2. Insiemi ed elementi di calcolo combinatorio

Marco Liverani

Università degli Studi Roma Tre
Dipartimento di Matematica e Fisica
Corso di Laurea in Matematica
E-mail liverani@mat.uniroma3.it

Marzo 2014

Revisione del 2 marzo 2014.

1 Generalità sugli insiemi

Un **insieme** è una collezione di oggetti distinti, nessuno dei quali è l'insieme stesso. Ad esempio l'insieme A può essere composto dai seguenti elementi $A = \{a, 27, 3.14, \pi\}$, ma non può contenere come elemento lo stesso insieme A. Se x è un elemento dell'insieme A scriveremo $x \in A$, viceversa per indicare che x non appartiene all'insieme A utilizzeremo la notazione $x \notin A$. Un insieme può essere definito elencando i suoi elementi, come nell'esempio precedente, oppure descrivendo una legge, una condizione, in base alla quale possono essere individuati con certezza gli elementi dell'insieme stesso, distinguendoli senza ambiguità dagli elementi che invece non appartengono all'insieme. Ad esempio, se volessimo definire l'insieme A come l'insieme dei numeri reali positivi, non potendo elencarli tutti, potremmo scrivere più semplicemente $A = \{x \in \mathbb{R} : x \geq 0\}$.

Quando si definisce un insieme elencando i suoi elementi, l'ordine con cui viene composto tale elenco è del tutto indifferente: ad esempio gli insiemi $A = \{1, 2, 3\}$ e $A' = \{3, 1, 2\}$ sono identici. Più in generale infatti possiamo dire che due insiemi A e A' sono uguali se e solo se contengono gli stessi elementi.

Un **sottoinsieme** B di un insieme A è un insieme i cui elementi appartengono anche all'insieme A; per indicare che B è un sottoinsieme di A si utilizza la notazione $B \subseteq A$. Un insieme B è un **sottoinsieme proprio** di A se $B \subseteq A$ ed esiste almeno un elemento di A che non appartiene a B; in questo caso scriveremo $B \subset A$. Non bisogna confondere il concetto di "elemento di un insieme" con quello di "sottoinsieme": è molto importante osservare che se $B \subset A$ è profondamente sbagliato scrivere $B \in A$, visto che B non è un *elemento* di A, ma è una *collezione di alcuni elementi* di A; quindi è corretto affermare che se $B \subset A$ allora per ogni $x \in B$ risulta $x \in A$.

L'insieme privo di elementi è l'**insieme vuoto** e si indica con il simbolo $\emptyset$. Qualunque sia l'insieme A, risulta $\emptyset \subseteq A$.

Nella definizione di insieme è importante precisare che un insieme A non può contenere se stesso come elemento. Se venisse rimosso questo vincolo dalla definizione di insieme, si andrebbe incontro ad un famoso paradosso, formulato da Bertrand Russell nel 1902. Supponiamo infatti che un insieme A possa includere anche se stesso tra gli elementi che lo compongono: ad esempio sia $A = \{1, 2, 3, A\}$. Chiamiamo questo tipo di insieme, che contiene anche se stesso come elemento, un insieme "straordinario", mentre chiameremo "ordinario" qualunque insieme che non contenga se stesso come elemento (ad esempio $B = \{3, 6, 9, 12\}$ è un insieme "ordinario", secondo questa definizione). Sia $\mathcal{S}$ la collezione di tutti gli insiemi "ordinari". Ci chiediamo se $\mathcal{S}$ sia un insieme ordinario oppure no: purtroppo, se ammettiamo l'esistenza degli insiemi "straordinari", qualunque risposta a tale quesito ci porta ad una contraddizione. Infatti se ammettessimo che $\mathcal{S}$ è un insieme "ordinario", allora per come è stato definito $\mathcal{S}$ dovrebbe anche contenere se stesso e dunque sarebbe "straordinario"; viceversa, se volessimo affermare che $\mathcal{S}$ è un insieme "straordinario" allora, sempre per la definizione stessa di $\mathcal{S}$, risulterebbe che $\mathcal{S}$ non contiene se stesso tra i suoi elementi, e quindi sarebbe un insieme "ordinario". Insomma, in ogni caso si giunge ad una contraddizione, $\mathcal{S}$ non può essere né "ordinario" né "straordinario". Dunque non possiamo far altro che rafforzare la definizione di insieme, stabilendo appunto che un insieme è una collezione di oggetti fra loro distinti e tali che nessuno di essi sia l'insieme stesso.

2 Tecniche di dimostrazione

Nel seguito cercheremo, per quanto possibile, di mantenere la trattazione degli argomenti che saranno presentati ad un livello che possa essere al tempo stesso accessibile e comprensibile, quindi con un'attenzione di carattere "didattico", ma al tempo stesso rispettando un certo rigore, necessario per l'applicazione del metodo matematico. In particolare spesso forniremo una dimostrazione rigorosa delle affermazioni che saranno proposte. La *dimostrazione* è una delle basi del metodo scientifico adottato in Matematica: se è vero che spesso un buon esempio o un controesempio brillante possono aiutarci a comprendere la validità e l'importanza di una determinata affermazione, è solo con una dimostrazione rigorosa che si può garantire che la stessa affermazione sia vera, al di là di ogni possibile dubbio. Un controesempio è sufficiente per smentire un'affermazione, ma un esempio non può certo bastare per provare una congettura: è necessaria una dimostrazione. Nel seguito, per non appesantire la trattazione, cercheremo di ricorrere allo strumento della dimostrazione solo nei casi in cui la validità dell'affermazione non risulti evidente; in questi casi, anche perché siamo convinti del valore *didattico* di una buona dimostrazione, ricorreremo ad una prova in termini più rigorosi e formali.

Per costruire una dimostrazione spesso si ricorre a delle tecniche ben consolidate: fermo restando che un teorema o una proposizione possono essere dimostrate proponendo qualunque ragionamento di carattere deduttivo o induttivo, in genere ricorreremo ad una modalità di dimostrazione che può essere ricondotta alle tecniche di *dimostrazione per assurdo*, di *dimostrazione per induzione* o di *dimostrazione costruttiva*.

Per dimostrare che una determinata proprietà $\mathcal{P}(x)$ vale per ogni $x \in A$, la tecnica di **dimostrazione per assurdo** parte dalla supposizione che, al contrario di quanto è stato affermato nella tesi del teorema, esista un elemento $\bar{x} \in A$ per il quale la proprietà $\mathcal{P}$ non sia valida; la dimostrazione procede poi con una serie di passaggi deduttivi per mostrare come la conseguenza di tale ipotesi aggiuntiva porti inevitabilmente a contraddire una delle ipotesi del teorema. Dunque, fissate determinate ipotesi, la tesi non può essere smentita per nessun elemento $\bar{x} \in A$ e quindi la tesi risulta valida per ogni elemento di A.

La **dimostrazione costruttiva**, basandosi sulle ipotesi fornite con l'affermazione del teorema che si intende dimostrare, mira a fornire gli strumenti necessari a costruire l'insieme per il quale tale affermazione deve risultare valida. In questo modo il teorema risulta automaticamente dimostrato provando che l'insieme frutto del procedimento costruttivo messo in atto nella dimostrazione, coincide con l'insieme su cui si voleva dimostrare la validità dell'affermazione formulata nella tesi del teorema.

La tecnica di **dimostrazione per induzione**, infine, si basa sull'omonimo **principio di induzione** che possiamo sintetizzare nel seguente Teorema.

Teorema 1 (Principio di induzione)**.** *Per ogni intero $n \geq 0$ si consideri l'affermazione $\mathcal{A}(n)$; inoltre si supponga che:*

1. *$\mathcal{A}(0)$ è vera;*
2. *per ogni $n > 0$, se $\mathcal{A}(k)$ è vera per ogni $k = 0, 1, \ldots, n-1$, allora è vera anche $\mathcal{A}(n)$.*

Allora $\mathcal{A}(n)$ è un'affermazione vera per ogni $n \geq 0$.

Dimostrazione. La dimostrazione procede per assurdo e si basa sull'assioma del buon ordinamento che afferma che ogni insieme non vuoto di interi positivi possiede un elemento minimo: in altri termini l'assioma del buon ordinamento afferma che se $A \subseteq \mathbb{N}$, $A \neq \emptyset$, allora esiste $m \in A$ tale che $m \leq a$ per ogni $a \in A$.

Sia $X \subseteq \mathbb{N}$ l'insieme degli interi $x \geq 0$ per cui $\mathcal{A}(x)$ è falsa. Supponiamo per assurdo che $X \neq \emptyset$; sia quindi $m \in X$ l'elemento minimo di X. Allora, per la definizione di X, l'affermazione $\mathcal{A}(m)$ è falsa e quindi $m > 0$ perché per l'ipotesi (1) $\mathcal{A}(0)$ è vera; inoltre $\mathcal{A}(k)$ è vera per ogni $k < m$, perché m è l'elemento minimo dell'insieme degli interi per cui l'affermazione $\mathcal{A}$ non è vera. Ma allora, per l'ipotesi (2), anche $\mathcal{A}(m)$ è vera e quindi aver ipotizzato l'esistenza di un intero $m > 0$ per il quale tale affermazione non fosse vera, ci ha condotto ad una contraddizione. Pertanto possiamo concludere che, se sono verificate le ipotesi (1) e (2), l'affermazione $\mathcal{A}(x)$ è vera per ogni intero $x \geq 0$. □

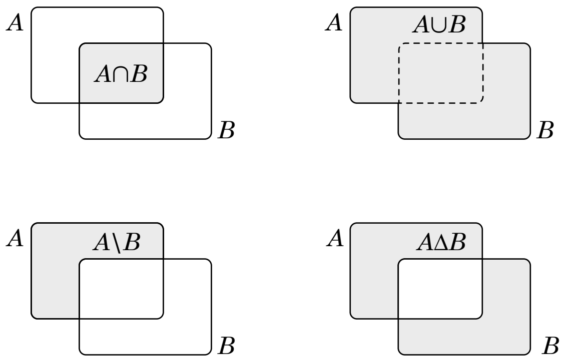

Figura 1: Una rappresentazione con i diagrammi di Venn delle operazioni di intersezione, unione, differenza e differenza simmetrica tra gli insiemi A e B

3 Operazioni sugli insiemi

È possibile definire un insieme di operazioni fondamentali sugli insiemi, che consentono di ottenere altri insiemi a partire da quelli su cui si applica l'operatore stesso. L'**intersezione** tra due insiemi A e B è l'insieme di tutti gli elementi che appartengono contemporaneamente sia ad A che a B e si indica con la notazione $A \cap B$; l'insieme intersezione può essere definito formalmente come segue: $A \cap B = \{x : x \in A \text{ e } x \in B\}$.

Due insiemi A e B si dicono **disgiunti** se la loro intersezione è l'insieme vuoto. Naturalmente se, dati due insiemi A e B, risulta $A \subseteq B$, allora $A \cap B = A$; è vero anche il viceversa: $A \cap B = A \implies A \subseteq B$.

L'operazione di intersezione tra insiemi può essere facilmente generalizzata ad una famiglia di n insiemi $A_1, A_2, \ldots, A_n$:

$$\bigcap_{i=1,2,\ldots,n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_i \text{ per ogni } i = 1, 2, \ldots, n\}$$

L'**unione** tra due insiemi A e B è l'insieme $A \cup B$ costituito da tutti gli elementi di A e da tutti gli elementi di B; formalmente possiamo scrivere $A \cup B = \{x : x \in A \text{ o } x \in B\}$. Naturalmente, trattandosi di un insieme, tutti i suoi elementi sono distinti, per cui se un determinato elemento y appartiene sia all'insieme A che all'insieme B (ossia, se l'intersezione tra A e B non è vuota), allora y comparirà in $A \cup B$ una sola volta. Ad esempio se $A = \{1, 2, 4, 8\}$ e $B = \{2, 3, 4, 5\}$ allora risulta $A \cap B = \{2, 4\}$ e $A \cup B = \{1, 2, 3, 4, 5, 8\}$.

Anche l'unione tra insiemi può essere generalizzata ad una famiglia di n insiemi $A_1, A_2, \ldots, A_n$:

$$\bigcup_{i=1,2,\ldots,n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_i \text{ per almeno un } i = 1, 2, \ldots, n\}$$

La **differenza** tra due insiemi A e B è l'insieme $A \setminus B$ dato da tutti gli elementi di A che non appartengono a B: $A \setminus B = \{x : x \in A \text{ e } x \notin B\}$. Ad esempio se $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{2, 4, 6, 8\}$ allora $A \setminus B = \{1, 3, 5\}$.

La **differenza simmetrica** tra due insiemi A e B è l'insieme $A \Delta B$ costituito da tutti gli elementi che appartengono ad A oppure a B, ma non ad entrambi: $A \Delta B = \{x : x \in A \text{ o } x \in B \text{ e } x \notin A \cap B\}$. Vale quindi l'identità $A \Delta B = (A \cup B) \setminus (A \cap B)$. Se consideriamo ad esempio i due insiemi $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{2, 4, 6, 8\}$ allora $A \Delta B = \{1, 3, 5, 8\}$.

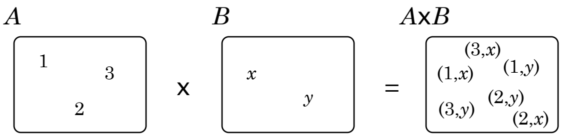

Figura 2: Rappresentazione del prodotto cartesiano tra gli insiemi A e B con diagrammi di Venn

Infine, dati due insiemi A e B con $A \subseteq B$, si definisce l'insieme **complementare** di A rispetto a B come la differenza $B \setminus A$. Se è definito un *insieme universo* U come l'insieme di tutti i possibili elementi, allora possiamo definire il **complemento** di un insieme A, indicato con $\bar{A}$ o A^c, come l'insieme di tutti gli elementi che non appartengono all'insieme A: $\bar{A} = \{x : x \notin A\}$.

L'**insieme delle parti** di un insieme A si denota con $\wp(A)$ ed è costituito da tutti i sottoinsiemi di A: $\wp(A) = \{A' : A' \subseteq A\}$. Ad esempio se $A = \{1,2,3\}$ l'insieme delle parti di A è $\wp(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A\}$.

Infine, una **partizione** dell'insieme A è una collezione di sottoinsiemi di A a due a due disgiunti, tali che la loro unione coincida con A; in termini più formali possiamo scrivere che una partizione P_A dell'insieme A è l'insieme $\{A_1, A_2, \dots, A_n : A_i \subseteq A \text{ e } A_i \cap A_j = \emptyset \text{ per ogni } i \neq j \text{ e } \cup_{i=1,2,\dots,n} A_i = A\}$. Ad esempio, se $A = \{1,2,3,4,5\}$ allora una delle partizioni di A è data dalla collezione di insiemi $A_1 = \{1,3\}, A_2 = \{2\}, A_3 = \{4,5\}$; infatti $A_1 \cap A_2 = \emptyset$, $A_2 \cap A_3 = \emptyset$, $A_1 \cap A_3 = \emptyset$ e $A = A_1 \cup A_2 \cup A_3$.

4 Corrispondenze e relazioni tra insiemi

Il **prodotto cartesiano** tra due insiemi A e B è l'insieme $A \times B$ di tutte le coppie composte da un elemento di A e da un elemento di B: $A \times B = \{(a,b) : a \in A \text{ e } b \in B\}$. Ad esempio, se si considerano gli insiemi $A = \{1,2,3\}$ e $B = \{x,y\}$, allora il prodotto cartesiano è

$$A \times B = \{(1,x), (1,y), (2,x), (2,y), (3,x), (3,y)\}.$$

In alcuni casi è utile considerare il prodotto cartesiano di un insieme A con se stesso: $A \times A = \{(a,b) : a,b \in A\}$; il prodotto cartesiano di un insieme A per se stesso può essere indicato anche con la notazione A^2. Gli elementi del prodotto cartesiano sono *coppie ordinate*: l'ordine degli elementi è importante, perché il primo membro della coppia è un elemento del primo insieme del prodotto cartesiano, mentre il secondo membro della coppia è un elemento del secondo insieme; in generale quindi, a meno che non sia diversamente specificato, le coppie (a,b) e (b,a) sono da considerasi differenti.

Il prodotto cartesiano può essere generalizzato, considerando il prodotto di tre o più insiemi: $A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, \dots, a_k) : a_i \in A_i, i = 1,2,\dots,k\}$. Se gli insiemi $A_1, A_2, \dots, A_k$ sono tutti uguali, ossia se $A_i = A$ per ogni $i = 1,2,\dots,k$, allora il prodotto cartesiano $A \times A \times \cdots \times A$ può essere indicato con la notazione A^k.

Una **corrispondenza** tra due insiemi A e B è una associazione degli elementi del primo insieme (tutti gli elementi o solo una parte di essi), detto **dominio** della corrispondenza, con alcuni elementi del secondo insieme, detto **codominio** della corrispondenza. Ad esempio possiamo costruire una corrispondenza tra l'insieme dei cittadini italiani e l'insieme delle città francesi, associando agli elementi del primo insieme (quello degli italiani), le città che hanno visitato in Francia. Naturalmente non tutti gli italiani saranno messi in corrispondenza con una città perché non tutti gli italiani hanno visitato la Francia, mentre ne esisteranno alcuni associati a più d'una città; d'altra parte è possibile (magari

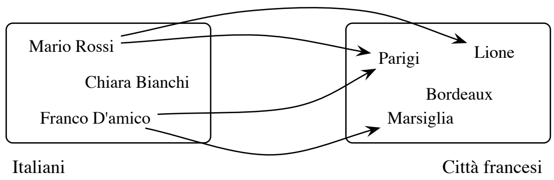

Figura 3: Un esempio semplificato di corrispondenza tra l'insieme dei cittadini italiani e l'insieme delle città francesi

è improbabile, ma pur sempre possibile) che alcune città francesi non siano state visitate da nessun italiano, mentre in generale le città della Francia saranno associate a molti cittadini italiani.

Una corrispondenza fra gli insiemi A e B, quindi, associa fra loro alcune coppie di elementi di A e di B. Allora, in modo più formale, possiamo dire che una corrispondenza tra due insiemi A e B è un sottoinsieme del prodotto cartesiano $A \times B$. Una corrispondenza tra gli insiemi A e B si dice **biunivoca** se ad ogni elemento di A corrisponde uno ed un solo elemento di B, e viceversa.

Nel caso particolare in cui il dominio ed il codominio di una corrispondenza coincidano, allora si parla di **relazione**, o di **relazione binaria**, definita sugli elementi di un insieme. Se è definita la relazione ρ sull'insieme A, allora per indicare che gli elementi $x, y \in A$ sono in relazione ρ fra di loro, scriveremo $x\rho y$.

Data una relazione ρ sull'insieme A, se per ogni elemento $a \in A$ risulta che a è in relazione con se stesso ($a\rho a$), allora si dice che la relazione è **riflessiva**. Ad esempio, la relazione "essere divisibile" definita sull'insieme $\mathbb{R}^+$ dei numeri reali positivi è riflessiva, infatti ogni $x > 0$, $x \in \mathbb{R}$, è divisibile per se stessa. Al contrario, la relazione "essere maggiore di" definita sullo stesso insieme non è riflessiva, infatti per ogni $x \in \mathbb{R}^+$ risulta $x \not> x$.

Una relazione ρ su A è **simmetrica** se, per ogni $a, b \in A$, $a\rho b$ implica che $b\rho a$. Ad esempio la relazione "essere cugini" è simmetrica, infatti se Gino è cugino di Pino, allora questo implica che Pino sia cugino di Gino. Se invece il fatto che a sia in relazione con b implica che sicuramente b non è in relazione con a, allora la relazione si dice **antisimmetrica**. Ad esempio la relazione "essere figlio" è antisimmetrica: infatti se Francesca è figlia di Maria, allora di certo Maria non è figlia di Francesca (a meno di omonimie tra nonna e nipote).

Infine una relazione ρ sull'insieme A si dice **transitiva** se, per ogni $a, b, c \in A$ tali che $a\rho b$ e $b\rho c$, questo implica che $a\rho c$. Ad esempio la relazione "essere discendente" è simmetrica, infatti se Aldo è discendente di Bruno e Bruno è discendente di Carlo, allora Aldo è discendente di Carlo.

Una relazione che gode delle tre proprietà riflessiva, simmetrica e transitiva è una **relazione d'equivalenza**. Ad esempio la relazione "essere parenti" è una relazione d'equivalenza: infatti ognuno è in qualche modo parente di se stesso (riflessività); inoltre se a è parente di b allora è vero anche il viceversa (simmetria); infine se a è parente di b e b è parente di c allora a è parente di c (transitività). Se su un insieme A è definita una relazione d'equivalenza ρ, si definisce la **classe di equivalenza** di $a \in A$ e la si indica con $[a]_\rho$, come il sottoinsieme di A i cui elementi sono in relazione con a. Naturalmente $a \in [a]_\rho$ per la riflessività della relazione; inoltre, fissata una relazione di equivalenza ρ, ogni elemento $x \in A$ appartiene ad una sola classe di equivalenza: infatti se $a, b \in A$, come abbiamo visto $a \in [a]_\rho$; se $a \in [b]_\rho$ allora, per la simmetria della relazione risulterebbe anche $b \in [a]_\rho$ e per la transitività se $c \in [b]_\rho$ allora risulta anche $c \in [a]_\rho$; per cui, in conclusione, se $a \in [b]_\rho$ allora le due classi di equivalenza $[a]_\rho$ e $[b]_\rho$ coincidono.

Proposizione 1. *Le classi d'equivalenza definite da una relazione d'equivalenza ρ sull'insieme A,* *costituiscono una partizione di A.*

Dimostrazione. Per la definizione di classe d'equivalenza ogni elemento $x \in A$ appartiene ad una classe di equivalenza definita su A dalla relazione ρ; infatti risulta $x \in [x]_\rho \subseteq A$. Dunque l'insieme A è dato dall'unione delle classi di equivalenza definite su di esso mediante la relazione ρ.

Inoltre se $x, y \in A$ e $[x]_\rho \neq [y]_\rho$, allora $[x]_\rho \cap [y]_\rho = \emptyset$. Infatti, se $[x]_\rho \neq [y]_\rho$ allora esiste almeno un elemento $z \in [x]_\rho$ tale che $z \notin [y]_\rho$, o viceversa. Senza perdita di generalità supponiamo quindi che $z \in [x]_\rho$ e $z \notin [y]_\rho$. Dalla proprietà transitiva della relazione ρ segue che per ogni $w \in [x]_\rho$, risulta $w \notin [y]_\rho$; infatti se $w \in [x]_\rho$ allora $w\rho z$ e quindi, siccome z non è in relazione con y non può esserlo neanche w. Per l'arbitrarietà di w segue che nessun elemento di $[x]_\rho$ appartiene a $[y]_\rho$ e quindi le due classi di equivalenza sono disgiunte. $\square$

Possiamo osservare che, data una relazione d'equivalenza ρ definita sull'insieme A, se $x, y \in A$ e $[x]_\rho \subseteq [y]_\rho$ allora $[x]_\rho = [y]_\rho$. Infatti, $x \in [y]_\rho$ e se per assurdo esistesse un elemento $z \in [y]_\rho$ tale che $z \notin [x]_\rho$, allora per transitività dovrebbe risultare $x\rho z$ e questo fatto sarebbe in contraddizione con $z \notin [x]_\rho$. Per cui tutti gli elementi di $[y]_\rho$ sono in relazione ρ con x e quindi le due classi di equivalenza, $[x]_\rho$ e $[y]_\rho$, coincidono.

Una relazione binaria ρ su un insieme A si dice **totale** se, per ogni $x, y \in A$, risulta $a\rho b$ o $b\rho a$ (o entrambe le relazioni); in altri termini la relazione ρ è totale su A se ogni coppia di elementi di A è in relazione.

Una relazione binaria ρ è **antisimmetrica** se, per ogni $x, y \in A$, $x\rho y$ e $y\rho x$ implica $x = y$. Ad esempio la relazione di inclusione tra gli insiemi di una famiglia $\mathcal{A} = \{A_1, A_2, \ldots, A_k\}$ gode della proprietà antisimmetrica: infatti se $A_i \subseteq A_j$ e $A_j \subseteq A_i$ allora risulta $A_i = A_j$. La stessa relazione di inclusione invece non è necessariamente una relazione totale su $\mathcal{A}$; infatti, presi due insiemi A_i e A_j elementi di $\mathcal{A}$, non è detto che valga una delle due relazioni $A_i \subseteq A_j$ o $A_j \subseteq A_i$. La relazione di inclusione su $\mathcal{A}$ è una relazione totale solo se $\mathcal{A}$ è una famiglia di insiemi *telescopici*, ossia tale che gli insiemi sono tutti contenuti l'uno nell'altro, come gli elementi di un telescopio: $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \subseteq A_k$. In tal caso la relazione è totale e valgono le relazioni riflessiva ($A_i \subseteq A_i$), antisimmetrica ($A_i \subseteq A_j$ e $A_j \subseteq A_i \implies A_i = A_j$) e transitiva ($A_i \subseteq A_j$ e $A_j \subseteq A_h \implies A_i \subseteq A_h$).

Una **relazione d'ordine** ρ sull'insieme A è una relazione che gode delle proprietà riflessiva, antisimmetrica e transitiva. Ad esempio la relazione di inclusione sull'insieme delle parti $\wp(\mathbb{N})$ dell'insieme dei numeri naturali $\mathbb{N}$ è una relazione d'ordine. Infatti risulta $A \subseteq A$ per ogni $A \subseteq \mathbb{N}$ (riflessività), $A \subseteq B$ e $B \subseteq A \implies A = B$ per ogni $A, B \subseteq \mathbb{N}$ (antisimmetria) e $A \subseteq B$ e $B \subseteq C \implies A \subseteq C$ per ogni $A, B, C \subseteq \mathbb{N}$ (transitività). Tale relazione d'ordine non è totale, perché come abbiamo già visto, non è sempre possibile mettere in relazione di inclusione fra loro due qualsiasi sottoinsiemi di $\mathbb{N}$.

Una relazione d'ordine totale è rappresentata dalla relazione "minore o uguale" ($\leq$) sull'insieme $\mathbb{N}$. Infatti tale relazione, oltre ad essere riflessiva ($x \leq x\ \forall x \in \mathbb{N}$), antisimmetrica ($x \leq y$ e $y \leq x \implies x = y\ \forall x, y \in \mathbb{N}$) e transitiva ($x \leq y$ e $y \leq z \implies x \leq z\ \forall x, y, z \in \mathbb{N}$), è anche una relazione totale, infatti per ogni coppia $x, y \in \mathbb{N}$ è possibile stabilire se $x \leq y$ o se $y \leq x$. Un insieme su cui è definita una relazione d'ordine si dice **insieme ordinato**; se la relazione d'ordine è totale, allora l'insieme si dirà **totalmente ordinato**, altrimenti diremo che l'insieme è **parzialmente ordinato** (in inglese *poset*, per *partially ordered set*).

5 Cardinalità

La **cardinalità** di un insieme è data dal numero di elementi che contiene. La cardinalità dell'insieme A si indica con la notazione $|A|$. Naturalmente la cardinalità dell'insieme vuoto è zero: $|\emptyset| = 0$.

L'insieme vuoto è un sottoinsieme di qualunque altro insieme: per ogni insieme A risulta $\emptyset \subseteq A$. Dalle definizioni di cardinalità e di sottoinsieme si deduce facilmente che se $B \subseteq A$ allora $|B| \leq |A|$.

Anche se il concetto dovrebbe essere abbastanza evidente senza ulteriori precisazioni, possiamo dire più formalmente che un insieme è **finito** se i suoi elementi possono essere messi in corrispondenza biunivoca con l'insieme $\{1,2,3,\ldots,n\}$, per qualche $n \geq 0$; naturalmente n è proprio la cardinalità dell'insieme stesso.

Un insieme A con un numero infinito di elementi è **numerabile** se ha la stessa cardinalità dell'insieme $\mathbb{N}$ dei numeri naturali, ossia se i suoi elementi possono essere messi in corrispondenza biunivoca con i numeri naturali associando a ciascun elemento dell'insieme A uno ed un solo elemento dell'insieme $\mathbb{N}$. La cardinalità di un insieme numerabile viene indicata con il simbolo $\aleph_0$ (*aleph zero* o *cardinalità del numerabile*). Ogni insieme numerabile può essere messo in corrispondenza biunivoca con un suo sottoinsieme di cardinalità infinita. Ad esempio l'insieme $\mathbb{N}$ può essere messo in corrispondenza biunivoca con il sottoinsieme dei numeri naturali pari, mediante la seguente corrispondenza biunivoca: $n \leftrightarrow 2n$, per ogni $n \in \mathbb{N}$. Dunque un insieme numerabile può contenere come sottoinsiemi propri degli insiemi numerabili.

Non tutti gli insiemi con un numero infinito di elementi sono numerabili, esistono insiemi **non numerabili**, come ha dimostrato per primo Georg Cantor evidenziando, con una celebre tecnica nota come l'*argomento diagonale di Cantor*, che l'insieme $\mathbb{R}$ dei numeri reali non possa essere messo in corrispondenza biunivoca con l'insieme $\mathbb{N}$ dei numeri naturali. La cardinalità di un insieme *continuo* come $\mathbb{R}$ viene indicata con il simbolo $\aleph_1$ (*aleph uno* o *cardinalità del continuo*).

È piuttosto semplice calcolare la cardinalità del prodotto cartesiano. Infatti, se si considerano gli insiemi A e B di cardinalità finita, rispettivamente n ed m; allora l'insieme ottenuto come prodotto cartesiano $A \times B$ ha una cardinalità $|A \times B| = nm$. È facile provare questo risultato, dal momento che gli elementi di $A \times B$ sono coppie ordinate composte da un elemento di A ed un elemento di B. Ciascun elemento di A costituisce una coppia con gli m elementi di B; dunque si ottengono m coppie per ogni elemento di A, per cui, visto che $|A| = n$, si otterranno complessivamente nm coppie, come elementi di $A \times B$.

Proposizione 2. *Sia A un insieme finito tale che $|A| = n$. Allora $|\wp(A)| = 2^n$.*

Dimostrazione. Procediamo per induzione sul numero di elementi di A. Se $A = \emptyset$, allora $|A| = 0$ e $\wp(A) = \{\emptyset\}$; quindi $|\wp(A)| = 2^{|A|} = 2^0 = 1$. In questo caso l'affermazione è provata.

Supponiamo quindi (ipotesi induttiva) che risulti $|\wp(A)| = 2^{n-1}$ se $|A| = n-1$ e dimostriamo che allora $|\wp(A')| = 2^n$ se $A' = A \cup \{x\}$, con $x \notin A$. La famiglia $\wp(A')$ è costituita da tutti i sottoinsiemi di A' che contengono x e da tutti i sottoinsiemi di A' che non contengono x; quest'ultima famiglia è proprio la famiglia dei sottoinsiemi di A ed è quindi costituita da 2^{n-1} elementi. L'insieme dei sottoinsiemi di A' che contengono x può essere ottenuta considerando ogni insieme $Y \in \wp(A)$ ed unendo a tale sottoinsieme anche l'elemento x: $Y' = Y \cup \{x\}$. Pertanto la famiglia dei sottoinsiemi di A' che contengono x è costituita da 2^{n-1} elementi: uno per ogni elemento dell'insieme $\wp(A)$. Dunque, concludendo, l'insieme delle parti di A' è costituito da due famiglie disgiunte di 2^{n-1} elementi ciascuna: complessivamente quindi $|\wp(A')| = 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$. □

È utile osservare che lo stesso risultato sulla cardinalità dell'insieme delle parti poteva essere raggiunto in modo "costruttivo" definendo una corrispondenza biunivoca tra gli elementi di $\wp(A)$ e gli elementi dell'insieme $P = \{0,1,2,\ldots,2^n - 1\}$, la cui cardinalità è $|P| = 2^n$. Si consideri infatti l'insieme $A = \{a_1, a_2, \ldots, a_n\}$, finito, con n elementi. Ogni sottoinsieme A' di A è una collezione di alcuni elementi di A, ad esempio $A' = \{a_3, a_4, a_7\}$ (supponendo che $n \geq 7$); ogni sottoinsieme $A' \subseteq A$ può essere associato al numero binario composto da n cifre $x = b_1 b_2 \ldots b_n$ tale che $b_i = 0$ se $a_i \notin A'$ e $b_i = 1$

se $a_i \in A'$. Come è noto, con n cifre binarie è possibile rappresentare tutti i numeri naturali compresi tra 0 e $2^n - 1$:

$$
\begin{aligned}
0 &= \overbrace{000\ldots0}^{n \text{ volte}} \\
2^n - 1 &= \overbrace{111\ldots1}^{n \text{ volte}}
\end{aligned}
$$

In questo modo, è possibile associare l'insieme vuoto al numero 0 e l'insieme $A = \{a_1, a_2, \ldots, a_n\}$, composto da n elementi, al numero $2^n - 1$; ogni altro sottoinsieme di A può essere associato univocamente ad un numero intero x, $0 < x < 2^n - 1$, utilizzando la costruzione esposta in precedenza: x corrisponde al numero la cui rappresentazione in base 2 è composta da n cifre $b_1, b_2, \ldots, b_n$ tali che $b_i = 1$ se a_i appartiene al sottoinsieme, mentre $b_i = 0$ in caso contrario.

Questa osservazione suggerisce in effetti un algoritmo per la costruzione di tutti i sottoinsiemi di un insieme A di cardinalità n. Di fatto si tratta di costruire tutte le "stringhe" binarie di n cifre $S = (s_1, s_2, \ldots, s_n)$, da $(0, 0, \ldots, 0)$ fino a $(1, 1, \ldots, 1)$ e, per ciascuna stringa, produrre il sottoinsieme di A costituito dai soli elementi $a_i \in A$ tali che $s_i = 1$. L'Algoritmo 1 produce tutte le stringhe binarie con n cifre.

Algoritmo 1 STRINGHEBINARIE(n)

Input: Un numero intero $n > 0$
Output: Tutte le stringhe binarie $S := (s_1, s_2, \ldots, s_n)$ con n cifre

1: sia $S := (0, 0, \ldots, 0)$ ($s_i := 0$ per ogni $i = 1, 2, \ldots, n$)
2: $i := 1$
3: **fintanto che** $i \leq n$ **ripeti**
4:     $i := 1$
5:     **fintanto che** $i \leq n$ e $s_i \neq 0$ **ripeti**
6:         $s_i := 0$
7:         $i := i + 1$
8:     **fine-ciclo**
9:     **se** $i \leq n$ **allora**
10:         $s_i := 1$
11:     **fine-condizione**
12:     scrivi la stringa $S = (s_1, s_2, \ldots, s_n)$
13: **fine-ciclo**

La strategia risolutiva adottata dall'algoritmo è piuttosto semplice. Partendo dalla stringa binaria composta da n elementi nulli (riga 1), per passare da una stringa binaria S alla successiva si pongono uguale a zero tutti gli elementi a sinistra del primo elemento nullo (righe 5–8) e si pone uguale ad 1 tale elemento (riga 9 – nella stringa S era il primo elemento nullo, partendo da sinistra). Questo procedimento viene ripetuto più volte e si interromperà solo quando quando tutti gli elementi di S, da s_1 fino ad s_n, risulteranno non nulli.

6 Elementi di analisi combinatoria

È utile innanzi tutto richiamare una relazione assai nota che utilizzeremo spesso in seguito. Tale relazione è nota come *formula di Gauss*, perché tradizionalmente la si fa risalire a Carl Friedrich Gauss[1], il celeberrimo matematico tedesco. Il risultato ottenuto da Gauss può essere espresso mediante la seguente Proposizione.

Proposizione 3. *Fissato un intero $n > 0$ risulta*

$$\sum_{k=1}^{n} k = \frac{n \cdot (n+1)}{2}$$

Dimostrazione. Procediamo seguendo una tecnica costruttiva. Iniziamo sommando due volte gli interi positivi da 1 ad n; possiamo farlo scrivendo quanto segue:

$$\begin{array}{ccccccccccccc} 1 & + & 2 & + & 3 & + & \dots & + & n-1 & + & n & + \\ n & + & n-1 & + & n-2 & + & \dots & + & 2 & + & 1 & \end{array}$$

Scrivendo in questo modo la sommatoria, il cui risultato, qualunque esso sia, è esattamente il doppio di quanto intendiamo calcolare, risulta che su ciascuna riga sono presenti n addendi e che la somma di ciascuna "colonna" è pari a $n+1$. Per cui complessivamente il valore della sommatoria è $n \cdot (n+1)$. Il risultato ottenuto deve essere diviso per due per ricavare la somma dei primi n interi positivi: si ottiene quindi l'espressione $\frac{n \cdot (n+1)}{2}$. □

Nel seguito ci dedicheremo a calcolare quanti insiemi possono essere ottenuti scegliendo o combinando fra loro gli elementi di un insieme assegnato.

Dato un insieme A, una corrispondenze biunivoche di A con se stesso si chiama **permutazione** di A. Ad esempio, se $A = \{1, 2, 3\}$, una permutazione di A è costituita dalla corrispondenza biunivoca definita ponendo $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$. Tale permutazione spesso viene espressa anche scrivendo

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

In generale quindi, dato un insieme $A = \{a_1, a_2, \dots, a_n\}$, una permutazione di A è una corrispondenza biunivoca che porta ciascun elemento di A in un altro elemento di A o in se stesso: $a_i \mapsto a'_i$, con $A = \{a'_1, a'_2, \dots, a'_n\}$ e $a'_i \neq a'_j$ per $i \neq j$:

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a'_1 & a'_2 & a'_3 & \dots & a'_n \end{pmatrix}$$

Proposizione 4. *Su un insieme $A = \{a_1, a_2, \dots, a_n\}$ con n elementi è possibile definire $n!$ permutazioni distinte.*[2]

---

[1] Si dice, ma non è provato il fondamento storico di questo aneddoto, che ad appena nove anni il giovanissimo Carl Friedrich Gauss, per punizione venne chiamato dal proprio insegnante a calcolare la somma dei primi cento interi positivi; Gauss, sorprendendo tutti, fornì dopo pochi istanti la risposta esatta, calcolata utilizzando la famosa identità che aveva scoperto proprio in quel momento.

[2] È sicuramente superfluo ricordare che con la notazione $n!$, per un intero $n > 0$, si indica il **fattoriale** di n, definito ponendo $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$. Per definizione si pone inoltre $0! = 1$.

Dimostrazione. Le permutazioni sono corrispondenze biunivoche di A in se stesso, per cui due elementi distinti $a_i, a_j \in A$ non possono essere in corrispondenza con il medesimo elemento $a_k \in A$; inoltre le permutazioni che vogliamo contare devono essere tutte diverse l'una dall'altra.

Ciò premesso, procederemo in modo costruttivo. Nel definire le permutazioni su A, per il primo elemento a_1 possiamo scegliere n elementi diversi con cui metterlo in corrispondenza; fissato l'elemento corrispondente ad a_1, per il secondo elemento a_2 di A abbiamo a disposizione $n-1$ scelte differenti; fissati gli elementi corrispondenti ad a_1 e a_2, per il terzo elemento a_3 avremo $n-2$ scelte differenti per definire l'elemento con cui metterlo in corrispondenza.

Estendendo questo ragionamento a tutti gli n elementi dell'insieme A otteniamo che il numero di modi differenti con cui possiamo costruire le permutazioni di A è dato dal seguente prodotto: $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$. □

Ad esempio, se $A = \{x, y, z\}$, possiamo definire su A le seguenti 6 permutazioni distinte:

$$\begin{pmatrix} x & y & z \\ x & y & z \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ x & z & y \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ y & x & z \end{pmatrix}$$

$$\begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ z & x & y \end{pmatrix} \quad \begin{pmatrix} x & y & z \\ z & y & x \end{pmatrix}$$

Non è banale costruire un algoritmo in grado di produrre tutte le $n!$ permutazioni di un insieme A con n elementi. Senza perdita di generalità supponiamo che l'insieme A di cui vogliamo ottenere le permutazioni sia $A = \{1, 2, \ldots, n\}$; la prima permutazione degli elementi di A è $P_1(A) = (a_1 = 1, a_2 = 2, \ldots, a_n = n)$, ottenuta ponendo semplicemente $a_i = i$ per ogni $i = 1, 2, \ldots, n$. A partire da una generica permutazione $P(A)$ si ricava la permutazione "successiva", $P'(A)$, mediante il seguente procedimento. Si individua l'indice k, $0 \leq k < n$, tale che $a_k < a_{k+1}$ e si scambia l'elemento a_k con il più piccolo elemento $a_h > a_k$, con $k < h \leq n$; infine si ordinano in ordine crescente gli elementi $a_k, a_{k+1}, \ldots a_n$. In questo modo vengono prodotte tutte le permutazioni in ordine "lessicografico" crescente, garantendo così, grazie proprio all'ordinamento lessicografico della sequenza di permutazioni, di non generare due volte sulla stessa permutazione. Possiamo sintetizzare con l'Algoritmo 2 la procedura appena descritta.

L'algoritmo opera iterando $n!$ volte un ciclo principale (righe 3–19) che produce le permutazioni dell'insieme A. Con il ciclo alle righe 5–7 si individua, se esiste, il più grande indice k per cui risulta $a_k < a_{k+1}$; siccome l'indice che si vuole individuare è appunto il più grande, il valore di k inizialmente è $n-1$ e viene diminuito di 1 ad ogni iterazione fino ad individuare un elemento a_k che soddisfa la condizione $a_k < a_{k+1}$. Se $k > 0$ allora esiste un elemento a_k che soddisfa tale condizione, altrimenti, se $k = 0$, vuol dire che non esiste nessun elemento $a_1, a_2, \ldots, a_n$ che soddisfa tale condizione: evidentemente sono state prodotte tutte le permutazioni di A arrivando alla permutazione finale $P = (a_1 = n, a_2 = n-1, a_3 = n-2, \ldots, a_{n-1} = 2, a_n = 1)$.

Con il ciclo alle righe 10–14 si cerca il più piccolo elemento $a_h > a_k$, con $k < h \leq n$. Quindi, con le istruzioni alle righe successive (15–17) vengono scambiati gli elementi a_k e a_h, vengono ordinati in ordine crescente gli elementi $a_{k+1}, \ldots, a_n$ ed infine viene stampata la nuova permutazione di A. Quindi, se $k > 0$, viene iterato nuovamente il ciclo principale, ritornando all'istruzione di riga 4, altrimenti, se $k = 0$, l'algoritmo termina.

Ad esempio, si consideri l'insieme $A = \{1, 2, 3, 4, 5\}$ e la permutazione $P = (a_1 = 1, a_2 = 3, a_3 = 5, a_4 = 4, a_5 = 2)$; la permutazione successiva a P in ordine lessicografico è $P' = (a_1 = 1, a_2 = 4, a_3 = 2, a_4 = 3, a_5 = 5)$. Per passare da P a P' mediante l'algoritmo 2 vengono eseguite le seguenti operazioni: scorrendo a ritroso la permutazione P si individua l'elemento a_k, con k massimo, che soddisfa

Algoritmo 2 PERMUTAZIONI(A, n)

Input: L'insieme $A = \{1, 2, \dots, n\}$
Output: Tutte le permutazioni dell'insieme A

sia $P := (a_1 = 1, a_2 = 2, \dots, a_n = n)$ la prima permutazione degli elementi di A
scrivi la permutazione P
ripeti
    $k := n - 1$
    fintanto che $k > 0$ e $a_k > a_{k+1}$ **ripeti**
        $k := k - 1$
    fine-ciclo
    se $k > 0$ **allora**
        $h := 0$
        per $i := k+1, k+2, \dots, n$ **ripeti**
            se $a_i > a_k$ e ($h = 0$ o $a_i < a_h$) **allora**
                $h := i$
            fine-condizione
        fine-ciclo
        scambia a_k e a_h
        ordina in ordine crescente gli elementi $a_{k+1}, a_{k+2}, \dots, a_n$
        scrivi la nuova permutazione $P = (a_1, a_2, \dots, a_n)$
    fine-condizione
fintanto che $k > 0$

la condizione $a_k < a_{k+1}$; nella permutazione P del nostro esempio tale elemento è $a_{k=2} = 3$. Quindi si individua il più piccolo elemento a_h ($h > k = 2$) che sia maggiore di a_2; tale elemento è $a_4 = 4$. Si scambiano allora gli elementi a_2 e a_4; infine si ordinano in ordine crescente gli elementi $a_3 = 5$, $a_4 = 3$ e $a_5 = 2$ ottenendo così la nuova permutazione $P' = (1, 4, 2, 3, 5)$.

Consideriamo un insieme $A = \{a_1, a_2, \dots, a_n\}$ di n elementi e, fissato un intero positivo $k \leq n$, definiamo un **disposizione** (o *disposizione semplice* o anche *disposizione senza ripetizioni*) di k elementi sull'insieme A, come una sequenza ordinata di k elementi distinti di A. La disposizione è una sequenza ordinata, per cui due disposizioni sono considerate diverse se differiscono almeno per un elemento o anche solo per l'ordine degli elementi. Ad esempio se $A = \{1, 2, 3\}$, le disposizioni su A con $k = 2$ elementi sono le coppie $(1,2)$, $(1,3)$, $(2,1)$, $(2,3)$, $(3,1)$, $(3,2)$.

Proposizione 5. *Il numero di disposizioni semplici di k elementi su un insieme A di cardinalità n è dato da*

$$D_{n,k} = \frac{n!}{(n-k)!}$$

Dimostrazione. Consideriamo l'insieme $A = \{a_1, a_2, \dots, a_n\}$ e procediamo in modo costruttivo. Le sequenze di k elementi possono essere definite scegliendo n elementi differenti come primo elemento della sequenza, $n-1$ elementi differenti come secondo elemento della sequenza, $n-2$ elementi differenti come terzo elemento della sequenza. Questo ragionamento può essere ripetuto fino ad arrivare ad avere $n-k+1$ possibilità differenti per scegliere il k-esimo elemento della sequenza. Dunque risulta:

$$D_{n,k} = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

□

Potremmo ripetere un ragionamento analogo a quello con cui abbiamo calcolato il numero di disposizioni semplici, nel caso in cui volessimo invece calcolare le **disposizioni con ripetizioni** di k su un insieme di n elementi. In questo caso il numero di disposizioni è n^k, con $0 < k \leq n$. Infatti per comporre le sequenze ordinate potremo contare su n scelte per ciascuno dei k elementi, dal momento che gli stessi elementi possono essere anche ripetuti nella sequenza. Per cui il numero complessivo di disposizioni con ripetizioni differenti con k elementi su un insieme di n elementi è dato da

$$\overbrace{n \cdot n \cdot \ldots \cdot n}^{k \text{ volte}} = n^k$$

Consideriamo ancora una volta un insieme $A = \{a_1, a_2, \ldots, a_n\}$ di n elementi e, fissato un intero positivo $k \leq n$, definiamo una **combinazione semplice** di k elementi su A, come un sottoinsieme di A con k elementi. Fissato l'insieme A con n elementi ci proponiamo di contare il numero di combinazioni di k elementi su A. Come ben sappiamo l'ordine con cui compaiono gli elementi in un insieme o in un sottoinsieme non conta, per cui nel costruire le combinazioni su A è importante solo la scelta degli elementi da inserire nel sottoinsieme e non l'ordine con cui tali elementi vengono scelti.

Pertanto il numero di combinazioni semplici di k elementi su un insieme di cardinalità n, $C_{n,k}$, è dato dal rapporto tra il numero di disposizioni semplici e il numero di permutazioni di k elementi:

$$C_{n,k} = \frac{n!}{k!(n-k)!} \tag{1}$$

Ad esempio, se $A = \{1,2,3,4,5\}$ le 10 combinazioni semplici di $k = 3$ elementi sull'insieme A di cardinalità $n = 5$ sono le seguenti: $\{1,2,3\}$, $\{1,2,4\}$, $\{1,2,5\}$, $\{1,3,4\}$, $\{1,3,5\}$, $\{1,4,5\}$, $\{2,3,4\}$, $\{2,3,5\}$, $\{2,4,5\}$, $\{3,4,5\}$.

Per costruire le combinazioni semplici di n elementi di un insieme A in classi di k si può utilizzare l'algoritmo 1 di pag. 10 per la generazione delle stringhe binarie con n cifre e scartare tutte quelle con un numero di elementi non nulli diverso da k; ogni stringa binaria con k elementi non nulli può essere messa in corrispondenza con una combinazione di k elementi di un insieme A di cardinalità n. Tuttavia questo metodo ci costringerebbe a generare tutti i possibili sottoinsiemi di A, dovendone poi scartare la maggior parte. Un metodo eccessivamente oneroso per il risultato che si vuole raggiungere. È opportuno quindi sviluppare un algoritmo costruttivo diverso, in grado di generare soltanto i sottoinsiemi di A con k elementi, con l'accortezza di non generare mai due volte lo stesso insieme.

Visto che A è un insieme finito, possiamo disporre gli elementi di A secondo un ordine arbitrario, in modo tale da metterli in corrispondenza biunivoca con gli elementi dell'insieme $\{1,2,\ldots,n\}$. A questo punto, senza perdita di generalità, possiamo produrre le combinazioni in classi di k degli elementi di $\{1,2,\ldots,n\}$. Genereremo le combinazioni come k-ple ordinate di elementi $(a_{c_1}, a_{c_2}, \ldots, a_{c_k})$, in modo tale che risulti $c_1 < c_2 < \cdots < c_k$; così sarà facile evitare che vengano prodotte due combinazioni che differiscono solo per l'ordine degli elementi, perché in tal caso le k-ple corrispondenti a tali combinazioni sarebbero identiche. L'algoritmo 3 genera tutte le combinazioni degli n elementi di un insieme A in classi di k.

La strategia adottata dall'algoritmo 3 consiste nel costruire, in ordine lessicografico crescente, tutte le k-ple $(c_1, c_2, \ldots, c_k)$ con $c_i = 1,2,\ldots,n$ e $c_i \neq c_j$ se $i \neq j$. I numeri $\{c_i\}_{i=1,2,\ldots,k}$ sono gli indici di k elementi di A scelti per formare una combinazione; al variare delle k-ple $\{c_i\}$ si ottengono tutte le combinazioni desiderate. Per passare da una k-pla $(c_1, c_2, \ldots, c_k)$ alla successiva nell'ordine lessicografico, si prendono in esame gli elementi c_i a partire da $i = k$ fino ad $i = 1$ (ciclo alle righe 8–10) fino a quando non si incontra un elemento c_i che non abbia assunto il valore massimo per la posizione i-esima: $c_i < n-(k-i)$; in tal caso si incrementa di 1 l'elemento c_i e si impostano di conseguenza il valore degli elementi successivi, $c_{i+1}, c_{i+2}, \ldots, c_k$ con il valore minimo per ciascun elemento.

Algoritmo 3 COMBINAZIONI(A, n, k)

Input: L'insieme $A = \{a_1, a_2, \ldots, a_n\}$ e un intero $k \leq n$
Output: Le combinazioni in classi di k degli n elementi di A

per $i := 1, 2, \ldots, k$ **ripeti**
    $c_i := i$
fine-ciclo
scrivi $\{a_{c_j}\}_{j:=1,\ldots,k}$
$i := k$
fintanto che $i > 0$ **ripeti**
    $i := k$
    fintanto che $i > 0$ e $c_i = n - (k - i)$ **ripeti**
        $i := i - 1$
    fine-ciclo
    se $i > 0$ **allora**
        $c_i := c_i + 1$
        per $j := i+1, i+2, \ldots, k$ **ripeti**
            $c_j := c_{j-1} + 1$
        fine-ciclo
        scrivi $\{a_{c_j}\}_{j:=1,\ldots,k}$
    fine-condizione
fine-ciclo

Se $A = \{1, 2, \ldots, n\}$, nel produrre combinazioni di elementi di A in classi di k con elementi disposti in ordine crescente, nella posizione i-esima della k-pla ordinata, dovrà esserci un intero compreso tra i e $n - (k - i)$; ad esempio nella prima posizione ($i = 1$) dovrà esserci necessariamente un intero compreso tra 1 e $n - k + 1$, mentre nella posizione k-esima si troverà un intero compreso tra k e n. Ad esempio se $n = 7$ e $k = 5$, in prima posizione si troverà un elemento $a_1 \in A$ tale che $1 \leq a_1 \leq 3$; se risultasse $a_1 = 4$ non potremmo assegnare valori distinti minori o uguali ad $n = 7$ agli elementi successivi al primo; analogamente all'elemento a_5 potremo assegnare un valore compreso tra 5 e 7. Per produrre una combinazione successiva ad una combinazione data, partendo da destra si cerca il primo elemento che non abbia già raggiunto il valore massimo per la sua posizione e lo si incrementa di 1; quindi si impostano con il valore minimo di ciascuna posizione gli elementi alla sua destra. Ad esempio, se $n = 7$ e $k = 5$:

$$C = (1, 2, \mathbf{3}, 6, 7) \rightarrow C' = (1, 2, \mathbf{4}, \mathbf{5}, \mathbf{6})$$

Il numero di combinazioni su n elementi in classi di k si chiama **coefficiente binomiale** e si indica con la seguente notazione:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{2}$$

Il termine "coefficiente binomiale" deriva dal fatto che i numeri $\binom{n}{k}$ sono i coefficienti dello sviluppo del binomio $(x + y)^n$:

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

È interessante osservare che esiste una sola combinazione con zero elementi su un insieme di n, ed è la combinazione costituita dal solo insieme vuoto; per cui si definisce:

$$\binom{n}{0} = \frac{n!}{0!n!} = 1 \tag{3}$$

Si è definito così, per convenzione, che $0! = 1$.

Osserviamo inoltre che valgono le seguenti relazioni:

$$\binom{n}{0} = \frac{n!}{0!\,n!} = \frac{n!}{n!\,0!} = \binom{n}{n} \tag{4}$$

e

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n!}{(n-k)!\,(n-(n-k))!} = \frac{n!}{(n-k)!\,k!} = \binom{n}{n-k} \tag{5}$$

La (4) trova una giustificazione anche osservando che su un insieme di n elementi è possibile definire una sola combinazione con zero elementi (l'insieme vuoto) ed una sola combinazione con n elementi (l'insieme stesso). Dalla (5) segue invece una sorta di "simmetria" nel numero di combinazioni semplici con k e $n-k$ elementi su un insieme di cardinalità n.

Dalla definizione di combinazione semplice e di coefficiente binomiale segue che un modo alternativo per contare gli elementi dell'insieme delle parti di A, $\wp(A)$, è quello di sommare il numero di combinazioni di n elementi in classi di k, per $k = 0, 1, 2, \ldots, n$:

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n \tag{6}$$

Osserviamo infine che, per $0 < k < n$, vale la seguente identità:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \tag{7}$$

Infatti risulta:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!\,(n-k)!} + \frac{(n-1)!}{k!\,(n-k-1)!} = \\
&= \frac{(n-1)!}{(k-1)!\,(n-k)\,(n-k-1)!} + \frac{(n-1)!}{k\,(k-1)!\,(n-k-1)!} = \\
&= \frac{k(n-1)! + (n-k)(n-1)!}{k\,(n-k)\,(k-1)!\,(n-k-1)!} = \\
&= \frac{(k+n-k)\,(n-1)!}{k\,(k-1)!\,(n-k)\,(n-k-1)!} = \\
&= \frac{n!}{k!\,(n-k)!} = \\
&= \binom{n}{k}
\end{aligned}$$

Sfruttando quest'ultima relazione, insieme alle (3) e (4), si può costruire uno "schema tabulare" per semplificare il calcolo del coefficiente binomiale $\binom{n}{k}$. Tale schema è noto con il nome di **Triangolo di Tartaglia** (o *Triangolo di Pascal*, per i francesi), e viene costruito proprio utilizzando quest'ultima relazione: partendo dal coefficiente binomiale $\binom{0}{0} = 1$, vengono calcolati i coefficienti binomiali $\binom{n}{k}$, per $n = 1, 2, \ldots$ e per $k = 0, 1, \ldots, n$:

$$\binom{n}{k} = \begin{cases} \binom{n-1}{0} & \text{se } k = 0 \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{se } 0 < k < n \\ \binom{n-1}{0} & \text{se } k = n \end{cases} \tag{8}$$

Mediante la (8) si può costruire uno schema triangolare con cui è facile calcolare il coefficiente binomiale degli elementi di una riga, utilizzando i coefficienti binomiali calcolati alle righe precedenti:

$$\begin{array}{ccccccccc} & & & & \binom{0}{0} & & & & \\ & & & \binom{1}{0} & & \binom{1}{1} & & & \\ & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\ & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\ \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \end{array}$$

Svolgendo i calcoli si ottiene il seguente schema triangolare in cui è evidente la modalità con cui i valori della n-esima riga sono ottenuti a partire dai valori della riga precedente.

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

La simmetria dello schema triangolare trova immediatamente un riscontro nella relazione (5). Numerando le righe del triangolo di Tartaglia a partire da 0, la sommatoria degli elementi della riga n-esima è data dalla (6) ed è pari a 2^n.

Algoritmo 4 COEFFICIENTEBINOMIALE(n, k)

Input: La coppia di interi $k \geq 0$ e $n \geq k$
Output: Il coefficiente binomiale $\binom{n}{k}$

se $n = 0$ **allora**
    $c := 1$
altrimenti
    se $k = 0$ o $k = n$ **allora**
        $c :=$ COEFFICIENTEBINOMIALE$(n-1, 0)$
    altrimenti
        $c :=$ COEFFICIENTEBINOMIALE$(n-1, k-1)$ + COEFFICIENTEBINOMIALE$(n-1, k)$
    fine-condizione
fine-condizione
restituisci c

La relazione (8) suggerisce immediatamente il modo con cui può essere costruito un algoritmo ricorsivo per il calcolo del coefficiente binomiale: invece di eseguire esplicitamente il calcolo del fattoriale di n e di k, operazioni di complessità lineare in n e in k, è possibile ottenere lo stesso risultato effettuando soltanto addizioni. L'Algoritmo 4 presenta la pseudo-codifica del procedimento ricorsivo per il calcolo di $\binom{n}{k}$.

7 Un rompicapo combinatorio

Il gioco del **Sudoku** è un rompicapo giapponese che ha riscosso un successo notevole nel cosiddetto "grande pubblico": pur essendo un gioco di tipo combinatorio e dunque con un *background* logico-matematico, riesce ad appassionare anche quanti non hanno competenze specifiche in questo settore della matematica. Il motivo del successo credo sia tutto nella grande semplicità delle regole del gioco, affiancate dal fatto che effettivamente a fronte di regole assai semplici, la soluzione del problema è tutt'altro che banale e propone una sfida intellettuale divertente, in grado di dare qualche soddisfazione al giocatore vincitore. Al di là degli aspetti puramente ludici, il Sudoku trae spunto da un insieme di problemi di carattere combinatorio molto interessanti e complessi.

Il problema da risolvere in una partita di Sudoku può essere riassunto nei seguenti termini: riempire una matrice quadrata M di ordine 9, in modo tale che ogni riga, ogni colonna ed ognuna delle nove sotto-matrici 3×3 contenga tutte le cifre da 1 a 9, naturalmente senza alcuna ripetizione. In Figura 4 è riportato un esempio di griglia correttamente completata.

In termini appena più precisi possiamo dire che è data una matrice quadrata di 9 righe e 9 colonne in cui ogni elemento $m_{i,j}$ può assumere come valore un numero naturale compreso tra 1 e 9: $1 \leq m_{i,j} \leq 9$ per $i, j = 1, \ldots, 9$. La matrice inizialmente contiene solo alcuni elementi non nulli, mentre la maggior parte delle posizioni è vuota. L'obiettivo del gioco è proprio quello di completare la matrice, collocando gli elementi in modo tale da rispettare i seguenti vincoli:

1. per ogni $i = 1, \ldots, 9$ deve risultare $m_{i,h} \neq m_{i,k}$ per ogni $h, k = 1, \ldots, 9$, $h \neq k$ (tutti gli elementi su una stessa riga devono essere differenti);

2. per ogni $j = 1, \ldots, 9$ deve risultare $m_{h,j} \neq m_{k,j}$ per ogni $h, k = 1, \ldots, 9$, $h \neq k$ (tutti gli elementi su una stessa colonna devono essere differenti);

3. per ogni $h = [i/3] + 1, \ldots, [i/3] + 3$ e per ogni $k = [j/3] + 1, \ldots, [j/3] + 3$ deve risultare $m_{i,j} \neq m_{h,k}$ (gli elementi di uno stesso riquadro 3×3 devono essere differenti; con $[x]$ indichiamo la parte intera di x).

Una configurazione di Sudoku è un caso particolare di **quadrato latino**: una matrice $n \times n$ i cui elementi sono tutti e soli gli elementi dell'insieme $\{1, 2, \ldots, n\}$, tale che gli elementi di una stessa riga e di una stessa colonna siano tutti diversi. Due quadrati latini di ordine n si dicono *ortogonali* se le n^2 coppie formate dagli elementi corrispondenti dei due quadrati, sono tutte distinte. Un quadrato latino *normalizzato* è ottenuto ponendo la prima riga e la prima colonna uguali a $(1, 2, \ldots, n)$: $m_{1,1} = 1, m_{1,2} = m_{2,1} = 2, m_{1,3} = m_{3,1} = 3, \ldots, m_{1,n} = m_{n,1} = n$.

		2	5		9	1		0
6	3			2			4	5
4								9
		5	1		4	8		
2								7
5	4			3			2	1
		8	7		6	5		

$\rightsquigarrow$

8	7	2	5	4	9	1	6	3
9	5	4	3	6	1	2	7	8
6	3	1	8	2	7	9	4	5
4	8	3	2	7	5	6	1	9
7	6	5	1	9	4	8	3	2
2	1	9	6	8	3	4	5	7
5	4	6	9	3	8	7	2	1
1	9	7	4	5	2	3	8	6
3	2	8	7	1	6	5	9	4

Figura 4: Una griglia di partenza e la soluzione finale

8	7	2	5	4	9	1	6	3
9	5	4	3	6	1	2	7	8
6	3	1	8	2	7	9	4	5
4	8	3	2	7	5	6	1	9
7	6	5	1	9	4	8	3	2
2	1	9	6	8	3	4	5	7
5	4	6	9	3	8	7	2	1
1	9	7	4	5	2	3	8	6
3	2	8	7	1	6	5	9	4

$\cong$

1	2	3	4	5	6	7	8	9
6	4	5	9	8	7	3	2	1
8	9	7	1	3	2	6	5	4
5	1	9	3	2	4	8	7	6
2	8	4	7	6	5	1	9	3
3	7	6	8	1	9	5	4	2
4	5	8	6	9	1	2	3	7
7	6	2	5	4	3	9	1	8
9	3	1	2	7	8	4	6	5

Figura 5: Due configurazioni equivalenti

Naturalmente, oltre a ragionare su eventuali strategie risolutive automatiche efficienti per vincere una partita di Sudoku, o su criteri tali da poter calcolare automaticamente la "mossa" migliore a fronte di una determinata configurazione di gioco, sono molti i problemi che possono essere derivati dal contesto suggerito dal gioco del Sudoku.

Ad esempio, un problema molto interessante ed assolutamente non banale è quello di stabilire il numero di possibili configurazioni differenti della scacchiera completata. Nell'affrontare la soluzione di questo problema, recentemente risolto da Felganhauer e Jarvis (vedi [3]), si deve innanzi tutto osservare che due matrici diverse, M ed M' possono invece rappresentare la stessa configurazione di gioco, nel caso in cui si possano rimappare tutti gli elementi dell'una sugli stessi elementi dell'altra; in altri termini le matrici M ed M' rappresentano la stessa configurazione se esiste un isomorfismo $\varphi : M \to M'$ tale che $\varphi(m_{i,j}) = \varphi(m_{h,k})$ se e solo se $m_{i,j} = m_{h,k}$. In Figura 5 sono riportate due configurazioni equivalenti: si può passare dalla prima matrice alla seconda con il seguente isomorfismo: $\varphi(8) = 1, \varphi(7) = 2, \varphi(2) = 3, \varphi(5) = 4, \varphi(4) = 5, \varphi(9) = 6, \varphi(1) = 7, \varphi(6) = 8, \varphi(3) = 9$.

Altre configurazioni equivalenti, possono essere ottenute per rotazione della matrice o per simmetria. Dunque le possibili configurazioni veramente differenti di Sudoku sono meno di quelle che potrebbero essere calcolate per semplice permutazione (pur nel rispetto di vincoli sopra elencati) degli elementi delle righe e delle colonne della matrice.

Calcolare il numero di quadrati latini di ordine n è molto difficile, tanto che tale risultato è noto solo per quadrati latini di ordine minore o uguale a 15. In generale esiste una relazione che lega il numero di quadrati latini di ordine n, $N(n,n)$, con il numero di quadrati latini normalizzati dello stesso ordine, $L(n,n)$:

$$N(n,n) = n!\ (n-1)!\ L(n,n)$$

Dunque il problema del calcolo del numero di quadrati latini differenti di ordine n, si riduce al calcolo del numero di quadrati latini normalizzati. Purtroppo non esiste una formula in grado di calcolare direttamente quel numero: al momento tale risultato è stato calcolato con algoritmi "esaustivi" che, applicando i cosiddetti metodi "a forza bruta", si limitano a costruire e contare tutte le possibili configurazioni. Ad esempio $L(2,2) = 1$, $L(3,3) = 1$, $L(4,4) = 4$, $L(7,7) = 16.942.080$, $L(9,9) = 377.597.570.964.258.816$.

Partendo da considerazioni di questo tipo, ma restringendo il calcolo a quadrati latini con i vincoli ulteriori posti dalle regole del Sudoku, Felgenhuer e Jarvis in [3] hanno mostrato che il numero di configurazioni valide del Sudoku è pari a $2^7 \cdot 27.704.267.971 = 3.546.146.300.288$. È sorprendente notare che il fattore 27.704.267.971 è un numero primo.

Altri problemi interessanti, legati al gioco del Sudoku, possono essere riassunti nelle seguenti domande:

- Qual è il numero minimo di elementi che devono essere presenti nella configurazione iniziale per dare luogo ad una partita “non ambigua”, ossia ad una partita con una sola soluzione?
- Qual è il criterio per cui, a parità di elementi iniziali non nulli, si può stabilire oggettivamente che una partita è più difficile di un’altra?
- Esiste un ordinamento (parziale o totale) delle partite di Sudoku in funzione della loro difficoltà?

7.1 Algoritmo ricorsivo per la soluzione del Sudoku

Il gioco del Sudoku può essere risolto facilmente attraverso un algoritmo che esegue la ricerca esaustiva di una soluzione ammissibile, tentando tutte le possibili combinazioni di elementi fino a trovare una configurazione valida, che risolve il gioco. Il problema principale, dovendo “sequenzializzare” il procedimento di ricerca della soluzione, è quello di identificare una strategia che consenta di passare da una combinazione illecita ad una successiva combinazione da valutare, senza perdere, nel passare dall’una all’altra, configurazioni potenzialmente valide.

L’Algoritmo 5 presenta una procedura ricorsiva piuttosto compatta per il calcolo della soluzione del Sudoku, a partire da una configurazione valida (ma incompleta) M. Indichiamo con $m_{i,j} = 0$ i valori non definiti della configurazione rappresentata dalla matrice M.

Algoritmo 5 SUDOKUSOLVE(M)

Input: Una matrice quadrata M che costituisce una configurazione di gioco incompleta
Output: 0: la matrice M rappresenta una configurazione, ancorché parziale, non ammissibile; 1: la matrice M rappresenta una soluzione del gioco

$rc := 0$
siano i e j gli indici minimi per cui $m_{i,j} = 0$
se esiste $m_{i,j} = 0$ **allora**
    per $k := 1, 2, \ldots, 9$ **ripeti**
        $m_{i,j} := k$
        se M è una configurazione valida localmente e SudokuSolve(M) $= 1$ **allora**
            $rc := 1$
        fine-condizione
    fine-ciclo
    se $rc = 0$ **allora**
        $m_{i,j} := 0$
    fine-condizione
altrimenti
    Sudoku risolto! Stampa la matrice M che rappresenta la soluzione
    $rc := 1$
fine-condizione
restituisci rc

La funzione ricorsiva SudokuSolve(M) restituisce 1 (*true*) se la configurazione M è compatibile, altrimenti restituisce 0 (*false*). Al termine della catena di chiamate ricorsive, quando tutti i valori della matrice sono stati assegnati in modo compatibile con le regole del gioco, la funzione stampa la matrice M che rappresenta la configurazione finale che risolve la partita.

L'istruzione al passo 2 rappresenta un'operazione non elementare di ricerca di una coppia di indici i e j per cui risulta $m_{i,j} = 0$: tipicamente potrebbe essere implementata con una coppia di cicli nidificati, al variare di i e j da 1 a 9.

La condizione espressa a riga 6, richiede di verificare se il valore assegnato all'elemento $m_{i,j}$ della matrice M soddisfa i vincoli del gioco, oppure no. Si dovrà quindi verificare che $m_{i,j} = m_{i,h}$ se e solo se $h = j$ per ogni $h = 1, \ldots, 9$ e, analogamente, che $m_{i,j} = m_{l,j}$ se e solo se $l = i$ per ogni $l = 1, \ldots, 0$; inoltre si deve controllare che $m_{i,j}$ sia unico nella sotto-matrice 3×3 che lo contiene.

Riferimenti bibliografici

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, *Introduzione agli algoritmi e strutture dati*, terza edizione, McGraw-Hill, 2010.

[2] Pierluigi Crescenzi, Giorgio Gambosi, Roberto Grossi, *Strutture di dati e algoritmi*, Pearson–Addison Wesley, 2006.

[3] Bertram Felganhauer, Frazer Jarvis, *Enumerating possible Sudoku grids*, http://www.afjarvis.staff.shef.ac.uk/sudoku/sudoku.pdf, Giugno 2005.

[4] Marco Fontana, Stefania Gabelli, *Insiemi, numeri e polinomi. Primo ciclo di lezioni del Corso di Algebra con esercizi svolti*, CISU, 1989.

[5] Giulia Maria Piacentini Cattaneo, *Algebra, un approccio algoritmico*, Decibel – Zanichelli, 2001.

[6] E. Russel, F. Jarvis, *Sudoku enumeration: the symmetry group*, pagina web all'indirizzo http://www.shef.ac.uk/~pm1afj/sudoku/sudgroup.html, Settembre 2005.

[7] Benedetto Scimemi, *Algebretta. Un'introduzione al corso di Algebra per la laurea in Matematica*, Zanichelli, 1989.

[8] E. W. Weisstein et al. *Sudoku*, From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/Sudoku.html, 2005.

[9] E. W. Weisstein, *Latin Square*, From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/LatinSquare.html, 2005.