^{(2)} = \sigma^{(2)} \circ \tau^{(2)}$. Per l'iniettività, siano $\sigma, \tau \in \mathcal{S}_n$ tali che $\sigma^{(2)} = \tau^{(2)}$, cioè per ogni $\{i, j\} \in \wp_2(\{1, \dots, n\})$ si ha $\{\sigma(i), \sigma(j)\} = \{\tau(i), \tau(j)\}$. Distinguiamo due casi.

Se per ogni $\{i, j\}$ si ha $\sigma(i) = \tau(i)$ e $\sigma(j) = \tau(j)$, allora $\sigma = \tau$. Supponiamo dunque che esistano i e j tali che $\sigma(i) = \tau(j)$ e $\sigma(j) = \tau(i)$. Sia $k \neq i, j$; per ipotesi $\sigma^{(2)}(i, k) = \tau^{(2)}(i, k)$, cioè $\{\sigma(i), \sigma(k)\} = \{\tau(i), \tau(k)\}$. Ma ora

- se $\sigma(i) = \tau(i)$, dal fatto che $\tau(i) = \sigma(j)$ otterremmo $\sigma(i) = \sigma(j)$;
- se $\sigma(i) = \tau(k)$, dal fatto che $\sigma(i) = \tau(j)$ otterremmo $\tau(j) = \tau(k)$;

in entrambi i casi giungiamo a una contraddizione. □

Pagina 140 – **Lemma A.9.** *Siano $G_1 < \mathcal{S}_a$, $G_2 < \mathcal{S}_b$ e $n := a + b$. Possiamo vedere $G_1 \times G_2$ come sottogruppo di $\mathcal{S}_n$ nel seguente modo: per ogni $(\sigma_1, \sigma_2) \in G_1 \times G_2$, definiamo $\iota(\sigma_1, \sigma_2) \in \mathcal{S}_n$ come*

$$\begin{array}{rccc} \iota(\sigma_1, \sigma_2) : \{1, \dots, n\} & \longrightarrow & \{1, \dots, n\} & \\ i & \longmapsto & \begin{cases} \sigma_1(i) & \text{se } i \leqslant a \\ a + \sigma_2(i - a) & \text{se } i > a \end{cases} & \end{array}$$

(in pratica, permutiamo $\{1, \dots, a\}$ con elementi da G_1 e $\{a + 1, \dots, a + b\}$ con elementi da G_2). La mappa $\iota\colon G_1 \times G_2 \to \mathcal{S}_n$ è un omomorfismo di gruppi iniettivo. Allora

$$Z(G_1 \times G_2; X_1, \dots, X_n) = Z(G_1; X_1, \dots, X_a) Z(G_2; X_1, \dots, X_b);$$

in particolare, in $Z(G_1 \times G_2; X_1, \dots, X_n)$ non compaiono indeterminate con indice maggiore di $\max\{a, b\}$.

Dimostrazione. Per costruzione, detto c_i il numero di i-cicli di una permutazione, si ha $c_i(\iota(\sigma_1, \sigma_2)) = c_i(\sigma_1) + c_i(\sigma_2)$ per ogni $i = 1, \dots, n$. Quindi

$$\begin{aligned} Z(G_1 \times G_2; X_1, \dots, X_n) &= \\ &= \frac{1}{\#(G_1)\,\#(G_2)} \sum_{(\sigma_1, \sigma_2) \in G_1 \times G_2} \prod_{k=1}^{n} X_k^{c_k(\iota(\sigma_1, \sigma_2))} = \\ &= \frac{1}{\#(G_1)\,\#(G_2)} \sum_{(\sigma_1, \sigma_2) \in G_1 \times G_2} \prod_{k=1}^{n} X_k^{c_k(\sigma_1) + c_k(\sigma_2)} = \end{aligned}$$

$$= \frac{1}{\#(G_1)} \left(\sum_{\sigma_1 \in G_1} \prod_{k=1}^{n} X_k^{c_k(\sigma_1)} \right) \frac{1}{\#(G_2)} \left(\sum_{\sigma_2 \in G_2} \prod_{k=1}^{n} X_k^{c_k(\sigma_2)} \right) =$$
$$= Z(G_1; X_1, \ldots, X_a) Z(G_2; X_1, \ldots, X_b). \qquad \square$$

Il risultato precedente si generalizza senza problemi a qualsiasi numero di sottogruppi $G_1 < \mathcal{S}_{a_1}, \ldots, G_k < \mathcal{S}_{a_k}$ con $a_1 + \cdots + a_k = n$.

Pagina 146 – **Proposizione A.10.** *Per i coefficienti* q*-binomiali vale*

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q.$$

Dimostrazione. Osserviamo che per ogni $k = 1, \ldots, n-1$ si ha

$$(n)_q = 1 + \cdots + q^{n-1} = 1 + \cdots + q^{k-1} + q^k(1 + \cdots + q^{n-k-1}) = (k)_q + q^k(n-k)_q.$$

Dunque

$$\begin{aligned}
\binom{n}{k}_q &= \frac{(n)_q!}{(k)_q!(n-k)_q!} = \frac{(n-1)_q!(n)_q}{(k)_q!(n-k)_q!} = \frac{(n-1)_q!((k)_q + q^k(n-k)_q)}{(k)_q!(n-k)_q!} = \\
&= \frac{(n-1)_q!}{(k-1)_q!(n-k)_q!} + q^k \frac{(n-1)_q!}{(k)_q!(n-k-1)_q!} = \\
&= \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q. \qquad \square
\end{aligned}$$

Pagina 168 – **Proposizione A.11.** *Una* k*-dissezione di un* n*-agono è formata al massimo da* $k = n - 3$ *diagonali.*

Dimostrazione. Per induzione su n.

$\boxed{n = 3}$ Ovviamente un triangolo non ammette dissezioni, perché non ha diagonali.

$\boxed{3, \ldots, n-1 \Rightarrow n}$ Osserviamo che una k-dissezione è fatta con il massimo numero di diagonali se e solo se divide il poligono in triangoli, cioè è una triangolazione. Infatti da una k-dissezione si può ottenere una $(k+1)$-dissezione solo tracciando una diagonale di un sottopoligono già presente. Quindi, se il poligono è triangolato, non si possono aggiungere altre diagonali perché i triangoli non ne possiedono; d'altra parte, se per assurdo il poligono avesse raggiunto il massimo numero di diagonali senza essere triangolato, un qualsiasi non-triangolo possiede una diagonale che potrebbe essere aggiunta alla dissezione.

Ora, una qualsiasi diagonale divide l'n-agono P in due poligoni con meno lati, ad esempio in un n_1-agono P_1 e un n_2-agono P_2 con $n_1 < n$, $n_2 < n$ e $n_1 + n_2 - 2 = n$ perché si deve togliere dalla somma dei lati la diagonale stessa, contata due volte. Per ipotesi induttiva, P_1 è $(n_1 - 3)$-dissecato con una

triangolazione e P_2 è (n_2-3)-dissecato con una triangolazione; l'unione di queste dà una triangolazione di P, che quindi ci fornisce il valore k richiesto. Ma quante sono queste diagonali? Ce ne sono n_1-3 da P_1, n_2-3 da P_2, e una che abbiamo aggiunto per dividere P in P_1 e P_2. Dunque il massimo numero di diagonali è

$$(n_1-3)+(n_2-3)+1=(n_1+n_2-2)-3=n-3. \qquad \square$$

Pagina 185 – **Teorema A.12.** *Siano* $a, b \in \mathbb{R}$ *con* $a < b$. *Allora* $\mathbb{R}^k \to (\{a,b\})_k$ *per ogni* k, *quindi* $\{a,b\} \subset \mathbb{R}$ *è di Ramsey.*

Dimostrazione. Consideriamo i $k+1$ punti $\mathbf{x}^{(i)} \in \mathbb{R}^{k+1}$, per $i = 1,\dots,k+1$, che hanno $(b-a)/\sqrt{2}$ nella i-esima coordinata e 0 altrove. Osserviamo che tutti questi punti appartengono all'iperpiano

$$H := \left\{ \mathbf{x} \in \mathbb{R}^{k+1} \;\middle|\; x_1 + \cdots + x_{k+1} = \frac{b-a}{\sqrt{2}} \right\} \simeq \mathbb{R}^k.$$

Se coloriamo H con k colori, poiché gli $\mathbf{x}^{(i)}$ sono $k+1$, per il *pigeonhole principle* esistono $\mathbf{x}^{(i)}$ e $\mathbf{x}^{(j)}$ dello stesso colore. Dato che

$$\|\mathbf{x}^{(i)} - \mathbf{x}^{(j)}\| = \sqrt{\left(\frac{b-a}{\sqrt{2}}\right)^2 + \left(\frac{b-a}{\sqrt{2}}\right)^2} = b-a,$$

abbiamo che $\{\mathbf{x}^{(i)}, \mathbf{x}^{(j)}\}$ è congruente ad $\{a,b\}$ e questo prova che $\mathbb{R}^k \to (\{a,b\})_k$. $\square$

Pagina 191 – **Proposizione A.13.** *Per un filtro* $\mathcal{F}$ *su* X, *sono equivalenti:*

1. *per ogni* $A \in \wp(X)$, *se* $A^c \notin \mathcal{F}$ *allora* $A \in \mathcal{F}$;[3]
2. *ogni volta che* $A \cup B \in \mathcal{F}$, *allora* $A \in \mathcal{F}$ *oppure* $B \in \mathcal{F}$;
3. $\mathcal{F}$ *è massimale (rispetto all'inclusione in* $\wp(X)$*).*

In particolare, il punto 1. ci dice che $\mathcal{F}$ è un ultrafiltro se e solo se per ogni $A \subseteq X$ esattamente uno tra A e A^c appartiene a $\mathcal{F}$. Inoltre si dimostra facilmente per induzione che il punto 2. è equivalente a

2′. ogni volta che un'unione finita $A_1 \cup \cdots \cup A_r \in \mathcal{F}$, allora esiste $i = 1,\dots,r$ tale che $A_i \in \mathcal{F}$.

Pagina 191 – **Corollario A.14.** *Sia* $\mathcal{U}$ *un ultrafiltro su* X. *Se* $A \sqcup B \in \mathcal{U}$, *allora esattamente uno tra* A *e* B *appartiene a* $\mathcal{U}$.

[3] Osserviamo che per ogni filtro $\mathcal{F}$ se $A \in \mathcal{F}$ allora $A^c \notin \mathcal{F}$, in quanto se così non fosse si avrebbe che anche $A \cap A^c = \varnothing \in \mathcal{F}$.

Naturalmente il corollario si generalizza a un'unione disgiunta di un numero finito di insiemi: se $A_1 \sqcup \cdots \sqcup A_n \in \mathcal{U}$, allora esiste ed è unico i tale che $A_i \in \mathcal{U}$.

Lemma A.15. *Sia $\mathcal{H} \subseteq \wp(X)$, $\mathcal{H} \neq \varnothing$, una famiglia di sottoinsiemi con la* proprietà dell'intersezione finita *(PIF), cioè tali che per ogni $n \geqslant 1$ e per ogni $A_1, \ldots, A_n \in \mathcal{H}$ si ha $A_1 \cap \cdots \cap A_n \neq \varnothing$. Allora esiste ed è unico il più piccolo filtro che contiene $\mathcal{H}$, detto* filtro generato da $\mathcal{H}$.

Dimostrazione. Sia

$$\mathcal{F} := \{B \subseteq X \mid \exists\, n \geqslant 1,\ \exists\, A_1, \ldots, A_n \in \mathcal{H} \text{ tali che } A_1 \cap \cdots \cap A_n \subseteq B\},$$

cioè l'insieme dei sovrainsiemi delle intersezioni finite di elementi di $\mathcal{H}$. Ovviamente $\mathcal{H} \subseteq \mathcal{F}$: per ogni $H \in \mathcal{H}$ è sufficiente prendere $n = 1$ e H stesso come testimoni. Dimostriamo che $\mathcal{F}$ è un filtro su X.

1. Supponiamo che $B_1, B_2 \in \mathcal{F}$ e siano $A_1, \ldots, A_n$, $A'_1, \ldots, A'_m$ insiemi di $\mathcal{H}$ tali che $A_1 \cap \cdots \cap A_n \subseteq B_1$ e $A'_1 \cap \cdots \cap A'_m \subseteq B_2$. Allora

   $$A_1 \cap \cdots \cap A_n \cap A'_1 \cap \cdots \cap A'_m \subseteq B_1 \cap B_2$$

   e questo prova che $B_1 \cap B_2 \in \mathcal{F}$.

2. Siano $B \in \mathcal{F}$ e $A_1, \ldots, A_n \in \mathcal{H}$ tali che $A_1 \cap \cdots \cap A_n \subseteq B$. Allora banalmente per ogni $C \supseteq B$ si ha $A_1 \cap \cdots \cap A_n \subseteq B \subseteq C$ e quindi $C \in \mathcal{F}$.

3. Un qualsiasi $H \in \mathcal{H}$ dimostra che $X \in \mathcal{F}$. D'altra parte, se per assurdo $\varnothing \in \mathcal{F}$, allora $A_1 \cap \cdots \cap A_n \subseteq \varnothing$ per certi $A_1, \ldots, A_n \in \mathcal{H}$, ma questo è assurdo perché $A_1 \cap \cdots \cap A_n \neq \varnothing$ per la PIF.

Sia ora $\mathcal{G}$ un filtro che contiene $\mathcal{H}$. Le proprietà di filtro garantiscono che per ogni $A_1, \ldots, A_n \in \mathcal{H}$ si ha $A_1 \cap \cdots \cap A_n \in \mathcal{G}$, quindi ogni B tale che $A_1 \cap \cdots \cap A_n \subseteq B$ appartiene a $\mathcal{G}$. Dunque $\mathcal{F} \subseteq \mathcal{G}$. □

Dimostrazione della Proposizione A.13. 1. ⇒ 2. Supponiamo per assurdo che $A \cup B \in \mathcal{F}$ ma $A \notin \mathcal{F}$ e $B \notin \mathcal{F}$. Segue dal punto 1. che $A^c \in \mathcal{F}$ e $B^c \in \mathcal{F}$, dunque $A^c \cap B^c = (A \cup B)^c \in \mathcal{F}$ e quindi $(A \cup B) \cap (A \cup B)^c = \varnothing \in \mathcal{F}$.
2. ⇒ 3. Sia $\mathcal{G} \supseteq \mathcal{F}$ un filtro che estenda $\mathcal{F}$. Per assurdo, sia $A \in \mathcal{G} \smallsetminus \mathcal{F}$. Poiché $A \cup A^c = X \in \mathcal{F}$ e $A \notin \mathcal{F}$, abbiamo che $A^c \in \mathcal{F} \subseteq \mathcal{G}$. Ma questo porta a un assurdo, perché si avrebbe $A \cap A^c = \varnothing \in \mathcal{G}$.
3. ⇒ 1. Sia $\mathcal{F}$ massimale e supponiamo per assurdo che esista A tale che $A \notin \mathcal{F}$ e $A^c \notin \mathcal{F}$. Osserviamo che $\mathcal{F} \cup \{A\}$ è una famiglia con la PIF: infatti, se $B_1, \ldots, B_n \in \mathcal{F} \cup \{A\}$,

- se $B_i \in \mathcal{F}$ per ogni i, allora $B_1 \cap \cdots \cap B_n \in \mathcal{F}$ ed è dunque diversa dal vuoto;

- se esiste i tale che $B_i = A$, possiamo scrivere $B := B_1 \cap \cdots \cap B_{i-1} \cap B_{i+1} \cap \cdots \cap B_n \in \mathcal{F}$ e, se $B \cap A = \varnothing$, allora $B \subseteq A^c$, ma $B \in \mathcal{F}$ implica in tal caso $A^c \in \mathcal{F}$ contro l'ipotesi.

Detto $\mathcal{G}$ il filtro generato da $\mathcal{F} \cup \{A\}$, abbiamo $\mathcal{F} \subseteq \mathcal{G}$ e quindi $\mathcal{F} = \mathcal{G}$ per massimalità di $\mathcal{F}$; ma questo significa che $A \in \mathcal{F}$, in contraddizione con l'ipotesi. □

Dimostrazione del Corollario A.14. Per l'equivalenza 2. della Proposizione A.13 almeno uno tra A e B appartiene a $\mathcal{U}$. D'altra parte non possono appartenervi entrambi, perché altrimenti $A \cap B = \varnothing \in \mathcal{U}$. □

Appendice B

Numeri di Kirkman-Cayley

Seminario del 27/05/2015 – prof. Giovanni Gaiffi

Abbiamo visto che il numero di $(k-1)$-dissezioni di un $(n+1)$-agono convesso (con i lati etichettati) è dato dal numero di Kirkman-Cayley

$$D_{n+1,k-1} = \frac{1}{k}\binom{n-2}{k-1}\binom{n+k-1}{k-1}. \tag{B.1}$$

Ci sono dimostrazioni dirette della formula precedente, ad esempio con le funzioni generatrici. Meno comuni sono le *dimostrazioni per biiezione*, in cui si stabilisce una corrispondenza biunivoca tra gli oggetti che si vorrebbe contare (nel nostro caso le dissezioni di poligoni) e altri insiemi dei quali è più facile trovare la cardinalità. In quest'appendice presentiamo l'*outline* di una dimostrazione per biiezione della Formula (B.1), senza scendere nel dettaglio delle dimostrazioni delle corrispondenze biunivoche usate.

Teorema B.1. *Il numero di* $(k-1)$*-dissezioni di un* $(n+1)$*-agono convesso con i lati etichettati (dai numeri* $0,\dots,n$*) è uguale al numero di modi di mettere* k *coppie di parentesi bilanciate nella sequenza* $1,\dots,n$ *tali che*

- *ci sia la parentesi "totale" che comprenda l'intera lista;*
- *ogni parentesi includa almeno due oggetti.*[1]

Indichiamo con $\mathcal{S}_2((1,\dots,n),k)$ *l'insieme dei modi di mettere le parentesi che soddisfano queste proprietà.*

Più in generale denotiamo con $\mathcal{S}_2((a_1,\dots,a_n),k)$ l'insieme dei modi di mettere le parentesi come indicato nel Teorema B.1 nella sequenza $a_1,\dots,a_n$.

[1] Ad esempio, $(12((34)5))$ è lecita, mentre né $1((234)5)$ né $(12(3)(45))$ lo sono.

Naturalmente la cardinalità di $\mathcal{S}_2((a_1, \ldots, a_n), k)$ dipende solo dal fatto che la sequenza $a_1, \ldots, a_n$ sia formata da n simboli, quindi in virtù del Teorema B.1 essa è sempre uguale a $D_{n+1,k-1}$.

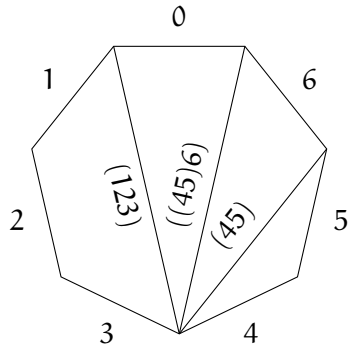


Figura B.1: Corrispondenza tra dissezioni e parentesi. In figura è rappresentata la dissezione corrispondente a $((123)((45)6))$.

La Figura B.1 mostra come ottenere una disposizione delle parentesi a partire da una dissezione. A grandi linee, il procedimento è il seguente:

1. si parte dalle etichette $0, \ldots, n$ sui lati dell'$(n+1)$-agono;
2. si sceglie un sottopoligono nella dissezione che abbia tutti i lati etichettati tranne uno e che non contenga il lato con l'etichetta 0;
3. si etichetta il lato mancante scrivendo in ordine le etichette degli altri lati e racchiudendo il tutto con una coppia di parentesi;
4. si riparte dal punto 2. finché non si arriva al poligono con il lato 0; a quel punto si scrivono in ordine le etichette dei lati di questo poligono e si termina con una coppia di parentesi che racchiuda l'intera stringa.

Pur avendo stabilito una corrispondenza biunivoca tra le $(k-1)$-dissezioni di un $(n+1)$-agono e $\mathcal{S}_2((1, \ldots, n), k)$, risulta più comodo contare la cardinalità dell'insieme

$$\mathcal{S}_2(n, k) := \bigcup_{\sigma \in \mathcal{S}_n} \mathcal{S}_2((\sigma(1), \ldots, \sigma(n)), k)$$

cioè tutti i modi di mettere le parentesi in una lista formata dai numeri $1, \ldots, n$ disposti in qualunque ordine. Naturalmente, essendo un'unione disgiunta, si ha che

$$\#(\mathcal{S}_2(n, k)) = n! \cdot D_{n+1,k-1}. \tag{B.2}$$

A questo punto abbiamo un insieme i cui elementi sono stringhe che contengono i numeri $1, \dots, n$ e k coppie di parentesi bilanciate. Esse possono essere rappresentate da alberi orientati con radice su n foglie (etichettate da 1 a n), in cui i figli di ciascun nodo sono ordinati.[2] In particolare,

- ogni nodo che non sia una foglia rappresenta una sottostringa che inizia con una parentesi aperta e termina con la rispettiva parentesi chiusa (la radice rappresenta l'intera stringa);
- c'è un arco dal nodo i al nodo j se la stringa j è contenuta nella stringa i e non c'è un'altra stringa ℓ tale che $j \subsetneq \ell \subsetneq i$.

La Figura B.2 mostra un esempio di questa associazione. Notiamo che, poiché ogni parentesi contiene almeno due oggetti, da ogni nodo interno partono almeno due archi.

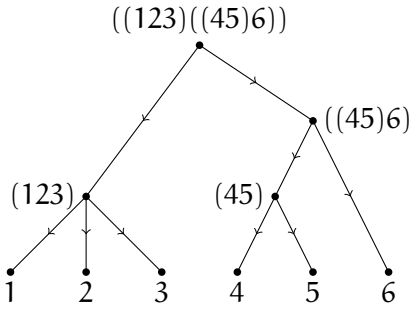


Figura B.2: Corrispondenza tra parentesi e alberi. In figura è rappresentato l'albero corrispondente a $((123)((45)6))$.

Teorema B.2. *Denotiamo con $\mathcal{T}_2(n, k)$ l'insieme degli alberi orientati con radice su n foglie, con k nodi interni, con i figli ordinati e tali che da ogni nodo interno partano almeno due archi. La costruzione descritta sopra induce una corrispondenza biunivoca tra $\mathcal{S}_2(n, k)$ e $\mathcal{T}_2(n, k)$.*

Non possiamo però fermarci qui, perché non sappiamo contare gli elementi di $\mathcal{T}_2(n, k)$: è necessario cercare altre corrispondenze biunivoche. Per fare ciò, dobbiamo etichettare anche i vertici interni con le etichette $\{n + 1, \dots, n + k\}$ e lo faremo nel modo seguente (si veda anche la Figura B.3).

[2] In altre parole, è possibile dire quale sia il primo figlio di un nodo, quale il secondo e così via: alberi in cui i figli sono ordinati in modo diverso devono essere considerati diversi. Nella rappresentazione grafica dell'albero, supporremo che l'ordine sia fissato dalla disposizione dei figli da sinistra a destra.

1. Sia $N := n + k - 1$ e fissiamo un ordinamento parziale su $\mathcal{P}(\{1, \dots, N\})$ tale che se $A \cap B = \varnothing$ allora A e B sono confrontabili: diciamo che $A \prec B$ se $\min A < \min B$.

2. Per ogni nodo interno i definiamo l'insieme A_i i cui elementi sono i nodi j per i quali esiste un arco da i a j, cioè l'insieme dei figli del nodo i.

3. Scegliamo i nodi $i_1, \dots, i_h$ tali che $A_{i_1}, \dots, A_{i_h}$ siano formati da nodi già etichettati. Senza perdita di generalità supponiamo $A_{i_1} \prec \cdots \prec A_{i_h}$.

4. Etichettiamo $i_1, \dots, i_h$ con le prime etichette non ancora usate, in modo che sia rispettato l'ordine indotto da $\prec$.

5. Ripetiamo i punti 3. e 4. finché tutti i nodi interni, tranne la radice, non siano stati etichettati con i numeri da $n + 1$ a N. Etichettiamo infine la radice con $N + 1$.

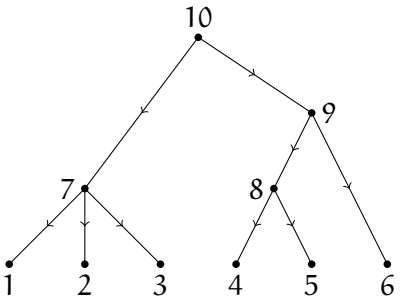


Figura B.3: Etichette assegnate ai nodi interni.

Sia $\mathcal{P}_2(N, k)$ l'insieme delle partizioni di $\{1, \dots, N\}$ in k parti tali che ciascuna classe abbia cardinalità almeno 2 e sia *internamente ordinata*, cioè consideriamo distinte due partizioni che abbiano le stesse classi (come insiemi) ma con gli elementi di una classe ordinati in modo diverso. Ad esempio, le due partizioni $(1, 2, 3) \cup (4, 5)$ e $(2, 1, 3) \cup (4, 5)$ sono considerate diverse. A un elemento di $\mathcal{T}_2(n, k)$ possiamo associare una partizione di $\mathcal{P}_2(N, k)$: nelle notazioni di prima, dopo aver etichettato anche i nodi interni (siano essi $i_1, \dots, i_k$) consideriamo la partizione

$$A_{i_1} \sqcup \cdots \sqcup A_{i_k}$$

in cui ciascun A_i, essendo formato dai figli dell'i-esimo nodo, è internamente ordinato. Per esempio, la partizione associata all'albero della Figura B.3 è

$$(1, 2, 3), (4, 5), (8, 6), (7, 9).$$

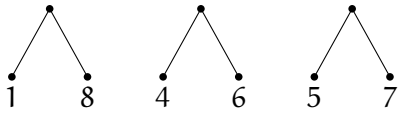
Teorema B.3. *C'è una corrispondenza biunivoca tra* $\mathcal{T}_2(n,k)$ *e* $\mathcal{P}_2(N,k)$.

Esempio B.1. In questo caso vediamo anche come andare nel verso opposto, cioè come costruire un albero in $\mathcal{T}_2(n,k)$ a partire da una partizione. Scegliamo, per esempio, $n = 9$, $k = 6$ e la partizione

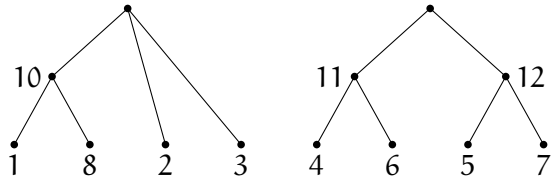
$$(10,2,3),(4,6),(5,7),(1,8),(11,12),(13,14,9).$$

Gli insiemi che compongono la partizione, vista la costruzione inversa, sono formati dai figli dei nodi interni: dobbiamo solo stabilire chi è figlio di chi, in modo che sia rispettato l'ordine dato dalle etichette.

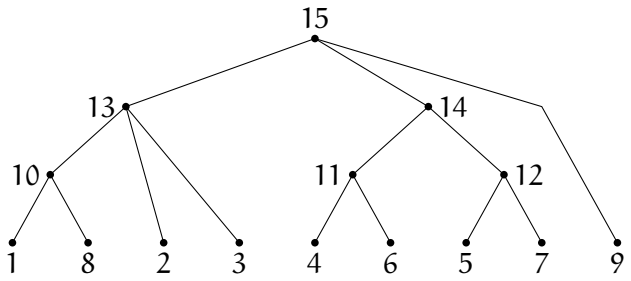
Innanzitutto osserviamo che per il *pigeonhole principle* esiste sempre almeno un insieme della partizione formato solo da foglie; nel nostro caso $(4,6)$, $(5,7)$ e $(1,8)$. Iniziamo a disporre questi nodi:



Il passo successivo consiste nell'assegnare un padre a tutti questi nodi. Per rispettare l'ordine delle etichette nei nodi intermedi, i tre padri devono essere i nodi 10, 11 e 12 e, dal momento che $(1,8) \prec (4,6) \prec (5,7)$, si ha che 10 è padre di 1 e 8, 11 lo è di 4 e 6 e 12 di 5 e 7. Consideriamo ora le parti che contengono 10, 11 e 12: esse sono $(10,2,3)$ e $(11,12)$. Di conseguenza siamo obbligati a continuare l'albero in questo modo:



Ora dobbiamo dare un padre ai nodi 10, 2, 3, 11 e 12. Le etichette successive sono 13 e 14 e, dato che $(10,2,3) \prec (11,12)$, ai primi è assegnato il 13 e ai secondi il 14. D'altra parte è rimasto solo l'insieme $(13,14,9)$: possiamo dunque completare l'albero, etichettando anche la radice con 15.



Osservazione. Notiamo che sull'insieme $\mathcal{T}_2(n,k)$ agisce il gruppo $\mathcal{S}_n$ permutando le foglie, mentre su $\mathcal{P}_2(N,k)$ agisce $\mathcal{S}_N$ permutando gli elementi degli insiemi. A causa della biiezione, possiamo leggere ciascuna azione nell'altro insieme. Scopriamo che esse *non sono compatibili*, nel senso che non c'è alcun legame tra loro: in effetti, potremmo considerare il sottogruppo $H < \mathcal{S}_N$ isomorfo a $\mathcal{S}_n$ dato dalle permutazioni che agiscono sui primi n elementi di $\{1,\dots,N\}$ e considerare l'azione di H sui due insiemi; ebbene, quest'azione e quella di $\mathcal{S}_n$ sono molto diverse tra loro. Ne vedremo un esempio alla fine di quest'appendice.

Siamo quasi arrivati in fondo alla catena di biiezioni; per far tornare più comodo il conto introduciamo un nuovo insieme, $\mathcal{P}_2^*(N,k)$, che è formato dagli elementi di $\mathcal{P}_2(N,k)$ in cui una delle parti è distinta dalle altre (ad esempio, $(1,2,3),{}^*(4,5),(8,6),(7,9)$ è una partizione con una parte "marcata"). Chiaramente per ogni elemento di $\mathcal{P}_2(N,k)$ possiamo scegliere una qualsiasi delle k parti da marcare, quindi

$$\#(\mathcal{P}_2^*(N,k)) = k \cdot \#(\mathcal{P}_2(N,k)).$$

Teorema B.4. *C'è una corrispondenza biunivoca tra $\mathcal{P}_2^*(N,k)$ e l'insieme formato dalle terne (I,σ,D) in cui*

- $I = (i_1,\dots,i_n)$, $i_1 < \cdots < i_n$, *è una sottolista di* $1,\dots,N$ *di cardinalità* n*;*
- $\sigma \in \mathcal{S}_n$*;*
- D *è una sottolista di* $i_{\sigma(2)},\dots,i_{\sigma(n-1)}$ *di cardinalità* $k-1$.

Finalmente abbiamo trovato un insieme i cui elementi si contano facilmente! Infatti abbiamo $\binom{n+k-1}{n} = \binom{n+k-1}{k-1}$ modi per scegliere I, $n!$ modi per σ e $\binom{n-2}{k-1}$ modi per scegliere D. Dunque, ricomponendo i pezzi, risulta

$$\begin{aligned} n! \cdot D_{n+1,k-1} &= \#(\mathcal{S}_2(n,k)) = \#(\mathcal{T}_2(n,k)) = \#(\mathcal{P}_2(N,k)) = \#(\mathcal{P}_2^*(N,k))/k = \\ &= \frac{1}{k} \cdot \binom{n+k-1}{k-1} \cdot n! \cdot \binom{n-2}{k-1} \end{aligned}$$

e la Formula (B.1) è dimostrata.

Esempio B.2. Vediamo la biiezione del Teorema B.4, cioè come costruire una partizione a partire da una terna. In questo esempio prendiamo $n = 7$ e $k = 4$; dobbiamo scegliere sette elementi in $1,\dots,10$, ad esempio $I := (i_1,\dots,i_7) = (1,2,3,4,6,9,10)$. Dopodiché scegliamo una permutazione $\sigma \in \mathcal{S}_7$ qualsiasi, diciamo $\sigma := (1\ 2\ 5\ 3)(4\ 7)$. Applicando σ ad I otteniamo

$$\sigma(I) = (i_2, i_5, i_1, i_7, i_3, i_6, i_4) = (2,6,1,10,3,9,4).$$

Togliendo primo ed ultimo elemento resta $(6, 1, 10, 3, 9)$ e tra questi elementi ne dobbiamo scegliere tre, ad esempio $D = (1, 3, 9)$.

Con questi dati vogliamo costruire una partizione di $\{1, \dots, 10\}$ in quattro parti, di cui una marcata, ciascuna con almeno due elementi e internamente ordinata. Iniziamo predisponendo quattro scatole vuote

$$^*(\quad), (\quad), (\quad), (\quad).$$

1. Percorriamo $\sigma(I)$ a partire da $i_{\sigma(n)}$ ciclicamente fino ad arrivare al primo elemento di D e mettiamo tutti i numeri così trovati nella scatola marcata.[3] Nel nostro esempio, partiamo da 4 e ci fermiamo quando arriviamo a 1, trovando (in ordine) 4, 2 e 6; quindi scriviamo

$$^*(4, 2, 6), (\quad), (\quad), (\quad).$$

2. Inseriamo al primo posto di ciascuna parte ancora vuota gli elementi di $\{1, \dots, N\}$ che erano stati esclusi da I, nell'esempio 5, 7 e 8:

$$^*(4, 2, 6), (5, \quad), (7, \quad), (8, \quad).$$

3. Prendiamo ora il primo elemento di D e scorriamo $\sigma(I)$ finché non troviamo l'elemento di D successivo (nel nostro caso, a partire da 1 troviamo 10 e ci fermiamo, perché il prossimo elemento di $\sigma(I)$ è 3 che appartiene a D). Sistemiamo l'elemento di D e tutti quelli trovati in questo modo nella prima scatola incompleta:

$$^*(4, 2, 6), (5, 1, 10), (7, \quad), (8, \quad).$$

4. Ripetiamo il passo precedente con il secondo elemento di D, poi il terzo, e così via fino ad arrivare all'ultimo elemento di D. Nel nostro caso occorre scorrere la lista altre due volte e in entrambi i casi troviamo un solo elemento: subito dopo il 3 c'è 9, che appartiene a D, e dopo il 9 siamo arrivati a $i_{\sigma(n)}$, dunque ci fermiamo. La partizione completa è

$$^*(4, 2, 6), (5, 1, 10), (7, 3), (8, 9).$$

Come corollario di questo lungo percorso fatto di corrispondenze biunivoche, sappiamo come contare i modi di mettere delle parentesi bilanciate in una stringa. Questi possono essere interpretati come vertici di uno speciale politopo, l'*associaedro*. Sono molto studiate le varietà che possono essere realizzate come

[3] Osserviamo che la cardinalità di questa parte è almeno 2.

CW-complessi usando copie dell'associaedro come mattoncini costitutivi. Ora, grazie ai numeri di Kirkman-Cayley, conosciamo il numero delle facce dell'associaedro e questo ci permette, per esempio, di ricavare la caratteristica di Eulero di tali varietà.

Per concludere, vediamo un esempio di incompatibilità delle varie azioni dei gruppi simmetrici sugli oggetti che abbiamo introdotto. Prendiamo $n = 5$ e $k = 4$ e consideriamo la stringa

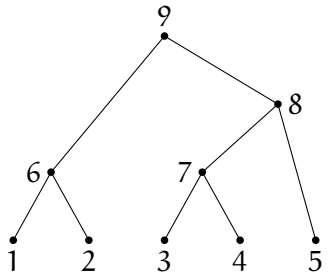
$$((12)((34)5)). \tag{B.3}$$

Consideriamo l'azione di $\mathcal{S}_5$ su $\mathcal{S}_2(5,4)$ e, ad esempio, scegliamo $\sigma = (1\ 3)$. Applicando σ a (B.3) otteniamo

$$((32)((14)5)). \tag{B.4}$$

Dall'altra parte, c'è un'azione di $\mathcal{S}_8$ ottenuta tramite le biiezioni. Se leggiamo σ dentro questo $\mathcal{S}_8$ e lo facciamo agire su (B.3), cosa succede?

Per prima cosa trasportiamo la stringa (B.3) lungo le biiezioni, in modo da leggere l'azione di $\mathcal{S}_8$ dove essa è più naturale. L'albero in $\mathcal{T}_2(5,4)$ associato a (B.3) è



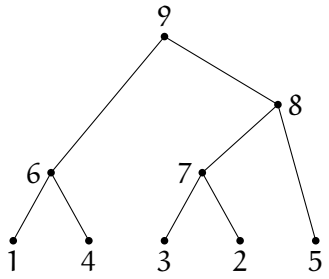
da cui ricaviamo la partizione in $\mathcal{P}_2(8,4)$

$$(1,2),(3,4),(7,5),(6,8).$$

Ora possiamo far agire $\sigma = (1\ 3) \in \mathcal{S}_8$ e ottenere la partizione

$$(3,2),(1,4),(7,5),(6,8).$$

Qual è l'elemento di $\mathcal{S}_2(5,4)$ che corrisponde a questa partizione? Ricostruiamo l'albero:



e infine ricaviamo

$$((14)((32)5)). \tag{B.5}$$

Confrontando i due risultati ottenuti, cioè (B.4) e (B.5), notiamo che

1. le due stringhe hanno un diverso ordine dei numeri $1, \ldots, 5$;
2. il blocco (14) è stato "liberato" dalla parentesi grossa, la quale ha "catturato" (32) al suo posto—in effetti, scambiando 1 e 3, il blocco (34) di (B.3) ha abbassato il suo minimo, guadagnando il diritto di essere assegnato a un padre con un'etichetta minore.

Esercizio. Provare a contare le orbite delle due azioni di $\mathcal{S}_5$ su $\mathcal{S}_2(5,4)$: si scopre che il loro numero è diverso. Questo a maggior ragione dimostra che le due azioni non sono affatto imparentate.

Appendice C

Svolgimento dell'Esercizio di pagina 167

a cura di Francesca Agostini

Esercizio. Sia C_n un gruppo ciclico di ordine n che agisce quasi liberamente su $\{1,\dots,N\}$. Sia X l'insieme dei multiinsiemi di $\{1,\dots,N\}$ di cardinalità k. Allora

$$\left(X, \binom{N+k-1}{k}_q, C_n\right)$$

manifesta il CSP.

Svolgimento. Procediamo come nella dimostrazione del Teorema 4.32. Ricordiamo che è sufficiente

1. trovare una rappresentazione (V,ρ) di C_n indicizzata da X tale che per ogni $\gamma \in C_n$ e per ogni $x \in X$ verifichi
$$\rho(\gamma)\colon \boldsymbol{v}_x \mapsto \omega(\gamma)^m \boldsymbol{v}_{\gamma\cdot x} \tag{C.1}$$
per un qualche $m \in \mathbb{Z}$ indipendente da γ e x: in tal caso, posti
$$A_X := \rho^{(-m)} \otimes V = \bigoplus_{i=0}^{n-1} (\rho^{(i)})^{\oplus k_i},$$
$$A_{X,i} := (\rho^{(i)})^{\oplus k_i}, \quad X(q) := \sum_{i\geqslant 0} \dim(A_{X,i}) q^i,$$
abbiamo che $(X, X(q), C_n)$ manifesta il CSP;
2. dimostrare che per ogni $\gamma \in C_n$
$$\binom{N+k-1}{k}_{\omega(\gamma)} = X(\omega(\gamma)).$$

Per il punto 1., sia $U := \mathbb{C}^N$ come nella dimostrazione del Teorema 4.32 e sia $V := S^k U$ l'algebra simmetrica. In questo caso, se $(e_1, \dots, e_N)$ è la base standard di $\mathbb{C}^N$, una base per V è data da

$$v_S := \bigodot_{i \in S} e_i$$

al variare di S tra i multiinsiemi di $\{1, \dots, N\}$ di cardinalità k e l'azione di C_n su V è data da

$$\rho(\gamma) \colon v_S \mapsto \bigodot_{i \in S} e_{\gamma \cdot i}.$$

L'azione di C_n su $\{1, \dots, N\}$ ne induce una su X; dimostriamo che quest'azione verifica

$$\gamma \cdot v_S = v_{\gamma \cdot S}$$

che è l'Equazione (C.1) con $m = 0$.

Esattamente come nella dimostrazione del Teorema 4.32, l'azione di C_n su V si spezza in sottorappresentazioni indotte dalle orbite dell'azione di C_n su X:

$$V = \bigoplus_{\mathcal{O} \text{ orbita in } X} V_{\mathcal{O}}$$

dove $V_{\mathcal{O}} = \langle v_S \mid S \in \mathcal{O} \rangle$ e supponiamo che un'orbita $\mathcal{O}$ abbia stabilizzatore $\mathcal{S}tab(\mathcal{O}) = \langle c^{n/d} \rangle$ (ove $C_n = \langle c \rangle$). Per ogni $S \in \mathcal{O}$ vale che

$$c^{n/d} \cdot v_S = \omega(c^{n/d})^{m(S)} v_S$$

con $m(S) \in \mathbb{Z}$ che dipende dall'elemento S. Ma osserviamo meglio quest'azione:

$$c^{n/d} \cdot v_S = c^{n/d} \cdot \left(\bigodot_{i \in S} e_i \right) = \bigodot_{i \in S} e_{c^{n/d} \cdot i} = \bigodot_{i \in S} e_i = v_S,$$

quindi ogni autovettore ha come autovalore $1 = \omega(c^{n/d})^0$. In altre parole, per ogni orbita $\mathcal{O}$ e per ogni $S \in \mathcal{O}$ possiamo scegliere $m(S) = 0$.

Passiamo al punto 2. Per quanto visto in precedenza, abbiamo che

$$X(\omega(\gamma)) = \chi_V(1, \dots, \omega(\gamma)^{N-1})$$

e dobbiamo dimostrare che lo stesso risultato si ottiene valutando $\binom{N+k-1}{k}_q$ in $\omega(\gamma)$. Per calcolare il carattere χ_V, scegliamo $(w_1, \dots, w_N)$ base di U di autovettori per $\iota(\gamma)$ con autovalori $\omega(\gamma)^{i-1}$ (ricordiamo che $\iota \colon C_n \to \mathsf{GL}_N(\mathbb{C})$ è la mappa della rappresentazione U) e osserviamo che

$$\left(\bigodot_{i \in S} w_i \;\middle|\; S \in X \right)$$

è una base di V fatta da autovettori per $\rho(\gamma)$: infatti

$$\rho(\gamma)\left(\bigodot_{i\in S} \boldsymbol{w}_i\right) = \bigodot_{i\in S} \iota(\gamma)\boldsymbol{w}_i = \bigodot_{i\in S} \omega(\gamma)^{i-1}\boldsymbol{w}_i = \left(\prod_{i\in S} \omega(\gamma)^{i-1}\right) \bigodot_{i\in S} \boldsymbol{w}_i,$$

dunque

$$\chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1}) = \operatorname{tr}(\rho(\gamma)) = \sum_{S\in X} \prod_{i\in S} \omega(\gamma)^{i-1}.$$

Ora notiamo che, per $S = [i_1, \dots, i_k]$ multiinsieme fissato, l'esponente di $\omega(\gamma)$, cioè $(i_1 - 1) + \cdots + (i_k - 1)$, è una partizione in k parti in cui il massimo addendo può essere $N - 1$; poiché tali partizioni sono in corrispondenza biunivoca con i multiinsiemi di X, concludiamo che

$$\chi_V(1, \omega(\gamma), \dots, \omega(\gamma)^{N-1}) = \sum_{t\geqslant 0} p(N-1, k, t)\omega(\gamma)^t = \binom{N+k-1}{k}_{\omega(\gamma)}. \quad \blacksquare$$

Bibliografia

[1] Béla Bollobás. *Graph Theory. An Introductory Course*. Springer-Verlag, 1979.

[2] Stefan A. Burr, Paul Erdős e Joel H. Spencer. Ramsey Theorems for Multiple Copies of Graphs. *Trans. Amer. Math. Soc.*, 209:87–99, 1975.

[3] Giacomo d'Antonio. Appunti del corso di Teoria delle Rappresentazioni. 2009. URL: `http://www.dm.unipi.it/~gaiffi/papers/teorapp.pdf` (visitato il 22/05/2015).

[4] Giovanni Gaiffi. Nested Sets, Set Partitions and Kirkman-Cayley Dissection Numbers. *European Journal of Combinatorics*, 43:279–288, 2015.

[5] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.

[6] Jacobus H. van Lint e Richard M. Wilson. *A Course in Combinatorics*. Cambridge University Press, seconda edizione, 2001.

[7] Victor Reiner, Dennis W. Stanton e Dennis E. White. The Cyclic Sieving Phenomenon. *J. Combin. Theory*. Series A 108(1):17–50, 2004.

[8] Richard P. Stanley. *Enumerative Combinatorics*. Volume 1. Cambridge University Press, seconda edizione, 2011.

[9] Herbert S. Wilf. *generatingfunctionology*. A K Peters, seconda edizione, 1994.