1

Capitolo B16
matrici, relazioni, permutazioni

Contenuti delle sezioni

a. matrici binarie e operazioni binarie p. 2
b. relazioni finite e digrafi p. 9
c. digrafi ordinati, digrafi graduati, arborescenze p. 14
d. permutazioni di insiemi finiti p. 20
e. permutazioni cicliche p. 23
f. classificazioni di funzioni finite e di permutazioni p.30

31 pagine

B16 0.01 Questo capitolo serve per una prima introduzione di varie nozioni che compaiono in vari contesti e che succcessivamente dovranno essere maggiormente approfondite.

Si inizia definendo matrici le funzioni aventi come dominio il prodotto cartesiano di due insiemi finiti. Si tratta di strutture di dati che consentono di rappresentare con buone possibilità operative le relazioni finite e i digrafi.
Questi due tipi di entit'a, sostanzialmente equivalenti, sono ampiamente utilizzati nelle definizioni di gran parte dei modelli discreti di situazioni e processi reali e si rivelano utili nozioni basilari per lo studio di gran parte degli algoritmi.

Servendosi di matrici e digrafi si procede poi ad avviare utili classificazioni delle collezioni di permutazioni degli insiemi finiti e a introdurre la nozione di gruppo di permutazioni, fondamentale per lo studio delle simmetrie.

Con le permutazioni, anche se qui applicate solo a configurazioni finite, si può avviare lo studio delle simmetrie di svariati oggetti matematici (configurazioni discrete, figure geometriche, formule, equazioni, strutture, sistemi di assiomi, ...).

Le simmetrie saranno in seguito viste in relazione all'obiettivo generale di realizzare economie auspicabilmente sistematiche in molteplici attività conoscitive: indagini entro settori specifici della matematica e delle sue applicazioni (in particolare sistemi atomici, molecolari e cristalli); studi volti alla documentazione e alla sistemazione organica dei risultati entro ampi quadri teorici; economie in calcoli particolari e nella organizzazione di specifici strumenti software; valutazioni estetiche concernenti le configurazioni e le costruzioni che si basano su nozioni matematiche.

B16 a. matrici binarie e operazioni binarie

B16 a.01 Consideriamo due liste nonripetitive $A = \langle a_1, a_2, ..., a_r \rangle$ e $B = \langle b_1, b_2, ..., b_c \rangle$, il loro prodotto cartesiano $A \times B$ e un insieme V; le due liste A e B si possono equivalentemente considerare due insiemi ordinati e lo stesso si può dire di $A \times B$.

Ogni funzione (finita) il cui dominio è l'intero $A \times B$ e il cui codominio è contenuto in V viene chiamata **matrice** con le righe etichettate da A, le colonne etichettate da B e con le i valori in V.
Spesso per i valori assunti da una matrice si usa il termine più specifico **entrate della matrice**; una tale matrice M viene introdotta con una presentazione della forma

$$M \in \lceil\!\lceil\, A \times B \longmapsto V \,\rceil\!\rceil \ .$$

Le coppie $\langle a, b \rangle \in A \times B$ che costituiscono gli elementi del suo dominio vengono dette **caselle della matrice** M.
Inoltre si dice che $A \times B$ costituisce il **profilo della matrice** M; talora invece di questo termine viene usato il termine formato.

L'insieme delle matrici il cui dominio è $A \times B$ e il cui codominio fa parte di un insieme V si denota con le due espressioni equivalenti

$$\mathbf{Mat}_{A,B,V} \ := \ \mathbf{Mat}[A, B, V] \ := \ \lceil\!\lceil\, A \times B \longmapsto V \,\rceil\!\rceil \ .$$

In particolare fissati due interi positivi r, c è chiaramente definito l'insieme di matrici $\mathbf{Mat}[(\mathrm{r}\ ], (\mathrm{c}\ ], V]$; per un tale insieme è comodo usare l'abbreviazione $\mathbf{Mat}[r, c, V]$.

Dato che $\mathsf{cod}(M)$ è un sottoinsieme finito di V, possiamo usare scritture come $\mathsf{cod}(M) = \{v_1, v_2, ..., v_s\}$ con $s := |\mathsf{cod}(M)|$.

Per la matrice $M \in \mathbf{Mat}_{A,B,V}$, A si dice costituire la lista delle **etichette delle righe della matrice**, mentre B è chiamato lista delle **etichette delle colonne della matrice**.

Spesso l'ordinamento degli items delle liste A e B non riveste interesse, queste due liste vengono considerate come due insiemi e sono chiamate insiemi di etichette.

Un elemento $\langle a, b \rangle$ del dominio $A \times B$ di una matrice $M \in \mathbf{Mat}_{A,B,V}$ viene chiamato **casella della matrice**.
Il valore di una funzione $M \in \lceil\!\lceil\, A \times B \longmapsto V \,\rceil\!\rceil$ corrispondente ad una casella $\langle a, b \rangle$, cioè $M(\langle a, b \rangle)$ si può abbreviare con la scritture $M\langle a, b \rangle$, e spesso più efficacemente si abbrevia con la scrittura $M_{a,b}$.

La lista delle caselle di M della forma $\big\langle b \in B :| \ \langle a, b \rangle \big\rangle$ per $a \in A$ si dice **riga della matrice** M avente etichetta a.
La lista delle caselle di M della forma $\big\langle a \in A :| \ \langle a, b \rangle \big\rangle$ per $b \in B$ si dice **colonna della matrice** M avente etichetta b.
Collettivamente, le righe e le colonne di una matrice M sono chiamate le **linee della matrice**.

B16 a.02 Useremo la notazione $\mathbf{Mat}[A, B; \overline{V}]$ per denotare l'insieme delle matrici di profilo $A \times B$ il cui codominio è l'insieme (finito) $\overline{V}$.

Spesso risulta conveniente fare riferimento a un definito ordinamento totale per $\overline{V}$, ovvero conviene fare riferimento a una lista delle entrate della matrice in esame che segua un ordinamento facilmente descrivibile.

In molte considerazioni sulle matrici non influiscono le caratteristiche delle etichette delle righe e quelle delle etichette delle colonne, ma solo la possibilità di distinguere tra le diverse righe e tra le diverse colonne.

Studiando tali matrici conviene limitarsi alle matrici appartenente al più circoscritto insieme di matrici con righe e colonne etichettate da interi positivi, insieme che genericamente si può denotare con $\mathsf{Mat}[r, c, V]$; alternativamente può convenire esaminare il più ridotto $\mathsf{Mat}[r, c; \overline{V}]$.

In alcune considerazioni su matrici di $\mathsf{Mat}[r, c; \overline{V}]$ non hanno influenza le caratteristiche degli elementi di $\overline{V}$ ma solo la loro distinguibilità e l'esame delle matrici di $\mathsf{Mat}[r, c; \overline{V}]$ si può sostituire con l'esame delle matrici le cui entrate costituiscono l'insieme dei primi s interi positivi, ossia $\mathsf{Mat}[r, c; (\mathrm{s}\,]]$.
La notazione di questo insieme conviene sia semplificata con la $\mathsf{Mat}[r, c; s]$ e la notazione per il suo sovrainsieme $\mathsf{Mat}[r, c, (\mathrm{s}\,]]$, costituito dalle matrici i cui valori non sono necessariamente tutti gli interi in $(\mathrm{s}\,]$, conviene semplificarla con la $\mathsf{Mat}[r, c, s]$.

B16 a.03 L'insieme di matrici $\mathsf{Mat}[r, c, s]$ è finito e facilmente esplicitabile.

Ogni matrice $M \in \mathsf{Mat}[r, c, s]$ viene rappresentata dai parametri r e c e da una lista della forma

$$\left\langle i = 1, 2, ..., r, j = 1, 2, ..., c :| \left\langle \langle a_i, b_j \rangle, M_{i,j} \right\rangle \right\rangle \quad \text{con ogni } M_{i,j} \in (\mathrm{s}\,] \ .$$

Dunque ciascuna delle matrici di $\mathsf{Mat}[r, c, s]$ si può rappresentare, con una sequenza di $r \cdot c$ interi appartenenti all'intervallo $(\mathrm{s}\,]$, avvalendosi di un carattere con il ruolo di separatore di righe.

L'algoritmo per la generazione di una lista di tutte le matrici in $\mathsf{Mat}[r, c, s]$ richiede semplicemente un ciclo primario per la corsa $i \in \hookrightarrow 1, ..., r$, un ciclo secondario per la corsa $j \in \hookrightarrow 1, ..., c$ e la iterazione di livello 3 per la generazione di tutte le disposizioni con ripetizione di lunghezza $r\,c$ le cui componenti si trovano in $\{1, ..., s\}$, manovra ottenibile con l'algoritmo presentato in B06g03.

L'applicazione della sostituzione biiettiva degli interi di $(\mathrm{r}\,]$ con gli items di A, di quella degli interi di $(\mathrm{c}\,]$ con gli items di B e di quella degli interi di $(\mathrm{s}\,]$ con gli items dell'insieme-s V consente di trasformare la lista generata dall'algoritmo precedente in una lista di stringhe che possono considerarsi rappresentazioni di tutte le matrici di $\mathsf{Mat}(A, B, V)$.

Quindi anche ogni $\mathsf{Mat}_{A,B,V}$ con V insieme finito va considerato un insieme esplicitabile.

A questo punto è evidente che per il cardinale di questi insiemi di matrici si ha

$$\left|\mathsf{Mat}[r, c, s]\right| \ = \ \left|\mathsf{Mat}[A, B; V]\right| \ = \ s^{r \cdot c} \ .$$

Dato che tutti gli insiemi espliciti si possono ordinare totalmente, ovvero porre in corrispondenza biunivoca con un insieme della forma $(\mathrm{n}\,]$ (o della forma $[\mathrm{n}\,)$), le matrici esplicite appartenenti a un insieme $\mathsf{Mat}_{A,B,V}$ si possono ricondurre alle matrici di profilo $(\mathrm{r}\,] \times (\mathrm{c}\,]$ o, se si preferisce, a quelle di profilo $[r) \times [c)$).

Queste a loro volta sono individuate semplicemente da r e c, oltre che da V, e si possono chiamare semplicemente matrici di profilo $r \times c$ a entrate in V, mentre il loro insieme si può denotare con $\mathsf{Mat}_{r,c,V}$, scrittura da considerare abbreviazione della $\mathsf{Mat}_{(\mathrm{r}\,],(\mathrm{c}\,],V}$.
Similmente spesso si abbrevia la scrittura $\mathsf{Mat}_{(\mathrm{r}\,],(\mathrm{c}\,],(v]}$ con la $\mathsf{Mat}_{r,c,v}$.

B16 a.04 Per molte questioni (tendenzialmente per quelle generali) ci si può limitare a studiare le proprietà di queste matrici, in quanto da queste si ricavano facilmente le proprietà delle altre.

Vi sono però attività concernenti matrici per le quali è importante precisare a quali oggetti introdotti ed esaminati in precedenza vanno riferite le etichette delle rispettive righe e le colonne.

Questo accade in molte applicazioni: alcuni esempi rilevanti si trovano nelle applicazioni gestionali [`Spreadsheet (we)`] e nella meccanica quantistica dei sistemi a più particelle [`Coefficienti di Clebsch-Gordan (wi)`].

Va detto anche che le scritture come $\mathsf{Mat}_{A,B,V}$, se alcune delle specificazioni A, B o V sono fornite da espressioni un poco elaborate, possono essere convenientemente sostituite dalle scritture della forma $\mathsf{Mat}[A, B, V]$ da considerare del tutto equivalenti. Similmente vanno considerate del tutto equivalenti le varianti delle scritture precedenti $\mathsf{Mat}_{r,c;V}$ e $\mathsf{Mat}[r, c; s]$.
Per esempio rispetto alla scrittura

$$\mathsf{Mat}_{n+n^2,\left\lfloor \frac{n+h\,k}{2^h} \right\rfloor,2^{31}-1}$$

può essere considerata più leggibile la

$$\mathsf{Mat}\left[n+n^2, \left\lfloor \frac{n+h\,k}{2^h} \right\rfloor, 2^{31}-1\right] .$$

B16 a.05 Una matrice si può raffigurare nel piano in più modi, essenzialmente 8, come accade per i prodotti cartesiani **(**n **]** $\times$ **(**c **]** [B06a06].

Noi ci serviremo prevalentemente di quella che viene chiamata **presentazione matriciale**, avente le righe disposte orizzontalmente e gli indici crescenti da sinistra a destra e avente le colonne in verticale e con indici crescenti dall'alto verso il basso.

Talora però risulta più conveniente (per la sua somiglianza con i grafici delle usuali funzioni di variabile reale) la cosiddetta **presentazione geografica** avente le righe disposte verticalmente e con indici crescenti dal basso verso l'alto e avente le colonne disposte orizzontalmente con gli indici crescenti da sinistra a destra.

Nel seguito ci serviremo quasi esclusivamente della presentazione maticiale delle matrici.
Vediamone alcuni esempi.

$$\begin{bmatrix} 2 & 0 & -5 \\ 11 & 3 & 1 \end{bmatrix} \qquad \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \\ j & k & l \end{bmatrix} \qquad \begin{bmatrix} a & b & c & d \\ b & f & g & h \\ c & g & k & l \\ d & h & l & p \end{bmatrix} ,$$

La prima è una matrice numerica, mentre le successive sono matrici di simboli che potrebbero esprimere entità di qualsiasi genere.

Vediamo anche un esempio di matrice di insiemi di stringhe di lettere minuscole:

$$\begin{bmatrix} \{alfa\} & \{beta, \gamma\} & \{i = 1, 2, 3 :\mid a^i\, b^{2i}\, a^{3i}\} \\ \{x^4, y^3, z^2\} & \emptyset & \{g^4, f^2, t^6\} \end{bmatrix}$$

Concludiamo con la notazione di una matrice generica appartenente a un insieme $\mathsf{Mat}[r, c, V]$ caratterizzato da estensioni r e c e da un insieme delle entrate che nell'ambito di considerazioni generali (astratte) potrebbero essere lasciati del tutto imprecisati:

$$\begin{bmatrix} K_{1,1} & K_{1,2} & \dots & K_{1,c} \\ K_{2,1} & K_{2,2} & \dots & K_{2,c} \\ \vdots & \vdots & \ddots & \vdots \\ K_{r,1} & K_{r,2} & \dots & K_{r,c} \end{bmatrix}$$

Aggiungiamo una considerazione generale sulla presentazione delle matrici. Le definizioni si servono di liste, ovvero di insiemi ordinati per etichettare le righe e le colonne. Spesso però questi ordinamenti non influiscono sui risultati, oppure sono facilmente adattabili alle esigenze del momento.
Questo giustifica che si parli sbrigativamente di insiemi che etichettano le linee di una matrice senza curarsi di loro ordinamenti.

Inoltre spesso le matrici vengono presentate in modo sbrigativo, senza precisare gli insiemi delle loro linee, come si è fatto per gli esempi precedenti.

In questi casi il lettore è autorizzato a intendere che le r righe siano etichettate dai primi r interi positivi e che le c colonne lo siano dagli interi dell'intervallo **(**c **]**.

B16 a.06 Privilegiando la raffigurazione matriciale chiamiamo **matrice riga** ogni matrice di profilo $1 \times c$, e diciamo **matrice colonna** ogni matrice di profilo $r \times 1$.

Una matrice di profilo $r \times c$ si può considerare ottenuta sovrapponendo ordinatamente r matrici riga oppure ottenuta affiancando ordinatamente c matrici colonna.

Una matrice si dice **matrice quadrata** sse il suo dominio è un quadrato cartesiano $A \times A$. L'insieme delle matrici quadrate $\mathbf{Mat}_{A,A,V}$ si denota anche con la scrittura più concisa $\mathbf{Mat}_{A,V}$.
Similmente l'espressioe $\mathbf{Mat}_{r,r,V}$ si può abbreviare con la scrittura $\mathbf{Mat}_{r,V}$.

Si dice **diagonale principale di una matrice** le cui righe e le cui colonne sono etichettate da due intervalli di numeri interi che iniziano con 0 o iniziano con 1 la lista delle sue caselle aventi le due etichette coincidenti. Per esempio per una matrice di $\mathbf{Mat}_{r,c,V}$ la diagonale principale è $\langle a = 1, 2, ..., \min(r, c) :| \langle a, a\rangle\rangle$.
Come vedremo, la diagonale principale gioca un ruolo importante per molte considerazioni sulle matrici quadrate [v. in particolare G47b e G47c].

B16 a.07 Le matrici hanno moltissime applicazioni sia all'interno della matematica che nelle sue applicazioni.

Le matrici più utilizzate sono le numeriche, cioè quelle con entrate costituite da numeri interi, razionali, reali o complessi o costituite da funzioni numeriche. I loro campi applicativi vanno dalla geometria alla statistica, dalla meccanica all'astronomia, dalla fisica atomica e nucleare alla chimica, dalla sociologia all'economia.
Di conseguenza sono stati messi a punto vari sistemi software per la elaborazione automatica delle matrici numeriche.

Hanno importanti applicazioni anche vari tipi di matrici a entrate nonnumeriche; in particolare varie matrici contenenti simboli o insiemi sono utilizzate nelle elaborazioni automatiche finalizzate alla compilazione dei linguaggi di programmazione e alla gestione delle basi di dati.

In effetti va segnalato che per molte problematiche sia cruciale sapere trattare le matrici da vari punti di vista, avvalendosi di diverse tecniche e in particolare utilizzando specifici prodotti software.

B16 a.08 Possiamo riprendere alcune nozioni viste in precedenza per riferirle alle matrici e ai termini che le riguardano.

Una lista di cardinale n può vedersi come matrice di profilo $1 \times n$ o $n \times 1$.

In alcuni contesti risulta utile considerare degli oggetto semplici come matrici del profilo 1×1.

Segnaliamo che questo è l'atteggiamento che assume un linguaggio di programmazione come Matlab, prodotto software il cui nome è l'abbreviazione di *Matrix laboratory* [`MATLAB (we)`] e che assegna alle matrici il ruolo di strumento primario per la esecuzione di una vasta gamma di calcoli.

Come abbiamo visto in a03, una funzione esplicita di dominio D equivale a una matrice di profilo $2 \times D$ o di profilo $D \times 2$.

Si dice **matrice binaria** ogni matrice su $\mathbb{B}$, cioè ogni matrice le cui entrate possono essere solo 0 ed 1.

Se A e B sono due insiemi ordinati ogni matrice binaria di profilo $A \times B$ si può considerare la funzione caratteristica di un sottoinsieme del prodotto cartesiano $A \times B$, ovvero di una relazione binaria tra A e B.
Più precisamente la nozione di matrici binarie di profilo $A \times B$ e la nozione di relazioni binarie tra A e B sono nozioni equivalenti, criptomorfe, e in molti sviluppi possono essere identificate (sew si preferisce possono essere confuse) senza incorrere in ambiguità.

La presentazione cartesiana bidimensionale di una funzione del genere $\lceil D \longmapsto C \rceil$ con D e C intervalli finiti di numeri interi si può considerare una matrice binaria che in genere conviene trattare attraverso la sua presentazione geografica; si tratta di una matrice binaria di tipo particolare, in quanto in ogni sua linea posta in verticale (in ogni sua riga) si trova uno ed un solo valore 1.

Le endofunzioni entro un insieme (finito) C sono presentabili come matrici binarie quadrate con righe e colonna etichettate dallo stesso C; chiaramente si tratta di casi particolari delle matrici precedenti.

Le funzioni caratteristiche dei sottoinsiemi di un insieme ambiente U possono essere viste come matrici binarie aventi come dominio $U \times \{0, 1\}$.

(1) Eserc. Caratterizzare le matrici binarie delle funzioni costanti, dei collassi, delle endofunzioni collassanti e delle endofunzioni idempotenti [B13c11].

B16 a.09 Nella pratica, come si è detto, le entrate di una matrice $M \in \mathbf{Mat}_{A,B,V}$ spesso si denotano con $M_{i,j}$, per $i \in A$ e $j \in B$.

Molte applicazioni richiedono di trattare matrici di dominio esteso, con migliaia o milioni di righe e di colonne e per elaborarle in modo efficiente si devono adottare procedimenti studiati specificamente.

In particolare vengono utilizzate matrici binarie con profili quali 1024×758 o 4096×3072 per trattare le immagini in bianco e nero presentate su uno schermo o stampate, mentre per trattare immagici colorate relativamente semplici, con i colori gestiti in tricromia, si usano matrici con profili come i precedenti e con valori nell'insieme $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Si incontrano inoltre matrici, talora di dominio esteso, le cui entrate si possono individuare attraverso una espressione algebrica o di genere analogo.
Se gli elementi di una matrice $M \in \mathbf{Mat}_{A,B,V}$ sono individuati da una espressioni che denotiamo con $\mathcal{E}_{i,j}$, la matrice si può esprimere con la scrittura $[\mathcal{E}_{i,j} \mid: i \in A, j \in B]$.
Inoltre presentano interesse anche matrici le cui entrate sono espressioni: in particolare si incontrano matrici di formule geometriche nella geometria analitica e matrici di formule fisiche in discipline come la meccanica dei corpi elastici, la fluidodinamica, l'elettromagnetismo, la relatività e la meccanica quantistica.

In vari contesti i campi di variabilità degli indici di riga i e di colonna j di una matrice si possono lasciare sottintesi e risulta possibile individuare la matrice stessa con una scrittura semplificata della forma $[\mathcal{E}_{i,j}]$.

B16 a.10 Si dice **trasposta di una matrice** $[M_{i,j} \mid: i \in A, j \in B]$ la matrice di profilo $B \times A$ fornita dall'espressione $[M_{j,i} \mid: i \in A, j \in B]$.

Essa sinteticamente si denota con M^{T} o con $\boldsymbol{Trsp}(M)$; in queste scritture si utilizzano i simboli ^{T} a esponente e $\boldsymbol{Trsp}$ a prefisso per denotare la **trasposizione delle matrici**, trasformazione che a ogni matrice di un qualche profilo $A \times B$ associa una matrice di profilo $B \times A$.

La matrice trasposta viene raffigurata da un quadro di valori ottenuta dal quadro che raffigura la matrice di partenza scambiando il ruolo delle righe con quello delle colonne; questa trasformazione si

può descrivere anche come riflessione dalla matrice (non necessariamente quadrata) rispetto alla sua diagonale principale.

La trasposizione trasforma matrici quadrate in matrici quadrate; questo si esprime anche dicendo che le matrici quadrate entro l'insieme delle matrici costituiscono un **sottoinsieme stabile** rispetto alla trasposizione.

Va notato che il termine "insieme delle matrici" va considerato un insieme-B, in quanto ogni stringa di caratteri che possono essere utilizzati per definire delle matrici può essere sottoposta ad un algoritmo realizzabile per decidere se esprime correttamente una matrice o meno.

Chiaramente per ogni matrice finita M la matrice trasposta della $M^\top$ è evidentemente la M stessa, ovvero: $(M^\top)^\top = M$.

Possiamo quindi affermare che la trasposizione è una endofunzione involutoria entro ciascuno degli insiemi di matrici quadrate $\mathsf{Mat}_{r,V}$ cossispondenti ai diversi $r \in \mathbb{P}$ ed entro ciascuno degli insiemi di matrici quadrate $\mathsf{Mat}_{D,V}$ per ogni insieme finito ordinato D.

B16 a.11 Si dice **matrice simmetrica** ogni matrice quadrata che non viene modificata dalla trasposizione. La matrice individuata da $M = [M_{i,j} \mid: i,j \in A]$ è simmetrica sse $\forall i,j \in A \ : \ M_{i,j} = M_{j,i}$.

Le matrici simmetriche sono dunque i punti fissi per la trasposizione delle matrici. Questo si esprime anche dicendo che le matrici simmetriche di un certo insieme $\mathsf{Mat}_{A,V}$ sono "elementi invarianti rispetto alla trasformazione costituita dalla trasposizione", o in breve, che sono degli **invarianti per trasposizione**.

Per individuare una matrice simmetrica di $\mathsf{Mat}_{r,V}$ è sufficiente fornire le componenti $M_{i,j}$ per $i = 1, ..., r$ e per $j = 1, ..., i$ (oppure per $j = 1, ..., r$ ed $i = 1, ..., j$).
Quindi le matrici simmetriche dell'insieme $\mathsf{Mat}_{2,V}$, dell'insieme $\mathsf{Mat}_{3,V}$ e dell'insieme $\mathsf{Mat}_{4,V}$ per ogni insieme finito V di valori devono avere, risp., le seguenti forme

$$\begin{bmatrix} a & b \\ b & d \end{bmatrix} \qquad \begin{bmatrix} a & b & c \\ b & e & f \\ c & f & i \end{bmatrix} \qquad \begin{bmatrix} a & b & c & d \\ b & f & g & h \\ c & g & k & l \\ d & h & l & p \end{bmatrix} \quad ,$$

dove le lettere denotano elementi che si possono scegliere arbitrariamente in V.

B16 a.12 Rivestono particolare importanza le matrici quadrate aventi le entrate nell'insieme che etichetta le sue righe e le sue colonne, cioè le funzioni del tipo $\lceil A \times A \longmapsto A \rceil$.

Queste matrici individuano le importanti entità chiamate **operazioni binarie finite**, funzioni del genere $\lceil F \times F \longmapsto V \rceil$ per F insieme finito e ordinato.

Esse costituiscono casi particolari delle **operazioni binarie**, le funzioni del genere $\lceil S \times S \longmapsto S \rceil$ con S insieme qualsiasi. Queste entità, come vedremo in particolare nel capitolo B41, svolgono un ruolo fondamentale per l'intera algebra.

Più particolari sono quelle che diciamo **operazioni binarie-Z**, funzioni del genere $\lceil \mathbb{Z} \times \mathbb{Z} \longmapsto \mathbb{Z} \rceil$.

Osserviamo che abbiamo già incontrato molti esempi di operazioni binarie: le operazioni su $\{0,1\}$ riguardanti gli operatori logici $\wedge$, $\vee$ e $+_2$; le operazioni di somma, differenza e prodotto tra numeri interi; l'operazione di composizione tra relazioni e altre.

Tra queste solo le operazioni logiche si possono esprimere mediante matrici finite, le operazioni aritmetiche sui numeri interi sono operazioni binarie-Z, mentre le composizioni tra relazioni si possono collocare solo tra le operazioni binarie, entità generali e talora generiche.

Osserviamo che le matrici delle operazioni logiche binarie e delle operazioni di somma e prodotto tra numeri interi sono simmetriche e questo, come già osservato, corrisponde alla proprietà di commutatività delle operazioni stesse.

Le matrici binarie $r \times r$ sono rappresentate fedelmente dalle sequenze binarie di lunghezza r^2. Questo dice che il loro numero ammonta a 2^{r^2} e che una loro lista completa si può ottenere con l'algoritmo per la generazione delle disposizioni con ripetizione su $\{0, 1\}$ di lunghezza r^2 [B06g03, a02] .
In particolare le matrici binarie di profilo 2×2 sono 16 e vedremo che rivestono un ruolo centrale nella logica elementare.

B16 b. relazioni finite e digrafi

B16 b.01 Consideriamo un insieme finito A ed M una matrice binaria (quadrata) di profilo $A \times A$. Come ogni funzione a valori in $\{0,1\}$ essa costituisce una funzione indicatrice di un sottoinsieme del suo dominio $A \times A$, cioè dell'insieme delle coppie $\langle a,b\rangle \in A \times A$ per le quali $M_{a,b} = 1$, ovvero dell'insieme $M^{-\mathbf{1}}(1)$; essa dunque si può scrivere

$$M \;=\; \mathcal{I}_{A\times A}[M^{-\mathbf{1}}(1)] \;.$$

Una coppia $\boldsymbol{D} = \langle A, R\rangle$ con $R \subseteq A \times A$ si dice **relazione entro l'insieme** A; se A è un insieme finito la coppia $\boldsymbol{D}$ viene chiamata anche **digrafo sui nodi di** A.

Gli elementi di A si dicono **nodi del digrafo** $\boldsymbol{D}$ e le coppie di nodi che appartengono a R si dicono **archi del digrafo** $\boldsymbol{D}$.
In particolare ogni coppia della forma $\langle a,a\rangle \in R$ con $a \in A$ si dice **cappio del nodo** a.

L'insieme dei nodi di un digrafo viene anche chiamato **terreno del digrafo**.

Ad ogni digrafo $\boldsymbol{D}$ (e quindi a ogni relazione binaria) si associa una matrice binaria di profilo $A \times A$ definita con l'assegnazione

$$M_{a,b} \;:=\; \begin{cases} 1 & \text{sse } \langle a,b\rangle \in R \\ 0 & \text{sse altrimenti} \end{cases} \;.$$

Questa si dice **matrice delle adiacenze del digrafo** $\boldsymbol{D}$ e la si denota con $\boldsymbol{D}^{\mathsf{adjm}}$.
Per essa si ha l'espressione

$$\langle A, R\rangle^{\mathsf{adjm}} \;:=\; \lceil\!\lceil\, \langle a,b\rangle \in R \;\mapsto\; 1 \,\rceil\!\rceil \;\dot\cup\; \lceil\!\lceil\, \langle a,b\rangle \in A\times A \setminus R \;\mapsto\; 0 \,\rceil\!\rceil \;. \tag{1}$$

Viceversa si dice **digrafo associato alla matrice binaria quadrata** di profilo $A \times A$ M la coppia $M^{\mathsf{dgrf}} := \big\langle A, M^{-\mathbf{1}}(1)\big\rangle$.

Abbiamo quindi le due trasformazione mutuamente inverse

$$\mathsf{adjm} \;:=\; \Big\lceil\, G = \langle A, R\rangle \in \mathbf{Dgrf} \;\mapsto\; \lceil\!\lceil\, \langle a,b\rangle \in A\times A \;\mapsto\; \delta(\langle a,b\rangle \in R) \in \big\{\mathbf{Dgrf} \lhd\!\!\longrightarrow\!\!\rhd \mathbf{Mat}_{\{0,1\}}\big\} \;.$$

$$\mathsf{dgrf} \;:=\; \Big\lceil\, M \in \mathbf{Mat}_{A,\{0,1\}} \;\mapsto\; \big\langle A, \{\langle a,b\rangle \in A\times A \;ST\; M(a,b) = 1\}\big\rangle \,\Big\rceil \;\in \big\{\mathbf{Mat}_{\{0,1\}} \lhd\!\!\longrightarrow\!\!\rhd \mathbf{Dgrf}\big\} \;.$$

B16 b.02 Ricordiamo che per ogni intero positivo n le matrici binarie di profilo $(\mathrm{n}\,]\times(\mathrm{n}\,]$ costituiscono l'insieme finito $\mathbf{Mat}_{n;\{0,1\}}$ il cui cardinale è 2^{n^2}, in quanto queste matrici sono in biiezione con le disposizioni di $\{0,1\}$ di lunghezza n^2. Possiamo quindi dire che costituiscono un insieme finito anche i digrafi aventi come terreno $(\mathrm{n}\,]$; tale insieme lo denotiamo con $\mathbf{Dgrf}_n$.

Si verifica facilmente che le due trasformazioni ^{dgrf} che associa alle matrici binarie quadrate dei digrafi e ^{adjm} che associa ai digrafi su terreno finito delle matrici binarie quadrate costituiscono un duetto di biiezioni mutuamente inverse.

Quindi le matrici quadrate binarie di profilo $A \times A$ e i digrafi aventi A come insieme dei nodi, ovvero le relazioni binarie entro A, sono strutture logicamente intercambiabili, fatto che si esprime anche dicendo che esse sono **strutture criptomorfe**, ovvero che si trova un criptomorfismo tra i digrafi su terreno finito e le matrici binarie quadrate.

Può essere utile fare riferimento alle due funzioni che fanno corrispondere a un digrafo $\boldsymbol{D} = \langle A, R\rangle$, risp., il suo terreno e l'insieme dei suoi archi:

$$\mathbf{SetY}(\boldsymbol{D}) = \mathbf{SetY}\langle A, R\rangle \;:=\; A \qquad , \qquad \mathbf{Arc}(\boldsymbol{D}) = \mathbf{Arc}\langle A, R\rangle \;:=\; R \;. \tag{1}$$

Vedremo che queste funzioni possono essere estese ai molti insiemi di strutture che si possono ottenere generalizzando e/o arricchendo i digrafi su terreno finito.

B16 b.03 I digrafi si possono presentare attraverso raffigurazioni che, quando i loro nodi sono in numero contenuto, possono essere molto efficaci.
In una raffigurazione ogni nodo del digrafo è rappresentato da un punto o da una piccola figura (pallino, quadratino, ...) ed ogni arco $\langle a, b\rangle$ è rappresentato da una freccia che va dal nodo a al nodo b.
Le posizioni dei nodi e degli archi di una raffigurazione in linea di principio possono essere scelti con arbitrarietà; quindi uno stesso digrafo può avere raffigurazioni a prima vista molto diverse.
Nella pratica quindi, se i nodi non sono pochi, è opportuno che le posizioni dei segni che li rappresentano vengano scelti in modo da rendere leggibili facilmente le caratteristiche del digrafo.

Conviene segnalare fin d'ora che in molti settori applicativi specifici servono i cosiddetti arricchimenti dei digrafi, strutture che oltre a un terreno e a un sistema di archi presentano altre informazioni che possono riguardare valutazioni numeriche e differenziazioni qualitative per i nodi e per gli archi.
La gamma dei digrafi arricchiti che presentano interesse nella matematica o nelle sue applicazioni, come vedremo [D28], è estremamente vasta e variegata.
Non stupisce quindi che per soddisfare la precedente esigenza di raffigurabilità significativa vengono sviluppati programmi piuttosto elaborati che in genere risultano efficaci solo per raffigurare insiemi specifici di digrafi arricchiti.

B16 b.04 Vediamo alcuni primi esempi di digrafi presentando le loro matrici delle adiacenze e loro raffigurazioni.

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Nelle raffigurazioni si notano in particolare gli archi che collegano un nodo con se stesso, cioè i cappi, e si osserva che queste coppie di nodi coincidenti corrispondono biunivocamente alle entrate uguali ad 1 sulla diagonale principale della matrice.
Si nota anche che gli archi uscenti dal nodo i corrispondono biunivocamente alle entrate 1 nella riga i della matrice, mentre gli archi entranti nel nodo j corrispondono biunivocamente agli 1 che si trovano nella colonna j.

Relativamente a un nodo a di un digrafo ogni arco $\langle a, b\rangle$ si dice **arco uscente dal nodo** a e ogni arco $\langle c, a\rangle$ si chiama **arco entrante nel nodo** a.

Il numero degli archi uscenti da a si dice **grado uscente dal nodo** a a e si denota con $degout\boldsymbol{D}(a)$, mentre il numero degli archi entranti in a si dice **grado entrante nel nodo** a e si denota con $degin_{\boldsymbol{D}}(a)$.
Sulla matrice delle adiacenze del digrafo si osserva che il grado uscente da un nodo si ottiene sommando le entrate della sua riga e che il suo grado entrante si ottiene sommando le entrate della sua colonna.

B16 b.05 Il criptomorfismo tra matrici quadrate binarie e relazioni finite e la possibilità di raffigurare queste ultime graficamente sono elementi vantaggiosi per lo studio dei digrafi e delle loro applicazioni: quando si devono affrontare problemi riguardanti questi oggetti sono disponibili punti di vista e linguaggi diversi ma riconducibili gli uni agli altri senza difficoltà.

Quindi le analisi e le costruzioni che si devono sviluppare per risolvere problemi riconducibili alle strutture delle suddette specie, per ciascuna delle fasi dello sviluppo, si possono scegliere i linguaggi e i punti di vista che appaiono più comodi e pratici.

In linea di massima le matrici binarie sono oggetti vantaggiosi quando si opera con il computer.

Le raffigurazioni dei digrafi e dei loro arricchimenti sono da preferire nelle discussioni interpersonali e nelle presentazioni delle proprietà che si possono descrivere significativamente attraverso esempi circoscritti; inoltre le raffigurazioni possono suggerire soluzioni descrivibili in termini visivi.

A sua volta il linguaggio delle relazioni si adatta meglio ad argomentazioni di tono più formale e a esposizioni nelle quali intervengono altre strutture matematiche come in alcune considerazioni insiemistiche e in alcune questioni di programmazione.

B16 b.06 In molte applicazioni servono **relazioni binarie** tra due insiemi finiti A_1 e A_2 che sono evidentemente disgiunti.
Per esempio, come vedremo in particolare in G37, sono relazioni tra insiemi disgiunti le relazioni di incidenza che riguardano le facce e gli spigoli dei poliedri, oppure i loro vertici e i loro spigoli, oppure i loro vertici e le loro facce.

Un digrafo $\langle A, U\rangle$ si dice **digrafo bipartito** sse per A si trova una si trova una bipartizione $A = A_1 \dot\cup A_2$ tale che i nodi di A_1 non presentano archi entranti e i nodi di A_2 non hanno archi uscenti.
Di conseguenza si trova $U \subseteq A_1 \times A_2$.
In particolare si possono esprimere mediante grafi bipartiti le sopra accennate relazioni di incidenza riguardanti elementi di poliedri.

Dei digrafi bipartiti in genere è utile la raffigurazione sagittale.

Una situazione semplice ed evidente che si può modellare con un digrafo bipartito riguarda lo schema dei collegamenti marittimi tra le due sponde del Mare Adriatico: sulla sponda italiana si trovano i porti di Ancona, Bari, Brindisi e Otranto, sulla opposta i porti di Split, Dubrovnik, Igoumenitza e Patras.

B16 b.07 Sono studiati molti tipi di digrafi che rivestono grande interesse.

Nell'ambito più strettamente matematico sono studiati digrafi specifici dotati di elevate proprietà di simmetria che rivestono importanza per studi di vari tipi di strutture matematiche (gruppi [D35c], `algebre di Lie (wi)`, poliedri [G37], `strutture di incidenza (wi)` [D47a, D64a], ...).

In molti settori applicativi sono ampiamente utilizzati svariati tipi di digrafi arricchiti al fine di definire modelli discreti di sistemi complessi di interesse tecnologico, amministrativo, organizzativo (diagrammi di flusso dei programmi, schemi funzionali di dispositivi di ogni genere, organigrammi, sistemi di trasporti, impianti industriali, ...) [v.a. D28].

Gli studi sui digrafi e sui loro arricchimenti conducono a teoremi sopra le loro proprietà, a loro classificazioni e ad algoritmi; questi concernono: l'analisi di digrafi specifici, la visita di loro nodi, la generazione di interi insiemi di strutture, la costruzione di digrafi con requisiti particolari e molto altro.

Molte applicazioni portano a esaminare digrafi con molti milioni di nodi, misura che rende inevitabile di trattarli con strumenti informatici.
In linea di massima le matrici delle adiacenze e alcune loro varianti sono un modo di presentare i digrafi particolarmente adatto ai calcoli automatici; all'opposto le raffigurazioni dei digrafi servono meglio per gli studi da parte degli umani e per le relative discussioni.

B16 b.08 Procediamo ora a introdurre alcune delle principali proprietà che consentono di distinguere tra i diversi tipi di digrafi e di relazioni binarie finite. Per queste considerazioni facciamo riferimento a un insieme finito $A = \{a_1, a_2, ..., a_n\}$ e a un digrafo $\boldsymbol{D} = \langle A, U\rangle$ che consideriamo criptomorfo con una relazione finita. Inoltre scriviamo $\boldsymbol{R}^\neg$ per l'opposta o negazione della relazione $\boldsymbol{R}$ ed per la corrispondente matrice delle adiacenze.

La relazione $\boldsymbol{R}$ si dice **relazione riflessiva** entro A sse $\forall a \in A : \langle a, a\rangle \in U$, ovvero sse $a\boldsymbol{R}a$.
Equivalentemente si ha che la matrice delle adiacenze ha tutte le entrate della diagonale principale uguali ad 1, ovvero che ogni nodo di $\boldsymbol{D}$ presenta un cappio.

La relazione $\boldsymbol{R}$ si dice **relazione antiriflessiva** entro A sse $\forall a \in A : \langle a, a\rangle \notin U$, ovvero sse $a(A \times A \setminus R)a$.
Equivalentemente si ha che la matrice delle adiacenze ha tutte le entrate della diagonale principale uguali a 0, ovvero che nessun nodo di $\boldsymbol{D}$ presenta un cappio.

La relazione $\boldsymbol{R}$ si dice **relazione simmetrica** sse $\forall\langle a, b\rangle \in U \setminus \mathsf{Id}_A : \langle b, a\rangle \in U$, cioè sse l'appartenenza di un arco al digrafo implica che di esso faccia parte anche l'arco opposto.
Equivalentemente si ha che la matrice delle adiacenze è simmetrica; questo accade sse per ogni coppia $\langle i, j\rangle \in A \times A$ quando la matrice delle adiacenze presenta l'entrata $M_{i,j} = 1$, allora accade che $M_{j,i} = 1$.
I digrafi delle relazioni simmetriche si dicono **digrafi simmetrici**

Si osserva che dato un digrafo simmetrico sono simmetrici anche i digrafi ottenibili da questo aggiungendo loro o togliendo loro dei cappi.

B16 b.09 Diciamo **grafo nonorientato** o in breve **grafo.no** una struttura finita della forma $\boldsymbol{G} = \langle Q, E\rangle$, dove Q è un insieme finito detto **insieme dei vertici del grafo.no** o **terreno del grafo-no** $\boldsymbol{G}$ ed E è un insieme costituito da duetti e singoletti di vertici. chiamato **insieme degli spigoli del grafo.no** o **insieme dei lati del grafo.no** di $\boldsymbol{G}$.
I singoletti che si possono trovare in E sono detti **cappi del grafo.no**.

Si individua facilmente una biiezione tra i grafi nonorientati su un dato terreno Q con i digrafi simmetrici aventi lo stesso terreno. Ad ogni spigolo del grafo nonorientato che non sia cappio $\{a, b\}$ corrisponde il duetto di archi opposti $\{\langle a, b\rangle, \langle b, a\rangle\}$ del digrafo e ai cappi del grafo nonorienatato corrispondono i cappi del digrafo.

Chiaramente quindi ogni relazione simmetrica si può raffigurare con il grafo nonorientato in corrispondenza biunivoca con il proprio digrafo simmetrico; questa raffigurazione risulta più concisa e pertinente di quella fornita dal digrafo.

B16 b.10 La relazione $\boldsymbol{D} = \langle Q, U\rangle$ si dice **antisimmetrica** sse $\forall\langle a, b\rangle \in U : \langle b, a\rangle \notin U$, cioè sse il digrafo non presenta alcun duetto di archi opposti.

Equivalentemente si ha che la matrice delle adiacenze $M := \boldsymbol{D}^{adjm}$ se presenta una entrata $M_{i,j} = 1$, allora deve essere $M_{j,i} = 0$, ovvero che $\forall\langle i, j\rangle \in Q \times Q : M_{i,j} + M_{j,i} \leq 1$.

Tipiche relazioni antisimmetriche sono le relazioni tra stringhe "prefisso di", "suffisso di", "infisso di", "sottosequenza di", le relazioni tra interi "minore di" e "minore o uguale a" e le relazioni tra insiemi (finiti) "sottoinsieme di".

Si osserva che una relazione è antisimmetrica sse lo è anche la sua riflessa. sono quindi antisimmetriche la relazione tra interi "maggiore di", la relazione tra stringhe "sovrastringa di", 'sovrasequenza di" e la relazione tra insiemi "sovrainsieme di"

Tra le relazioni antisimmetriche spesso interessa distinguere le riflessive, le antiriflessive e quelle che presentano una parte dei nodi dotati di cappio e i rimanenti privi di cappio.

Si osserva anche che data una relazione antisimmetrica sono antisimmetriche anche tutte le relazioni che si ottengono da questa aggiungendole o togliendole dei cappi. Anche la proprietà di simmetria rimane invariata in seguito alla aggiunta o alla eliminazione di cappi.

La relazione $\boldsymbol{D} = \langle A, U\rangle$ si dice **relazione transitiva** sse $\forall a, b, c \in A \ : \ \langle a, b\rangle \in U \wedge \langle b, c\rangle \in U \implies \langle a, c\rangle \in U$, cioè sse nel digrafo la presenza dell'arco da a a b e quella dell'arco da b a c implicano che sia presente anche l'arco da a a c.

Questa proprietà in genere non è immediatamente evidente nella matrice delle adiacenze; per molte relazioni solo una attenta analisi della raffigurazione riesce a stabilire se si tratta di relazioni transitive o nontransitive.
Anche la proprietà di transitività non viene modificata dall'aggiunta e dall'eliminazione di cappi.

B16 b.11 Una relazione $\boldsymbol{E} = \langle A, E\rangle$ si dice **equivalenza** sse è riflessiva, simmetrica e transitiva.

Ad ogni elemento a del terreno A di una tale relazione $\boldsymbol{E}$ risulta associato l'insieme degli elementi di A equivalenti ad a; tale sottoinsieme lo denotiamo con $a_{/E}$ o con la sua espressione approssimata $a\,E$. Un tale insieme viene detto **classe di equivalenza** di a.

Chiaramente di tale sottoinsieme fa parte a e se $b\,E\,a$, grazie alla riflessività a fa parte anche di $b\,E$; quindi $a\,E = b\,E$.
Se viceversa un $c \in A$ non è equivalente ad a deve essere $a \notin c\,E$.

Dunque una equivalenza E entro l'insieme A porta a individuare i sottoinsiemi di A della forma $a\,E$ chiamati classi dell'equivalenza; essi risultano mutuamente disgiunti.
Inoltre evidentemente ogni elemento di A fa parte di una classe di equivalenza, la $a\,E$; quindi l'unione (disgiunta) delle classi dell'equivalenza E coincide con A, o, come si dice, lo copre, costituisce una copertura di A.

Una collezione di sottoinsiemi di un insieme A con le due suddette proprietà della mutua disgiunzione e della copertura di A si dice che individua una **partizione** di A.

La matrice delle adiacenze di una relazione di equivalenza E è caratterizzata dal fatto di essere fattorizzata a blocchi, cioè di essere tale che tutte le caselle $\langle a, b\rangle$ con a e b appartenenti alla stessa classe di equivalenza presentano l'entrata uguale ad 1, mentre le caselle rimanenti $\langle a, c\rangle$ con a e c non equivalenti presentano l'entrata 0.

Se si riordinano gli elementi del terreno della relazione in modo che gli elementi di ogni classe siano consecutivi, la caratteristica della fattorizzazione a blocchi della è subito evidente. Due matrici fattorizzate a blocchi, la prima evidentemente, la seconda meno, sono le seguenti.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

B16 c. digrafi ordinati, digrafi graduati, arborescenze

B16 c.01 Una relazione $\boldsymbol{R} = \langle A, U \rangle$ si dice **relazione d'ordine**, **ordine parziale** o **poset** sse è riflessiva, antisimmetrica e transitiva.

Abbiamo già incontrato alcune relazione d'ordine semplici e importanti.
Per qualsiasi intero positivo u è piuttosto semplice la relazione $\leq$ tra gli interi costituenti l'intervallo della forma $\mathbf{(}u\mathbf{]}$ (o della forma $\mathbf{[}u\mathbf{)}$, o simili).
Dati due interi positivi m ed n sappiamo decidere se m è divisore di n o meno.
Dati due insiemi finiti espliciti S e T un semplice algoritmo consente di decidere se S è sottoinsieme di T o meno.
Per un qualsiasi intero positivo u sappiamo elencare tutte le coppie di interi positivi m ed n minori o uguali ad u tali che m divida n; quindi l'insieme di queste coppie costituisce un poset finito.
Per un qualsiasi insieme esplicito U sappiamo elencare tutte le coppie di suoi sottoinsiemi S e T tali che sia $S \subseteq T$; quindi anche l'insieme di queste coppie costituisce un poset finito.

Se S denota un insieme-B non necessariamente finito, ogni insieme finito R di coppie di $S \times S$ costituisce l'insieme degli archi di una relazione finita.
Denotiamo con $\mathsf{RelOrdF}_S$ o con PosetF_S l'insieme delle relazioni d'ordine finite sull'insieme A; è abbastanza evidente che questo insieme di relazioni è un insieme-B.
Più particolarmente denotiamo con RelOrd_S o con il simbolo equivalente Poset_S l'insieme delle relazioni d'ordine aventi come terreno l'insieme S.
Questo insieme è un sovrainsieme di $\mathsf{RelOrdF}_S$, ma possiamo affermare solo che si tratta di un insieme-P.

La definizione di relazione d'ordine implica che anche la relazione riflessa di una relazione d'ordine sia una relazione d'ordine. In effetti molti studi sopra una relazione d'ordine si conducono facendo sistematicamente riferimento anche alla sua riflessa.
Questo per esempio è accaduto per le relazioni prefisso e simili nell'ambito delle stringhe, per le relazioni $\leq$ e $\geq$ tra numeri interi e tra le relazioni $\subseteq$ e $\supseteq$ tra insiemi.

B16 c.02 Tra le relazioni d'ordine parziale si distinguono le **relazioni d'ordine totale**, quelle tali che per ogni coppia di elementi dell'insieme terreno accade aut che il primo precede il secondo, aut che i due coincidono, aut che il secondo precede il primo.

Le relazioni "minore o uguale a" e maggiore o uguale a" tra interi positivi sono relazioni di ordine totale. La relazione di divisibilità tra interi e la relazione di inclusione tra insiemi non lo sono; infatti, per esempio, tra 6 e 10 non accade che 6 divida 10, né che 10 divida 6; inoltre tra i due insiemi $A := \{1, 2, 5\}$ e $B := \{2, 3, 4, 5, 6\}$ non vale alcuna delle relazioni $A \subset B$, $B \subset A$ e $A = B$.

Evidentemente la relazione riflessa di una relazione d'ordine totale è anch'essa una relazione d'ordine totale, mentre la riflessa di una relazione d'ordine nontotale deve essere una relazione d'ordine nontotale.

Denotiamo con $\mathsf{RelOrdT}_S$ o con PosetT_S l'insieme delle relazioni d'ordine totale aventi come terreno l'insieme S.
Per un S infinito possiamo dire solo che PosetT_S è un insieme-P, mentre l'intero insieme **PosetF** dei posets finiti va considerato un insieme-B.

B16 c.03 Consideriamo un insieme S non necessariamente finito, una relazione d'ordine $\boldsymbol{R} = \langle S, \preceq \rangle$ e la sua relazione riflessa $\boldsymbol{R}^\top = \langle S, \succeq \rangle$.

Per ogni elemento a del terreno S si possono individuare

l'insieme dei **minoranti** $\mathsf{Mnrnt}_{\preceq}(a) := \{x \in A \;\big[\!\big]\; x \preceq a\}$

e l'insieme dei **maggioranti** $\mathsf{Mjrnt}_{\preceq}(a) := \{x \in A \;\big[\!\big]\; a \preceq x\}$.

L'insieme dei minoranti e l'insieme dei maggioranti si possono attribuire anche ai sottoinsiemi del terreno di un poset.

Ad ogni sottoinsieme B di S si associano:

l'insieme dei minoranti $\mathsf{Mnrnt}_{\preceq}(B) := \{x \in S \;\big[\!\big]\; \forall b \in B : x \preceq b\}$

e l'insieme dei maggioranti $\mathsf{Mjrnt}_{\preceq}(B) := \{x \in S \;\big[\!\big]\; \forall b \in B : b \preceq x\}$.

Chiaramente per ogni $x \in S$ si ha $\mathsf{Mnrnt}_{\preceq}(x) = \mathsf{Mnrnt}_{\preceq}(\{x\})$, $\mathsf{Mjrnt}_{\preceq}(x) = \mathsf{Mjrnt}_{\preceq}(\{x\})$.

Si trovano inoltre le seguenti uguaglianze insiemistiche.

$$\mathsf{Mnrnt}_{\preceq}(X) = \bigcap_{x\in X} \mathsf{Mnrnt}_{\preceq}(x) \qquad \text{e} \qquad \mathsf{Mjrnt}_{\preceq}(X) = \bigcap_{x\in X} \mathsf{Mjrnt}_{\preceq}(x) \ .$$

In modo prevedibile si definiscono gli insiemi dei minoranti propri e gli insiemi dei maggioranti propri di singoli elementi e di sottoinsiemi del terreno di una relazione d'ordine.

Dati due elementi a e b di un ordine parziale finito $\langle A, \preceq\rangle$, se esiste un elemento inferiore a tutti i loro maggioranti viene detto **supremo** di a e b e si denota con $\sup_{\preceq}(a, b)$; se esiste un elemento superiore a tutti i loro minoranti viene dett **infimo** di a e b e si denota con $\inf_{\preceq}(a, b)$.

Nei discorsi nei quali si tratta una sola relazione d'ordine in genere le notazioni vengono semplificate trascurando i deponenti che la segnalano esplicitamente.

Due esempi di infimo e supremo:

in un poset della divisibilità tra interi positivi $\sup(6, 10) = 30$, mentre $\inf(6, 10) = 2$;

in un poset di sottoinsiemi di numeri di un intervallo di numeri positivi abbiamo
$\sup(\{1, 2, 5\}, \{2, 3, 4, 5, 6\}) = \{1, 2, 3, 4, 5, 6\}$, mentre $\inf(\{1, 2, 5\}, \{2, 3, 4, 5, 6\}) = \{2, 5\}$.

Più in generale si individua un algoritmo che per ogni relazione d'ordine esplicita e per ogni sottoinsieme del suo terreno ricerca e possibilmente individua il suo infimo e il suo supremo.

B16 c.04 Spesso risulta opportuno esaminare insieme una relazione d'ordine $\preceq$ e la corrispondente relazione d'ordine stretto $\preceq \setminus \mathsf{Id}_S$, relazione evidentemente antiriflesiva.
Per queste varianti si usano notazioni quali
$< := \leq \setminus \mathsf{Id}_{\mathbb{Z}}$, $> := \geq \setminus \mathsf{Id}_{\mathbb{Z}}$, $\subset := \subseteq \setminus \mathsf{Id}_S$, $\supset := \supseteq \setminus \mathsf{Id}_S$, $\prec := \preceq \setminus \mathsf{Id}_S$ e $\succ := \succeq \setminus \mathsf{Id}_S$.

Facciamo riferimento a un poset $\langle S, \preceq\rangle$.
Si dice **maggiorante immediato** di a ogni b tale che $a \preceq b$, $b \neq a$ e $\forall x \in S \;\big[\!\big]\; a \preceq x \preceq b \;:\; a = x \vee x = b$.
In tale caso si scrive $a \prec_{\mathbf{I}} b$ e si dice che a precede immediatamente b.
Si dice **minorante immediato** di a ogni c tale che $c \preceq a$, $c \neq a$ e $\forall x \in S \;\big[\!\big]\; c \preceq x \preceq a : c = x \vee x = a$. In tale caso si scrive $a \succ_{\mathbf{I}} b$ e si dice che a segue immediatamente b.

Va detto che vi sono posets e loro elementi che non posseggono nessun minorante immediato e/o nessun maggiorante immediato.
Nei poset finiti sono in genere molti gli elementi dotati di maggioranti immediati e/o di minoranti immediati.
Chiaramente in ogni poset $a \prec_{\mathbf{I}} b \iff b \succ_{\mathbf{I}} a$.

È anche evidente che $\prec_{\mathbf{I}}{}^{\top} = \succ_{\mathbf{I}}$.

B16 c.05 Una relazione d'ordine si dice **relazione d'ordine graduata** o **poset graduato** sse il suo terreno si può ripartire:

in un numero finito di parti L_0, L_1, ...,L_h

o in una collezione di parti in biiezione con ai numeri naturali della forma L_0, L_1, ...,L_h, ...

o in una collezione di parti in biiezione con i numeri interi della forma L_0, L_1, ...,L_h, ... tali che ogni elemento a appartenente a un L_i (livello i) se possiede maggioranti immediati questi si trovano tutti in L_{i+1}, mentre se possiede minoranti immediati questi si trovano tutti in L_{i-1}.

Evidentemente per ogni L_i $L_{i+1} = \bigcup_{x \in L_i} \mathsf{Mjrnt}_{\prec\mathbf{I}}(x)$ e dualmente $L_i = \bigcup_{x \in L_{i+1}} \mathsf{Mnrnt}_{\prec\mathbf{I}}(x)$.
Possiamo anche esprimere questi fatti applicando la relazione $\prec_{\mathbf{I}}$ ai sottoinsiemi L_i e affermando che se $x_i \in L_i$ e $x_j \in \text{Ł}_j$, allora $x_i \prec y_i \implies i < j$.
Con questa estensione della relazione $\preceq$ ai livelli del poset gli stessi livelli costituiscono una collezione di entità (sottoinsiemi del terreno A) totalmente ordinata.

Nel caso di sequenza finita di livelli $\langle L_0, L_1, ...L_h \rangle$ l'intero h si dice **altezza del poset graduato**. e l'intero che caratterizza il sottoinsieme L_i si dice indice di tale livello.

L'insieme dei divisori di $210 = 2 \cdot 3 \cdot 5 \cdot 7$ è un insieme graduato avente altezza 4. Al livello 0, il più basso, si colloca il nodo 1; al livello 1 i nodi relativi ai fattori primi 2, 3, 5 e 7; al livello 2 si trovano i prodotti di due fattori primi 6, 10, 14, 15, 21 e 35; al livello 3 i prodotti di tre fattori primi 30, 42, e 70; al livello 4 il solo 210.

L'insieme dei sottoinsiemi di $\{1, 2, 3, 4, 5, 6\}$ è un insieme graduato di altezza 6 e il suo sottoinsieme di livello $i = 0, 1, 2, 3, 4, 5, 6$ è costituito dalla collezione dei sottoinsiemi aventi cardinale i.
Questo insieme di sottoinsiemi possiede un elemento minimo costituito dall'insieme vuoto e un elemento massimo costituito dall'intero ambiente $\{1, 2, 3, 4, 5, 6\}$.

B16 c.06 Una relazione d'ordine graduata $\langle A, \preceq \rangle$ si può individuare a partire dalle sole coppie di elementi che si trovano a due livelli successivi. La relazione costituita da queste coppie non è che la $\prec_{\mathbf{I}}$. Essa viene detta **radice-starc della relazione d'ordine graduata** $\preceq$ e se questa viene detta relazione di "precedenza" la $\preceq_{\mathbf{I}}$ viene letta relazione di "precedenza immediata".

La $\preceq$ si ottiene dalla $\prec_{\mathbf{I}}$ mediante la cosiddetta **chiusura riflessivo-transitiva** o **potenza*c**.
Questa trasformazione si può definire per ogni relazione binaria $\boldsymbol{R} = \langle A, U \rangle$ e consiste nell'ampliamento dell'insie delle coppie di $\boldsymbol{R}$ con i cappi di tutti gli elementi del terreno A e con tutti gli archi $\langle p, q \rangle$ che collegano due elementi il secondo dei quali raggiungibile dal primo mediante un cammino di due o più archi di $\boldsymbol{R}$.

Si constata che questo ampliamento per ogni poset finito è ottenibile con un algoritmo.

Nell'esempio de poset dei sottoinsiemi di un insieme finito X, $\langle \mathfrak{P}(X), \subseteq \rangle$ la radice.star-c dell'inclusione è costituita da tutte le coppie $\langle E, E \cup \{p\} \rangle$ formate da un sottoinsieme proprio $E \subset X$ e da un sottoinsieme ottenuto da E aggiungendogli un elemento del terreno che non gli appartiene, cioè un $p \in X \setminus E$.

Nell'esempio dell'insieme dei divisori di un intero positivo N la radice.star-c della relazione "dividere" è costituita dalle coppie $\langle k, k\,p \rangle$ dove k divide N e p è un numero primo tale che $k\,p$ divide N.

B16 c.07 Insiemi graduati particolari di grande interesse sono le arborescenze, digrafi con molteplici applicazioni che saranno trattati più ampiamente nel capitolo D30.

Preliminarmente diamo una definizione intuitiva di **cammino sopra un digrafo**, un'altra nozione che riprenderemo più dettagliatamente in D30. Si tratta di una sequenza di archi del digrafo $\langle a_1, a_2, ..., a_s \rangle$ tali che per $i = 1, 2, ..., s-1$ il nodo finale di a_i coincide con il nodo iniziale di a_{i+1}.

Per il generico arco a_i possiamo denotare con q_{i-1} il suo nodo iniziale e con q_i il suo nodo iniziale, in modo che il cammino stesso può essere individuato dalla sequenza dei suoi nodi $\langle q_0, q_1, q_2, ..., q_{s-1}, q_s \rangle$. Tra due dei nodi di un tale cammino q_i e q_j con $i \leq j$ si dice che q_i è predecessore di q_j e che q_j è successore di q_i.

Definiamo dunque **arborescenza** un digrafo nel quale si distingue un nodo che chiamiamo **radice dell'arborescenza** dal quale sono raggiungibili tutti gli altri con uno e un solo cammino.

In una arborescenza si distinguono i **nodi padre**, dotati di successori, e i **nodi foglia**, nodi privi di successori.
Qui trascuriamo la possibilità che una arborescenza presenti un solo nodo e quindi diciamo che la radice di ogni arborescenza è un nodo padre.

Per altezza di una arborescenza si intende la lunghezza massima dei suoi cammini, cammini che devono iniziare nella sua radice.
I successori immediati di un nodo padre si dicono suoi **nodi figli**. Si dice **arborescenza elementare** un'arborescenza formata solo da un nodo padre e da suoi nodi figli.

Ogni arborescenza si può considerare ottenuta "allacciando" un numero finito di arborescenze elementari. Anche questa operazione di allacciamento qui ci limitiamo a presentarla intuitivamente, rinviando la definizione formale a D30.

Si vede che in ogni nodo diverso dal padre entra uno e un solo arco, mentre la radice ha grado entrante nullo.
Un'arborescenza con $n \geq 2$ nodi quindi presenta $n-1$ nodi figli ed $n-1$ archi padre-figlio; inoltre se presenta $f(\leq n-1)$ nodi padre, e quindi $n-f$ nodi foglia, si può ottenere allacciando f arborescenze elementari.

B16 c.08 Le arborescenze si possono raffigurare in vari modi. Qui preferiamo la cosiddetta **raffigurazione alto-basso** nella quale la radice occupa la posizione più alta e tutti i figli di ogni nodo padre sono collocati sotto di esso su una stessa linea orizzontale.

Va osservato che si possono definire altre raffigurazioni, la raffigurazione basso-alto, la destra-sinistra o la sinistra-destra ottenibili dalla alto-basso con opportune rotazioni e/o riflessioni.
Si tratta di raffigurazioni sostanzialmente equivalenti alla prima definita che per talune applicazioni presentano dei vantaggi.
Per esempio le raffigurazioni basso-alto presentano radici più realisticamente poste in basso, mentre qualche raffigurazione sinistra-destra può essere presentata con una comune stampante e risulta più utilizzabile per presentare sistemi di classificazione come il seguente.

Precambriano
- Adeano
- Archeano
- Proterozoico
- Fanerozoico
  - Paleozoico
    - Cambriano
    - Ordoviciano
    - Siluriano
    - Devoniano

- Carbonifero
  - Missisipiano
  - Pennysylvaniano
- Permiano

Mesozoico
- Triassico
- Giurassico
- Cretacico

Cenozoico
- Paleogene
  - Paleocene
  - Eocene
  - Oligocene
- Neogene
  - Miocene
  - Pliocene
- Quaternario
  - Pleistocene
  - Olocene

B16 c.09 Hanno grande interesse due arricchimenti delle arborescenze.
Il primo riguarda il genere di struttura **arborescenza distesa**, in breve **arborescenza.d**, arborescenze arricchite dalle informazioni che tra i figli di ciascun padre distinguono il primo, il secondo e così via.

La precisazione di un'arborescenza distesa si ottiene da una sua **raffigurazione piana alto basso sinistra destra**, raffigurazione senza archi che si incrociano nella quale i padri si collocano al di sopra dei nodi figli e l'ordine totale tra i figli si ricava dal loro posizionarsi da sinistra a destra, intendendo che un figlio più a sinistra preceda quelli alla sua destra.

Si osserva che i periodi geologici presentati in precedenza sono organizzati in una arborescenza distesa nella quale l'ordine dei figli corrisponde, per evidenti ragioni di chiarezza, all'ordine temporale.

B16 c.10 Un'altro arricchimento delle arborescenze consiste nell'aggiunta di un'etichetta a ogni nodo. In tal caso si parla di **arborescenza etichettata**.

Se invece si aggiunge un'etichetta a ogni nodo di un'arborescenza distesa si ottiene quella che, prevedibilmente, chiamiamo **arborescenza distesa etichettata**.

Ciascuna di queste ultime arborescenze arricchite è in grado di fornire varie stringhe spesso significative.

Un primo genere di stringhe si legge sui nodi dai cammini che portano da un nodo a un suo discendente ed in particolare sui cammini dalla radice a una foglia; questi cammini sono detti **cammini massimali**, in quanto non possono essere prolungati.

Altre stringhe si leggono sui nodi costituenti i cosiddetti tagli dell'arborescenza distesa.
Si dice in generale **taglio di un digrafo ordinato** un insieme C dei suoi nodi tale che ogni cammino sul digrafo aut ha l'estremità inferiore che non è non superiore ad alcun nodo di C, aut ha l'estremità superiore che non è inferiore ad alcun nodo di C, aut è costituito da un solo nodo appartenente a C.
Si constata che ogni taglio è costituito da nodi noncomparabili; più precisamente ogni taglio è un insieme di nodi noncomparabili massimale, cioè non ulteriormente ampliabile.

In particolare per i digrafi graduati per ciascuno dei suoi livelli l'insieme dei nodi di tale livello costituisce un taglio. Si possono tuttavia avere tagli costituiti da nodi in diversi livelli.

Nelle arborescenze si hanno in particolare il taglio costituito dalla sola radice e il taglio costituito dall'insieme delle foglie.

B16 c.11 Nel caso di un'arborescenza distesa Ψ ogni taglio risulta ordinato totalmente in conseguenza del seguente algoritmo che consente di confrontare tutti i duetti di nodi (diversi).
Dati due nodi p e q se p è predecessore di q si decide che p preceda q; in caso contrario si risale all'inferiore dei predecessori comuni, per il quale scriviamo $s := \inf(p, q)$; p e q discendono da due diversi figli di s e si assume come precedente tra p e q il nodo che discende dal figlio di s più a sinistra.

Scorrendo i nodi di un taglio di ogni arborescenza Ψ secondo questo ordinamento totale le etichette dei successivi nodi forniscono una stringa. In particolare si ottiene una stringa scorrendo secondo l'ordinamento sinistra-destra le foglie della Ψ.

Va segnalato che vari tipi di espressioni matematiche presentano una struttura formale che si può ricondurre alle stringhe ottenute dai tagli di opportune arborescenze distese etichettate [C14f].

B16 d. permutazioni di insiemi finiti

B16 d.01 Esaminando le permutazioni in un contesto applicativo, in genere, occorre tenere conto di come sono individuati o costruiti gli oggetti che vengono permutati; in altre considerazioni, tendenzialmente più astratte, non serve tenere conto delle caratteristiche "genetiche" degli oggetti che vengono trasferiti, ma occorre solo poterli individuare distintamente.

Nel secondo caso risulta conveniente ricondursi al caso canonico delle permutazioni degli interi di $(\mathrm{n}\,] = \{1, 2, ..., n\}$; in tal modo si considerano oggetti naturalmente ordinati e gli oggetti si possono confondere con le posizioni delle scatole allineate, ciascuna in grado di contenerne esattamente uno dopo l'attuazione di una qualsiasi permutazione.

Nelle considerazioni sulle permutazioni che seguono ci limiteremo a considerare trasformazioni dei primi n interi positivi. Una permutazione P corrisponde allora a una trasformazione della sequenza $\langle 1, 2, ..., n\rangle$ nella sequenza $\left\langle 1{,}P, 2{,}P, ..., n{,}P\right\rangle$.

In questa scrittura si può pensare una permutazione come un operatore la cui applicazione a un intero $i \in (\mathrm{n}\,]$ (espressa dalla scrittura suffissa $i{,}P$) fornisce l'intero che contrassegna la scatola destinazione.

B16 d.02 Una permutazione P di $(\mathrm{n}\,]$, quindi, quando la si descrive come un processo di trasformazione, può essere rappresentata con la notazione data da una matrice $2 \times n$

$$P \;=\; \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1{,}P & 2{,}P & \dots & n{,}P \end{matrix} \right\downarrow \;. \tag{1}$$

Nel seguito le permutazioni su un qualsiasi insieme X saranno utilizzate esclusivamente in espressioni nelle quali hanno il ruolo di operatori collocati a destra dei loro operandi; di conseguenza la composizione di due permutazioni P e Q sullo stesso X va scritta nella forma $P \circ_{lr} Q$.

Nella precedente matrice, l'ordine delle colonne è ininfluente: queste potrebbero essere riordinate arbitrariamente. Quindi se T denota una generica permutazione di $(\mathrm{n}\,]$, si può anche scrivere:

$$P \;=\; \left\downarrow \begin{matrix} 1{,}T & 2{,}T & \dots & n{,}T \\ 1{,}T{,}P & 2{,}T{,}P & \dots & n{,}T{,}P \end{matrix} \right\downarrow \;, \tag{2}$$

dove si intende che per ogni $i \in (\mathrm{n}\,]$

$$i{,}T{,}P \;:=\; (i{,}T){,}P \;=\; i{,}(T \circ_{lr} P) \;.$$

Se in particolare T è la permutazione inversa della P, ossia se $T = P^{-\mathbf{1}}$,
si ha:

$$P \;=\; \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1{,}P & 2{,}P & \dots & n{,}P \end{matrix} \right\downarrow \;=\; \left\downarrow \begin{matrix} 1{,}P^{-\mathbf{1}} & 2{,}P^{-\mathbf{1}} & \dots & n{,}P^{-\mathbf{1}} \\ 1 & 2 & \dots & n \end{matrix} \right\downarrow \;. \tag{3}$$

La precedente uguaglianza serve a chiarire il collegamento che sussiste tra una permutazione e la sua inversa.

Oltre alla notazione a due righe, per presentare una permutazione P si può usare l'equivalente più concisa rappresentazione sequenziale formata dalla seconda riga della prima rappresentazione matriciale; per tale presentazione usiamo la scrittura

$$P \;=\; \left\langle_{prm} 1{,}P, 2{,}P, ..., n{,}P\right\rangle \;. \tag{4}$$

Nel seguito spesso, per semplicità, trascureremo l'infisso " , " .

Talora invece delle notazioni $i{,}P$ e $i\,P$ conviene servirsi della notazione funzionale secondo la quale la (1) viene sostituita dalla

$$P \;=\; \Big\downarrow \begin{matrix} 1 & 2 & \dots & n \\ P(1) & P(2) & \dots & P(n) \end{matrix} \Big\downarrow \tag{5}$$

e la notazione sequenziale asume la forma

$$P \;=\; \Big\langle_{prm} P(1), P(2), ..., P(n) \Big\rangle \; . \tag{6}$$

B16 d.03 Il prodotto di composizione di due permutazioni di **(**n **]** P e Q si può così definire:
(1)

$$P \circ_{lr} Q \;:=\; \Big\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,P & 2\,P & \dots & n\,P \end{matrix} \Big\downarrow \circ_{lr} \Big\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,Q & 2\,Q & \dots & n\,Q \end{matrix} \Big\downarrow \;:=\; \Big\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,PQ & 2\,PQ & \dots & n\,PQ \end{matrix} \Big\downarrow \; .$$

In seguito denoteremo con Sym_X l'insieme di tutte le permutazioni di un insieme finito X.
L'insieme delle permutazioni degli interi 1, 2, ..., n, cioè $\mathsf{Sym}_{\text{(n]}}$, sarà anche denotato più concisamente con Sym_n.

Introduciamo ora la nozione di gruppo, ora limitandoci al caso degli insiemi di permutazioni entro insiemi finiti e riferendoci spesso per semplicità alle permutazioni di **(**n **]**. Più avanti allargheremo questo discorso alle permutazioni di insiemi qualsiasi [B41b].

B16 d.04 Dato un insieme finito $X = \{x_1, x_2, ..., x_n\}$, si dice **gruppo di permutazioni** di X un insieme di permutazioni di X che gode delle quattro proprietà che seguono, proprietà chiamate "assiomi per la specie di strutture gruppo".

[Grp 1] $\forall P, Q \in \mathsf{Sym}_X \;:\; P \circ Q \in \mathsf{Sym}_X$ (in accordo con l'uguaglianza d05(1)).

[Grp 2] Il prodotto di composizione è associativo (questo in effetti vale per ogni composizione di trasformazioni).

[Grp 3] Sym_X contiene un elemento neutro per il prodotto, la trasformazione identica di X:

$$\mathsf{Id}_X \;=\; \Big\downarrow \begin{matrix} x_1 & x_2 & \dots & x_n \\ x_1 & x_2 & \dots & x_n \end{matrix} \Big\downarrow \; .$$

[Grp 4] $\forall P \in \mathsf{Sym}_X \;:\; \mathsf{Sym}_X \ni P^{-\mathbf{1}}$. come si è visto in d04(3), si tratta di

$$P^{-\mathbf{1}} \;=\; \Big\downarrow \begin{matrix} x_1P & x_2P & \dots & x_nP \\ x_1 & x_2 & \dots & x_n \end{matrix} \Big\downarrow \;=\; \Big\downarrow \begin{matrix} x_1 & x_2 & \dots & x_n \\ x_1(P^{-\mathbf{1}}) & x_2(P^{-\mathbf{1}}) & \dots & x_n(P^{-\mathbf{1}}) \end{matrix} \Big\downarrow \; ,$$

permutazione reciproca della P per la quale si ha: $P \circ P^{-\mathbf{1}} \;=\; P^{-\mathbf{1}} \circ P \;=\; \mathsf{Id}_n$.

L'insieme di tutte le permutazioni di X munito della operazione di composizione delle trasformazioni viene chiamato **gruppo simmetrico dell'insieme** X o gruppo totale delle permutazioni di X.

In seguito spesso non distingueremo tra un gruppo di permutazioni $\langle X, \mathsf{Sym}_X \rangle$ e il suo insieme terreno Sym_X e adotteremo la semplificazione Sym_X per il corrispondente gruppo.
Denotiamo in particolare con Sym_n il gruppo delle permutazioni dell'insieme numerico **(**n **]**.

Dati due gruppi di permutazioni su un insieme X $\boldsymbol{P} = \langle \mathsf{P}, X \rangle$ e $\boldsymbol{Q} = \langle \mathsf{Q}, X \rangle$, si dice che $\boldsymbol{Q}$ è un **sottogruppo** di $\boldsymbol{R}$ sse $\mathsf{Q} \subseteq \mathsf{P}$,
Stante questa definizione, possiamo dire che ogni gruppo di permutazioni su X è un sottogruppo di Sym_X.

B16 d.05 Per le permutazioni di Sym_X l'insieme X costituisce il dominio e, come si è detto, il cardinale di questo insieme viene detta **grado del gruppo** Il cardinale dell'insieme delle permutazioni costituenti Sym_X lo chiamiamo **cardinale del gruppo** , anche se in genere viene chiamato "ordine del gruppo".

Sappiamo che dato un insieme di n oggetti, e in particolare dato (n], il numero delle sue permutazioni è $n!$: questo dice che il cardinale del gruppo Sym_n è $n!$, fatto che si esprime scrivendo $|\mathsf{Sym}_n| = n!$.

Per esempio il gruppo Sym_3 delle permutazioni su $\{1,2,3\}$ è formato da $3! = 3 \cdot 2 \cdot 1 = 6$ elementi:

$$e = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{vmatrix} \quad a = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{vmatrix} \quad b = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}$$
$$c = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{vmatrix} \quad d = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{vmatrix} \quad f = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{vmatrix}$$

Notiamo esplicitamente che al crescere del grado n l'ordine $|\mathsf{Sym}_n|$ cresce molto vistosamente; come vedremo contemporaneamente cresce la sua complessità.

B16 d.06 I gruppi simmetrici sono oggetti matematici di importanza primaria, in quanto su di essi e sui loro sottogruppi si basa lo studio delle simmetrie di tutte le configurazioni finite e di tutti gli oggetti di interesse per la matematica e per le sue applicazioni che si possono caratterizzare con componenti in numero finito. Tipici esempi sono forniti dai poligoni, dai poliedri e dalle equazioni polinomiali dotati di qualche tipo di regolarità.

Il loro studio è stato portato molto avanti e si collega a una grande varietà di settori della matematica: combinatorica, geometria, topologia, funzioni spaciali, fisica matematica, teorie relativistiche e quantistiche, chimica molecolare, cristallografia, crittografia, ...

Alle elaborazioni sul gruppo simmetrico sono dedicati anche sofisticati pacchetti software, come `Magma (computer algebra system) (we)` e `GAP (computer algebra system) (we)`.
Su questi strumenti è interessante consultare `List of computer algebra systems (we)`.

B16 e. permutazioni cicliche

B16 e.01 Consideriamo due interi positivi m ed n con $m \leq n$ e una permutazione della forma:

$$C \;=\; \left\downarrow \begin{matrix} i_1 & i_2 & \dots & i_{m-1} & i_m & i_{m+1} & \dots & i_n \\ i_2 & i_3 & \dots & i_m & i_1 & i_{m+1} & \dots & i_n \end{matrix} \right\downarrow , \tag{1}$$

dove $\langle_{prm} i_1, i_2, \dots, i_m \rangle$ è una qualsiasi permutazione dell'insieme $\mathbf{(}m\mathbf{]}$ dei primi m interi positivi.
Questa permutazione presenta $n-m$ punti fissi, $i_{m+1}, ..., i_n$, e viene detta **permutazione circolare** o **permutazione ciclica** di lunghezza m.
Sbrigativamente una tale permutazione viene hiamata **ciclo**.
Per maggiore generalità non escludiamo la possibilità che sia $m = n$, cioè la possibilità di non avere alcun punto fisso.

Nei contesti nei quali si può sottintendere che si trattano permutazioni di $\mathbf{(}$n $\mathbf{]}$, per una permutazione ciclica C come la precedente adottiamo la notazione semplificata

$$\langle_{cy} i_1 \; i_2 \; \dots \; i_m \rangle \; . \tag{2}$$

Per questa notazione la scelta dell'elemento che si pone nella prima posizione tra le parentesi è irrilevante, conta solo il succedersi ciclico degli oggetti tra le parentesi. Si ha cioè:

$$C \;=\; \langle_{cy} i_r \; i_{r+1} \; \dots \; i_m \; i_1 \; \dots \; i_{r-1} \rangle \;\; \text{per } r = 1, 2, ..., m \; . \tag{3}$$

Per ogni permutazione vale la seguente uguaglianza equivalente della precedente:

$$\langle_{cy} i_1, ..., i_r, j_1, ..., j_s \rangle \;=\; \langle_{cy} j_1, ..., j_s, i_1, ..., i_r \rangle \; . \tag{4}$$

B16 e.02 Denotiamo con $\boldsymbol{Cycl}_n$ il sottoinsieme di Sym_n costituito dalle permutazioni cicliche e con $\boldsymbol{Cycl}_{n,m}$ il suo sottoinsieme costituito dalle permutazioni cicliche su $\mathbf{(}$n $\mathbf{]}$ con $n-m$ punti fissi, ovvero il sottoinsieme delle permutazioni di $iInJ$ esprimibili con un ciclo di lunghezza m.

Evidentemente $\boldsymbol{Cycl}_n$ si ripartisce negli insiemi delle permutazioni cicliche delle diverse lunghezze ammissibili e queste vanno da 1 a n:

(1) Prop.: $\boldsymbol{Cycl}_n \;= \bigcup_{m=1}^{:\,n} \boldsymbol{Cycl}_{n,m}$ ∎

Si osserva subito che $\boldsymbol{Cycl}_{n,1} = \{\mathsf{Id}_n\}$, che $\boldsymbol{Cycl}_{n,2} \;=\; \{i = 1, ..., n-1 \;\wedge\; j = i+1, ..., n :|\; \langle_{cy} i, j \rangle\}$ e quindi si hanno le formule enumerative

$$|\boldsymbol{Cycl}_{n,1}| \;=\; 1 \qquad \text{e} \qquad |\boldsymbol{Cycl}_{n,2}| \;=\; \mathsf{CombN}(n,2) \;=\; \frac{n(n-1)}{2} \; .$$

I cicli di lunghezza 2 sono detti anche **scambi** o trasposizioni (di due elementi); queste trasformazioni sono le più semplici involuzioni.

I cicli di lunghezza n sono rappresentati dalle scritture $\langle_{cy} i_1, ..., i_n \rangle$.
Queste scritture sono in biiezione con le permutazioni di $\mathbf{(}$n $\mathbf{]}$, e quindi sono $n!$; accade però che le n scritture ottenibili l'una dall'altra per permutazione circolare individuano lo stesso ciclo.
Quindi abbiamo $\boldsymbol{Cycl}_{n,n} \;=\; \dfrac{n!}{n} \;=\; (n-1)!$.

B16 e.03 Esaminiamo i cicli costituenti gli insiemi $\boldsymbol{Cycl}_{n,m}$ per $m = 2, ..., n-1$.

Ogni scrittura $\langle_{cy} i_1, ..., i_m \rangle$ individua un ciclo di lunghezza m; queste scritture sono in biiezione con le disposizioni senza ripetizioni di $\mathbf{(}$n $\mathbf{]}$ di lunghezza m e quindi sono $n(n-1)\cdots(n-m+1)$; accade però

che queste scritture si ripartiscono in classi, ciascuna di m oggetti ottenibili da una di esse mediante una delle m permutazioni circolari e tutte le scritture di una tale classe individuano la stessa permutazione di m oggetti. Quindi, in coerenza con la $\boldsymbol{Cycl}_{n,n} = (n-1)!$, si ha

$$|\boldsymbol{Cycl}_{n,m}| = \frac{n(n-1)\cdots(n-m+1)}{m} = \frac{n^{\underline{m}}}{m} .$$

Tenendo conto di c02(1), si ottiene dunque:

(1) Prop.: $|\boldsymbol{Cycl}_n| = 1 + \sum_{m=2}^{n} \frac{n(n-1)\cdots(n-m+1)}{m}$ ∎

Per esempio le 3!=6 permutazioni di $\{1,2,3\}$ si ripartiscono in:

1 ciclo di lunghezza 1;
3 cicli di lunghezza 2 $\Big(\langle_{cy}1,2\rangle$, $\langle_{cy}1,3\rangle$ e $\langle_{cy}2,3\rangle\Big)$;
cicli 2 di lunghezza 3 $\Big(\langle_{cy}1,2,3\rangle$ e $\langle_{cy}3,2,1\rangle\Big)$.

Per trovare permutazioni non cicliche occorre cercarle nei Sym_n con $n \geq 4$. Le permutazioni non cicliche di Sym_4 sono $\langle_{cy}1,2\rangle \circ \langle_{cy}3,4\rangle$, $\langle_{cy}1,3\rangle \circ \langle_{cy}2,4\rangle$ e $\langle_{cy}1,4\rangle \circ \langle_{cy}2,3\rangle$. In Sym_n si trovano inoltre l'identità, 6 permutazioni cicliche di 2 oggetti, 8 di 3 oggetti e 6 di 4 oggetti.

B16 e.04 (1) Eserc. Verificare che $\big\langle m = 1,...,5 :| \, |\boldsymbol{Cycl}_{5,m}|\big\rangle = \langle 1,10,20,30,24\rangle$ e che vi sono 35 permutazioni di **(5]** non cicliche.

(2) Eserc. Determinare la sequenza $\big\langle m = 1,...,n :| \, |\boldsymbol{Cycl}_{n,m}|\big\rangle$ e il cardinale $|\mathsf{Sym}_n \setminus \boldsymbol{Cycl}_n|$ per $n = 6, 7$.

(3) Eserc. Caratterizzare le matrici quadrate binarie delle involuzioni e quelle delle permutazioni circolari.

B16 e.05 Prop. Ogni permutazione $\boldsymbol{P}$ su X può essere associata a un digrafo raffigurando gli elementi del suo dominio con i nodi 1,2,...n e congiungendo con un arco le coppie di punti $\langle i, P(i)\rangle$ (e solo queste).
Per esempio, per

$$\boldsymbol{P} = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{matrix} \right\downarrow = \langle_{cy} 1\ 3\ 4\ 2\rangle$$

abbiamo la seguente raffigurazione:

Poiché $\boldsymbol{P}$ è una biiezione, in ogni vertice i esiste uno e uno solo arco entrante e uno e uno solo arco uscente.

Un altro esempio è dato dalla seguente permutazione:

$$\boldsymbol{Q} = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{matrix} \right\downarrow = \big\langle_{cy} 1\ 3\ 2\big\rangle ;$$

questa che è una permutazione circolare sugli elementi 1,2,3 e la sua rappresentazione mediante un grafo è:

B16 e.06 Due permutazioni di un insieme terreno X si dicono **permutazioni disgiunte-t** sse sono disgiunti i due insiemi di oggetti che esse modificano. Qui la specificazione "-t" sta per "target".

Quindi due permutazioni di X chiamate disgiunte-t sono due insiemi di coppie di $X \times X$ la cui intersezione è contenuta nell'identità Id_X (potendo in particolare essere vuota).

Evidentemente due permutazioni disgiunte-t di X, in quanto trasformazioni dello stesso terreno, commutano.

Particolari permutazioni disgiunte-t sono i cicli disgiunti-t; in generale ciascun membro di una coppia di permutazioni disgiunte-t è un prodotto di cicli e i cicli di entrambe le permutazioni agiscono su sottoinsiemi del terreno mutuamente disgiunti.

(1) Prop.: Ogni permutazione può essere espressa come prodotto di cicli disgiunti.

Dim.: Consideriamo la generica permutazione $\boldsymbol{P} = \langle \mathsf{P}, X \rangle$ e uno qualsiasi degli elementi del suo terreno X i_{11}; si osserva che questo viene trasformato in $i_{11}\mathsf{P} =: i_{12}$, che questo a sua volta va in $i_{11}\mathsf{P}^2 =: i_{13}$, e così via finchè si ottiene di nuovo l'elemento i_{11} che supponiamo possa essere individuato dall'espressione $i_{11} = i_{11}\mathsf{P}^{m_1}$.

A questo punto, aut si sono esauriti tutti gli elementi di **(**n **]** e si ha una permutazione ciclica di lunghezza n, aut un certo numero di essi non è stato incontrato.

In questo secondo caso si riprende il procedimento precedente a partire da uno qualsiasi degli elementi di X rimanenti; chiamatolo i_{21}, si ottiene la sequenza ciclica $\langle {}_{cy} i_{21},\ i_{21}P,\ ..., i_{21}\boldsymbol{P}^{m_2} =: i_{21} \rangle$.

Questo ricerca di nuove permutazioni cicliche si può portare avanti fino a esaurire tutti gli elementi di X ∎

Alla generica permutazione di **(**n **]** si può quindi dare la forma:

$$\boldsymbol{P} = \left\downarrow \begin{matrix} 1 & \dots & n \\ 1P & \dots & nP \end{matrix} \right\downarrow = \left\downarrow \begin{matrix} i_{11} & i_{12} & \dots & i_{1m_1} & i_{21} & i_{22} & \dots & i_{2m_2} & \dots & i_{r1} & i_{r2} & \dots & i_{rm_r} \\ i_{12} & i_{13} & \dots & i_{11} & i_{22} & i_{23} & \dots & i_{21} & \dots & i_{r2} & i_{r3} & \dots & i_{r1} \end{matrix} \right\downarrow$$

$$= \langle {}_{cy} i_{11}\ i_{11}\boldsymbol{P}\ i_{11}\boldsymbol{P}^2\ ...\ i_{11}\boldsymbol{P}^{m_1-1} \rangle \circ \langle {}_{cy} i_{21}\ i_{21}\boldsymbol{P}\ i_{21}\boldsymbol{P}^2\ ...\ i_{21}\boldsymbol{P}^{m_2-1} \rangle \circ \dots \quad (2)$$
$$\circ \langle {}_{cy} i_{r1}\ i_{r1}\boldsymbol{P}\ i_{r1}P^2\ ...\ i_{r1}\boldsymbol{P}^{m_r-1} \rangle \ .$$

Non si esclude che qualcuno degli m_i sia uguale a 1, cioè che qualcuno degli i sia un punto fisso della permutazione $\boldsymbol{P}$.

B16 e.07 La precedente espressione e06 s(2) per la permutazione $\boldsymbol{P}$ viene detta **fattorizzazione di una permutazione mediante cicli mutuamente disgiunti**.

Evidentemente nella precedente espressione è lecito cambiare ad arbitrio l'ordine dei cicli fattori; inoltre in essa l'operazione $\circ$ può interpretarsi sia come $\circ_{lr}$ che come $\circ_{rl}$.

Questo fatto si esprime anche dicendo che la fattorizzazione in cicli disgiunti di una permutazione è "unica a meno di" permutazioni dei fattori.

Una permutazione può essere utilmente caratterizzata dal multiinsieme [B13f16] che vede assegnare ai suoi elementi i rispettivi periodi ossia la lunghezza del ciclo de quale fa parte.

Una sua caratterizzazione più essenziale consiste in una partizione.i del cardinale del suo dominio $n := |X|$.

Per ogni permutazione $\boldsymbol{P}$ di grado n denotiamo con $prti(\boldsymbol{P})$ la partizione.i di n che essa induce.

Ogni partizione.i di n può essere convenientemente raffigurata da una cosiddetta **forma di Ferrers**.

Si tratta di una figura piana costituita da n quadratini accostati che si può considerare una matrice privata da alcune sue caselle; i quadratini componenti si possono quindi chiamare anche le sua "caselle".

Come le matrici ed altre figure piane una forma di Ferrers si può presentare in 8 modi trasformabili gli uni negli altri con rotazioni di 90° e con riflessioni rispetto a lineemediane parallele agli assi o rispetto alle caselle nelle posizioni diagonali.

Qui privilegiamo una sua rappresentazione che chiamiamo "rappresentazione matriciale-NW".
Diciamo quindi **forma di Ferrers associata alla partizione.i noncrescente** $\vec{\lambda} = \langle \lambda_1, ..., \lambda_r \rangle$ la figura che presenta r righe di caselle adiacenti e allineate a sinistra che nella riga $i = 1, 2, ..., r$ sono in numero di λ_i.

Tale figura la denotiamo con $frrs(\vec{\lambda})$.
Il numero delle caselle di questa forma di Ferrers $F = frrs(\vec{\lambda})$, viene chiamato anche **peso della forma di Ferrers**, viene denotato con $wgt(F)$ e viene definito come

$$wgt(F) \ := \ \sum_{i=1}^{r} \lambda_i \ .$$

Evidentemente $wgt(F) = n$.

Diciamo **rango della forma di Ferrers** $F = frrs(\vec{\lambda})$ e denotiamo con $\mathrm{rnk}(F)$. il numero delle caselle che costituiscono la sua diagonale decrescente.

Introduciamo anche le notazioni $\mathbf{Frrs}_n$ per l'insieme delle forme di Ferrers aventi peso n, $\mathbf{Frrs}^{(r)}$ per l'insieme delle forme aventi rango r e $Frrs$ per l'insieme delle forme di Ferrers dei diversi pesi positivi.

Si constata che le altre 7 raffigurazioni di una forma di Ferrers si ottengono dalla matriciale con rotazioni di multipli di 90° e con le riflessioni verticali e orizzontali. JP Si osserva che le forme di Ferrers sono raffigurazioni fedeli delle partizioni.i, ossia che la specie delle forme di Ferrers e la speci delle partizioni.i sono specie di strutture criptomorfe.

B16 e.08 Quando si trattano solo permutazioni di (n] per un particolare n 'e comodo individuare tali trasformazioni mediante le cosiddette **notazioni a parentesi** delle permutazioni cicliche disgiunte.
Questa si ottiene dalla notazione a cicli i cicli di lunghezza 1 e semplificando ogni scrittura della forma $\langle_{cy} i_1, i_2, ..., j_s \rangle$ nella $(i_1 \ i_2 \ ... \ i_s)$, ossia trascurando i segni "$\circ$"; per queste notazioni inoltre si usa la scrittura (1) per denotare l'identità di (n].

Considerazioni simili valgono, evidentemente, per le permutazioni di un terreno i cui elementi si possono identificare con semplici caratteri.

Consideriamo l'esempio della permutazione

$$P = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 3 & 5 & 9 & 6 & 8 & 7 \end{matrix} \right\downarrow \ .$$

La sua fattorizzazione mediante cicli si scrive:

$$P \ = \ (1\ 2\ 4\ 3)\,(5)\,(6\ 9\ 7)\,(8) \ = \ (1\ 2\ 4\ 3)\,(6\ 9\ 7)$$

B16 e.09 La rappresentazione delle permutazioni mediante cicli può risultare conveniente nel calcolo del prodotto di più permutazioni. Per esempio consideriamo le permutazioni:

$$\boldsymbol{P} \ = \ \langle_{cy} 1, 3, 4\rangle \circ \langle_{cy} 2, 6\rangle \quad , \quad \boldsymbol{Q} \ = \ \langle_{cy} 1, 5, 2\rangle \circ \langle_{cy} 3, 6, 4\rangle \quad \text{e} \quad \boldsymbol{R} \ = \ \langle_{cy} 1, 4, 5, 6\rangle$$

e calcoliamo il loro prodotto

$$\boldsymbol{S} = (1\ 3\ 4)\,(2\ 6) \circ_{lr} (1\ 5\ 2)\,(3\ 6\ 4) \circ_{lr} (1\ 4\ 5\ 6) \ .$$

Conviene individuare la rappresentazione ciclica del prodotto iniziando dal numero 1 e individuando le modifiche alle quali viene sottoposto dai fattori ciclici considerati da sinistra a destra; in tal modo si ricava la sequenza delle trasformazioni:

$$1 \to 3 \to 3 \to 3 \to 6 \to 1 \ ;$$

Quindi $1,\boldsymbol{S} = 1$. Si individuano poi le trasformazioni subite dal numero 2:

$$2 \to 6 \to 6 \to 4 \to 5$$

ottenendo $2{,}\boldsymbol{S} = 5$; ricominciando dal numero 5 si trova:

$$5 \to 2 \ .$$

Avendo ottenuto di nuovo il numero 2 da cui siamo partiti, risulta concluso il ciclo (2 5).

Dato che non si sono sistemati tutti gli interi di $\mathbf{(}6\mathbf{]}$, ripartiamo dal più piccolo intero non incluso nel ciclo trovato, il numero 3, e costruiamo con lo stesso procedimento un nuovo ciclo; si trova allora che:

$$3 \to 4 \to 4 \to 3 \to 3 \ ,$$

cioè che 3 è punto fisso.

Occorre poi ripartire da 4 e si ottiene:

$$4 \to 1 \to 5 \to 6 \ ;$$

a questo punto è sicuro che $6{,}\boldsymbol{S} = 4$ e si ottiene lo scambio $\mathbf{[}4 \longleftrightarrow 6\mathbf{]}$. Con questo ciclo si esaurisce $\mathbf{(}6\mathbf{]}$ e si può concludere con:

$$\boldsymbol{P} \circ_{lr} \boldsymbol{Q} \circ_{lr} \boldsymbol{R} \ = \ (1)\,(2\ 5)\,(3)\,(4\ 6) \ .$$

B16 e.10 Due permutazioni $\boldsymbol{P}$ e $\boldsymbol{Q}$ sullo stesso dominio X si dicono appartenere alla stessa **classe di coniugio** sse si trova una permutazione $\boldsymbol{T}$ sullo stesso X tale che sia:

$$\boldsymbol{Q} \ = \ \boldsymbol{T^{-1}} \circ_{lr} \boldsymbol{P} \circ_{lr} \boldsymbol{T} \ .$$

L'appartenenza alla stessa classe di coniugio è una relazione tra le permutazioni di ogni gruppo di permutazioni e per affermare la validità della relazione precedente scriviamo $\boldsymbol{R} \sim_{prm} \boldsymbol{Q}$.

Infatti la relazione $\sim_{prm}$ è riflessiva (per $\boldsymbol{T}$ basta assumere Id_X), è simmetrica (se $\boldsymbol{Q} = \boldsymbol{T^{-1}PT}$ si ha $\boldsymbol{P} = \boldsymbol{TQT^{-1}}$) ed è transitiva (se $\boldsymbol{Q} = \boldsymbol{T^{-1}PT}$ ed $\boldsymbol{R} = \boldsymbol{U^{-1}QU}$, allora $\boldsymbol{R} = \boldsymbol{U^{-1}T^{-1}PTU} = (\boldsymbol{TU})^{-1}\boldsymbol{P}(\boldsymbol{TU})$; quindi $\sim_{prm}$ è una equivalenza.
In molti contesti $\sim_{prm}$ si può abbreviare con $\sim$.

La scrittura mediante cicli di una permutazione di n oggetti, ovvero, più essenzialmente, la corrispondente partizione.i di n oppure la equivalenteb forma di Ferrers di peso n [e07], permettono di caratterizzare completamente ed efficacemente le classi di coniugio del gruppo Sym_X .

(1) Prop.: Consideriamo due permutazioni $\boldsymbol{P}$ e $\boldsymbol{Q}$ sullo stesso dominio X di grado n.

$$\boldsymbol{P} \sim_{prm} \boldsymbol{Q} \iff \mathit{prti}(\boldsymbol{P}) = \mathit{prti}(\boldsymbol{Q}) \ .$$

Dim.: "$\Longrightarrow$" Per la permutazione $\boldsymbol{P}$ scriviamo

$$\boldsymbol{P} \ = \ \left\downarrow \begin{matrix} i_1 & i_1\boldsymbol{P} & \dots & i_1\boldsymbol{P}^{m_1-1} & \dots & i_r & i_r\boldsymbol{P} & \dots & i_r\boldsymbol{P}^{m_r-1} \\ i_1\boldsymbol{P} & i_1\boldsymbol{P}^2 & \dots & i_1 & \dots & i_r\boldsymbol{P} & i_r\boldsymbol{P}^2 & \dots & i_r \end{matrix} \right\downarrow \ .$$

Se $\boldsymbol{Q}$ appartiene alla sua stessa classe di coniugio possiamo scrivere per una opportuna permutazione $\boldsymbol{T}$:

$$\boldsymbol{Q} = \boldsymbol{T^{-1}} \circ_{lr} \boldsymbol{P} \circ_{lr} \boldsymbol{T} \ = \left\downarrow \begin{matrix} i\boldsymbol{T} \\ i \end{matrix} \right\downarrow \ \circ_{lr} \ \boldsymbol{P} \ \circ_{lr} \ \left\downarrow \begin{matrix} i \\ i\boldsymbol{T} \end{matrix} \right\downarrow \ =$$

$$\left\downarrow \begin{matrix} i_1\boldsymbol{T} & i_1\boldsymbol{PT} & \cdots & i_1\boldsymbol{P}^{m_1-1}\boldsymbol{T} & \cdots & i_r\boldsymbol{T} & i_r\boldsymbol{PT} & \cdots & i_r\boldsymbol{P}^{m_r-1}\boldsymbol{T} \\ i_1\boldsymbol{PT} & i_1\boldsymbol{P}^2\boldsymbol{T} & \cdots & i_1\boldsymbol{T} & \cdots & i_r\boldsymbol{PT} & i_r\boldsymbol{P}^2\boldsymbol{T} & \cdots & i_r\boldsymbol{T} \end{matrix} \right\downarrow \ =$$

$$\left\downarrow \begin{matrix} i_1 & i_1\boldsymbol{T}^{-1}\boldsymbol{PT} & \cdots & i_1\boldsymbol{T}^{-1}\boldsymbol{P}^{m_1-1}\boldsymbol{T} & \cdots & i_r & i_r\boldsymbol{T}^{-1}\boldsymbol{PT} & \cdots & i_r\boldsymbol{T}^{-1}\boldsymbol{P}^{m_r-1}\boldsymbol{T} \\ i_1\boldsymbol{T}^{-1}\boldsymbol{PT} & i_1\boldsymbol{T}^{-1}\boldsymbol{P}^2\boldsymbol{T} & \cdots & i_1 & \cdots & i_r\boldsymbol{T}^{-1}\boldsymbol{PT} & i_r\boldsymbol{T}^{-1}\boldsymbol{P}^2\boldsymbol{T} & \cdots & i_r \end{matrix} \right\downarrow$$

$$= \left\langle_{cy}\ i_1\ \ i_1\boldsymbol{Q}\ \ i_1\boldsymbol{Q}^2\ \ \cdots\ \ i_1\boldsymbol{Q}^{m_1-1}\ \right\rangle\cdots\left\langle_{cy}\ i_r\ \ i_r\boldsymbol{Q}\ \ i_r\boldsymbol{Q}^2\ \ \cdots\ \ i_r\boldsymbol{Q}^{m_r-1}\ \right\rangle .$$

Quindi per $\boldsymbol{Q}$ si è trovata una struttura ciclica uguale a quella di $\boldsymbol{P}$.

"$\Longleftarrow$" Se $\boldsymbol{P}$ e $\boldsymbol{Q}$ hanno la stessa struttura ciclica:

$$\boldsymbol{P} = \left\langle_{cy} i_1\ i_1\boldsymbol{P}\ i_1\boldsymbol{P}^2\ \cdots\ i_1\boldsymbol{P}^{m_1-1}\right\rangle\cdots\left\langle_{cy} i_r\ i_r\boldsymbol{P}\ i_r\boldsymbol{P}^2\ \cdots\ i_r\boldsymbol{P}^{m_r-1}\right\rangle$$

$$\boldsymbol{Q} = \left\langle_{cy} j_1\ j_1\boldsymbol{Q}\ j_1\boldsymbol{Q}^2\ \cdots\ j_1\boldsymbol{Q}^{m_1-1}\right\rangle\cdots\left\langle_{cy} j_r\ j_r\boldsymbol{Q}\ j_r\boldsymbol{Q}^2\ \cdots\ j_r\boldsymbol{Q}^{m_r-1}\right\rangle$$

si trova un'altra permutazione su X $\boldsymbol{T}$ tale che $\boldsymbol{Q} = \boldsymbol{T}^{-1} \circ \boldsymbol{P} \circ \boldsymbol{T}$; essa precisamente è:

$$\boldsymbol{Q} = \left\downarrow \begin{matrix} j_1 & j_1\boldsymbol{Q} & \cdots & j_1\boldsymbol{Q}^{m_1-1} & \cdots & j_r & j_r\boldsymbol{Q} & \cdots & j_r\boldsymbol{Q}^{m_r-1} \\ i_1 & i_1\boldsymbol{P} & \cdots & i_1\boldsymbol{P}^{m_1-1} & \cdots & i_r & i_r\boldsymbol{P} & \cdots & i_r\boldsymbol{P}^{m_r-1} \end{matrix} \right\downarrow \circ_{lr}$$

$$\left\downarrow \begin{matrix} i_1 & i_1\boldsymbol{P} & \cdots & i_1\boldsymbol{P}^{m_1-1} & \cdots & i_r & i_r\boldsymbol{P} & \cdots & i_r\boldsymbol{P}^{m_r-1} \\ i_1\boldsymbol{P} & i_1\boldsymbol{P}^2 & \cdots & i_1 & \cdots & i_r\boldsymbol{P} & i_r\boldsymbol{P}^2 & \cdots & i_r \end{matrix} \right\downarrow \circ_{lr}$$

$$\left\downarrow \begin{matrix} i_1\boldsymbol{P} & \cdots & i_1\boldsymbol{P}^{m_1-1} & i_1 & \cdots & i_r\boldsymbol{P} & \cdots & i_r\boldsymbol{P}^{m_r-1} & i_r \\ j_1\boldsymbol{Q} & \cdots & j_1\boldsymbol{Q}^{m_1-1} & j_1 & \cdots & j_r\boldsymbol{Q} & \cdots & j_r\boldsymbol{Q}^{m_r-1} & j_r \end{matrix} \right\downarrow$$

Quindi $\boldsymbol{P}$ e $\boldsymbol{Q}$ appartengono alla stessa classe di coniugio ∎

B16 e.11 Dunque le permutazioni di Sym_n costituenti una classe di coniugio sono caratterizzate dall'avere una stessa struttura ciclica, cioè dal contenere lo stesso numero α_1 di cicli a un elemento (punti fissi), lo stesso numero α_2 di cicli a due elementi (scambi), . . . , lo stesso numero α_n di cicli ad n elementi.
Questi α_i sono numeri interi positivi o nulli caratterizzati dal soddisfare l'equazione:

(1) $$\sum_{i=1}^{n} i\,\alpha_i \ = \ n\ .$$

Una classe di coniugio di Sym_n risulta completamente definita dando una sequenza $\underline{\alpha} = \langle \alpha_1, ..., \alpha_n \rangle$ di n interi naturali le cui componenti verificano l'equazione precedente.
Riferendosi a tale allineamento, la classe di coniugio viene solitamente denotata con $\mathcal{C}^{(\underline{\alpha})}$.

B16 e.12 L'insieme $\boldsymbol{Cycl}_{n,2}$ degli scambi (o trasposizioni) di Sym_n si denota anche con $\boldsymbol{Excgs}_n$ e si è visto che $|\boldsymbol{Excgs}_n| = \dfrac{n(n-1)}{2}$.
Evidentemente uno scambio coincide con il proprio inverso,

(1) $$\langle_{cy} i, j\rangle^{-1} \ = \ \langle_{cy} i, j\rangle\ .$$

Gli scambi quindi sono permutazioni involutorie; più precisamente l'insieme delle permutazioni involutorie di un gruppo simmetrico è costituito dalle permutazioni esprimibili come prodotti di scambi mutuamente disgiunti-t.

La permutazione inversa di una ciclica è anch'essa ciclica e può esprimersi con la riflessa della notazione sequenziale:

(2) $$\left\langle_{cy} i_1, i_2, ..., i_{r-1}, i_r\right\rangle^{-1} \ = \ \left\langle_{cy} i_r, i_{r-1}, ..., i_2, i_1\right\rangle\ .$$

Questa formula si giustifica facilmente osservando la raffigurazione dei cicli mediante digrafi.

(1) Prop.: L'inversa di una permutazione $\boldsymbol{P}^{-1}$ appartiene alla stessa classe di cui fa parte $\boldsymbol{P}$.

Dim.: Infatti da una espressione di $\boldsymbol{P}$ come prodotto di cicli disgiunti

$$\boldsymbol{P} = (i_{11}\ i_{12}\ \cdots\ i_{1m_1}) \circ (i_{21}\ i_{22}\ \cdots\ i_{2m_2}) \circ \ldots \circ (i_{r1}\ i_{r2}\ \cdots\ i_{rm_r})\ ,$$

si ricava l'espressione analoga

$$\boldsymbol{P^{-1}} = (i_{1m_1}\ \cdots\ i_{12}\ i_{11}) \circ (i_{2m_2}\ \cdots\ i_{22}\ i_{21}) \circ \ldots \circ (i_{rm_r}\ \cdots\ i_{r2}\ i_{r1})\ ,$$

caratterizzata dalla stessa partizione.i di n ∎

B16 e.13 Prop. Il numero delle classi di coniugio di Sym_n è dunque uguale al numero delle partizioni-i di n, numero che esamineremo in D23 e che denotiamo con $Prti(n)$.

Adottando la definizione $Prti(0) := 1$ si ottiene:

$$Prti(n) \ = \sum_{1 \leq \frac{3k^2 \pm k}{2} \leq n} (-)^{k-1} Prti\left(n - \frac{3k^2 \pm k}{2}\right)\ .$$

B16 e.14 Prop. Si pone naturalmente il problema di determinare il cardinale di ciascuna classe di coniugio: più precisamente si vuole determinare il numero di permutazioni che contengono α_1 cicli di lunghezza uno, α_2 cicli binari, …, α_n cicli di lunghezza n.

Per essa troveremo in D23 una formula classica.

(1) Prop.: Formula di Cauchy

$$|\mathcal{C}^{(\underline{\alpha})}| \ = \ \frac{n!}{\prod_{i=1}^{n} i^{\alpha_i} \alpha_i!}\ .$$

Per esempio, per $n = 3$ e $\alpha = (1, 1, 0)$, il numero di permutazioni con un ciclo di lunghezza 1 e un ciclo di lunghezza 2 sono:

$$|\mathcal{C}^{(1,1,0)}| = \frac{3!}{1 \cdot 1! \cdot 2 \cdot 1!} = 3,$$

Queste permutazioni sono:

$$a \ = \ (1\ 2)(3) \qquad b \ = \ (1\ 3)(2) \qquad c \ = \ (3\ 2)(1).$$

B16 f. classificazioni di funzioni finite e di permutazioni

B16 f.01 In questa sezione consideriamo due insiemi finiti A con $|A| = k$ e B con $|B| = m$, l'insieme delle funzioni di A in B $\{Afunbc B\} = B^A$ e i casi particolari dell'insieme **Endo**$[A] = A^A$ delle endofunzioni di A e dell'insieme **Perm**$[A] = A!$ delle permutazioni di A.

I due insiemi saranno visti come insiemi generici costituiti da elementi da considerare oggetti distinguibili ma senza caratteristiche individuali che possono interessare; peraltro ci riserviamo di trattare loro repliche mutuamente indistinguibili e quondi da rappresentare con uno stesso simbolo.
Inoltre faremo riferimento ad un loro possibile ordine totale espresso dai simboli $\prec$, $\preceq$, $\succ$ e $\succeq$.

In alcuni passaggi risulterà più agevole considerare i casi particolari $A = \{1, 2, ..., k\}$ e $B = \{1, 2, ..., m\}$, senza che questo riduca la generalità dei risultati.

B16 f.02 Lo scopo di questa sezione è lo studio di problemi di classificazione riguardanti B^A, A^A e $A!$ iniziando da considerazioni generali sulle classificazioni in matematica.

Per dare un primo chiarimento sulle classificazioni cominciamo con definire classificazione dell'insieme $A!$ ogni partizione di $A!$ in sottoinsiemi di permutazioni, le classi della classificazione, in ciascuno dei quali si trovano permutazioni con caratteristiche simili facilmente riconoscibili e proficuamente utilizzabili nelle applicazioni delle permutazioni in esame.

Definizioni assai simili si possono formulare Per le classificazioni degli insiemi A^A e $A!$ si possono formulare definizioni del tutto simili: basta cambiare la parola permutazioni con endofunzioni o funzioni.

La esigenza di classificazioni utilizzabili per le applicazioni all'interno e all'esterno della matematica si può ulteriormente ampliare a insiemi U di tanti tipi di oggetti matematici.

Si tratta di trovare partizioni di U nelle cui classi si trovano oggetti con caratteristiche simili tanto da rendere questi oggetti trattabili equivalentemente da deduzioni utili all'avanzamento delle conoscenze e da algoritmi utili per risolvere problemi significativi.

Queste prospettive si possono considerare rivolte a famiglie illimitate di insiemi finiti di oggetti discreti della forma $\langle i \in \mathbb{N} :| U_i \rangle$ o di una forma che presenta più indici.

Ad esempio si possono prospettare classificazioni di partizioni di insiemi finiti di dato cardinale, partizioni di interi positivi, di grafi con numeri finiti di nodi, di grammatiche con determinati insiemi di caratteri terminali e ausiliari, di sistemi di codifica, di funzioni speciali, ...

B16 f.03 Occorre segnalare chela prospettiva della classificazione si può sviluppare con una relativa facilità per successioni di insiemi che si possono visitare per stabilire le caratteristiche discriminanti utili alla classificazione degli oggetti con algoritmi poco impegnativi come accade a funzioni finite e a partizioni di insiemi finiti.

Per classificare altri insiemi finiti servono invece algoritmi di visita e di deteminazione delle caratteristiche discriminanti più complessi e costosi e anche algoritmi non ancora chiariti.

Occorre aggiungere che è auspicabile che le caratteristiche che accomunano le partizioni di una classe di una classificazione non dipendano dalle peculiarità delle entità sulle quali si basano gli oggetti da classificare: questa indipendenza infatti rende i risultati sulla classificazione più ampiamente utilizzabili..
Questa indipendenza è evidente per gli insiemi A e B sui quali agiscono le funzioni finite, le endofunzioni e le permutazioni. In molti altri casi resta da stabilire.

B16 f.04 La classificazione di maggior rilievo delle permutazioni di $A!$ riguarda le loro decomposizione in cicli, partizione di $A!$ che fa riferimento alle partizioni di A.
Più grossolana di questa è la partizione che distingue tra del equivalente alla mente e all'interno di questa Una classificazione ossia una partizione del loro insieme $A!$, riguarda i diversi numeri di punti fissi le permutazioni possono presentare.
Denotiamo a questo scopo con $\mathsf{PermNft}(A, f)$ l'insieme delle permutazioni di A con f punti fissi per $f = 0, 1, 2, ..., k$.
Evidentemente $\mathsf{Perm}(A, k) = \bigcup_{f=0}^{:k} \mathsf{PermNft}(A, f)$.

B16 f.05 Riferiamoci ancora all'insieme finito A di cardinale k. Si dice **sconvolgimento** di A una permutazione di A priva di punti fissi.

Gli sconvolgimenti relativi agli insiemi con 2, 3 e 4 elementi sono forniti dalle seguenti notazioni semplificate:
$\mathsf{Drng}(\{1,2\}) = \{(12)\}$, $\mathsf{Drng}(\{1,2,3\}) = \{(123),(321)\}$,
$\mathsf{Drng}(\{1,2,3,4\}) = \{(12)(34),(13)(24),(14)(23),(1234),(1243),(1324),(1342),(1423),(1432)\}$

In alternativa a sconvolgimento si usano anche i termini dismutazione e permutazione completa, mentre il corrispondente termine inglese è **derangement**.

L'insieme degli sconvolgimenti di A lo denotiamo con $\mathsf{Drng}(A)$ o concisamente con $A_{¡}$.

Per il suo cardinale scriviamo $\mathsf{DrngN}(A) := \mathsf{Drng}(A) := |A_{¡}|$.

Evidentemente il numero degli sconvolgimenti di un insieme finito A dipende solo dal suo cardinale $k = |A|$.
Interessa quindi conoscere la dipendenza da k del numero degli sconvolgimenti degli insiemi di k elementi che denotiamo con ${}_{¡k}$ o anche con $k_{¡}$.
Per queste numerosità taluni usano il termine "subfattoriale " e la notazione $!k$ o la D_k.

B16 f.06 Ci proponiamo ora di trovare una formula enumeratrice per Dopo aver osservato che ogni singoletto non possiede sconvolgimenti, ossia che ${}_{¡1} = 0$, risulta opportuno stabilire che ${}_{¡0} = 1$, in accordo con la assunzione che sia $0! = 1$, ossia che l'insieme vuoto possegga una permutazione e osservando che questa non presenta alcun punto fisso.

Anche per questa funzione del genere $\{\mathbb{N}funbc\mathbb{N}\}$ si trova una ricorrenza piuttosto semplice.

Consideriamo un insieme A di k elementi, due oggetti estranei x_1 e x_2 e gli insiemi $A_1 := A \dot\cup \{x_1\}$, $A_2 := A \dot\cup \{x_2\}$ e $A_{12} := A \dot\cup \{x_1, x_2\}$.
Esaminiamo i diversi sconvolgimenti $\sigma \in Drng[A_{12}]$ ripartendoli in due sottoinsiemi R_1 e R_2.
In R_1 poniamo gli sconvolgimenti σ per i quali $\sigma(x_1) = y$ e scriviamo $y := \sigma(x_1)$. Se $y \neq x_2$
Abbiamo quindi la relazione tra i cardinali

$$(k+2)_{¡} = (k+1)\big((k+1)_{¡} + k_{¡}\big) .$$

Questa insieme alle uguaglianze $0_{¡} = 1$ e $1_{¡} = 0$ costituisce la ricorrenza che consente di calcolare l'intera successione.

$$k_{¡} = \Big\downarrow \begin{array}{cccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \dots \\ 1 & 0 & 1 & 2 & 9 & 44 & 265 & 1854 & 14833 & 133496 & 1334961 & 14684570 & 176214841 & \dots \end{array} \Big\downarrow$$

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php