# Fondamenti dell'Informatica

Tiziano Marzocchella

A.A. 2022/2023

## Indice

# 1 Introduzione

In questo corso affronteremo...

- Linguaggio matematico di base: insiemi, relazioni, funzioni, ecc...
- Strutture discrete: coppie, n-uple, stringhe, grafi, alberi, ecc..
- Calcolo combinatorio: permutazioni, disposizioni, combinazioni
- Tecniche di dimostrazione: simboliche, discorsive, per induzione
- Specifiche formali: linguaggi formali, logica, ricorsione

# 2 Insiemi

Un *insieme* è una collezione di oggetti, detti elementi.

## 2.1 Notazione

- Utilizziamo $A, B, C, \ldots$ per denotare insiemi generici o direttamente un nome specifico
- Utilizziamo $a, b, c, \ldots$ per denotare gli elementi di un insieme
- $a \in A$, a *appartiene a* A
- $a \notin A$, a *non appartiene a* A

## 2.2 Rappresentazione

- *Estensionale*, per enumerazione, ovvero elencare in una lista tutti gli elementi
- *Intenzionale*, per proprietà

Nella rappresentazione intenzionale, un insieme $X$ contiene tutti gli elementi $x$ dell'insieme di riferimento $A$ che soddisfano la proprietà $P$.

$$X = \{x \in A \mid P(x)\}$$

**Esempio.**

$$\mathbb{N}^p = \{n \mid n \in N \text{ e n è divisibile per 2}\}$$
$$\mathbb{Q} = \{\frac{n}{m} \mid n \in \mathbb{Z}, m \in \mathbb{N}^+\}$$

## 2.3 Confronto di insiemi

**Definizione.** Due insiemi sono uguali ($A = B$) se hanno gli stessi elementi, altrimenti sono diversi ($A \neq B$)

**Esempio.**

$$V = \{a, e, i, o, u\} V1 = \{a, e, i, o, e, a\}$$

## 2.4 Inclusione

**Definizione.** $A$ è un sottoinsieme di $B$ ($A \subseteq B$) se ogni elemento di $A$ appartiene anche a $B$. $A$ è un sottoinsieme proprio di $B$ se ($A \subseteq B$) e $A \neq B$

## 2.5 Proprietà di uguaglianza e inclusione

- Riflessività, vale sempre per un insieme e se stesso

$$A = A \quad A \subseteq A$$

- Transitività

$$\text{Se } A = B \text{ e } B = C \text{ allora } A = C$$
$$\text{Se } A \subseteq B \text{ e } B \subseteq C \text{ allora } A \subseteq C$$

- Simmetria
$$\text{Se } A = B \text{ allora } B = A$$

- Anti-simmetria
$$\text{Se } A \subseteq B \text{ e } B \subseteq A \text{ allora } A = B$$

## 2.6 Operazioni su insiemi

- Unione
- Intersezione
- Differenza
- Complemento

## 2.7 Uguaglianze e leggi

Una uguaglianza valida, cioè vera per tutti i possibili casi, si chiama *legge*.

## 2.8 Operatori booleani

Sono operazioni su valori booleani (vero o falso) che possiamo utilizzare per scrivere espressioni complesse che denotano insiemi.

Per dimostrare la validità di una uguaglianza si utilizzano dimostrazioni di tipo:

- discorsive
- grafiche
- per sostituzione

## 2.9 Leggi per operatori su insiemi

- Leggi per **unione** e **intersezione**
  - associatività
  - unità
  - commutatività
  - idempotenza
  - assorbimento
- Leggi che collegano $\cup$, $\cap$ e $\overline{()}$
- Leggi per $\setminus$
- Complemento
- Convoluzione
- De Morgan
- Universo e insieme vuoto

## 2.10 Cardinalità

La cardinalità di un insieme finito è il numero di elementi al suo interno.

- $|\varnothing| = 0$
- $A \subseteq B \implies |A| \leq |B|$
- $A = B \implies |A| = |B|$
- $A \subset B \implies |A| < |B|$, non vale per insiemi infiniti

## 2.11 Insiemi di insiemi

## 2.12 Numeri naturali come insiemi

## 2.13 Insieme delle parti

Dato un insieme $A$, l'insieme delle parti di $A$ è:

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}$$

- $\mathcal{P}(\{0,1,2\}) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$
- $\mathcal{P}(\varnothing) = \{\varnothing\}$
- $|\mathcal{P}(A)| = 2^{|A|}$

## 2.14 Prodotto cartesiano

Il prodotto cartesiano di due insiemi è l'insieme formato da tutte le coppie ordinate $(a, b)$ tali che $a \in A$ e $b \in B$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

## 2.15 Famiglie di insiemi

Sia $I$ un insieme finito (di indici).
Una famiglia di insiemi $F$ indicizzata da $I$ è:

$$F = \{A_i \mid i \in I\} = \{A_i\}_{i \in I}$$

- $\cup F = \cup_{i \in I} A_i$
- $\cap F = \cap_{i \in I} A_i$

## 2.16 Partizioni

Una partizione su un insieme $A$ è una famiglia di sottoinsiemi di $A$ tale che:

- ogni insieme $A_i$ è diverso da $\varnothing$
- $\cup_{i \in I} A_i = A$ (copertura di A)
- Presi $i \neq j$ si ha: $A_i \cap A_j = \varnothing$

Serve a classificare "esclusivamente" gli elementi di un insieme.

## 2.17 Paradosso di Russel

# 3 Relazioni

## 3.1 Nozioni di base

Dati gli insieme $A$ e $B$, una relazione $R \subseteq A \times B$ si scrive

$$R \in Rel(A, B)$$

$$R : A \leftrightarrow B$$

dove

$$Rel(A, B) = \mathcal{P}(A \times B)$$

- relazione vuota: $\varnothing \subseteq A \times B$ oppure $\varnothing_{A,B}$
- relazione completa: $A \times B$

### 3.1.1 Relazioni su un singolo insieme

Chiamiamo le relazioni con insieme di partenza e arrivo coincidenti **Relazioni su** $A$

**Esempio.**

$$Succ = \{(x, y) \in \mathbb{N} \in \mathbb{N} \mid y = x + 1\} \in Rel(\mathbb{N}, \mathbb{N}) \quad \text{Relazione su } \mathbb{N}$$

### 3.1.2 Relazione identità

Per un insieme $A$ la relazione identità è:

$$Id_A = \{(x, x) \mid x \in A\}$$

una relazione che associa ogni elemento di $A$ con se stesso. Viene definita solo per relazioni su singoli insiemi

## 3.2 Operazioni su relazioni

Possiamo definire nuove relazioni usando vari operatori insiemistici.
Date due relazioni $R$ e $S$ su $A$ e $B$,

$$R, S \in Rel(A, B)$$

- $R \cup S \subseteq A \times B$, unione tra $R$ e $S$
- $R \cap S \subseteq A \times B$, intersezione tra $R$ e $S$
- $R \setminus S \subseteq A \times B$, tutti gli elementi di $R$ tolti gli elementi di $S$
- $\overline{R} = (A \times B \setminus R) \subseteq A \times B$, complemento di $R$. Scelgo $A \times B$ come universo per garantire l'inclusione

Valgono tutte le leggi che abbiamo visto per gli insiemi, ma con $A \times B$ preso come insieme universo.

## 3.3 Composizione di relazioni

Siano $R : A \leftrightarrow B$ e $S : B \leftrightarrow C$, la **composizione** di $R$ con $S$ è:

$$R; S : A \leftrightarrow C$$

$$R; S = \{(x, y) \in A \times C \mid (\exists y \in B.(x, y) \in R \wedge (y, z) \in S\}$$

$R; S$ contiene tutti le coppie per le quali c'è un "cammino" da $A$ a $C$, seguendo le frecce delle relazioni.

### 3.3.1 Leggi per la composizione

Per tutti gli insiemi $A, B, C, D$ e tutte le relazioni $R : A \leftrightarrow B$, $S : B \leftrightarrow C$ e $T : C \leftrightarrow D$ valgono le seguenti leggi

- Associatività: $R; (S; T) = (R; S); T$
- Unità: $Id_A; R = R = R; Id_B$
- Assorbimento: $R; \varnothing_{B,C} = \varnothing_{A,C} = \varnothing_{A,B}; S$
- Distributività

## 3.4 Relazione opposta

Sia $R : A \leftrightarrow B$ una relazione. La sua relazione **opposta** è:

$$R^{op} = \{(y, x) \in B \times A \mid (x, y) \in R\}$$

### 3.4.1 Leggi per la relazione opposta

Per tutti gli insiemi $A, B, C$ e tutte le relazioni $R : A \leftrightarrow B$, $S : B \leftrightarrow C$ valgono le seguenti leggi

- Composizione: $R^{op}; S^{op} = (R; S)^{op}$
- Distributività:

## 3.5 Proprietà delle relazioni

### 3.5.1 Totalità

### 3.5.2 Univalenza

### 3.5.3 Suriettività

### 3.5.4 Iniettività

### 3.5.5 Osservazioni

**Schema TUSI**
**Dualità**

- $R$ è totale $\iff$ $R^{op}$è suriettiva
- $R$ è univalente $\iff$ $R^{op}$è iniettiva
- $R$ è suriettiva $\iff$ $R^{op}$è totale
- $R$ è iniettiva $\iff$ $R^{op}$è univalente

**Caratterizzazione**

$$R \text{ è totale} \iff Id_A \subseteq R; R^{op} \qquad R \text{ è suriettiva} \iff Id_B \subseteq R^{op}; R$$
$$R \text{ è univalente} \iff R; R^{op} \subseteq Id_A \qquad R \text{ è iniettiva} \iff R^{op}; R \subseteq Id_B$$

# 4 Funzioni

Dati due insiemi $A$ e $B$, $R : A \leftrightarrow B$ è una funzione se

$$\forall a \in A(\exists \text{ esattamente un } b \in B.(a, b) \in R$$

ovvero se $R$ è **totale** e **univalente**. Vediamo alcuni esempi:

- $Id_A$ è una funzione
- $A \times B$ non è una funzione, ma
  - se $|B| = 1$, è una funzione
  - se $|A| = 0$ e $|B| = 0$, è una funzione
- $\varnothing : A \leftrightarrow B$, non è una funzione, ma
  - se $|A| = 0$, è una funzione

## 4.1 Composizione di funzioni

Per tutti gli insiemi $A$, $B$ e $C$ e tutte le funzioni $f : A \to B$ e $g : B \to C$, la relazione $f; g$ è una funzione

$$f; g : A \to C$$

$g \circ f$ o $gf$, notazione matematica

## 4.2 Biiezioni

Dati $A$ e $B$, la relazione $R : A \leftrightarrow B$ è una biiezione se è totale, univalente, iniettiva e surgettiva.

$$\forall a \in A \text{ esiste esattamente un } b \in B.(a, b) \in R \wedge \forall b \in B \text{ esiste esattamente un } a \in A.(a, b) \in R$$

Il numero di biiezioni tra due insiemi $A$ e $B$ con $|A| = |B| = n$ è uguale a

$$n!$$

### 4.2.1 Osservazioni

Per tutti gli $A, B, C$ e $i : A \to B$ e $j : B \to C$ vale che

- $Id_A$ è una biiezione
- $i; j$ è una biiezione
- $i^{op}$ è una biiezione

### 4.2.2 Teorema di caratterizzazione

Per tutti gli insiemi $A$,$B$, la relazione $R : A \leftrightarrow B$ è biiezione se e solo se:

$$Id_A = R; R^{op} \text{ e } Id_B = R^{op}; R$$

$$R \text{ biiezione } \iff Id_A \subseteq R; R^{op} \wedge R; R^{op} \subseteq Id_A \wedge Id_B \subseteq R^{op}; R \wedge R^{op}; R \subseteq Id_B$$

### 4.2.3 Insiemi in biiezioni

$$A \cong B$$

Due insiemi sono in biiezione se esiste una biiezione $i : A \to B$
**Proprietà della biiezione** Dati gli insiemi $A, B, C$ vale:

- Riflessività, $A \cong A$
- Simmetria, $A \cong B \implies B \cong A$
- Transitività, $A \cong A \wedge B \cong C \implies A \cong C$

# 5 Induzione

L'induzione ci permette di definire insiemi, anche infiniti.

**Esempio.** Se prendiamo la definizione dell'insieme dei naturali

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

possiamo dire che non è una definizione soddisfacente perché

- cambiando l'ordine degli elementi nell'insieme la notazione con i puntini sospensivi non ha più senso.
$$\mathbb{N} = \{2, 0, 1, \ldots\}$$
- Un programma non saprebbe determinare il significato dei puntini sospensivi.

La definizione per induzione si può applicare sia agli insiemi che alle funzioni.

## 5.1 Definizione induttiva di insieme

Per definire un insieme $A$ con la definizione induttiva occorre definire 3 clausole:

1. Clausola **base**, che esplicita gli elementi di $A$
2. Clausola **induttiva**, che definisce come utilizzare gli elementi già presenti in A per costruire gli altri elementi
3. Clausola **terminale**, che stabilisce quando l'insieme $A$ non contiene altri elementi, ovvero è il più piccolo insieme che soddisfa le clausole 1 e 2.

## 5.2 Definizione induttiva di funzione

Una funzione $f : A \to B$ definita per induzione segue le seguenti clausole

1. Clausola **base**, ovvero il valore di $f(a)$ per ogni $a \in A$ (secondo la clausola base della definizione di A)
2. Clausola **induttiva**, ovvero le regole utilizzate per calcolare $f(a)$ usando i valori di $f$ per elementi che sono già in $A$

La definizione induttiva garantisce una funzione totale

## 5.3 Dimostrazione per induzione

Si ha una proprietà $P$ sui naturali

$$P : \mathbb{N} \to Bool$$

Verifichiamo le seguenti affermazioni

- Caso base: $P(0)$ è vera
- Passo induttivo: Per ogni $m \in \mathbb{N}$

$$(P(n) \implies P(n+1))$$

Se entrambe sono vere allora $P(m)$ è vera per ogni $m \in \mathbb{N}$

### 5.3.1 Regola di inferenza

Possiamo esprimere la dimostrazione per induzione attraverso la notazione di regola di inferenza

$$\frac{P(0), \forall n \in \mathbb{N}.\,(P(n) \implies P(n+1))}{\forall m \in \mathbb{N}.P(m)}$$

che si legge: “Per dimostrare ciò che sta sotto la riga, basta dimostrare ciò che sta sopra la riga”

# 6 Grafi

I grafi ci permettono di modellare precisamente e in modo visualmente intuitivo relazioni tra elementi di un insieme.

Esistono grafi *orientati* e *non orientati*. I grafi orientati sono più direttamente collegati al concetto di relazione.

## 6.1 Grafo orientato

Un *grafo orientato* è una relazione $E : V \leftrightarrow V$ su un insieme **finito** $V$. Scriviamo: $G = (E, V)$

- $V$: insieme di **nodi** o **vertici**
- $E$: insieme di **archi** o **lati** (coppie)

Questi grafi sono *orientati* perchè ad un arco dal nodo $x$ al nodo $y$ possiamo assegnare un verso, e quindi possiamo anche creare archi che partono e arrivano nello stesso nodo, chiamati **cappio** o **loop**. Ne risulta che presi due nodi distinti $x$ e $y$, un arco $(x, y) \in E \neq (y, x) \in E$.

Dato un grafo $G$ indicheremo:

- con $n$ il numero dei nodi del grafo, cioè $n = |V|$
- con $m$ il numero di archi, ovvero $m = |E|$

## 6.2 Vicinato e grado dei nodi

Due nodi x e y sono adiacenti se c'è un arco da x a y o c'è un'arco da y a x

$$(x, y) \in E \lor (y, x) \in E$$

Per ogni nodo possiamo indicare

- Vicinato in uscita (stella uscente) di x
$$N^+(x) = \{y \mid (x, y) \in E\}$$
- Vicinato in ingresso (stella entrante) di x
$$N^-(x) = \{y \mid (y, x) \in E\}$$
- Grado in uscita di x:
$$d^+_x = |N^+(x)|$$
- Grado in ingresso di x:
$$d^-_x = |N^-(x)|$$

**Hand-Shaking Lemma per grafi orientati**

$$\sum_{x \in V} d^-_x = \sum_{x \in V} d^+_x = |E|$$

## 6.3 Grafo come relazione

Essendo un grafo una relazione su un insieme finito di nodi, ovviamente possiamo verificare le proprietà TUSI. Le proprietà TUSI (Totale, Univalente, Surgettiva, Iniettiva) diventano condizioni sul grado dei nodi.

1. $E : V \leftrightarrow V$ è **totale** se e solo se per ogni nodo $x \in V$ vale $d_x^+ \geq 1$;
2. $E : V \leftrightarrow V$ è **univalente** se e solo se per ogni nodo $x \in V$ vale $d_x^+ \leq 1$;
3. $E : V \leftrightarrow V$ è **surgettiva** se e solo se per ogni nodo $x \in V$ vale $d_x^- \geq 1$;
4. $E : V \leftrightarrow V$ è **iniettiva** se e solo se per ogni nodo $x \in V$ vale $d_x^- \leq 1$;

## 6.4 Cammini

- Un *walk* è una sequenza di nodi $P = v_0, \ldots, v_k$ con $k \in \mathbb{N}$ tale che $(v_i, v_{i+1}) \in E$ per ogni $i \in \{1, \ldots, k\}$.
- Un *trail* è un *walk* che non attraversa più volte lo stesso **arco**.
- Un *path* è un *trail* che non attraversa più volte lo stesso **nodo**.

La lunghezza di un walk è $k$ e gli estremi sono $v_0$ e $v_k$.
Un walk di lunghezza zero è costituito solo dal nodo $v_0$.
Esiste un walk di lunghezza $n \in \mathbb{N}$ da $x$ a $y$ se e solo se $(x, y) \in E^n$.

**Dimostrazione.** Dimostriamo per induzione questa proprietà

- **Caso base**: Sia $v \in V$, v è walk di lunghezza 0 per definizione v è un walk da v a v, ma $E^0 = Id_v$, quindi $(v, v) \in E^0 = Id_v$.
- **Passo induttivo**: Esiste $v_1 v_2, \ldots, v_{n+1}$ un walk di lunghezza n + 1 se e solo se c'è un arco $(v_0, v_1) \in E$ e un walk $v_0, v_1, \ldots, v_{n+1}$ di lunghezza n.

Se esiste un walk da $x$ a $y$ allora esiste un trail da $x$ a $y$.

## 6.5 Walk chiusi, circuiti e cicli

Un walk è detto chiuso se

## 6.6 Connettività

Un grafo orientato $G = (V, E)$ è fortemente connesso se per ogni coppia di nodi $x, y \in V$ esiste un walk da $x$ a $y$.

Una componente fortemente connessa di G è un sotto insieme non vuoto di nodi $U \subseteq V$ tale che

1. Per ogni copppia di nodi $x, y \in U$ esiste un walk da $x$ a $y$.
2. Se $U' \subseteq V$ soddisfa la 1. e $U \subseteq U'$, allora $U = U'$.

**Altre proprietà**

- $G = (V, E)$ è fortemente connessa se e solo se $V \times V \subseteq E^*$
- $(x, y) \in E^* \cap (E^*)^{op}$ se e solo se $x$ e $y$ appartengono alla stessa SCC.
- $x$ e $y$ appartengono alla stessa SCC se e solo se esiste un walk chiuso che li attraversa entrambi.

## 6.7 Directed Acyclic Graphs

Un grafo orientato senza cicli si chiama **Directed Acyclic Graph** (DAG)

I nodi con grado di ingresso 0 vengono chiamati *sorgenti* e i nodi con grado di uscita 0 si chiamano *pozzi.*

Se $G = (V, E)$ è un DAG, allora $E^*$ è un ordinamento parziale.

**Definizione.** Ordinamenti topologici: Dato un DAG, un ordinamento topologico di G è una biiezione $\eta : V \to n = \{0, 1, 2, \ldots, n-1\}$ tale che

$$\text{Per ogni arco } (x, y) \in E \text{ vale che } \eta(x) < \eta(y)$$

## 6.8 Cammini e cicli Euleriani

**Definizione.** Circuito euleriano: Un circuito euleriano è un circuito che passa esattamente una volta per tutti gli archi del grafo.

**Definizione.** Trail euleriano: Un percorso euleriano è un trail che passa esattamente una volta per tutti gli archi del grafo.

Eulero ha sviluppato un teorema per decidere se esiste o meno un circuito o trail che passa per tutti gli archi.

**Definizione.** Teorema di Eulero
Dato un grafo non orientato e connesso,

1. Eiste un circuito euleriano se e solo se tutti i nodi hanno grado pari.
2. Esiste un trail euleriano da $x$ a $y$ se e solo se $x$ e $y$ sono gli unici nodi di grado dispari

## 6.9 Cicli e path hamiltoniani

Dato un grafo connesso (orientato o no orientato), un ciclo hamiltoniano è un ciclo che passa esattamente una volta per tutti i nodi del grafo.

Un path hamiltoniano può partire e arrivare in nodi distinti.

# 7 Alberi

Un albero è un grafo non orientato, connesso, aciclico e non vuoto.

## 7.1 Terminologia

- Una **foresta** è un grafo non orientato, aciclico e non vuoto.
- Una **foglia** è un nodo con grado 1.
- Un **nodo interno** è un nodo con grado ¿ 1
- Un **albero radicato** è un albero con un "nodo speciale" ovvero la **radice**