Appunti di Fondamenti

Fondamenti dell'Informatica - CdL Informatica 23/24

Federico Zotti

2023-10-15

Indice

Matematica discreta

> **Discreto**: composto di elementi distinti, separati tra di loro.

Un sistema è: - **Discreto** se è costituito da elementi isolati - **Continuo** se non ci sono *vuoti* tra gli elementi

I sistemi informatici si basano su un sistema *binario*, perciò discreto.

Possiamo approssimare un sistema continuo dividendolo in piccole parti (*discretizzazione* o *digitalizzazione*).

Fasi della matematica discreta

- **Classificazione**: individuare le caratteristiche comuni di entità diverse (*teoria degli insiemi*)
- **Enumerazione**: assegnare ad ogni oggetto un numero naturale (*contare*)
- **Combinazione**: permutarne e combinarne gli elementi (*grafi*)

Queste fasi guidano un **algoritmo**.

Logica

In filosofia, la **logica** è lo studio del ragionamento, dell'argomentazione, e dei procedimenti **inferenziali** per distinguere quelli *validi* da quelli *non validi*.

La **logica matematica** vede questi procedimenti come calcoli formali, con una struttura algoritmica.

Infatti, è tutto basato sull'**algebra di Boole**.

Algebra astratta

L'algebra astratta studia le **strutture algebriche**, ovvero insiemi muniti di operazioni.

Insiemi e Operazioni

Numeri

Numeri naturali

I numeri **naturali** sono i primi che impariamo, e nascono dall'attività di contare.

Essi formano un **insieme**, chiamato *insieme dei numeri naturali* ($\mathbb{N}$).

$$\mathbb{N} = \{ 0, 1, 2, 3, 4, \dots, n, n+1, \dots \}$$

Contare non è altro che assegnare ad ogni oggetto un numero naturale (in ordine).

$\mathbb{N}$ ha un *limite inferiore* (0), ma non ha un *limite superiore*, quindi $\mathbb{N}$ è infinito.

Definizione semiformale

- I numeri naturali hanno l'elemento 0
- Ogni elemento n ha (**esattamente**) un successore $s(n)$
- 0 non è un successore di nessun elemento
- Due elmenti diversi hanno successori diversi

Questa definizione è la base del **processo di induzione**.

Una proprietà è vera in tutto $\mathbb{N}$ se e solo se:

- È vera in 0
- Se è vera in n allora è vera in $s(n)$

È possibile anche iniziare da un numero arbitrario.

Numeri interi

I numeri **interi** (relativi) è l'insieme dei numeri naturali preceduti da un segno "$+$" o "$-$". Questo insieme si denota con il simbolo $\mathbb{Z}$.

$$\mathbb{Z} = \{\, \ldots, -(n+1), -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, n+1, \ldots \}$$

Ogni intero ha un successore, ma anche un **predecessore** (non c'è un *minimo*).

I numeri interi positivi (più 0) formano $\mathbb{N}$.

$$\mathbb{N} \subset \mathbb{Z}$$
$$\mathbb{N} = \mathbb{Z}^{+} \cup \{\, 0 \,\}$$

Valore assoluto Il **valore assoluto** di un numero intero è il numero privo di segno.

$$|-n| = n$$
$$|n| = n$$

L'**opposto** di un numero si ottiene cambiandogli il segno.

Numeri razionali

Razionale in questo caso si riferisce a **ratio** ossia **proporzione**. Indicano dunque una proporzione risultante da una divisione.

Si esprimono come rapporto di due numeri interi (*frazioni*).

$$\frac{m}{n}$$

Si indicano con il simbolo $\mathbb{Q}$.

Rappresentazioni e Relazioni Ogni numero razionale può essere rappresentato da un numero decimale finito o periodico.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

Densità I numeri razionali sono **densi**: fra due razionali c'è sempre un altro numero.

Sono comunque **discreti**.

Numeri reali

I **numeri irrazionali** ($\mathbb{I}$) sono quelli che non si possono esprimere tramite frazioni: hanno un'espansione decimale infinita e non periodica.

L'insieme dei **numeri reali** ($\mathbb{R}$) contiene tutti i numeri che ammettono una rappresentazione decimale.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$
$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

La Retta reale L'insieme dei numeri reali spesso viene rappresentato su una **retta** (ordine implicito).

A ogni punto della retta è associato un numero reale e viceversa (*corrispondenza biunivoca*).

Numeri complessi

I **numeri complessi** ($\mathbb{C}$) estendono i reali per eseguire operazioni che non sono ben definite altrimenti.

Nascono dalla necessità di estrarre radici a numeri negativi.

Definiscono l'**unità immaginaria** $i = \sqrt{-1}$. Un numero complesso è $a + bi$, con $a, b \in \mathbb{R}$

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Numeri booleani

L'insieme dei **numeri booleani** è

$$\mathbb{B} = \{\, 0, 1 \,\}$$

Insiemi

Gli **insiemi**, le loro proprietà e le loro **operazioni** sono alla base della matematica moderna e dell'informatica.

Un sistema è **discreto** se costituito da elementi isolati e **continuo** se non vi sono spazi vuoti. In matematica, discreto si basa sul concetto di **cardinalità** (il "numero" di elementi che contiene).

Un insieme è discreto se (e solo se) i suoi elementi si possono **numerare**.

> Un insieme è un raggruppamento di oggetti distinti e ben definiti.

Gli oggetti che formano l'insieme sono i suoi **elementi**. In un insieme, tutti gli elementi sono **distinti** e l'ordine non è rilevante.

> Gli elementi di un insieme possono essere anch'essi insiemi.

Un tempo si pensava che la **teoria degli insiemi** poteva dare una base solida alla matematica. Esistono paradossi però che dicono il contrario.

Per esempio il paradosso del barbiere

> In un villaggio vi è un solo barbiere, che rade tutti e soli gli uomini del villaggio che non si radono da soli. *Chi rade il barbiere?*

o il paradosso eterologico

> Una parola è **autologica** se descrive se stessa (*"polisillabica"*, *"corta"*, *"leggibile"*). Una parola è **eterologica** se non è autologica (*"polillabica"*, *"lunga"*, *"illeggibile"*). "*Eterologica*" è eterologica?

Il più famoso di essi è il paradosso degli insiemi (*Bertrand Russel*)

> Considerate l'insieme N di tutti gli insiemi che non appartengono a se stessi.
> N appartiene a se stesso?

Per costruire questo tipo di paradossi è necessario usare un'**autoreferenza** e una **negazione**.

Questa idea torna in diversi contesti per dimostrare l'impossibilità o inesistenza di certe strutture.

Notazione

Gli insemi generici saranno denotati da lettere latine maiuscole

$$A, B, C, \ldots$$

e i loro elementi con lettere latine minuscole

$$a, b, c, \ldots$$

L'insieme senza elementi si chiama **vuoto** e si denota con $\varnothing$.

L'**uguaglianza** fra oggetti (elementi, insemi, entità, ecc.) si denota con "$=$". La **disuguaglianza** si denota con "$\neq$".

L'uguaglianza ha tre importanti proprietà:

- **Riflessività**: $A = A$
- **Simmetria**: $A = B \iff B = A$
- **Transitività**: se $A = B$ e $B = C$ allora $A = C$

Un insieme può avere diverse rappresentazioni:

- **Diagramma Eulero-Venn**
- **Rappresentazione estensionale**: elenco di tutti gli elementi ($\{x, y, z\}$)
  - $\{\text{rosso}, \text{giallo}, \text{arancio}\}$: insieme con tre elementi
  - $\{\text{rosso}, \text{giallo}, \text{rosso}\}$: insieme con due elementi
  - $\{\varnothing\}$: insieme con un elemento
  - $\{0, 1, 2, 3, \dots\}$: insieme dei numeri naturali
  - $\{\varnothing, 1, 2, \{3\}\}$
- **Rappresentazione intensionale**: consiste nel formulare una proprietà $\mathcal{P}$ caratteristica che distingue precisamente gli elementi dell'insieme ($S = \{x \mid \mathcal{P}(x)\}$)
  - $\{x \mid x \in \mathbb{Z}, x > 0\}$: insieme dei numeri interi positivi
  - $\{x \mid x \text{ è un colore dell'arcobaleno}\}$
  - $\{x \mid x \in \mathbb{Z}, x > 3, x \leq 100\} = \{4, 5, \dots, 99, 100\}$
  - $\{x \mid x \text{ è un numero primo}\}$

Per ogni elemento x esiste l'insieme **singoletto** $\{x\}$.

Proprietà complesse si possono costruire combinando proprietà più semplici mediante operazioni **vero-funzionali**.

Un **sottoinsieme** di A è un insieme formato unicamente per (alcuni) elementi di A. Un sottoinsieme B di A è **proprio** se è diverso da A e da $\varnothing$.

L'insieme vuoto ammette esattamente un sottoinsieme: $\varnothing$ (*sottoinsieme non proprio*). Un singoletto $\{a\}$ ammette due sottoinsiemi: $\varnothing$ e $\{a\}$ (*sottoinsiemi non propri*).

Se A e B hanno gli stessi elementi, sono mutuamente sottoinsiemi

$$A = B \text{ se } A \subseteq B, B \subseteq A$$

L'inclusione soddisfa le proprietà:

- **Riflessività**: $A \subseteq A$
- **Antisimmetria**: $A \subseteq B \land B \subseteq A \iff A = B$

- **Transitività**: $A \subseteq B \land B \subseteq C \iff A \subseteq C$

L'insieme potenza (o insieme delle parti) di un insieme S, scritto $\mathscr{P}(S)$ è l'insieme formato da tutti i sottoinsiemi di S.

$$\mathscr{P}(S) = \{\, x \mid x \subseteq S \,\}$$

Esempi:

- $\mathscr{P}(\varnothing) = \{\, \varnothing \,\}$
- $\mathscr{P}(\{\, \varnothing \,\}) = \{\, \varnothing, \{\, \varnothing \,\} \,\}$
- $\mathscr{P}(\{\, x, y \,\}) = ?$

Se S ha n elementi ($n \geq 0$) allora $\mathscr{P}(S)$ ha 2^n elementi.

Operazioni

Unione L'**unione** di due insiemi A e B si denota

$$A \cup B$$

ed è definita come

$$A \cup B = \{\, x \mid x \in A \lor x \in B \,\}$$

Le proprietà dell'unione sono:

- **Idempotenza**: $A \cup A = A$
- **Commutatività**: $A \cup B = B \cup A$
- **Associatività**: $A \cup (B \cup C) = (A \cup B) \cup C$
- **Esistenza del neutro**: $A \cup \varnothing = A$
- **Assorbimento**: $A \cup B = B$ se $A \subseteq B$
- **Monotonicità**: $A \subseteq A \cup B$ e $B \subseteq B \cup A$

Intersezione L'**intersezione** di due insiemi A e B si denota

$$A \cap B$$

ed è definita come

$$A \cap B = \{\, x \,|\, x \in A \wedge x \in B \,\}$$

Le proprietà dell'intersezione sono:

- **Idempotenza**: $A \cap A = A$
- **Commutatività**: $A \cap B = B \cap A$
- **Associatività**: $A \cap (B \cap C) = (A \cap B) \cap C$
- **Annichilazione**: $A \cap \varnothing = \varnothing$
- **Assorbimento**: $A \cap B = B$ se $A \subseteq B$
- **Monotonicità**: $A \cap B \subseteq A$ e $A \cap B \subseteq B$

L'unione e l'intersezione distribuiscono una sull'altra

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Sottrazione La **sottrazione** tra due insiemi A e B è definita come

$$A \setminus B = \{\, x \,|\, x \in A \wedge x \notin B \,\}$$

Le proprietà della sottrazione sono:

- $A \setminus A = \varnothing$
- $A \setminus \varnothing = A$
- $\varnothing \setminus A = \varnothing$
- $A \setminus B = A \cap \overline{B}$
- $(A \setminus B) \setminus C = A \setminus (B \cup C) = (A \setminus C) \setminus B$

- $A \setminus B \neq B \setminus A$

Differenza simmetrica La differenza simmetrica tra A e B è

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

Proprietà:

- $A \triangle A = \varnothing$
- $A \triangle \varnothing = A$
- $A \triangle B = B \triangle A$

Complementazione Dato un insieme di riferimento U (chiamato **Universo**), il **complemento** assoluto di A è definito come:

$$\overline{A} = \{\, x \,|\, x \in U, x \notin A \,\} = U \setminus A$$

Le proprietà della complementazione sono:

- $\overline{U} = \varnothing$
- $\overline{\varnothing} = U$
- $\overline{\overline{A}} = A$
- $A \cap \overline{A} = \varnothing$ (*terzo escluso*)
- $A \cup \overline{A} = U$
- $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ (*legge di De Morgan*)
- $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$ (*legge di De Morgan*)
- $A \subseteq B \iff \overline{B} \subseteq \overline{A}$

Famiglie di insiemi

Un insieme i cui elementi sono tutti insiemi viene chiamato **famiglia di insiemi** ($\mathcal{F}$).

Le operazioni su una famiglia di insiemi sono:

$$\cup\mathcal{F} = \{\, x \,|\, x \in A \text{ per almeno un insieme } A \in \mathcal{F} \,\}$$
$$\cap\mathcal{F} = \{\, x \,|\, x \in A \;\forall\, A \in \mathcal{F} \,\}$$

Dunque

$$\cup\mathcal{P}(A) = A \;\forall\, A$$

Partizioni

Una partizione di un insieme $A \neq \varnothing$ è una famiglia $\mathcal{F}$ di sottoinsiemi di A tale che:

- $\forall\, c \in \mathcal{F}, c \neq \varnothing$ (*non trivialità*)
- $\cup\mathcal{F} = A$ (*copertura*)
- se $c \in \mathcal{F}$, $D \in \mathcal{F}$ e $C \neq D$, allora $C \cap D = \varnothing$ (*disgiunzione*)

Relazioni

Ordinamenti negli insiemi

Ricordate che gli insiemi **non** sono ordinati

$$\{\, x, y \,\} = \{\, y, x \,\}$$

A volte è utile poter ordinare i loro elementi in modo chiaro.

Coppia ordinata Una **coppia ordinata** è una collezione di due elementi, dove si può distringuere il **primo** e il **secondo** elemento

$$\langle x, y \rangle$$

Il primo elemento è x e il secondo è y. Notare che esiste la coppia ordinata $\langle x, x \rangle$.

Formulazione Insiemistica La coppia ordinata $\langle x, y \rangle$ non è altro che l'insieme

$$\{\,\{\,x\,\}, \{\,x, y\,\}\,\}$$

Sia $\mathcal{F} = \{\,\{\,x\,\}, \{\,x, y\,\}\,\}$. x è il **primo elemento** $\iff$ $x \in \cap\mathcal{F}$ (*appartiene a tutti gli insiemi*). y è il **secondo elemento** $\iff$ $y \in \cup\mathcal{F} \setminus \cap\mathcal{F}$ (*non appartiene a tutti gli insiemi*) oppure $\{\,y\,\} = \cup\mathcal{F}$ ($\mathcal{F} = \{\{y\}\}$).

Notare che $\langle x, x \rangle = \{\{x\}, \{x, x\}\}$.

Definizione giusta Vogliamo vedere che questa definizione **caratterizza** le coppie ordinate. Cioè, che

$$\langle a, b \rangle = \langle x, y \rangle \iff \{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$$

Le coppie ordinate sono **ben definite**.

Generalizzazione Possiamo generalizzare le coppie ordinate a **tuple ordinate** di lunghezza $n \geq 2$ (n-tuple ordinate) definendo

$$\langle x_1, x_2, \ldots, x_n, x_{n+1} \rangle = \langle \langle x_1, x_2, \ldots, x_n \rangle, x_{n+1} \rangle$$

> [!warning] Correggere lo spacing #todo/uni

Prodotto cartesiano Dati due insiemi A e B, definiamo il prodotto cartesiano come

$$A \times B = \{\,\langle x, y \rangle \mid x \in A, y \in B\,\}$$

$A \times B$ è l'insieme di tutte le coppie ordinate dove:

- il primo elemento appartiene ad A
- il secondo elemento appartiene a B

Notare che:

- $A \times B \neq B \times A$
- $A \times \varnothing = \varnothing = \varnothing \times A$

$A \times A$ è a volte denotato con A^2.

Sequenze S^n è l'insieme di tutte le n-tuple di elementi di S definito tramite prodotti cartesiani di S. Una **sequenza finita** di elementi di S è un elemento di S^n per qualche $n \in \mathbb{N}$.

In altre parole, una sequenza è una tupla ordinata

$$\langle s_1, \dots s_n \rangle$$

dove $n \in \mathbb{N}$ e ogni $s_i \in S$.

Segmento Data una sequenza finita $\sigma = \langle s_1, \dots, s_n \rangle$, una sequenza $\sigma' = \langle s_k, s_{k+1}, \dots, s_\ell \rangle$ dove $1 \leq k \leq \ell \leq n$ è chiamata un **segmento** di σ.

Il segmento è **iniziale** sse $k = 1$.

Relazioni

Una **relazione** tra gli elementi di due insiemi A e B non è altro che un sottoinsieme di $A \times B$.

Una relazione rappresenta un **collegamento** tra gli elementi di A e quelli di B.

Relazioni tra oggetti

Se la coppia ordinata $\langle x, y \rangle$ appartiene a una relazione $R \subseteq A \times B$, si dice che $x \in A$ ha come **corrispondente** $y \in B$ nella relazione R oppure che x è *in relazione con* y.

Rappresentazione tabulare

Ogni relazione si può rappresentare graficamente tramite una tabella.

Rappresentazione matriciale

R si può anche rappresentare tramite una **matrice booleana**.

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

Ogni riga rappresenta un elemento dell'insieme A e ogni colonna rappresenta un elemento di B.

Elementi di una relazione

Sia $R \subseteq A \times B$ una relazione

- Il **dominio** di R (dom(R)) è l'insieme di tutti gli oggetti $x \in A$ tali che $\langle x, y \rangle \in R$ per qualche $y \in B$.

  dom$(R) = \{ x \in A \,|\, \exists\, y \in B, \langle x, y \rangle \in R \}$.

- Il **codominio** è l'insieme di tutti gli oggetti $y \in B$ tali che $\langle x, y \rangle \in R$ per qualche $x \in A$.

  codom$(R) = \{ y \in B \,|\, \exists\, x \in A, \langle x, y \rangle \in R \}$.

- Il **campo** o **estensione** di R è dom$(R) \cup$ codom(R).

Relazioni n-arie

Il concetto di relazione può estendersi a tuple ordinate con **più di due** elementi.

Se gli elementi delle tuple appartengono allo stesso insieme A, allora una relazione n-aria è un sottoinsieme di A^n.

Esempi:

- $\{\, \langle x, x \rangle \mid x \in A \,\}$ è una relazione binaria su A
- $\{\, \langle x, y \rangle \mid x, y \in \mathbb{N}, x \leq y \,\}$ è la relazione d'ordine naturale su $\mathbb{N}$
- $\{\, \langle x, y, z \rangle \mid x, y, z \in \mathbb{R}, x^2 + y^2 = z^2 \,\}$ è un'area geometrica

Operazioni su relazioni

Siano $R, S \subseteq A \times B$ due relazioni

- $R \cup S$ ha tutte le coppie che appartengono a R o a S
- $R \cap S$ ha tutte le coppie che appartengono ad entrambi R e S
- $\overline{R} = \{\, \langle x, y \rangle \mid \langle x, y \rangle \notin R \,\} \subseteq A \times B$ è il **complemento** di R
- $R^{-1} = \{\, \langle y, x \rangle \mid \langle x, y \rangle \in R \,\} \subseteq A \times B$ è la **relazione inversa** di R

Proprietà delle relazioni

Siano $R, S \subseteq A \times B$ due relazioni

- Se $R \subseteq S$ allora $\overline{S} \subseteq \overline{R}$
- $\overline{(R \cap S)} = \overline{R} \cup \overline{S}$
- $\overline{(R \cup S)} = \overline{R} \cap \overline{S}$
- se $R \subseteq S$ allora $R^{-1} \subseteq S^{-1}$
- $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
- $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

Esempi Siano $A = \{ a, b \}, R = \{ \langle a, b\rangle, \langle b, a\rangle \}, S = \{ \langle a, b\rangle, \langle a, a\rangle \}$ ($R \subseteq A^2; S \subseteq A^2$).

1. $R \cap S = \{ \langle a, b\rangle \}$
2. $\overline{R \cup S} = \{ \langle b, b\rangle \}$
3. $R^{-1} = R$
4. $S^{-1} \neq S$

Identità

Dato un insieme A, la relazione

$$I_A = \{ \langle x, x\rangle \mid x \in A \}$$

dove ogni elemento è in relazione con se stesso è chiamata l'**identità** su A.

Proprietà delle relazioni binarie

Una relazione $R \subseteq A^2$ è

- **Riflessiva** se $\langle x, x\rangle \in R \,\forall x \in A$ ($I_A \subseteq R$)
- **Simmetrica** se $\langle x, y\rangle \in R \implies \langle y, x\rangle \in R$ ($R = R^{-1}$)
- **Antisimmetrica** se $\langle x, y\rangle, \langle y, x\rangle \in R \implies x = y$ ($R \cap R^{-1} \subseteq I_A$)
- **Antisimmetrica** (*def alternativa*) se $x \neq y \wedge \langle x, y\rangle \in R \implies \langle y, x\rangle \notin R$ ($R \cap R^{-1} \subseteq I_A$)
- **Transitiva** se $\langle x, y\rangle, \langle y, z\rangle \in R \implies \langle x, z\rangle \in R$

Funzioni

Una classe di relazioni binarie di particolare importanza sono le **funzioni** (o **applicazioni**).

Una funzione è una relazione $R \subseteq A \times B$ tale che ad ogni $a \in A$ corrisponde **al più** un elemento $b \in B$.

Formalmente: se $\langle a, b\rangle, \langle a, c\rangle \in R$ allora $b = c$.

Notazione: $f : A \to B$

Se per ogni $a \in A$ esiste **esattamente un** $b \in B$ tale che $\langle a, b\rangle \in R$, allora f è una **funzione totale**.

Riformulazione: una relazione $f \subseteq A \times B$ è una funzione se per ogni $x \in \text{dom}(f)$ esiste un unico $y \in B$ tale che $\langle x, y\rangle \in f$. $f(x)$ denota tale elemento y.

Se $x \in \text{dom}(f)$, allora si dice che f è **definita** in x. Se $A = \text{dom}(f)$ allora f è una funzione **totale**.

Funzione iniettiva

Una funzione f è **iniettiva** se porta elementi distinti del dominio in elementi distinti del codominio (immagine).

$$f : A \to B \text{ è iniettiva sse per ogni } x, y \in A, x \neq y \implies f(x) \neq f(y).$$

Funzione suriettiva

Una funzione f è **suriettiva** quando ogni elemento di B è immagine di almeno un elemento di A ossia, quando $B = \text{codom}(f)$.

$$f : A \to B \text{ è suriettiva sse per ogni } y \in B \text{ esiste un } x \in A \text{ tale che } f(x) = y.$$

Funzione biiettiva

Una funzione $f : A \to B$ è **biettiva** sse è iniettiva e suriettiva.

Attenzione: f può non essere totale.

- Ad ogni $x \in \text{dom}(f)$ corrisponde esattamente un $y \in B$
- Ad ogni $y \in B$ corrisponde esattamente un $x \in \text{dom}(f)$

Corrispondenza biunivoca

Una **corrispondenza biunivoca** tra A e B è una relazione binaria $R \subseteq A \times B$ tale che ad ogni elemento di A corrisponde uno ed un solo elemento di B e viceversa, ad ogni elemento di B corrisponde uno ed un solo elemento di A.

Tale R deve essere una funzione *totale*, *iniettiva* e *suriettiva*.

Formalizzazione

$f \subseteq A \times B$

$$\mathsf{dom}(f) = \{\, x \in A \mid \exists\, y \in B. \langle x, y \rangle \in f \,\}$$
$$\mathsf{codom}(f) = \{\, y \in A \mid \exists\, x \in B. \langle x, y \rangle \in f \,\}$$

Funzione (parziale)

$$\forall\, a \in A. \forall\, x, y \in B. (\langle a, x \rangle \in f \wedge \langle a, y \rangle \in f) \implies x = y$$

Funzione totale

$$\forall\, a \in A. \exists!\, x \in B. \langle a, x \rangle \in f$$

Funzione iniettiva

$$\forall\, a \in A. \forall\, x, y \in B. (\langle a, x \rangle \in f \wedge \langle a, y \rangle \in f) \implies x = y \wedge$$
$$\forall\, a, b \in A. \forall\, x \in B. (\langle a, x \rangle \in f \wedge \langle b, x \rangle \in f) \implies a = b$$

Funzione suriettiva

$$\forall\, a \in A. \forall\, x, y \in B. (\langle a, x \rangle \in f \wedge \langle a, y \rangle \in f) \implies x = y \wedge$$
$$\forall\, x \in B. \exists\, a \in A. \langle a, x \rangle \in f$$

Funzione biiettiva

$$\forall\, a \in A. \forall\, x, y \in B. (\langle a, x\rangle \in f \wedge \langle a, y\rangle \in f) \implies x = y \wedge$$
$$\forall\, a, b \in A. \forall\, x \in B. (\langle a, x\rangle \in f \wedge \langle b, x\rangle \in f) \implies a = b \wedge$$
$$\forall\, x \in B. \exists\, a \in A. \langle a, x\rangle \in f$$

Punto fisso

Sia A un insieme e $f : A \to A$ una funzione.

Un **punto fisso** di f è un elemento di A che coincide con la sua immagine

$$x = f(x)$$

Operazioni

Sia A un insieme.

Un'**operazione** (n-aria) su A è una funzione $A^n \to A$.

L'operazione è totale sse la funzione è totale.

Immagine inversa

Sia $f : A \to B$ una funzione e $y \in B$ l'**immagine inversa** di f in y è

$$f^{-1} : B \to \mathcal{P}(A)$$
$$f^{-1}(y) = \{\, x \in A \mid f(x) = y \,\}$$

Nota: f è iniettiva sse per ogni $y \in B$, $f^{-1}(y)$ ha al più un elemento.

Funzione inversa

Una funzione $f : A \to B$ è **invertibile** se esiste una funzione $g : B \to A$ tale che per ogni $x \in A$ e ogni $y \in B$o

$$g(f(x)) = x$$
$$f(g(y)) = y$$

In questo caso, g è l'**inverso** di f e si rappresenta come f^{-1}.

Una funzione f è invertibile sse è iniettiva. f_{-1} è totale sse f è suriettiva.

Composizione di Funzioni

La **composizione** di due funzioni si riferisce all'applicazione di una funzione al risultato di un'altra.

Siano $f : A \to B$ e $g : B \to C$ due funzioni. La funzione composta $g \circ f : A \to C$ è definita per ogni $x \in A$ da

$$(g \circ f)(x) = g(f(x))$$

$(g \circ f)(x)$ è definita sse $f(x)$ e $g(f(x))$ sono definite.

Se $f : A \to B$ e $g : C \to D$ sono due funzioni, allora la composizione $g \circ f$ è solo definibile se codom$(f) \subseteq C$.

Le proprietà della composizione:

- **Associativa:** $f \circ (g \circ h) = (f \circ g) \circ h$
- Se f e g sono entrambe iniettive, allora $f \circ g$ è **iniettiva**
- Se f e g sono entrambe suriettive, allora $f \circ g$ è **suriettiva**
- Se f e g sono entrambe invertibili, allora $f \circ g$ è **invertibile** ($(g \circ f)^{-1} = f^{-1} \circ g^{-1}$)

Funzione caratteristica

I sottoinsiemi di un insieme A si possono anche rappresentare tramite una funzione detta **caratteristica**.

La funzione caratteristica di un insieme $S \subseteq A$ è la funzione $f_S : A \to \{ 0, 1 \}$ dove

$$f_S(x) = \begin{cases} 0 & x \notin S \\ 1 & x \in S \end{cases}$$

Per ogni $x \in A$

- $f_{S \cap T}(x) = f_S(x) \cdot f_T(x)$
- $f_{S \cup T}(x) = f_S(x) + f_T(x) - f_S(x) \cdot f_T(x)$
- $f_{S \triangle T}(x) = f_S(x) + f_T(x) - 2 \cdot f_S(x) \cdot f_T(x)$

Multinsiemi

Un **multinsieme** è una variante di un insieme dove gli elementi si possono ripetere

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

Formalmente un multinsieme è una funzione da un insieme a $\mathbb{N}$

$$f : A \to \mathbb{N}$$

che esprime quante volte si ripete ogni elemento nel multinsieme ($A = \{ a, b, c, d \}$)

$$\{ \langle a, 2 \rangle, \langle b, 1 \rangle, \langle c, 3 \rangle, \langle d, 0 \rangle \}$$

Cardinalità

I **numeri cardinali** si utilizzano per misurare gli insiemi (indicare la loro *grandezza*). Se un insieme è **finito**, la sua cardinalità è un numero naturale (il numero di elementi). Con i numeri cardinali, possiamo anche misurare e classificare insiemi **infiniti**.

Cardinalità tramite funzioni

Georg Cantor utilizzò le proprietà delle funzioni per paragonare la cardinalità degli insiemi.

Sia f una funzione $f : A \to B$

- Se f è *suriettiva* allora B non è "più grande" di A
- Se f è *totale* e *iniettiva* allora A non è "più grande" di B

Due insiemi sono **equipotenti** (hanno la stessa cardinalità) sse esiste una funzione **biunivoca** fra di loro.

$$A \sim B$$

Cardinalità finite

Se A ha n elementi, allora $A \sim \{1, \ldots, n\}$. In questo caso si dice che A è **finito** e ha **cardinalità** (o potenza) n.

Utilizziamo la notazione

$$|A| = n$$

I numeri naturali si utilizzano come cardinali finiti.

Se$|A| = n$ allora $|\mathscr{P}(A)| = 2^n$.

Numerabili

Basati su questa definizione, chiamiamo **numerabili** tutti gli insiemi che hanno la cardinalità di $\mathbb{N}$. I suoi elementi possono essere posti in corrispondenza biunivoca con i naturali.

$$A \sim \mathbb{N} \sim \mathbb{N}^+$$

La cardinalità di $\mathbb{N}$ è chiamata $\aleph_0$.

$$|\mathbb{N}| = \aleph_0$$

$\aleph_0$ è il più piccolo dei numeri cardinali **transfiniti** (i cardinali per misurare insiemi infiniti). Ovviamente $\aleph_0$ non è un numero naturale.

I seguenti insiemi sono numerabili:

- L'insieme dei numeri pari
- L'insieme dei numeri primi
- L'insieme dei numeri interi $\mathbb{Z}$

$$f : \mathbb{N} \to \mathbb{Z}$$

$$f(x) = \begin{cases} -\frac{x}{2} & \text{se } x \text{ pari} \\ \lceil \frac{x}{2} \rceil & \text{se } x \text{ dispari} \end{cases}$$

- Il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$
- I numeri razionali $\mathbb{Q}$ ($\subset \mathbb{N} \times \mathbb{N}$)

Il continuo

$$[0, 1] = \{\, x \in \mathbb{R} \mid 0 \leq x \leq 1 \,\} \sim \mathscr{P}(\mathbb{N})$$

Denotiamo per convenzione $|\mathscr{P}(\mathbb{N})| = 2^{\aleph_0}$. Allora $|\mathbb{R}| \geq 2^{\aleph_0}$.

Cantor dimostro che $\aleph_0 < 2^{\aleph_0}$ (in realtà che $|A| < |\mathscr{P}(A)|$). Dunque $\mathbb{R}$ non è numerabile.

Teorema di Cantor

$$\aleph_0 < 2^{\aleph_0}$$

Dobbiamo dimostrare che *non esiste* una funzione biunivoca $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$.

Supponiamo che esiste una tale funzione f. Definiamo

$$Z = \{\, z \in \mathbb{N} \mid n \notin f(n) \,\} \subseteq \mathbb{N}$$

Siccome f è biunivoca (quindi suriettiva), esiste $k \in \mathbb{N}$ tale che $f(k) = Z$.

Domanda: $k \in Z$?

Se $k \in Z$, allora per definizione $k \notin f(k) = Z$. Se $k \notin Z$, allora $k \notin f(x)$ e quindi per definizione $k \in Z$.

Conclusione: la funzione f non può esistere.

Gerarchia transfinita

Cantor definì la gerarchia dei numeri transfiniti

$$\aleph_0 < \aleph_1 < \aleph_2 < \dots$$

L'**ipotesi del continuo** dice che $\aleph_1 = 2^{\aleph_0}$. Non ci sono insiemi di cardinalità intermedia fra $\mathbb{N}$ e $\mathbb{R}$.

Strutture relazionali, Grafi e Ordinamenti

Rappresentazioni

Le relazioni possono essere rappresentate da diverse forme:

- **Rappresentazione per elencazione:** descrivere l'insieme di coppie ordinate ($R = \{\, \langle 1,2\rangle, \langle 2,4\rangle, \langle 3,6\rangle \,\}$)
- **Rappresentazione sagittale:** collegare con delle frecce gli elementi che verificano la relazione
- **Rappresentazione tramite diagramma cartesiano:** se S e T sono sottoinsiemi di $\mathbb{R}$, rappresentare le coppie come coordinate sul piano cartesiano
- **Rappresentazione tramite tabella:** una matrice booleana con per colonne gli elementi dell'insieme di arrivo e per righe l'insieme di partenza.

Relazioni in un insieme

Una relazione $R \subseteq S \times S$ è detta **relazione in** S. In una relazione in S, la rappresentazione sagittale collassa in un **grafo**. Usiamo lo stesso insieme per l'origine e la destinazione di ogni freccia. Formalmente un grafo è costituito da **nodi** collegati fra loro da frecce (o **spigoli**). Se $\langle x, y\rangle \in \mathbb{R}$, disegnamo uno spigolo da x a y.

Le proprietà di una relazione sonon (*again*):

- **Riflessiva** se: $\langle x, x\rangle \in R \, \forall x \in S$ (*ogni nodo ha un cappio*)
- **Irriflessiva** se: $\langle x, x\rangle \notin R \, \forall x \in S$ (*nessun nodo ha un cappio*)
- **Simmetrica** se: $\langle x, y\rangle \in R \implies \langle y, x\rangle \in R$ (*ogni spigolo ha il suo inverso*)
- **Asimmetrica** se: $\langle x, y\rangle \in R \implies \langle y, x\rangle \notin R$ (*nessuno spigolo ha il suo inverso e nessun nodo ha un cappio*)
- **Antisimmetrica** se: $\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \implies x = y$ (*nessuno spigolo ha il suo inverso (escluso il cappio)*)
- **Transitiva** se: $\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \implies \langle x, z\rangle \in R$

Una relazione $R \subseteq S \times S$ in S è

- **Connessa** se ogni due elementi sono collegati. $\forall x, y \in S$x se $x \neq y$ allora $\langle x, y\rangle \in R$ oppure $\langle y, x\rangle \in R$
- **Relazione di equivalenza** se è riflessiva, transitiva e simmetrica

La relazione vuota $\varnothing \subseteq S \times S$ è irriflessiva, simmetrica, asimmetrica, antisimmetrica e transitiva. L'identità I_S è riflessiva, simmetrica e transitiva (è una relazione di equivalenza).

Riflessività ed operazioni

Siano R ed R' due relazioni su S

1. Se R è riflessiva, R^{-1} è riflessiva (*stesso per irriflessibilità*)
2. R è riflessiva sse $\overline{R}$ è irriflessiva
3. Se R ed R' sono riflessive, allora anche $R \cup R'$ e $R \cap R'$ sono riflessive (*stesso per irriflessibilità*)

Simmetria ed operazioni

Siano R ed R' due relazioni su S

1. R è simmetrica sse $R = R^{-1}$
2. Se R è simmetrica, allora R^{-1} e $\overline{R}$ sono simmetriche
3. R è antisimmetrica sse $R \cap R^{-1} \subseteq I_S$
4. R è asimmetrica sse $R \cap R^{-1} = \varnothing$
5. Se R ed R' sono simmetriche, allora anche $R \cup R'$ e $R \cap R'$ sono simmetriche

Transitività ed operazioni

Se R ed R' sono transitive allora $R \cap R'$ è transitiva. $R \cup R'$ non è necessariamente transitiva.

Matrici booleane

Una matrice booleana è una matrice a valori $\{0, 1\}$. La matrice booleana associata a $R \subseteq S \times T$ si denota M_R. Se $|S| = n$ e $|T| = m$, M_R ha n righe e m colonne.

La riga i corrisponde all'elemento $s_i \in S$, la colonna j corrisponde all'elemento $t_j \in T$ ed è tale che

$$m_{ij} = \begin{cases} 1 & \langle s_i, t_j \rangle \in R \\ 0 & \text{altrimenti} \end{cases}$$

Proprietà di una matrice booleana Se R è una relazione su S, M_R ha le stesse proprietà della visualizzazione tabulare.

- R è **riflessiva** sse M_R ha tutti 1 sulla diagonale principale
- R è **irriflessiva** sse M_R ha tutti 0 sulla diagonale principale
- R è **simmetrica** sse M_R è simmetrica
- R è **asimmetrica** sse per ogni i, j, se $m_{ij} = 1$, allora $m_{ji} = 0$
- R è **antisimmetrica** sse per ogni $i \neq j$, se $m_{ij} = 1$, allora $m_{ji} = 0$
- $M_{R^{-1}}$ è la trasposta di M_R
- $M_{\overline{R}}$ si ottiene scambiando 0 e 1 in M_R

$$R = \{ \langle 0, 0 \rangle, \langle 1, 2 \rangle \}$$

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow M_{R^{-1}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Operazioni su matrici booleane

Se M e N sono due matrici booleane di dimensini $n \times m$, $M \sqcup N$ (il **join** di M e N) è la matrice booleana L di dimensine $n \times m$ i cui elementi sono

$$\ell_{ij} = \begin{cases} 1 & m_{ij} = 1 \lor n_{ij} = 1 \\ 0 & \text{altrimenti} \end{cases}$$

$M \sqcap N$ (il **meet** di M e N) è la matrice booleana L di dimensione $n \times m$ i cui elementi sono

$$\ell_{ij} = \begin{cases} 1 & m_{ij} = 1 \land n_{ij} = 1 \\ 0 & \text{altrimenti} \end{cases}$$

$\sqcup$ e $\sqcap$ sono commutative, associative e distributive fra di loro.

Prodotto booleano

Siano M e N matrici booleane di dimensioni $n \times m$ e $m \times p$ rispettivamente. Il loro **prodotto booleano** è la matrice $L = M \odot N$ di dimensioni $n \times p$ dove

$$\ell_{ij} = \begin{cases} 1 & \exists k, 1 \leq k \leq m \text{ t.c. } m_{ik} = 1 \land n_{kj} = 1 \\ 0 & \text{altrimenti} \end{cases}$$

Esempio:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Questa operazione è associativa ma non commutativa.

YT Link con spiegazione[1].

[1] https://youtu.be/BjTeDlpj-ts?si=snvhzdZvQByBGinl

Composizione di relazioni

Dati $R_1 \subseteq S \times T$, $R_2 \subseteq T \times Q$:

$$R_2 \circ R_1 = \{ \langle x, y \rangle \in S \times Q \mid \exists \in T. \langle x, z \rangle \in R_1, \langle z, y \rangle \in R_2 \}$$

$R_2 \circ R_1$ è la **composizione** di R_1 e R_2.

La composizione si può calcolare tramite il prodotto di matrici booleane.

$$M_{R_2 \circ R_1} = M_{R_1} \odot M_{R_2}$$

Relazioni di Equivalenza

Una **relazione di equivalenza** ci aiuta a creare blocchi di elementi che hanno *qualcosa* in comune. Sono relazioni che si comportano "come l'uguaglianza" tra oggetti. Dal punto di vista di una proprietà data, **non** esistono differenze tra due elementi in una relazione di equivalenza.

Def: una relazione riflessiva, simmetrica e transitiva è detta **relazione di equivalenza**.

Esempio:

- Appartenenere alla stessa classe
- Essere nati nello stesso anno
- Essere parallele nell'insieme delle rette
- ...

Se $f : A \to B$ è una funzione totale, allora la relazione

$$R := \{ \langle x, y \rangle \in A \times A \mid f(x) = f(y) \}$$

è una relazione di equivalenza.

La rappresenzazione sagittale di una relazione di equivalenza consiste di diversi grafi totalmente collegati.

Partizioni e classi di equivalenza

Dividendo S in gruppi i cui elementi sono "uguali", possiamo studiare insiemi grandi osservando soltanto pochi elementi. Questi gruppi sono chiamati **classi di equivalenza**.

Sia S un insieme. Una partizione di S è una famiglia di insiemi $\mathcal{P} = \{ T_1, \ldots, T_n \}, T_i \subseteq S, 1 \leq i \leq n$ tali che:

- $T_i \neq \varnothing$ per ogni i, $1 \leq i \leq n$
- $T_i \cap T_j \neq \varnothing$ per ogni i, j, $1 \leq i \leq j \leq n$
- $\cup \mathcal{P} = S$

Se R è una **relazione di equivalenza** su S allora $T \neq \varnothing \subseteq S$ è una classe di equivalenza se per ogni $x \in S$:

$$x \in T \iff \{ y \in S \mid \langle x, y \rangle \in R \} = T$$

Cioè, x è in relazione con tutti e soltanto quegli elementi di T.

Sia S un insieme e R una relazione di equivalenza su S. Ogni elemento $x \in S$ definisce una classe di equivalenza

$$[x]_R = \{ y \in S \mid \langle x, y \rangle \in R \}$$

La famiglia di insiemi $\{ [x]_R \mid x \in S \}$ (gli elementi sono le classi di equivalenza di S) è chiamato l'**insieme quoziente** di S rispetto a R (indicato con S/R). L'insieme quoziente è una partizione di S.