Appunti di Fondamenti

Fondamenti dell'Informatica - CdL Informatica 23/24

Federico Zotti

2023-09-30

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 e Insiemi

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

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* ($\mathbb{N}$).

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

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 $\mathbb{Z}$.

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

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

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 vilaggio 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
  - $\{x \mid x$ è un colore dell'arcobaleno $\}$
  - $\{x \mid x \in \mathbb{Z}, x > 3, x \leq 100\} = \{4, 5, \dots, 99, 100\}$
  - $\{x \mid x$ 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

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

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

$$A \cap B = \{ x \mid x \in A \wedge x \in B \}$$

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

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

Le proprietà della sottrazione sono:

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

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

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*)