Corso di Combinatoria

A. Machì

Dispensa I

1 Progressioni aritmetiche e geometriche

Sia

$$u_0, u_1, u_2, \dots, u_k, u_{k+1}, \dots, u_{n-1}, \dots \tag{1}$$

una successione di numeri. Se la differenza $u_{k+1} - u_k$ tra due termini successivi è costante la (1) prende il nome di *progressione aritmetica*. Se d è la differenza costante, la successione ha allora la forma:

$$a,\ a+d,\ a+2d, \dots, a+kd,\ a+(k+1)d, \dots,\ a+(n-1)d, \dots \tag{2}$$

per certi numeri a e d (reali o complessi).

Calcoliamo la somma dei termini della (2), considerando dapprima il caso $a = d = 1$, cioè la sequenza $1, 2, \dots, n$; calcoliamo cioè la somma:

$$S_n = 1 + 2 + \cdots + n. \tag{3}$$

Cambiando l'ordine degli addendi la somma non cambia:

$$S_n = n + (n-1) + (n-2) + \cdots + 2 + 1. \tag{4}$$

Sommando membro a membro (3) e (4) otteniamo:

$$2S_n = (n+1) + (n+1) + \cdots + (n+1) = n(n+1), \tag{5}$$

da cui

$$S_n = \frac{n(n+1)}{2}. \tag{6}$$

Si noti che la somma di (3) e (4) permette di trasformare la somma (3), nella quale gli addendi sono tutti diversi (i numeri $1, 2, \dots, n$), in una somma di numeri tutti uguali (n volte l'intero $n+1$), semplificando così l'operazione di somma.

Esempio. $S_{100} = 1 + 2 + \cdots + 99 + 100 = \frac{100 \cdot (101)}{2} = 5050.$

Nel caso generale (2) di a e d qualunque la somma dei primi n termini è:

$$\begin{aligned} a &+ (a+d)+(a+2d)+\cdots+(a+(n-1)d) \\ &= na+d+2d+\cdots+(n-1)d \\ &= na+d(1+2+\cdots+(n-1)). \end{aligned}$$

Per la (6) il termine in parentesi vale $\frac{(n-1)n}{2}$, e dunque la somma della (2) è

$$na+\frac{d(n-1)n}{2}.$$

In altre parole, dalla conoscenza della somma (6) si ottiene quella di una qualunque progressione aritmetica.

Dimostriamo ora la (6) usando il principio di induzione.

Ricordiamo che il principio di induzione si esprime come segue. Supponiamo di avere, per ogni numero naturale n, una proposizione P_n, e supponiamo di sapere che:

i) la proposizione P_1 è vera;
ii) se P_n è vera allora anche P_{n+1} è vera.

Allora la proposizione P_n è vera per ogni numero naturale n.

Ricordiamo inoltre che questo principio è equivalente al principio del minimo intero: *ogni insieme non vuoto di interi positivi contiene un intero minimo.*

Riguardo alla (6), P_n è la proposizione:

$$P_n\text{: } \textit{la somma dei primi } n \textit{ interi è } \tfrac{n(n+1)}{2}.$$

Vediamo la P_1. Per $n=1$ la somma $1+2+\cdots+n$ si riduce a 1, e anche $\frac{n(n+1)}{2}=\frac{1\cdot(1+1)}{2}$ vale 1. Dunque P_1 è vera.

Supponiamo la P_n vera per un certo n; per quell'n si abbia quindi:

$$1+2+\cdots+n=\frac{n(n+1)}{2},$$

e consideriamo $1+2+\cdots+n+(n+1)$. Questa somma è uguale alla somma $(1+2+\cdots+n)+(n+1)$. Poiché P_n è supposta vera, la somma in parentesi vale $\frac{n(n+1)}{2}$; ne segue:

$$1+2+\cdots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{n(n+1)+2(n+1)}{2}=\frac{(n+1)(n+2)}{2},$$

che è la proposizione P_{n+1}. Abbiamo dimostrato P_{n+1}, che dunque risulta vera. E poiché P_1 è vera, e supposta vera P_n segue che P_{n+1} è vera, per il principio di induzione P_n è vera per ogni n.

Se nella (1) invece della differenza è costante il rapporto tra due termini successivi la successione prende il nome di *progressione geometrica*. In questo caso la (1) ha la forma:

$$a,\ aq,\ aq^2,\ \dots,\ aq^k,\ aq^{k+1},\ \dots, aq^{n-1}, \dots \tag{7}$$

(il termine generico $u_k = a+kq$ della progressione aritmetica viene sostituito da $a \cdot q^k$: il prodotto sostituisce la somma e la potenza il multiplo). Il numero q si chiama *ragione* della progressione.

Vediamo ora la somma dei primi n termini della (7). Come sopra consideriamo dapprima il caso $a = 1$:

$$T_n = 1 + q + q^2 + \cdots + q^{n-1}. \tag{8}$$

Moltiplichiamo i due membri per q:

$$qT_n = q + q^2 + q^3 + \cdots + q^n;$$

Sottraendo:

$$T_n - qT_n = 1 - q^n,$$

da cui $(1-q)T_n = 1 - q^n$. Se $q \neq 1$ si ha allora:

$$T_n = \frac{1-q^n}{1-q} \tag{9}$$

(se $q = 1$ dalla (8) si ha subito $T_n = n$).

Nel caso generale, $a + aq + aq^2 + \cdots + aq^{n-1} = a(1 + q + q^2 + \cdots + q^{n-1}) = aT_n$, e

$$a + aq + aq^2 + \cdots + aq^{n-1} = a\frac{1-q^n}{1-q}. \tag{10}$$

Esempi. *a*) Per $q = 2$ e $a = 1$ dalla (10) abbiamo:

$$1 + 2 + 2^2 + \cdots + 2^{n-1} = \frac{1-2^n}{1-2} = 2^n - 1.$$

b) Per $q = \frac{1}{2}$ e $a = 1$:

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^{n-1}} = \frac{1 - \frac{1}{2^n}}{1 - \frac{1}{2}} = 2 - \frac{1}{2^{n-1}}.$$

2 Successioni ricorsive

Le progressioni aritmetiche e geometriche sono casi particolari di successioni dette ricorsive. La (1) è una *successione ricorsiva* se esistono un numero naturale k e numeri (reali o complessi) $a_1, a_2, \ldots, a_k$ tali che, a partire da un certo n e per tutti gli interi successivi a n, si abbia la relazione:

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n \tag{11}$$

($n \geq k \geq 1$). La (11) è una *relazione ricorsiva* o di *ricorrenza lineare* di ordine k. Una progressione geometrica $u_k = aq^k$ è una successione ricorsiva: si ha la (11) con $k = 1$ e $a_1 = q$:

$$u_{n+1} = qu_n, \tag{12}$$

e poiché $k = 1$ si tratta di una relazione del primo ordine: un termine dipende solo dal termine precedente.

Se la (1) è una progressione aritmetica allora $u_{n+1} = u_n + d$. Questa relazione non è della forma (11) in quanto vi compare il termine d che non è un multiplo di uno dei termini della successione. Per dimostrare che si tratta di una successione ricorsiva consideriamo anche $u_{n+2} = u_{n+1} + d$, e sottraiamo la precedente da questa: $u_{n+2} - u_{n+1} = u_{n+1} - u_n$. Si ottiene:

$$u_{n+2} = 2u_{n+1} - u_n. \tag{13}$$

Si vede allora che un termine dipende dai due precedenti: si tratta di una relazione del secondo ordine ($k = 2$). I termini di una progressione aritmetica come la (2) si ottengono assegnando le condizioni iniziali $u_1 = a, u_2 = a + d$. Inoltre, dalla (13) si vede che in una progressione aritmetica ciascun termine è la media aritmetica del precedente e del successivo:

$$u_{n+1} = \frac{u_n + u_{n+2}}{2},$$

come nel caso della successione dei naturali.

Esempi. 1. La (13), con le condizioni iniziali $u_1 = 1$ e $u_2 = 2$ (o anche $u_1 = -1, u_2 = 0$) fornisce la successione dei numeri naturali $1, 2, 3, \ldots$

2. Consideriamo la successione dei quadrati dei numeri naturali:

$$u_1 = 1^2, u_2 = 2^2, u_3 = 3^2, \ldots, u_n = n^2, \ldots,$$

e cerchiamo di determinare la relazione di ricorrenza (11). Si ha $u_{n+1} = (n+1)^2 = n^2 + 2n + 1 = u_n + 2n + 1$ che non è del tipo (11). Consideriamo allora $u_{n+2} = (n+2)^2 = n^2+4n+4 = u_{n+1}+2n+3$. Sottraendo otteniamo $u_{n+2}-u_{n+1} = u_{n+1}-u_n+2$, da cui $u_{n+2} = 2u_{n+1}-u_n+2$, che non è ancora del tipo (11). Passiamo a u_{n+3}. Si ha $u_{n+3} = (n+3)^2 = n^2 + 6n + 9 = 2u_{n+2} - u_{n+1} + 2$. Sottraendo: $u_{n+3} - u_{n+2} = 2u_{n+2} - 3u_{n+1} + u_n$ e infine

$$u_{n+3} = 3u_{n+2} - 3u_{n+1} + u_n, \tag{14}$$

una relazione del terzo ordine. Ad esempio, per $n = 6$ abbiamo $u_9 = 3u_8 - 3u_7 + u_6$, e infatti $9^2 = 3 \cdot 8^2 - 3 \cdot 7^2 + 6^2 = 192 - 147 + 36 = 81$.

Dal calcolo ora svolto si vede che la (14) è la relazione ricorsiva per ogni successione il cui termine generico u_n è un polinomio di secondo grado in n: $u_n = an^2 + bn + c$.

3. Una successione nella quale ogni termine è la somma dei due precedenti è la *successione di Fibonacci.* E' data dalla relazione

$$u_{n+2} = u_{n+1} + u_n.$$

Per $u_1 = u_2 = 1$ si ottiene la successione $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

4. Numerose successioni elementari di numeri *non* sono successioni ricorsive. Ad esempio, la successione dei numeri primi:

$$2, 3, 5, 7, 11, 13, 17, \ldots;$$

la successione degli inversi dei numeri interi:

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{n}, \ldots;$$

o dei logaritmi degli interi:

$$\log 1, \log 2, \log 3, \ldots, \log n, \ldots.$$

Esercizi

1. Determinare la relazione ricorsiva:

i) per la successione il cui termine u_n è un polinomio di primo grado in n;

ii) per la successione dei cubi dei numeri interi $1, 2^3, 3^3, 4^3, \ldots$, ovvero per una qualunque successione il cui termine u_n è un polinomio di terzo grado in n.

2. *i*) Determinare la relazione ricorsiva per la successione:

$$1, 3, 7, 15, \ldots, 2^n - 1, \ldots.$$

ii) (*Gioco della torre di Hanoi*) Su un piano vi sono tre aste verticali una delle quali (la *torre*) porta infilati uno sull'altro n anelli di diametro decrescente, con il più grande in basso. Il gioco consiste nello spostare gli anelli da quest'asta su un'altra delle tre, servendosi della rimanente come ausiliaria, con le seguenti regole:

1. si può spostare un anello per volta;
2. un anello non deve mai trovarsi su uno più piccolo.

Qual è il minimo numero di mosse necessarie per portare a termine il gioco?

(*Sugg.* Sia T_n il numero di mosse per n dischi. E' chiaro che $T_1 = 1$, $T_2 = 3$; si vede facilmente che $T_3 = 7$, e con un po' più di lavoro che $T_4 = 15$. Ora si veda *i*)).

3. Sia u_n, rispettivamente:

a) il numero delle successioni di 1 e 2 la cui somma è n;

b) il numero di modi di salire una scala di n gradini salendo uno o due gradini alla volta;

c) il numero delle successioni di 0 e 1 di lunghezza n che non contengono due zeri consecutivi;

d) il numero dei sottoinsiemi degli interi da 1 a n (compreso l'insieme vuoto) che non contengono due interi consecutivi.

Determinare nei quattro casi una relazione ricorsiva per la successione $\{u_n\}$.

4. Se u_n è la successione di Fibonacci, dimostrare che:

i) $u_{2n+1} = u_2 + u_4 + \ldots + u_{2n} + 1$;

ii) $u_1^2 + u_2^2 + \ldots + u_n^2 = u_n u_{n+1}$;

iii) $u_{n+1}u_{n-1} - u_n^2 = (-1)^n$.

5. Dimostrare per induzione:

i) per ogni $n \geq 1$, $5^n - 1$ è divisibile per 4;

ii) per ogni $n \geq 1$, $11^n - 6$ è divisibile per 5;

iii) per ogni $n \geq 4$, $n! > 2^n$;

iv) per ogni $n \geq 3$, $2n + 1 \leq n^2$.

3 Combinazioni

Una *combinazione* o una *scelta* di k elementi appartenenti a un insieme di n elementi è un sottoinsieme di quest'ultimo che contiene k elementi. Il numero di questi sottoinsiemi si denota con $\binom{n}{k}$, simbolo che per ragioni che vedremo più in là si chiama coefficiente *binomiale*.

Supponiamo di avere n oggetti e di voler contare in quanti modi se ne possono scegliere due; vogliamo cioè contare le coppie non ordinate su n elementi. Il primo elemento della coppia si può scegliere in n modi (uno qualunque degli n elementi), il secondo in $n-1$ (uno qualunque che non sia quello già scelto). Si osservi che le $n-1$ scelte del secondo elemento sono indipendenti dalla scelta del primo, e quindi si ottiene un totale di $n(n-1)$ coppie. Così facendo però si contano le coppie ordinate di elementi, mentre una coppia non ordinata $\{a, b\}$ viene contata due volte, una volta quando si sceglie prima a e poi b, l'altra quando si sceglie prima b e poi a. Occorre perciò dividere per 2, e il numero delle coppie è allora

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

Come nel caso della prima dimostrazione della (6), anche qui abbiamo contato gli oggetti due volte e poi diviso per 2. Contiamo ora le coppie in modo diverso. Numeriamo in un modo qualunque gli elementi con $1, 2, \cdots, n$, e contiamo le coppie di elementi dividendole in classi disgiunte come segue: coppie nelle quali il più piccolo elemento è 1:

$$\{1, 2\}, \{1, 3\}, \ldots, \{1, n\},$$

e queste sono in numero di $n-1$. Poiché formare una coppia $\{1, i\}$ significa scegliere un elemento i tra gli $n-1$ diversi da 1, abbiamo $n-1 = \binom{n-1}{1}$.

Coppie nelle quali il più piccolo elemento è 2:

$$\{2, 3\}, \{2, 4\}, \ldots, \{2, n\},$$

che sono in numero di $n-2$. Analogamente al caso $n-1$ abbiamo $n-2 = \binom{n-2}{1}$;. . . ; coppie nelle quali il più piccolo elemento è $n-2$:

$$\{n-2, n-1\}, \{n-2, n\},$$

che sono $2 = \binom{2}{1}$, e infine la coppia in cui il più piccolo elemento è $n-1$,

$$\{n-1, n\},$$

una sola: $1 = \binom{1}{1}$. Abbiamo in definitiva:

$$\binom{n}{2} = \binom{n-1}{1} + \binom{n-2}{1} + \cdots + \binom{n-k}{1} + \cdots + \binom{2}{1} + \binom{1}{1}.$$

Sostituendo ai simboli binomiali il loro valore numerico abbiamo:

$$\frac{n(n-1)}{2} = (n-1) + (n-2) + \cdots + 2 + 1$$

cioè la (6) con $n-1$ al posto di n.

Consideriamo ora i sottoinsiemi con 3 elementi (cioè le terne non ordinate) di un insieme con n elementi. Contando in due modi come sopra abbiamo nel primo caso n scelte per il primo elemento, $n-1$ per il secondo e $n-2$ per il terzo; in tutto $n(n-1)(n-2)$. Ma in questo modo una stessa terna viene contata 6 volte:

$$\{a,b,c\},\{a,c,b\},\{b,a,c\},\{b,c,a\},\{c,a,b\},\{c,b,a\}$$

e dunque il numero cercato è $\frac{n(n-1)(n-2)}{6}$.

Come prima, contiamo ora in un altro modo, dividendo le terne in classi disgiunte. Numeriamo gli elementi dell'insieme con $1,2,\ldots,n$, e consideriamo le terne che hanno 1 come più piccolo elemento. Gli altri due elementi della terna vanno scelti tra $2,3,\ldots,n$, e dunque sono tanti quante le coppie non ordinate su $n-1$ elementi, cioè: $\binom{n-1}{2}$. Questo è allora anche il numero delle terne che contengono 1. Le terne che cominciano con 2 sono tante quante le coppie non ordinate su $n-2$ elementi: $\binom{n-2}{2}$, e in generale, le terne che cominciano con k sono tante quante le coppie non ordinate su $n-k$ elementi, cioè $\binom{n-k}{2}$. In totale dunque:

$$\binom{n}{3}=\binom{n-1}{2}+\binom{n-2}{2}+\cdots+\binom{n-k}{2}+\cdots+\binom{3}{2}+\binom{2}{2}.$$

E' facile ora vedere come tutto ciò si possa generalizzare. Contando le $k-$ple che cominciano con 1, poi quelle che cominciano con 2, ecc., arriviamo all'uguaglianza:

$$\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-2}{k-1}+\cdots+\binom{n-k}{k-1}+\cdots+\binom{k}{k-1}+\binom{k-1}{k-1}. \tag{15}$$

Nella dimostrazione della (15) non si è fatto uso del valore numerico dei simboli che vi compaiono: l'uguaglianza (15) afferma che contare il numero dei sottoinsiemi con k elementi di un insieme con n elementi equivale a contare quelli con $k-1$ elementi di un insieme con $n-1$ elementi, quelli con $k-1$ elementi di un insieme con $n-2$ elementi,..., e infine quelli con $k-1$ elementi di un insieme con $k-1$ elementi, e sommare poi i risultati. Si tratta di una dimostrazione *combinatoria*: essa sfrutta cioè soltanto la natura combinatoria dei simboli binomiali che vi intervengono, senza utilizzare il loro valore numerico. Vedremo più avanti altre dimostrazioni combinatorie di uguaglianze, nelle quali i due membri saranno il risultato del contare:

i) gli elementi di uno stesso insieme in due modi diversi (ad esempio, in una matrice di 0 e 1, contando il numero totale di 1 per righe o per colonne si ottiene lo stesso risultato);

ii) gli elementi di due insiemi tra i quali si dimostra esistere una corrispondenza biunivoca.

Per quanto riguarda il valore numerico di $\binom{n}{k}$ abbiamo n scelte per il primo elemento, $n-1$ per il secondo,..., $n-(k-1)$ per il $k-$esimo. Ma in questo modo si ottengono $k-$ple ordinate; ciascuna $k-$pla non ordinata si ottiene $k!$ volte, cioè quante sono le permutazioni su k elementi. Dunque:

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

La formula (15) permette di definire ricorsivamente i simboli binomiali: conoscendo $\binom{m}{k}$ per $m < n$ possiamo infatti determinare $\binom{n}{k}$.

Per definizione si pone poi $\binom{n}{k} = 0$ per $k < 0$ o $k > n$. Inoltre, $\binom{n}{0} = 1$ (vi è un solo sottoinsieme con zero elementi: l'insieme vuoto).

Esempi. 1.

$$\binom{n}{k} = \binom{n}{n-k}.$$

La corrispondenza che associa a ogni sottoinsieme di k elementi di un insieme di n elementi il suo complementare è una corrispondenza biunivoca tra l'insieme dei sottoinsiemi con k elementi e quello dei sottoinsiemi con $n-k$ elementi. Si tratta, in altri termini, del fatto ovvio che ogni volta che si scelgono k elementi se ne scartano $n-k$.

2.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Sia A un insieme con n elementi, e fissiamo un elemento $a \in A$. I sottoinsiemi di k elementi di A o non contengono a oppure lo contengono. Nel primo caso essi sono tanti quanti i sottoinsiemi di $A \setminus \{a\}$, cioè $\binom{n-1}{k}$. Nel secondo, essi si ottengono dai sottoinsiemi con $k-1$ elementi, che sono in numero di $\binom{n-1}{k-1}$, ai quali si aggiunge a.

3. *a*) In una parola di lunghezza n sull'alfabeto a due lettere $\{0, 1\}$ la prima lettera può essere 0 o 1, e quindi si hanno 2 scelte per questa lettera, la seconda può ancora essere 0 o 1 e perciò ancora 2 scelte, ecc. Vi sono dunque in tutto $\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{n\ volte} = 2^n$ parole di lunghezza n su un alfabeto a due lettere.

Contiamo ora le stesse parole in un altro modo, suddividendole in classi disgiunte a seconda del numero di zeri che contengono:

(0) parole che non contengono 0. Ce n'è una sola, $\binom{n}{0}$, quella con tutti 1;

(1) parole che contengono 1 zero. Scelto il posto dove mettere lo zero ($\binom{n}{1}$ scelte) non vi sono più scelte: negli altri posti vi sono tutti 1;

(2) parole con 2 zeri. Una per ogni scelta dei due posti per gli zeri; dunque in tutto $\binom{n}{2}$ parole;

$$\cdots\cdots$$

(k) parole con k zeri. Una per ogni scelta dei k posti: $\binom{n}{k}$;

$$\cdots\cdots$$

(n) parole con n zeri. Una sola: $\binom{n}{n}$.

Uguagliando i due risultati abbiamo:

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n}. \tag{16}$$

b) Insieme delle parti $\mathcal{P}(A)$ di un insieme A, $|A| = n$, compresi l'insieme vuoto e tutto l'insieme. Se $X \subseteq A$, associamo a X la parola di lunghezza n su $\{0,1\}$ che ha 1 nel posto i se $a_i \in X$, e 0 se $a_i \notin X$. Viceversa, se una parola di lunghezza n su $\{0,1\}$ ha 1 nei posti $i_1, i_2, \ldots, i_k$ ad essa resta associato il sottoinsieme $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$. Per 3*a*) si ha allora $\mathcal{P}(A) = 2^n$.

c) Funzioni da un insieme A, $|A| = n$, all'insieme $\{0,1\}$. Per definire una funzione $f : A \longrightarrow \{0,1\}$ vi sono due scelte per l'immagine di ciascun elemento di A, e dunque in tutto 2^n scelte. Due scelte diverse per uno degli elementi danno luogo a funzioni diverse.

d) se X è un sottoinsieme di un insieme A, la *funzione caratteristica* di X è la funzione $f_X : A \longrightarrow \{0,1\}$ così definita:

$$f_X(a) = \begin{cases} 1, & \text{se } a \in X \\ 0, & \text{se } a \notin X. \end{cases}$$

Viceversa, se $f : A \longrightarrow \{0,1\}$, ad f corrisponde il sottoinsieme X degli elementi $a \in A$ tali che $f(a) = 1$. Le funzioni caratteristiche dei sottoinsiemi di A sono in corrispondenza biunivoca con i sottoinsiemi di A, e dunque, se $|A| = n$, sono in numero di 2^n.

4. Le parole di lunghezza n su 3 lettere $\{0,1,2\}$ sono in numero di 3^n (vi sono tre scelte per ognuno degli n posti). Contiamole suddividendole in classi (v. 3 *a*).

(0) parole che non contengono lo zero: sono tante quante le parole su 2 lettere cioè 2^n;

(1) parole che contengono uno zero. Per ogni scelta del posto per lo zero abbiamo tutte le parole su due lettere sui restanti $n-1$ posti che sono in numero di 2^{n-1};

(2) parole che contengono due zeri. I posti per questi due zeri si possono

scegliere in $\binom{n}{2}$ modi, e per ciascuno di questi modi vi sono tutte le parole su due lettere sui restanti $n-2$ posti. Dunque in tutto $\binom{n}{2} \cdot 2^{n-2}$ parole;

$\cdots\cdots$

(k) parole con k zeri. $\binom{n}{k}$ modi di scegliere k posti per gli zeri, e per ciascuna scelta abbiamo tutte le parole su due lettere sui restanti $n-k$ posti. In tutto quindi $\binom{n}{k} \cdot 2^{n-k}$ parole;

$\cdots\cdots$

(n) parole con n zeri. Una sola scelta: tutti zeri.

Uguagliando i due risultati abbiamo allora:

$$\binom{n}{0}2^n + \binom{n}{1}2^{n-1} + \cdots + \binom{n}{k}2^{n-k} + \cdots + \binom{n}{n}2^0 = 3^n.$$

Con un ragionamento analogo si vede, più in generale, che contando nei due modi visti le parole di lunghezza n su un alfabeto di m lettere si ha l'uguaglianza:

$$\sum_{k=0}^{n} \binom{n}{k}(m-1)^{n-k} = m^n. \tag{17}$$

(Come nell'*es. 3d*), dove $m = 2$, m^n è anche il numero delle funzioni da un insieme con n elementi a un insieme con m elementi).

5.

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}. \tag{18}$$

Supponiamo di avere $2n$ persone, n donne e n uomini, e di dover scegliere un gruppo di n. Questo gruppo può essere composto da 0 donne e n uomini, oppure da 1 donna e $n-1$ uomini, ecc. In generale vi saranno k donne e $n-k$ uomini, $k = 0, 1, \ldots, n$. Le k donne si possono scegliere in $\binom{n}{k}$ modi, e gli $n-k$ uomini in $\binom{n}{n-k}$ modi, cioè in totale in $\binom{n}{k}\binom{n}{n-k}$ modi, che per **1.** è uguale a $\binom{n}{k}^2$.

6. Consideriamo ora lo sviluppo della potenza $n-$esima del binomio $1+x$:

$$(1+x)^n = (1+x)(1+x)\cdots(1+x),$$

e chiediamoci quante volte compare x^k nel prodotto, e cioè qual è il coefficiente di x^k nello sviluppo. Il monomio x^k si ottiene facendo k volte il prodotto di x per se stesso, e quindi ogni volta che si sceglie x in k fattori e 1 nei restanti $n-k$. Poiché le scelte di k fattori tra gli n sono in numero di $\binom{n}{k}$, x^k compare $\binom{n}{k}$ volte, e perciò questo è il coefficiente di x^k nello sviluppo di $(1+x)^n$ (di qui il nome di coefficiente binomiale dato al simbolo $\binom{n}{k}$). Ne segue il *teorema del binomio* :

$$(1+x)^n = \binom{n}{0}x^0 + \binom{n}{1}x^1 + \binom{n}{2}x^2 + \cdots + \binom{n}{k}x^k + \cdots + \binom{n}{n}x^n. \qquad (19)$$

Si osservi che posto $x = 1$ si ottiene la (16), e in generale, per $x = m-1$, la (17) (ricordando che $\binom{n}{k} = \binom{n}{n-k}$). A partire dallo sviluppo (19) possiamo riottenere anche la (18). Infatti, per quanto appena visto, $\binom{2n}{n}$ è il coefficiente di x^n nello sviluppo di $(1+x)^{2n}$. Calcoliamo questo coefficiente in un altro modo. Sviluppando il prodotto:

$$(1+x)^{2n} = \cdots + \binom{2n}{n}x^n + \cdots = (1+x)^n \cdot (1+x)^n =$$

$$(\binom{n}{0}x^0 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n) \cdot (\binom{n}{0}x^0 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n)$$

si trova per x^n:

$$\binom{n}{0}x^0\binom{n}{n}x^n + \binom{n}{1}x \cdot \binom{n}{n-1}x^{n-1} + \cdots + \binom{n}{k}x^k \cdot \binom{n}{n-k}x^{n-k} + \cdots + \binom{n}{n}x^n \cdot \binom{n}{0}x^0.$$

Ma $\binom{n}{k} = \binom{n}{n-k}$ e perciò il coefficiente di x^n è $\sum_{k=0}^{n}\binom{n}{k}^2$; ne segue la (18).

Più in generale, $\binom{n}{k}$ è il coefficiente del monomio $x^k y^{n-k}$ nello sviluppo di $(x+y)^n = \sum_{k=0}^{n} x^k y^{n-k}$.

7. Vediamo ora una descrizione della (18) come somma dei cammini di lunghezza minima su una griglia quadrata (le cifre in un vertice indicano il numero di cammini di lunghezza minima per arrivare a quel vertice a partire da A). Per una griglia di lato 1, vi sono due cammini da A a B:

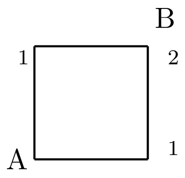

Figura 1

Per una di lato 2 vi sono 6 cammini:

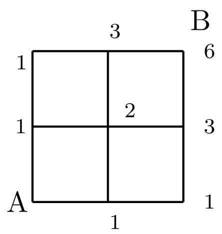

Figura 2

Per una di lato 4 vi sono 70 cammini:

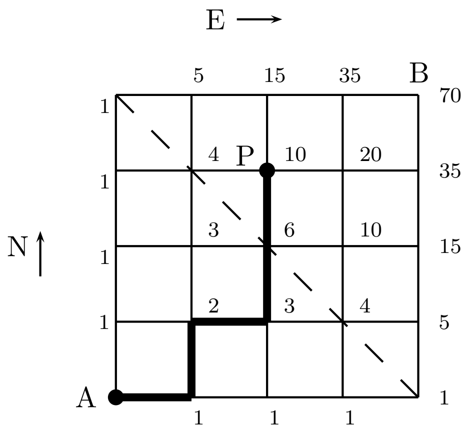

Figura 3

Vediamo come contare questi cammini. Ogni punto della griglia ha due coordinate Est e Nord. Ad esempio, il punto P ha coordinate (2,3), e il cammino più breve da A a P è lungo 2+3=5 (2 passi in direzione E e 3 in direzione N). Essi sono in numero uguale ai modi di scegliere 2 elementi da un insieme di 5, cioè $\binom{5}{2} = 10$, ovvero, ciò che è lo stesso, 3 elementi da 5. Questo numero 10 è quello che contrassegna il punto P.

In generale, in una griglia quadrata di lato n i cammini di lunghezza minima da A a B hanno lunghezza $2n$ e constano di n passi verso E e n verso N. Sono quindi tanti quanti sono i modi di scegliere n passi verso E (o verso N), cioè n segmenti da un insieme di $2n$; in tutto $\binom{2n}{n}$.

Contiamo ora questi cammini da A a B in un altro modo. Essi passano tutti per un punto della diagonale (tratteggiata in Fig. 3), e il numero di cammini da A a un punto D della diagonale di coordinate $(k, n-k)$ è $\binom{n}{k}$.

Questo numero è evidentemente lo stesso del numero dei cammini da D a B, e poichè per ogni cammino da A a D ne abbiamo uno da D a B, i cammini da A a B passanti per D sono in numero di $\binom{n}{k}^2$. Per $k = 1, 2, \dots, n$ abbiamo tutti i punti della diagonale, e dunque il numero dei cammini da A a B è in totale:

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \dots + \binom{n}{n}^2.$$

Abbiamo perciò di nuovo la (18). Nell'esempio della Figura 3:

$$\binom{4}{0}^2 + \binom{4}{1}^2 + \binom{4}{2}^2 + \binom{4}{3}^2 + \binom{4}{4}^2 = 1^2 + 4^2 + 6^2 + 4^2 + 1^2 = 70.$$

Più in generale per una griglia rettangolare $n \times m$:

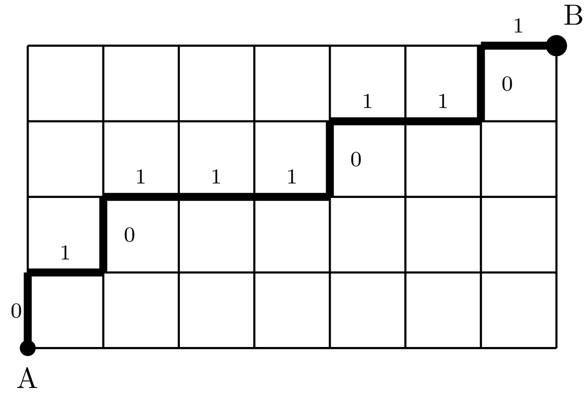

Figura 4

il numero dei cammini di lunghezza minima tra A e B è $\binom{n+m}{m}$ $(= \binom{n+m}{n})$, che diventa $\binom{n+n}{n} = \binom{2n}{n}$ nel caso $n = m$ (griglia quadrata). Se denotiamo con 0 un passo in direzione N e con 1 uno in direzione E, un cammino minimo su una griglia $n \times m$ è individuato da una parola di 0 e 1 in cui compare n volte 0 ed m volte 1 (vedi Fig. 4, una griglia 4×7, la parola 01011101101, che ha quattro 0 e sette 1); se la griglia è quadrata, da una parola che ha n volte 0 ed n volte 1, come sappiamo.

Esercizi

1. Dimostrare per induzione la formula:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

2. Dimostrare la (17) per induzione.

3. Dimostrare che :

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

(*Sugg.*: utilizzare la $\binom{n-1}{k-1} - \binom{n}{k} = -\binom{n-1}{k}$).

4. *a*) Utilizzare il risultato precedente per dimostrare che le somme:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots$$

(sottoinsiemi di cardinalità pari), e

$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$$

(sottoinsiemi di cardinalità dispari), sono entrambe uguali a 2^{n-1}.

b) Per *a*), i sottoinsiemi di cardinalità pari sono tanti quanti quelli di cardinalità dispari, e cioè 2^{n-1}. Stabilire una corrispondenza biunivoca che associa a un sottoinsieme di cardinalità pari uno di cardinalità dispari.

5. Dare una dimostrazione combinatoria delle uguaglianze:

a)

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

b)

$$n! = \binom{n}{k}k!(n-k)!.$$

Si osservi come la *a*) generalizzi la $\binom{n}{2} = \frac{n(n-1)}{2}$, e come dall'uguaglianza *b*) segua la formula dell'*es*. **1**.

c)

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}.$$

6. Vi sono n persone in fila per entrare in un cinema. In quanti modi si possono far entrare a blocchi di una o più persone?

7. Dimostrare l'identità di Cauchy–Vandermonde:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}.$$

(*Sugg.*: v. (18)).

8. Dimostrare che l'insieme delle coppie (A, B) di sottoinsiemi distinti di un insieme di n elementi tali che $A \subset B$, $A \neq B$, è $3^n - 2^n$. (*Sugg.*: $3^n = (2+1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^k$, e $2^n = \sum_{k=0}^{n} \binom{n}{k}$).

3.1 Combinazioni con ripetizione

Nel paragrafo precedente abbiamo considerato i modi in cui si possono scegliere r elementi distinti da un insieme di n elementi ($r-$combinazioni). Se lasciamo cadere l'ipotesi che gli r elementi siano tutti distinti, se cioè si può scegliere più volte lo stesso elemento, abbiamo quelle che si chiamano *$r-$combinazioni con ripetizione.* Ad esempio, le $2-$combinazioni dell'insieme $\{1, 2, 3\}$ sono $\{1, 2\}, \{1, 3\}, \{2, 3\}$, mentre le $2-$combinazioni con ripetizione sono:

$$\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 1\}, \{2, 2\}, \{3, 3\}.$$

(Quando un elemento compare più volte, come negli ultimi tre casi qui sopra, si parla più esattamente di *multi*–insiemi, e non di insiemi).

Quente sono le $r-$combinazioni con ripetizione di un insieme con n elementi? Si osservi che una $r-$combinazione di un insieme di elementi $\{a_1, a_2, \ldots, a_n\}$ si può considerare come una $r-$combinazione di un multinsieme nel quale ciascun a_i compare infinite volte. In altre parole abbiamo a disposizione un numero infinito di a_i, per ogni i, per cui ognuno di essi può comparire quante volte si vuole in una $r-$combinazione.

Teorema 1. *Il numero delle $r-$combinazioni con ripetizione di un insieme con n elementi è:*

$$\binom{n-1+r}{r}.$$

Dim. Suddividiamo la retta in n parti mediante $n-1$ barre:

$$\underbrace{\quad | \quad | \quad | \quad \ldots \quad | \quad}_{n-1 \text{ barre definiscono } n \text{ regioni}}$$

e mettiamo in tutti i modi possibili n oggetti nelle regioni così ottenute (lasciando eventualmente vuote alcune regioni). Ad esempio, per $n = 5$:

$$* \;\; | \;\; *\,*\,* \;\; | \quad\quad | \;\; * \;\; | \;\; *$$

Facciamo corrispondere a questa disposizione di oggetti la $6-$combinazione con ripetizione $\{1, 2, 2, 2, 4, 5\}$ (la terza regione è vuota: il 3 infatti non compare nella 6–combinazione). In generale, a una disposizione di oggetti nelle n regioni facciamo corrispondere la $r-$combinazione con ripetizione che ha tante cifre i quanti sono i oggetti nella $i-$esima regione. Viceversa, data una $r-$combinazione con ripetizione facciamo corrispondere la distribuzione di oggetti nelle n regioni ottenuta mettendo un oggetto nella $i-$esima regione ogni volta che la cifra i compare nella combinazione. Questa corrispondenza è biunivoca, e quindi il numero di $r-$combinazioni con ripetizione di un insieme con n elementi è uguale al numero di stringhe che contengono $n-1$ barre e r oggetti (stringhe su un alfabeto di due elementi, diciamo 1 e 0, che contengono $n-1$ volte 1 e r volte 0). Ogni stringa è quindi lunga $n-1+r$. Qual è il numero di queste stringhe? Per determinare una stringa occorre scegliere r posti dove mettere 0 tra gli $n-1+r$ disponibili. Il numero totale di stringhe è quindi uguale al numero di modi di scegliere r elementi in un insieme di $n-1+r$ elementi, e questo numero è $\binom{n-1+r}{r}$, come si voleva. (Se invece degli r posti dove mettere 0 si scelgono gli $n-1$ posti dove mettere 1 si ottiene $\binom{n-1+r}{n-1}$ che è uguale a $\binom{n-1+r}{n-1+r-(n-1)} = \binom{n-1+r}{r}$, cioè lo stesso risultato). $\diamondsuit$

Il risultato del Teor. 1 si può porre nella forma seguente. Se la cifra i compare y_i volte in una $r-$combinazione, allora:

$$y_1 + y_2 \cdots + y_n = r, \tag{20}$$

con $y_i \geq 0$, $0 \leq i \leq n$. Viceversa, ogni soluzione in interi y_i dell'equazione (20) fornisce una $r-$combinazione con ripetizione di un insieme con n elementi. Ne segue:

Corollario. *Il numero delle soluzioni intere $y_i \geq 0$ della* (20) *è* $\binom{n-1+r}{r}$. $\diamondsuit$

Si osservi che (3,2,1) e (2,3,1) sono due soluzioni diverse $y_1 + y_2 + y_3 = 6$ (la (20) con $n = 3$ e $r = 6$). Nella prima $y_1 = 3, y_2 = 2, y_3 = 1$, mentre nella seconda $y_1 = 2, y_2 = 3, y_3 = 1$. Le soluzioni richieste sono quindi $n-$ple $(y_1, y_2, \ldots, y_n)$ (successioni ordinate degli y_i).

Possiamo riassumere quanto sopra come segue. Sono uguali:

- il numero di modi di disporre r oggetti indistinguibili in n urne;
- il numero di modi di scegliere r oggetti tra n ammettendo ripetizioni;
- il numero di soluzioni intere della (20) con $y_i \geq 0$.

In tutti e tre i casi il numero è $\binom{n-1+r}{r}$.

Esempi. 1. Quanti coni con tre palline di gelato si possono formare avendo a disposizione dieci gusti? Se le tre palline devono essere di tre gusti diversi, allora il numero è il numero delle combinazioni di 10 elementi a 3 a 3, e cioè $\binom{10}{3} = 120$. Se invece si permettono palline di uguale gusto, anche tutte e tre uguali, allora il numero richiesto è il numero delle 3–combinazioni di un insieme con 10 elementi, e cioè $\binom{10-1+3}{3} = \binom{12}{3} = 220$.

2. Supponiamo di avere 2 palline identiche e 3 urne. In quanti modi si possono disporre le palline nelle urne? Se pensiamo alle urne come alle tre regioni in cui viene divisa la retta da due barre allora siamo nel caso visto nel teorema, e il numero cercato è: $\binom{3-1+2}{2} = \binom{4}{2} = 6$.

3. La tecnica delle barre e degli oggetti si può utilizzare per risolvere un problema di compressione di dati. Quanti bits sono necessari per specificare un insieme di N interi (anche ripetuti) compresi tra 0 e $2N$? Ad esempio, quanto spazio sul disco serve per archiviare un milione di numeri tra 0 e 2 milioni? Se si archiviano i numeri traducendoli in binario, allora sono necessari almeno $\log_2(2N+1)$ bits per ciascun numero, e quindi in tutto almeno $N\log_2(2N+1)$ bits. Nel caso di un milione di numeri, $N = 10^6$, abbiamo $\log_2(2\cdot 10^6+1) = 21$, e quindi sono necessari 21 milioni di bits per archiviare tutti i numeri.

Un modo più astuto è il seguente. Un insieme di N interi tra 0 e $2N$ si può considerare come una $N-$combinazione con ripetizione di un insieme con $2N+1$ elementi (i numeri da 0 a $2N$), e quindi, come nel teorema, come una stringa di N oggetti (un stringa con N volte 0) e $2N$ barre (N volte 1). Un tale stringa si può archiviare usando $N + 2N = 3N$ bits.

Ad esempio, per archiviare un insieme di $N = 5$ numeri compresi tra 0 e 10, e sia $\{2,4,4,6,6\}$, possiamo rappresentare questo multinsieme con oggetti (=0) e barre (= 1) e poi con $3N = 15$ bits come segue:

$$| \ | \ * \ | \ | \ ** \ | \ | \ * \ | \ * \ | \ | \ |$$

e cioè con i 15 bit seguenti:

$$1\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1$$

Nel caso di $N = 10^6$ visto sopra possiamo archiviare il multinsieme usando 3 milioni di bits, migliorando il risultato di un fattore 7.

Ci poniamo ora il seguente problema: quante sono le $r-$combinazioni di n elementi che contengono ciascun elemento almeno una volta?

Esempio. Se abbiamo delle palline colorate in 3 colori, in quanti modi possiamo sceglierne 5 in modo da averne almeno una di ogni colore? Cominciamo intanto a sceglierne una di ogni colore; le 2=5–3 rimanenti possono essere qualunque. Il problema si riduce allora a quello di scegliere 2 colori da un insieme di 3 permettendo ripetizioni. Per il teorema precedente questo numero è $\binom{3-1+2}{2} = 6$:

$$\{g, r, b, g, g\}, \{g, r, b, r, r\}, \{g, r, b, b, b\}, \{g, r, b, g, r\}, \{g, r, b, g, b\}, \{g, r, b, r, b\}.$$

Questo esempio si generalizza immediatamente: il numero delle $r-$combinazioni con ripetizione di un insieme con n elementi nelle quali ogni elemento compare almeno una volta è uguale a quello delle $(r-n)$–combinazioni senza restrizioni di n elementi. Per il Teor. 1 questo numero è $\binom{n-1+(r-n)}{r-n} = \binom{r-1}{r-n} = \binom{r-1}{n-1}$ (l'ultima uguaglianza segue dalla $\binom{n}{k} = \binom{n}{n-k}$). Abbiamo quindi il teorema seguente.

Teorema 2. *Il numero delle $r-$combinazioni di n elementi nelle quali ogni elemento compare almeno una volta è*:

$$\binom{r-1}{n-1}.$$

Come per Teor. 1, anche il risultato del Teor. 2 è un numero di soluzioni intere della (20). In questo caso, poiché ogni elemento dell'insieme deve comparire almeno una volta, gli y_i devono essere tutti maggiori o uguali a 1; viceversa ogni $r-$pla di interi $y_i \geq 1$ fornisce una $r-$combinazione del tipo di quelle del Teor. 2. Ne segue:

Corollario. *Il numero delle soluzioni intere $y_i \geq 1$ della* (20) *è* $\binom{r-1}{n-1}$.

Anche qui le soluzioni sono $n-$ple, cioè successioni ordinate. Una $n-$pla di interi maggiori o uguali a 1 la cui somma è r si chiama *partizione ordinata* di r. (Il caso delle partizioni non ordinate di un intero è molto più difficile).

Esercizi

1. Quante tessere di domino in cui compaiono i numeri da 1 a 6 si possono fare?

2. In quanti modi si possono scegliere 10 oggetti di 6 tipi diversi in modo che vi sia almeno un oggetto di ciascun tipo?

3. In quanti modi si possono scegliere 8 palle da un insieme di palle di colore bianco, rosso e verde in modo da avere almeno 3 palle rosse? E se si vogliono al più 3 palle rosse?

4. Dimostrare il Teor. 1 contando i cammini in una griglia che ha n righe orizzontali e che comprendono k passi verso E (i cammini si intendono da un angolo al suo opposto).

5. I geni, cioè i portatori di caratteri ereditari, compaiono in coppia in ogni cellula di un individuo. Nel caso più semplice ogni gene può presentarsi sotto due forme distinte (dette *alleli*) che indichiamo con A_1 e A_2: possiamo allora rappresentare questi tre diversi tipi di geni (detti appunto genotipi) come A_1A_1, A_1A_2, A_2A_2. Quanti genotipi dà un gene con 3 alleli? E in generale con n alleli?

4 Permutazioni

Sia $\Omega = \{1, 2, \ldots, n\}$ un insieme finito. Una *permutazione* σ di Ω è una corrispondenza biunivoca di Ω in sé. Il modo usuale di rappresentare σ è scrivere su una riga gli elementi di Ω e sotto ciascun elemento la sua immagine secondo σ.

Esempi. 1. Sia $\Omega = \{1, 2, 3, 4, 5, 6\}$. Allora la corrispondenza

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 4 & 3 & 5 \end{pmatrix} \tag{21}$$

è una permutazione di Ω. Ciò che conta in una scrittura di questo tipo sono le colonne, non l'ordine in cui esse compaiono. A volte si dà il nome di *sostituzione* alla σ scritta nel modo ora visto, e di permutazione alla $n-$pla ordinata dei valori di σ: $\sigma(1)\sigma(2)\ldots\sigma(n)$. Se $\sigma(i) = i$, $1 \leq i \leq n$ (tutti gli elementi restano fissi), allora σ è la *sostituzione* (*o permutazione*) *identica*, o *identità*; si denota con I.

Prendiamo ora un elemento qualunque, ad esempio 6. Con σ, 6 va in 5, 5 in 3 e 3 torna in 6: scriviamo (6,5,3) Abbiamo ottenuto un *ciclo* di σ: i tre elementi si susseguono infatti ciclicamente. Lo stesso ciclo si può anche scrivere (3,6,5) oppure (5,3,6). Prendiamo ora un elemento non appartenente a questo ciclo, ad esempio 2; abbiamo il ciclo (2,1). Infine con l'elemento 4 abbiamo il ciclo che consta di un solo elemento: (4).

Possiamo scrivere la permutazione σ come

$$(1, 2)(3, 6, 5)(4) \text{ ovvero come } (4)(1, 2)(6, 5, 3)$$

o cambiando in qualunque altro modo l'ordine dei cicli e circolarmente le cifre all'interno dei cicli: l'informazione contenuta è sempre la stessa. Può ben accadere che σ sia essa stessa un ciclo. Ad esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 2 & 4 \end{pmatrix} = (1, 5, 2, 6, 4, 3).$$

Il procedimento è ovviamente generale. Abbiamo cosí:

Teorema 3. *Se σ è una permutazione di Ω, allora Ω si spezza nell'unione disgiunta di sottoinsiemi su ciascuno dei quali σ è un ciclo.*

Per costruzione, la decomposizione di una permutazione in prodotto di cicli è unica, a meno dell'ordine dei cicli e di permutazioni circolari delle cifre all'interno di questi.

Un ciclo di lunghezza k si dice $k-$ciclo. Un ciclo di lunghezza 2 *trasposizione*, un ciclo di lunghezza 1 *punto fisso*. I sottoinsiemi sui quali σ è un ciclo sono le *orbite* della permutazione.

L'insieme delle permutazioni su Ω, $|\Omega| = n$, si denota con S^n.

Teorema 4. *Il numero di elementi di S^n è $n!$.*

Dim. Una σ di S^n è individuata una volta assegnate le immagini degli elementi di Ω. Vi sono n scelte per l'immagine di 1; fatta questa scelta, ne restano $n-1$ per l'immagine di 2, e quindi $n-2$ per l'immagine di 3,..., 2 per l'immagine di $n-1$ e una sola per quella di n. In tutto quindi $n(n-1)(n-2)\cdots 2\cdot 1 = n!$. ♢

Abbiamo visto che nella scrittura di una permutazione contano solo le colonne, non l'ordine in cui esse compaiono. In altre parole, l'ordine degli elementi in in cui compaiono le cifre $1, 2, \ldots, n$ nella prima riga non ha importanza: l'insieme $\{1, 2, \ldots, n\}$ non è ordinato. Fissiamo ora invece l'ordine naturale $1, 2, \ldots, n$ nella prima riga. Ogni permutazione dà allora luogo a una ben determinata disposizione delle n cifre nella riga inferiore. Ad esempio, la σ della (21) dà luogo alla disposizione 216435. Poiché ad ogni permutazione corrisponde una disposizione, e viceversa (data una disposizione, basta scriverla sotto la disposizione $12\ldots n$ per ottenere una permutazione), la parola *permutazione* si usa in riferimento sia a una corrispondenza biunivoca σ dell'insieme $\{1, 2, \ldots, n\}$ in sé sia alla disposizione $\sigma(1)\sigma(2)\ldots\sigma(n)$.

Diamo ora un'altra dimostrazione del Teor. 4 parlando di permutazioni nel senso ora visto.

Dim. Per induzione su n. Per $n = 1$ abbiamo la sola permutazione identica, e si ha $1! = 1$. Supponiamo il teorema vero per $n-1$: $|S^{n-1}| = (n-1)!$. Ma per ogni permutazione di S^{n-1} vi sono n posizioni per inserire la cifra n. Dunque $|S^n| = n \cdot |S^{n-1}| = n(n-1)! = n!$. ♢

Il seguente algoritmo fornisce una lista delle permutazioni di S^n, e si basa

su quest'ultima dimostrazione. Inoltre, in questa lista, ogni permutazione differisce dalla precedente soltanto per una trasposizione di cifre adiacenti.
ALGORITMO (Johnson–Trotter):

Sia $\sigma_0, \sigma_1, \ldots, \sigma_{(n-1)!}$ la lista delle permutazioni di S^{n-1}. Inserire n in tutti i modi possibili nelle n posizioni di σ_i in questo modo: da destra verso sinistra se i è pari, da sinistra a destra se i è dispari.

Vediamo i casi $n = 1, 2, 3, 4$:

$$
1 \begin{cases}
1\mathbf{2} \begin{cases}
12\mathbf{3} \begin{cases} 123\mathbf{4} \\ 12\mathbf{4}3 \\ 1\mathbf{4}23 \\ \mathbf{4}123 \end{cases} \\
1\mathbf{3}2 \begin{cases} \mathbf{4}132 \\ 1\mathbf{4}32 \\ 13\mathbf{4}2 \\ 132\mathbf{4} \end{cases} \\
\mathbf{3}12 \begin{cases} 312\mathbf{4} \\ 31\mathbf{4}2 \\ 3\mathbf{4}12 \\ \mathbf{4}312 \end{cases}
\end{cases} \\
\mathbf{2}1 \begin{cases}
\mathbf{3}21 \begin{cases} \mathbf{4}321 \\ 3\mathbf{4}21 \\ 32\mathbf{4}1 \\ 321\mathbf{4} \end{cases} \\
2\mathbf{3}1 \begin{cases} 231\mathbf{4} \\ 23\mathbf{4}1 \\ 2\mathbf{4}31 \\ \mathbf{4}231 \end{cases} \\
21\mathbf{3} \begin{cases} \mathbf{4}213 \\ 2\mathbf{4}13 \\ 21\mathbf{4}3 \\ 213\mathbf{4} \end{cases}
\end{cases}
\end{cases}
$$

La lista delle permutazioni che ne risulta è la seguente

$n = 1$: $S^1 = 1$;

$n = 2$: $S^2 = \{12, 21\}$;

$n = 3$: $S^3 = \{123, 132, 312, 321, 231, 213\}$,

ecc.

Si definisce *prodotto* $\sigma \cdot \tau$ (o semplicemente $\sigma\tau$ di due permutazioni σ e τ di S^n la permutazione ottenuta facendo agire prima σ e poi τ (*prodotto operatorio*)[1]. Si osservi che la scrittura in cicli di una permutazione $\sigma = c_1 c_2 \ldots c_t \in S^n$ è in realtà il prodotto $\gamma_1\gamma_2 \ldots \gamma_t$ delle permutazioni $\gamma_i \in S^n$, dove γ_i agisce come c_i sulle cifre di c_i e fissa tutti gli altri elementi. Ad esempio:

$$\sigma = (1,2,3)(4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}.$$

L'identità I è l'elemento neutro del prodotto ora definito : $\sigma \cdot I = I \cdot \sigma = \sigma$, per ogni σ. L'*inversa* di una permutazione σ è la permutazione che moltiplicata per σ dà l'identità; si denota con σ^{-1}. Si ha quindi $\sigma\sigma^{-1} = \sigma^{-1}\sigma = I$. Il *periodo* o *ordine* di una permutazione σ è il più piccolo intero m tale che σ ripetuta m volte dà l'identità: $\sigma^m = I$. È chiaro che l'ordine di un $k-$ciclo è pari alla sua lunghezza k. Più in generale:

Teorema 5. *Se $\sigma = c_1 c_2 \ldots c_t$, con c_i di lunghezza k_i, allora l'ordine di σ è il minimo comune multiplo degli ordini dei c_i.*

Dim. Se m =mcm(c_i), allora $\sigma^m = (c_1 c_2 \ldots c_t)^m = c_1^m c_2^m \cdots c_t^m = I$ in quanto i c_i agiscono su cifre distinte e se l'ordine di c_k è m_k si ha $m = m_k s$ e dunque $c_k^m = c_k^{m_k s} = (c_k^{m_k})^s = I^s = I$. D'altra parte l'ordine m di σ deve essere un multiplo di ciascun m_k, altrimenti per almeno un k si avrebbe $c_k^m \neq I$. $\diamondsuit$

In particolare, una trasposizione τ ha periodo 2 (operando due volte una trasposizione si ritorna alla situazione iniziale): $\tau^2 = I$, e ciò significa anche che essa coincide con la propria inversa, come si vede moltiplicando entrambi i membri della $\tau^2 = I$ per τ^{-1}:

$$\tau^2 \cdot \tau^{-1} = I \cdot \tau^{-1}, \text{ ovvero } \tau = \tau^{-1}.$$

Sia $\Omega = \{1,2,3\}$, e consideriamo le due permutazioni

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Allora $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, mentre $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Dunque $\sigma\tau \neq \tau\sigma$: in generale, due permutazioni non sono permutabili. Se $n \geq 3$, consideriamo due permutazioni σ e τ che agiscono su 1,2 e 3 come sopra e lasciano fissi gli altri elementi. È chiaro che si ha ancora $\sigma\tau \neq \tau\sigma$. Dunque: *se $n \geq 3$, due permutazioni di S^n non sono in generale permutabili.*

[1]Scrivendo $\sigma\tau$, alcuni autori fanno agire prima τ e poi σ.

4.1 Trasposizioni e inversioni. Parità

Sappiamo che una permutazione si spezza in cicli. Un ciclo (1,2,...,k) si può scrivere come prodotto di trasposizioni in questo modo:

$$(1,2,\ldots,k) = (1,2)(1,3)\cdots(1,k),$$

e facendo questa operazione per ognuno dei cicli nei quali si spezza una permutazione abbiamo che *ogni permutazione è prodotto di trasposizioni*:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 4 & 6 & 1 \end{pmatrix} = (1,3,7)(2,5,4)(6) = (1,3)(6,7)(1,7)(2,5)(2,4)(1,6).$$

Ma le trasposizioni che compaiono non sono in generale permutabili:

$$(1,2,3) = (1,2)(1,3) \neq (1,3)(1,2) = (1,3,2).$$

Inoltre, una permutazione si può scrivere in più modi come prodotto di trasposizioni:

$$(1,2,3) = (1,2)(1,3) = (1,3)(2,3)(1,2)(1,3)(1,2)(2,3).$$

Tuttavia, nelle varie scritture come prodotto di trasposizioni c'è qualcosa che non varia, ed è la parità del numero di trasposizioni che compaiono (nell'esempio qui sopra abbiamo scritto (1,2,3) come prodotto rispettivamente di 2 e 6 trasposizioni, e 2 e 6 sono entrambi numeri pari). In altri termini, una permutazione non si può scrivere come prodotto di un numero pari e allo stesso tempo di un numero dispari di trasposizioni. Una volta dimostrato questo fatto, cioè che la parità è ben determinata, potremo definire la *parità* di una permutazione σ come la parità del numero di trasposizioni che per prodotto danno σ (v. Teor. 6). Diremo allora che una permutazione è *pari* se si può scrivere come prodotto di un numero pari di trasposizioni, *dispari* nell'altro caso.

Con $z(\sigma)$ denotiamo il numero dei cicli di σ (contando anche i cicli di lunghezza 1).[2]

Lemma. (Serret). *Siano σ una permutazione di S^n e $\tau = (i,j)$ una trasposizione. Allora*:

$$z(\sigma\tau) = \begin{cases} z(\sigma)+1 & \text{se } i \text{ e } j \text{ appartengono allo stesso ciclo di } \sigma, \\ z(\sigma)-1 & \text{altrimenti.} \end{cases}$$

Nel primo caso diremo che τ separa *σ, nel secondo che τ* unisce *σ.*

[2] La lettera z è l'iniziale del tedesco *Zyklus*.

Dim. Sia $\sigma = (1, 2, \ldots, i-1, i)(i+1, \ldots, j-1, j, j+1, \ldots, n)\ldots$. Allora $\sigma\tau = (1, 2, \ldots, i-1, j, j+1, \ldots, n, i+1, \ldots, j-1, i)\ldots$, e dunque $\sigma\tau$ ha un ciclo di meno di σ (si osservi che il secondo ciclo viene inserito nel primo tra $i-1$ e i). Se $\sigma = (1, 2, \ldots, i, \ldots, j, \ldots, m)\ldots$, allora $\sigma\tau = (1, 2, \ldots, i-1, j, \ldots, m)(i, i+1, \ldots, j-1)\ldots$, e $\sigma\tau$ ha un ciclo di più di σ. $\diamondsuit$

Corollario. *Il minimo numero di trasposizioni che per prodotto danno un ciclo di lunghezza n è $n-1$.*

Dim. Sia $\sigma = (1, 2, \ldots, n) = \tau_1\tau_2\cdots\tau_k$. Moltiplicando a destra per τ_k, $\sigma\tau_k$ ha due cicli, $\sigma\tau_k\tau_{k-1}$ al più tre (esattamente tre se le due cifre di τ_{k-1} appartengono allo stesso ciclo di $\sigma\tau_k$),..., $\sigma\tau_k\tau_{k-1}\cdots\tau_1$ al più $k+1$. ma quest'ultima permutazione è l'identità, che ha n cicli. Dunque $n \leq k+1$, e $k \geq n-1$. $\diamondsuit$

Se σ ha k cicli di lunghezza rispettivamente $n_1, n_2, \ldots, n_k$, il minimo numero di trasposizioni che servono per scrivere σ è

$$(n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - 1 - 1 - \ldots - 1,$$

con tanti 1 quanti sono i cicli. E poiché $n_1 + n_2 + \cdots + n_k = n$ abbiamo:

Corollario. *Il minimo numero di trasposizioni che per prodotto danno una permutazione σ è $n - z(\sigma)$.*

Teorema 6. *La parità di una permutazione è ben determinata.*

Dim. Le permutazioni di S^n si suddividono in due classi a seconda che abbiano un numero pari o dispari di cicli (contando anche i cicli di lunghezza 1)[3]. Per il lemma di Serret, se una permutazione viene moltiplicata per un numero k di trasposizioni la permutazione che ne risulta appartiene o no alla stessa classe della prima a seconda che k sia pari o dispari. L'identità I appartiene alla classe delle pari se n è pari (I ha n cicli) e a quella delle dispari nell'altro caso. Sia σ una permutazione; scriviamola come prodotto di trasposizioni e moltiplichiamo la permutazione identica I per σ. Se σ si scrive con un numero pari di trasposizioni, allora $I \cdot \sigma$ appartiene alla stessa classe di I; se σ si scrive con un numero dispari, $I \cdot \sigma$ appartiene all'altra classe. Ma $I \cdot \sigma = \sigma$, e poiché σ non può appartenere a entrambe le classi, essa non può essere allo stesso tempo prodotto di un numero pari e di un numero dispari di trasposizioni. $\diamondsuit$

Dimostriamo ora che *le permutazioni pari su n elementi sono tante*

[3]Non si confonda la parità del numero di cicli con la parità della permutazione.

quante quelle dispari, e quindi metà sono pari e metà sono dispari. Sia $A = \{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ l'insieme delle permutazioni pari, $B = \{\eta_1, \eta_2, \ldots, \eta_s\}$ l'insieme di quelle dispari, e sia τ una trasposizione. Moltiplicando le σ_i per τ otteniamo tutte permutazioni dispari (hanno una trasposizione in più). Inoltre, se $\sigma_i\tau = \sigma_j\tau$ moltiplicando ancora per τ abbiamo $\sigma_i\tau^2 = \sigma_i = \sigma_j\tau^2 = \sigma_j$, mentre σ_i e σ_j sono distinte. Quindi al variare di i, le $\sigma_i\tau$ sono tra le η_i e sono tutte distinte, e pertanto la corrispondenza $A \to B$ data da $\sigma_i \to \sigma_i\tau$ è iniettiva; quindi $s \geq r$. Analogamente, moltiplicando le η_i per τ otteniamo permutazioni pari tutte distinte, e una corrispondenza iniettiva tra B e A, e quindi $r \geq s$. La moltiplicazione per τ stabilisce allora una corrispondenza biunivoca tra A e B, e dunque $r = s$, come si voleva.

Una cifra i ha un duplice funzione: da un lato rappresenta *l'elemento i* dell'insieme $\{1, 2, \ldots, n\}$, dall'altro indica *l'i–esimo posto* in una permutazione. Una trasposizione (i, j) può significare due cose: scambiare tra loro le cifre i e j (la permutazione opera per *alias*), oppure scambiare tra loro le cifre che stanno nei posti i e j (la permutazione opera per *alibi*). Qual è la traduzione algebrica di questa differenza?

Connsideriamo la permutazione $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}$, e moltiplichiamola a destra per la trasposizione $\tau = (3, 4)$:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}.$$

Il risultato è la permutazione 531642, che si ottiene da quella data scambiando le cifre 3 e 4. Se invece moltiplichiamo a sinistra per τ:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 1 & 3 & 2 \end{pmatrix}$$

il risultato è la permutazione 546132, che si ottiene da quella data scambiando le cifre 1 e 6, cioè quelle che stanno nei posti 3 e 4. Il risultato è ovviamente generale.

Teorema 7. *Moltiplicando a destra una permutazione σ per una trasposizione $\tau = (i, j)$ si ottiene una permutazione $\sigma\tau$ che differisce dalla σ per lo scambio delle cifre i e j. Moltiplicando σ a sinistra per τ, la permutazione $\tau\sigma$ che si ottiene differisce dalla σ per lo scambio delle cifre che si trovano nei posti i e j.*

Nota. È appena il caso di osservare che il risultato delle moltiplicazioni a destra o a sinistra per τ ora viste dipendono da come si fa agire il prodotto $\sigma\tau$: prima σ e poi τ oppure prima τ e poi σ.

La parità di una permutazione si può determinare anche in un altro modo. Consideriamo per esempio la permutazione $\sigma = 541632$. Diremo che la cifra 1 *presenta due inversioni*, in quanto vi sono due cifre che precedono 1 e che sono maggiori di 1: le cifre 4 e 5. Analogamente, 2 presenta quattro inversioni, date dalle cifre 3,4,5 e 6, 3 ne presenta tre, date da 4,5 e 6, 4 una sola (5), 5 nessuna, e 6 nessuna (ovviamente, essendo 6 la cifra più grande). Il numero totale di inversioni è dunque $I(\sigma) = 2+4+3+1+0+0 = 10$. In generale il numero di inversioni di una cifra i in una permutazione è il numero di cifre a sinistra della i che sono maggiori di i, e il numero di inversioni $I(\sigma)$ della permutazione σ è la somma delle inversioni delle singole cifre. La *permutazione fondamentale* $12\ldots n$ presenta ovviamente zero inversioni.

Riprendiamo ora la 541632 e cerchiamo di ridurla alla permutazione fondamentale $12\ldots n$, di portare cioè 1 al primo posto, 2 al secondo,..., n all'ultimo mediante opportuni scambi (trasposizioni): possiamo ad esempio scambiare la cifra 1 con la 5, ottenendo 145632; quindi 2 con 4: 125634; poi 3 con 5: 123654, e infine 4 con 6: 123456. Per quanto visto sopra, uno scambio di cifre (i, j) corrisponde a moltiplicare la permutazione σ a destra per la trasposizione (i, j), e quindi nel nostro esempio la permutazione identica si ottiene dalla data moltiplicando a destra successivamente per (1,5),(2,4), (3,5) e (4,6):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}(1,5)(2,4)(3,5)(4,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Ne segue:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix} = (4,6)(3,5)(2,4)(1,5)$$

Avremmo potuto procedere in un altro modo. Portare la cifra 1 al primo posto scambiandola prima con 4, ottenendo 514632 e poi con 5, ottenendo 154632. Scambiare 1 con 4 significa scambiare tra loro le cifre che stanno nel secondo e nel terzo posto, e ciò si traduce nelle moltiplicazione a sinistra della σ per la trasposizione (2,3):

$$\sigma' = (2,3)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 3 & 2 \end{pmatrix}$$

e quindi nella moltiplicazione di σ' a sinistra per (1,2) perché abbiamo scambiato le cifre che stanno al primo e al secondo posto:

$$\sigma'' = (1,2)\sigma' = (1,2)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 3 & 2 \end{pmatrix}.$$

Procedendo in questo modo, arriviamo alla permutazione identica:

$$(4,5)(3,4)(4,5)(5,6)(2,3)(3,4)(4,5)(5,6)(1,2)(2,3)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

da cui:

$$\sigma = (2,3)(1,2)(5,6)(4,5)(3,4)(2,3)(5,6)(4,5)(3,4)(4,5).$$

In questo modo abbiamo scritto σ come prodotto di 10 trasposizioni mentre prima erano solo 4. Ma in questo caso si hanno due vantaggi: le trasposizioni sono tutte della stessa forma $(i, i+1)$, e inoltre il loro numero è pari al numero di inversioni di σ (come abbiamo visto sopra la 541632 presenta 10 inversioni). Il teorema che segue ci dice infine che questo numero di trasposizioni della forma $(i, i+1)$ è minimo.

Teorema 8. *Il minimo numero di trasposizioni della forma $(i, i+i)$ che per prodotto danno una permutazione σ è uguale al numero di inversioni di σ.*

Dim. Come visto sull'esempio precedente, scrivere σ come prodotto di trasposizioni della forma $(i, i+1)$ equivale a ridurre σ all'identità moltiplicandola per trasposizioni di quel tipo. Per ridurre allora σ all'identità portiamo 1 al primo posto mediante un numero di scambi di termini consecutivi in numero uguale al numero di inversioni $I(1)$ che presenta 1; ciò significa moltiplicare σ per opportune trasposizioni $(i, i+1)$ in numero pari a $I(1)$. Otteniamo una permutazione σ'. Portiamo ora 2 al secondo posto nella σ' mediante un numero $I(2)$ di scambi di termini consecutivi pari a $I(2)$; e così via, finché otteniamo l'identità. In questo modo, abbiamo ridotto σ all'identità mediante $I(1) + I(2) + \ldots + I(n) = I(\sigma)$ trasposizioni.

Con meno trasposizioni della forma $(i, i+1)$ non si raggiunge lo scopo. Infatti, moltiplicando σ a sinistra per $(i, i+1)$ si ottiene una permutazione che ha una inversione in meno o in più a seconda che le due cifre che si trovano nei posti i e $i+1$ sono invertite o meno. Ne segue che moltiplicando per k trasposizioni della forma $(i, i+1)$ la permutazione α che si ottiene ha un numero $I(\alpha)$ di inversioni tale che $I(\alpha) \geq I(\sigma) - k$ (si ha uguaglianza se ogni volta il numero delle inversioni diminuisce di uno). Se si vuole che α sia l'identità, che non ha inversioni, deve essere $I(\alpha) = 0$, e quindi $0 \geq I(\sigma) - k$, da cui $k \geq I(\sigma)$. $\diamondsuit$

Una permutazione determina una *tavola delle inversioni*:

$$b_1, b_2, \ldots, b_n,$$

dove b_i è il numero di inversioni della cifra i. Si ha allora

$$0 \leq b_1 \leq n-1,\ 0 \leq b_2 \leq n-2, \dots, 0 \leq b_{n-1} \leq 1,\ b_n = 0.$$

Ad esempio, la tavola delle inversioni della 541632 è la 2,4,3,1,0,0. Viceversa, la tavola delle inversioni determina la permutazione, come dimostra il seguente teorema.

Teorema 9. *Data una lista di interi non negativi b_i tali che $b_i \leq n-i$, esiste una e una sola permutazione che ammette questa lista come tavola delle inversioni.*

Dim. La dimostrazione è contenuta nel seguente algoritmo.

ALGORITMO

Data una lista di interi $b_1, b_2, \dots, b_n$, con $b_i \leq n-i$, $i = 1, 2, \dots, n$, per $i = 1, 2, \dots, n$, e una stringa a n posti, mettere la cifra i nel $(b_i+1)-$esimo posto libero partendo da sinistra. $\diamondsuit$

Esempio. Consideriamo la lista 2,4,3,1,0,0 ora vista. Un rapido controllo mostra che $b_i \leq 6-i$. Segnamo 6 posti:

$$|\quad\ |\quad\ |\quad\ |\quad\ |\quad\ |\quad\ |$$

Poiché $a_1 = 2$, mettiamo la cifra 1 nel $(2+1)-$esimo, cioè nel terzo posto libero (che in questo caso è semplicemente il terzo posto):

$$|\quad\ |\quad\ |\ 1\ |\quad\ |\quad\ |\quad\ |$$

Mettiamo ora a posto la cifra 2. Essa presenta 4 inversioni, e quindi va nel quinto posto libero (l'ultimo):

$$|\quad\ |\quad\ |\ 1\ |\quad\ |\quad\ |\ 2\ |$$

Il 3 presenta 3 inversioni: va nel quarto posto libero:

$$|\quad\ |\quad\ |\ 1\ |\quad\ |\ 3\ |\ 2\ |$$

Il 4 ne presenta una: va a occupare il secondo posto libero:

$$|\quad\ |\ 4\ |\ 1\ |\quad\ |\ 3\ |\ 2\ |$$

Il 5 ne presenta zero, e quindi va nel posto libero 0+1, cioè nel primo posto libero:

$$|\ 5\ |\ 4\ |\ 1\ |\quad\ |\ 3\ |\ 2\ |$$

Il 6 ha zero inversioni: va nel primo posto libero (l'unico):

$$| \ 5 \ | \ 4 \ | \ 1 \ | \ 6 \ | \ 3 \ | \ 2 \ |$$

Ritroviamo quindi la permutazione 541632.

Un altro modo di ritrovare la permutazione a partire dalla tavola di inversioni è il seguente. Contrariamente al modo visto, nel quale si sistemano le cifre nell'ordine 1,2,. . . ,n, qui si parte da n, e poi si sistemano di seguito $n-1, n-2, \ldots, 2, 1$. Con la tavola 2,4,3,1,0,0 dell'esempio precedente si procede come segue. Scriviamo l'ultima cifra, $n = 6$:

$$6$$

Poiché $b_5 = 0$, 5 non è invertito rispetto a 6, e quindi sta a sinistra di 6 (anche se non sappiamo di quanti posti). Scriviamo 5:

$$5 \quad 6.$$

Essendo $b_4 = 1$, la cifra 4 non può stare a destra di 5 e 6 (si avrebbe $b_4 = 2$), né a sinistra di entrambi (si avrebbe $b_4 = 0$). Dunque 4 sta tra 5 e 6:

$$5 \quad 4 \quad 6.$$

Ora, $b_3 = 3$, e dunque 3 è a destra delle tre cifre scritte:

$$5 \quad 4 \quad 6 \quad 3.$$

Da $b_2 = 4$ segue:

$$5 \quad 4 \quad 6 \quad 3 \quad 2$$

e da $b_1 = 2$:

$$5 \quad 4 \quad 1 \quad 6 \quad 3 \quad 2,$$

che è la permutazione di partenza.

Si possono definire altre tavole di inversioni. Nella tavola di b_i, già vista:

- $b_1 b_2 \ldots b_n$: b_i è il numero di cifre a *sinistra* di i che sono *maggiori* di i,

e quindi $b_i \leq n - i$. Se scambiamo "destra" con "sinistra" e "maggiori" con "minori" otteniamo la tavola "duale" della $b_1 b_2 \ldots b_n$:

- $c_1 c_2 \ldots c_n$: c_i è il numero di cifre a *destra* di i che sono *minori* di i.

Ad esempio, per la permutazione 541632 la tavola dei c_i è 0,0,1,3,4,2. Le cifre minori di i sono $1, \ldots, i-1$, e quindi $0 \leq c_i < i$.

Invece delle inversioni di una *cifra* i, si possono poi considerare le inversioni della cifra che occupa il *posto* i: se $x_1 x_2 \ldots x_n$ è una permutazione:

- $d_1 d_2 \ldots d_n$: d_i è il numero di cifre a *sinistra* di x_i che sono *maggiori* di x_i.

Per la 541632 la tavola dei d_i è 0,1,2,0,3,4. Poiché a sinistra di x_i c'è posto per al più $i-1$ elementi, si ha $0 \leq d_i < i$.

Dualmente, si ha la tavola:

- $l_1 l_2 \ldots l_n$: l_i è il numero di cifre a *destra* di x_i che sono *minori* di x_i.

Questa tavola si chiama anche *codice di Lehmer*. Per la 541632 otteniamo 4,3,0,2,1,0. E poiché a destra di x_i c'è posto per al più $n-i$ elementi, abbiamo $l_i \leq n-i$.

Poiché ognuna queste tavole determina univocamente una permutazione (v. *es.* 12), e per questo si chiamano anche "codici", esse si possono utilizzare per generare permutazioni, con il vantaggio di far uso in generale di un alfabeto con un numero di lettere inferiore a n.

Esercizi

1. Scrivere la permutazione $(1,2,3)(4,5)$ come prodotto di un 4–ciclo e di un 5–ciclo.

2. Quanti sono i cicli di lunghezza n in S^n? E quelli di lunghezza k?

3. La parità di una permutazione $\sigma \in S^n$ è quella del numero $n - z(\sigma)$.

4. Scegliamo a caso una permutazione $\sigma \in S^n$. Se spezziamo σ in cicli, qual è la probabilità che la cifra 1 appartenga a un ciclo di lunghezza k?

5. Scegliamo a caso una permutazione $\sigma \in S^n$. Se spezziamo σ in cicli, qual è la probabilità che le cifre 1 e 2 appartengano allo stesso ciclo?

6. Se si moltiplica a destra una permutazione σ per un ciclo $(i_1, i_2, \ldots, i_k)$, si ottiene una permutazione nella quale le cifre $i_1, i_2, \ldots, i_k$ di σ sono permutate secondo il ciclo inverso $(i_1, i_k, \ldots, i_2)$. Lo stesso accade, moltiplicando a sinistra, per le cifre che stanno nei posti $i_1, i_2, \ldots, i_k$.

Una matrice $n \times n$ di 0 e 1 si dice *matrice di permutazione* se in ogni riga e colonna compare un solo 1. Una tale matrice si ottiene dalla matrice identica pemutandone le colonne (o le righe) secondo una $\sigma \in S^n$. Applicando una tale matrice a un vettore colonna (riga) $[1, 2, \dots, n]$, le componenti di questo vettore vengono permutate secondo la σ.

7. Dimostrare (per induzione su n) che il determinante di una matrice di permutazione è ± 1.

8. Se la permutazione $x_1, x_2, \dots, x_n$ presenta k inversioni, quante ne presenta la $x_n, x_{n-1}, \dots, x_1$?

9. Quante inversioni presenta una trasposizione (i, j)?

10. Qual è la permutazione che presenta il massimo numero di inversioni?

11. Se una permutazione σ presenta k inversioni, quante ne presenta σ^{-1}?

12. Dimostrare che il numero delle permutazioni di S^n è $n!$ considerando le tavole di inversioni viste nel testo.

13. Determinare per ciascuna delle tavole di inversione viste nel testo un algoritmo che permetta di risalire dalla tavola alla permutazione.

4.2 Permutazioni con ripetizione

Come per le combinazioni, dove l'ordine degli elementi che si scelgono non conta, anche per le permutazioni, dove invece conta, si possono considerare ripetizioni. Ad esempio, per un insieme di tre elementi $\{1, 2, 3\}$, le coppie ordinate con ripetizione, cioè le 2–permutazioni, sono:

$$\{1,1\},\ \{1,2\},\ \{1,3\},\ \{2,1\},\ \{2,2\},\ \{2,3\},\ \{3,1\}, \{3,2\},\ \{3,3\}.$$

Teorema 10. *Il numero delle r-permutazioni di n elementi è n^r.*

Dim. Per costruire una successione ordinata di r elementi, ciascun elemento si può scegliere in n modi. $\diamondsuit$

Consideriamo ora il caso delle permutazioni in cui ogni elemento è ripetuto un fissato numero di volte (ovvero il numero di permutazioni di oggetti alcuni dei quali sono indistinguibili).

Teorema 11. *Sia $\{a_1, a_2, \dots, a_n\}$ un insieme con n elementi. Allora il numero di permutazioni degli n elementi nelle quali l'elemento a_i è ripetuto r_i volte è:*

$$\frac{(r_1 + r_2 + \cdots + r_n)!}{r_1! r_2! \cdots r_n!}. \tag{22}$$

Dim. In ogni permutazione consideriamo gli oggetti come tutti distinti. Il numero di tutte le permutazioni è allora $(r_1 + r_2 + \cdots + r_n)!$. Gli oggetti di tipo a_1, che sono in numero di r_1 possono essere scambiati tra loro in tutti i modi possibili, e dunque in in $r_1!$ modi; quelli di tipo a_2 in $r_2!$ modi, ecc. Se ora torniamo a considerare gli a_1 come tutti uguali, ogni permutazione viene ripetuta $r_1!$ volte; se poi consideriamo anche gli a_2 come tutti uguali, ogni permutazione è ripetuta $r_2!$ volte, ecc. In totale ogni permutazione è ripetuta $r_1!r_2!\cdots r_n!$ volte, da cui il risultato. $\diamondsuit$

La quantità (22) si denota anche con:

$$\binom{r_1 + r_2 + \cdots + r_n}{r_1, r_2, \cdots, r_n} \tag{23}$$

e prende il nome di *coefficiente multinomiale*. Dato un insieme con $r_1+r_2+\cdots+r_n$ elementi, il simbolo (23) rappresenta il numero di modi di scegliere r_1 elementi, quindi r_2 tra gli elementi rimanenti, ecc. Analogamente al caso del coefficiente binomiale (del quale è una generalizzazione), si ha:

$$(x_1 + x_2 + \cdots + x_n)^m = \sum_{r_1+r_2+\cdots+r_n=m} \binom{r_1 + r_2 + \cdots + r_n}{r_1, r_2, \cdots, r_n} x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}.$$

Esempi. 1. Il coefficiente del monomio xy^3z^5 nello sviluppo di $(x+y+z)^9$ è $\binom{9}{1,3,5}$.

2. Lanciando un dado 10 volte, qual è la probabilità che si ottenga una successione contenente tre 1, quattro 5 e tre 6? Il numero totale delle successioni possibili è 6^{10}, e tra queste occorre stabilire quante sono quelle del tipo richiesto. La risposta ce la dà il Teor. 11, con $r_1 = 3, r_2 = 4$ e $r_3 = 3$. Il numero cercato è dunque $\binom{10}{3,4,3} = 4200$, e la probabilità $4200/6^{10}$.

Esercizi

1. Scrivere i coefficienti binomiali nello sviluppo di $(x + y)^n$ come coefficienti multinomiali.

2. Se mettiamo in un scaffale 5 libri in lingua inglese, 4 di francese e 2 di tedesco, in quanti modi essi si possono raggruppare per argomento?

3. Dimostrare che il coefficiente multinomiale si può esprimere come prodotto di coefficienti binomiali nel modo seguente:

$$\binom{r_1 + r_2 + \cdots + r_n}{r_1, r_2, \cdots, r_n} = \binom{r_1 + r_2 + \cdots + r_n}{r_1}\binom{r_2 + \cdots + r_n}{r_2}\cdots\binom{r_{n-1} + r_n}{r_{n-1}}\binom{r_n}{r_n}.$$

4. Determinare i coefficienti dei termini $x^4y^5z^3$ e $x^3y^5z^2$ nello sviluppo di $(x + 2y + 3z)^{12}$.