# Metodi matematici per l'informatica

Nicola Calvio

February 7, 2024

# TEORIA

## 1 Introduzione

Appunti del corso di Metodi matematici per l'informatica, tenuto dal prof. Cenciarelli presso l'università Sapienza di Roma.

## 2 Insiemi

La teoria degli insiemi è una branca della matematica che studia le collezioni di oggetti, denominate insiemi, e le operazioni che possono essere effettuate su di essi.

### 2.1 Definizioni Base

Un **insieme** è una collezione di oggetti distinti, chiamati elementi dell'insieme. Gli insiemi vengono di solito denotati con lettere maiuscole, mentre gli elementi con lettere minuscole.

- Un insieme può essere definito elencando i suoi elementi tra parentesi graffe: $A = \{a, b, c\}$.
- La notazione $a \in A$ significa che $a$ è un elemento dell'insieme $A$.
- La notazione $b \notin A$ significa che $b$ non è un elemento dell'insieme $A$.

### 2.2 Operazioni sugli Insiemi

Le principali operazioni sugli insiemi includono l'unione, l'intersezione e la differenza di insiemi.

- **Unione**: L'unione di due insiemi $A$ e $B$, denotata con $A \cup B$, è l'insieme degli elementi che appartengono ad $A$ o a $B$ (o ad entrambi).
- **Intersezione**: L'intersezione di due insiemi $A$ e $B$, denotata con $A \cap B$, è l'insieme degli elementi che appartengono sia ad $A$ che a $B$.
- **Differenza**: La differenza di due insiemi $A$ e $B$, denotata con $A - B$ o $A \setminus B$, è l'insieme degli elementi che appartengono ad $A$ e non a $B$.

### 2.3 Sottoinsiemi

Un insieme $A$ si dice **sottoinsieme** di un insieme $B$, denotato con $A \subseteq B$, se ogni elemento di $A$ è anche un elemento di $B$. Se $A$ è un sottoinsieme di $B$ ma $A$ non è uguale a $B$, allora $A$ si dice **sottoinsieme proprio** di $B$, denotato con $A \subset B$.

### 2.4 Insiemi Speciali

Alcuni insiemi hanno un'importanza particolare nella matematica:

- L'**insieme vuoto**, denotato con $\emptyset$, è l'insieme che non contiene elementi.
- Gli insiemi di numeri come gli **insiemi dei numeri naturali** $\mathbb{N}$, **interi** $\mathbb{Z}$, **razionali** $\mathbb{Q}$, **reali** $\mathbb{R}$, e **complessi** $\mathbb{C}$.

### 2.5 Proprietà degli Insiemi

Gli insiemi e le operazioni su di essi soddisfano diverse proprietà matematiche, come la commutatività, l'associatività, e le leggi distributive.

## 3 Coppie Ordinate

Una coppia ordinata è una collezione di due elementi in cui l'ordine degli elementi ha importanza. Le coppie ordinate sono comunemente utilizzate per definire concetti matematici come funzioni, relazioni e prodotti cartesiani.

### 3.1 Definizione

Una coppia ordinata $(a, b)$ è composta da due elementi dove $a$ è il primo elemento e $b$ è il secondo elemento. L'ordine degli elementi è significativo, il che significa che $(a, b) \neq (b, a)$ a meno che $a = b$.

### 3.2 Notazione e Proprietà

La notazione per una coppia ordinata è la seguente:

- $(a, b)$ indica una coppia ordinata dove $a$ è il primo membro e $b$ è il secondo membro.

Le proprietà principali delle coppie ordinate includono:

- **Unicità**: Due coppie ordinate $(a, b)$ e $(c, d)$ sono uguali se e solo se $a = c$ e $b = d$.
- **Ordine**: L'ordine degli elementi è cruciale. $(a, b) \neq (b, a)$ a meno che $a = b$.

### 3.3 Prodotto Cartesiano

Il prodotto cartesiano di due insiemi $A$ e $B$, denotato con $A \times B$, è l'insieme di tutte le possibili coppie ordinate $(a, b)$ dove $a \in A$ e $b \in B$.

#### 3.3.1 Esempio

Dati gli insiemi $A = \{1, 2\}$ e $B = \{x, y\}$, il prodotto cartesiano $A \times B$ è:

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

### 3.4 Applicazioni delle Coppie Ordinate

Le coppie ordinate sono utilizzate in vari ambiti della matematica e delle sue applicazioni, inclusi:

- Definizione di funzioni come collezioni di coppie ordinate.
- Rappresentazione di punti nel piano cartesiano.
- Costruzione di relazioni tra elementi di due insiemi.

# 4 Relazioni

Le relazioni sono sottoinsiemi di prodotti cartesiani, ad esempio $R \subseteq A \times B$, dove $A$ e $B$ sono insiemi. Ci sono varie tipologie di relazioni (o arità), come relazioni binarie, ternarie, unarie, e nullarie.

## 4.1 Principi per Relazioni Binarie

Le seguenti sono proprietà comuni delle relazioni binarie su un insieme $A$:

## 4.2 Principi

- **Principio di simmetria**: se un certo x è in relazione con y allora y è in relazione con X una relazione si dice simmetrica quando per ogni $(a, b) \in A$ se $(a, b) \in R$ allora $(b, a) \in R$ oppure usando una notazione infissa possiamo scrivesre se $aRb$ allora $bRa$
- **Principio di riflessività**: una relazione binaria su un insieme $A$ si dice riflessiva quando ogni elemento è in relazione con se stesso ossia per ogni $a \in A$ la coppia $(a, a)$ è in relazione
- **Principio di transitività**: una relazione binaria su un insieme $A$ si dice transitiva quando per ogni $a, b, c \in A$ se $(a, b) \in R$ e $(b, c) \in R$ allora $(a, c) \in R$
- **Principio di antisimmetria**: una relazione binaria su un insieme $A$ si dice antisimmetrica quando per ogni $a, b \in A$ se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$
- **Principio di antitransitività**: una relazione binaria su un insieme $A$ si dice antitransitiva quando per ogni $a, b, c \in A$ se $aRb$ e $bRc$ allora non deve essere $aRc$
- **Principio di antiriflessività**: una relazione binaria su un insieme $A$ si dice antiriflessiva quando per ogni $a \in A$ non deve essere $(a, a) \in R$

## 4.3 Considerazioni Aggiuntive

- Le relazioni possono essere di varie arità, non solo binarie. Ad esempio, una relazione ternaria coinvolge triple di elementi.

# 5 Funzioni

Una funzione è un particolare tipo di relazione binaria che associa ogni elemento di un insieme $A$ (detto dominio) con uno e un solo elemento di un insieme $B$ (detto codominio).

## 5.1 Definizione Formale

Una funzione da un insieme $A$ a un insieme $B$ è una relazione $R \subseteq A \times B$ tale che per ogni elemento $a \in A$, esiste uno ed un solo elemento $b \in B$ tale che $(a, b) \in R$.

## 5.2 Tipi di Funzioni

- **Iniettività**: Una funzione $f : A \to B$ è iniettiva se, per ogni $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implica $a_1 = a_2$.
  Se due elementi di A sono uguali devono avere lo stesso elemento in B come corrispondente
- **Suriettività**: Una funzione $f : A \to B$ è suriettiva se, per ogni $b \in B$, esiste almeno un $a \in A$ tale che $f(a) = b$.
  Ogni elemento in B deve avere un collegamento in A
- **Biettività**: Una funzione $f : A \to B$ è biettiva (o biunivoca) se è sia iniettiva che suriettiva. Ciò significa che $f$ stabilisce una corrispondenza uno-a-uno tra tutti gli elementi di $A$ e $B$.

## 5.3 Funzione Inversa e Equipotenza

- **Funzione Inversa**: Se $f : A \to B$ è biettiva, esiste una funzione inversa $f^{-1} : B \to A$ tale che $f^{-1}(f(a)) = a$ per ogni $a \in A$ e $f(f^{-1}(b)) = b$ per ogni $b \in B$.
- **Equipotenza**: Due insiemi $A$ e $B$ sono equipotenti se esiste una funzione biettiva $f : A \to B$.

## 5.4 Composizione e Proprietà

- La composizione di due funzioni mantiene certe proprietà: la composizione di due funzioni iniettive è iniettiva; la composizione di due funzioni suriettive è suriettiva; la composizione di due funzioni biettive è biettiva.
- Invertendo l'ordine delle coppie di una funzione non iniettiva si ottiene una relazione che non è necessariamente una funzione, perché potrebbero esserci elementi in $B$ associati a più elementi in $A$.
- Una funzione $f : A \to B$ è biettiva se e solo se invertendo l'ordine delle sue coppie si ottiene una funzione, la quale è l'inversa di $f$ e si indica con $f^{-1} : B \to A$.

## 5.5 Considerazioni Aggiuntive

- **Dominio e Codominio**: È importante specificare il dominio e il codominio di una funzione, poiché questi insiemi influenzano le proprietà di iniettività, suriettività e biettività.
- **Immagine e Controimmagine**: L'immagine di una funzione è l'insieme degli elementi di $B$ che sono associati ad almeno un elemento di $A$. La controimmagine è l'insieme degli elementi di $A$ che sono mappati su un dato elemento di $B$.
- **Funzioni Parziali**: Esistono anche funzioni parziali, dove alcuni elementi di $A$ potrebbero non avere un'immagine in $B$.

# 6 Cardinalità

La **cardinalità** di un insieme si riferisce alla sua classe di **equipotenza**.

## 6.1 Definizione di Equipotenza

Due insiemi $A$ e $B$ si dicono **equipotenti** se esiste una biiezione tra $A$ e $B$. In altre parole, $A$ ha la stessa cardinalità di $B$ se e solo se esiste una corrispondenza uno-a-uno e su tutto tra gli elementi di $A$ e quelli di $B$.

## 6.2 Proprietà dell'Equipotenza

L'equipotenza è una relazione di equivalenza che presenta le seguenti proprietà:

- **Riflessiva**: Ogni insieme è equipotente a se stesso, poiché la funzione identità è una biiezione.
- **Simmetrica**: Se $A$ è equipotente a $B$, allora $B$ è equipotente a $A$.
- **Transitiva**: Se $A$ è equipotente a $B$ e $B$ è equipotente a $C$, allora $A$ è equipotente a $C$.

## 6.3 Notazione e Confronto di Cardinalità

La cardinalità di un insieme $A$ viene indicata con $|A|$. La relazione di cardinalità tra due insiemi è definita come segue:

- $|A| \leq |B|$ se e solo se (sse) esiste una iniezione da $A$ a $B$.
- $|A| = |B|$ se e solo se esiste una biiezione tra $A$ e $B$.
- $|A| < |B|$ se $|A| \leq |B|$ ma $|A| \neq |B|$.

## 6.4 Teoremi Fondamentali

- **Teorema**: Se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$. Questo è noto come il **teorema di Cantor-Bernstein-Schroeder**, che afferma che se esistono funzioni iniettive da $A$ a $B$ e da $B$ a $A$, allora esiste una biiezione tra $A$ e $B$.

## 6.5 Teorema di Cantor

Georg Cantor ha dimostrato che non esiste una biiezione tra un insieme e il suo insieme delle parti. In altre parole:

- **Teorema**: $|A| < |P(A)|$ per ogni insieme $A$, dove $P(A)$ indica l'insieme delle parti di $A$.

# 7 Algebra di Boole

## 7.1 Definizione

L'algebra di Boole è definita su un gruppo con delle operazioni e dei valori, queste strutture e operazioni verificano alcune proprietà, l'algebra.

## 7.2 operazioni

Le operazioni dell'algebra di Boole sono:

- **meet** che si indica con il simbolo $\wedge$ e ha valenza dell'AND logico
- **join** che si indica con il simbolo $\vee$ e ha valenza dell'OR logico
- **complemento** che si indica con il simbolo $\overline{a}$ e ha valenza del NOT logico ($\neg$)

## 7.3 proprietà dell'algebra di Boole

- **Associativa**
  $A \vee (B \vee C) = (A \vee B) \vee C$
  $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
- **Commutativa**
  $A \vee B = B \vee A \qquad A \wedge B = B \wedge A$
- **Assorbimento**
  $A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$
- **Idempotenza**
  $A \vee A = A \qquad A \wedge A = A$
- **Distributiva**
  $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
  $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
- **Identità**
  $A \vee \bot = A \qquad A \vee \top = A$
- **Complemento**
  $A \vee \overline{A} = \top \qquad A \wedge \overline{A} = \bot$
- **De Morgan**
  $\overline{A \vee B} = \overline{A} \vee \overline{B} \qquad \overline{A \wedge B} = \overline{A} \vee \overline{B}$

## 7.4 Considerazioni Aggiuntive

- Le operazioni booleane sono definite su un insieme di due elementi, tipicamente rappresentati come $0, 1$, $\bot, \top$, o $\text{false}, \text{true}$.

# 8 Assiomi di Hilbert per la Logica Proposizionale

Gli assiomi di Hilbert sono formule di base in un sistema logico che, insieme alle regole di inferenza, permettono la deduzione di teoremi.

## 8.1 Assiomi

- $A \to (B \to A)$
- $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- $(\neg A \to \neg B) \to (B \to A)$

## 8.2 Regola di Inferenza

La **modus ponens** è l'unica regola di inferenza nel sistema di Hilbert, che afferma: se abbiamo $A$ e $A \to B$, allora possiamo dedurre $B$.

### 8.2.1 Esempio

Se abbiamo una formula che afferma "se piove allora porto l'ombrello" e un'affermazione che dice "piove", allora possiamo dedurre "porto l'ombrello".

## 8.3 Teorema di Deduzione

### 8.3.1 Sequente

Un sequente è un'espressione in cui abbiamo un simbolo di deduzione $\vdash$ e un insieme di formule. Per esempio, $A, B, C \vdash D$ significa che da $A, B, C$ possiamo dedurre $D$.

### 8.3.2 Derivazione

Una derivazione è una sequenza di formule dove ogni formula è un'istanza di un assioma o è ottenuta tramite la regola di inferenza (modus ponens), usando come premesse due formule che la precedono.

## 8.4 Formula della Transitività dell'Implicazione

La transitività dell'implicazione è espressa dalla formula:

$$(A \to B) \land (B \to C) \to (A \to C)$$

# 9 Logica Proposizionale

La logica proposizionale è un ramo della logica matematica che studia i modi in cui le proposizioni possono essere combinate e le relazioni tra di esse.

## 9.1 Linguaggio della Logica Proposizionale

Il **linguaggio** della logica proposizionale è composto da:

- **Simboli proposizionali atomici**: Sono le lettere che rappresentano proposizioni semplici e indivisibili, come $p$, $q$, $r$, ecc.
- **Operatori logici**: Sono utilizzati per costruire formule più complesse a partire da quelle semplici. Gli operatori includono:
  - **Implicazione** ($\rightarrow$): Indica una relazione di conseguenza logica.
  - **Negazione** ($\neg$): Esprime il contrario di una proposizione.
  - **Disgiunzione** ($\vee$): Corrisponde all'operatore logico "or".
  - **Coniunzione** ($\wedge$): Corrisponde all'operatore logico "and".
  - **Doppia implicazione** ($\leftrightarrow$): Indica una relazione di equivalenza logica, anche detta "se e solo se" (sse).

## 9.2 Semantica

La **semantica** si occupa del significato delle formule della logica, attribuendogli un valore di verità: vero ($\top$) o falso ($\bot$).

### 9.2.1 Tabelle di Verità

Le tabelle di verità sono uno strumento fondamentale nella logica proposizionale, in quanto permettono di analizzare le formule per determinare il loro valore di verità in base ai valori delle proposizioni atomiche da cui sono composte.

## 9.3 Modello della Logica Proposizionale

Un **modello** in logica proposizionale è un'attribuzione specifica di valori di verità ai simboli proposizionali atomici. Ad esempio, in un dato modello, le proposizioni $A$, $B$, e $C$ possono essere tutte vere, tutte false, o avere una combinazione di valori di verità.

# 10 Come Usare i Tableau Proposizionali

I tableau proposizionali sono un potente strumento utilizzato nella logica per determinare la soddisfacibilità di formule proposizionali. Questo metodo si basa sull'espansione di un albero di decisione seguendo regole specifiche per gli operatori logici.

## 10.1 Principi Base

Il procedimento inizia con la formula che si vuole analizzare. L'obiettivo è decomporre la formula in componenti più semplici fino a raggiungere proposizioni atomiche, seguendo un insieme di regole di decomposizione che variano in base agli operatori logici presenti.

## 10.2 Regole di Decomposizione

Le regole di decomposizione per i vari operatori logici sono le seguenti:

- **Negazione** ($\neg$): La negazione di una proposizione atomica o di una formula complessa viene decomposta invertendo il suo valore di verità.
- **Coniunzione** ($\wedge$): Una formula del tipo $A \wedge B$ viene decomposta in due rami, uno per $A$ e uno per $B$, che devono entrambi essere veri.
- **Disgiunzione** ($\vee$): Una formula del tipo $A \vee B$ genera due sottorami separati, uno con $A$ vero e l'altro con $B$ vero, indicando che almeno uno dei due deve essere vero.
- **Implicazione** ($\rightarrow$): Un'implicazione $A \rightarrow B$ viene trattata come $\neg A \vee B$, generando due sottorami: uno con $A$ falso e l'altro con $B$ vero.
- **Doppia implicazione** ($\leftrightarrow$): Una doppia implicazione $A \leftrightarrow B$ viene decomposta in due parti: $A \rightarrow B$ e $B \rightarrow A$.

## 10.3 Chiusura del Tableau

Un ramo del tableau si dice *chiuso* se contiene una contraddizione, ovvero la stessa proposizione atomica appare sia in forma affermativa che negativa. Se tutti i rami del tableau sono chiusi, la formula iniziale è insoddisfacibile. Se almeno un ramo rimane aperto (senza contraddizioni), la formula è soddisfacibile, e le assegnazioni di verità lungo il ramo aperto forniscono un modello che soddisfa la formula.

## 10.4 Esempio di Applicazione

Consideriamo la formula $(P \rightarrow Q) \wedge (\neg Q \vee R)$. Per analizzarla con un tableau proposizionale, si inizia scrivendo la formula sulla cima del tableau e poi si procede a decomporla seguendo le regole sopra descritte, espandendo l'albero fino a raggiungere proposizioni atomiche o contraddizioni.

## 10.5 Conclusioni

I tableau proposizionali sono uno strumento essenziale per la verifica della soddisfacibilità delle formule logiche. Grazie alla loro struttura sistematica, permettono di esplorare tutte le possibili assegnazioni di valori di verità per determinare la veridicità di una formula.

# 11 Esercizi

questi esercizi sono tratti dali web seminar:

- **5 luglio 2021**
- **Esercizio 2**

## 11.1 Relazioni

**Domanda**: Perché si parla sempre di relazione riflessiva, anti-riflessiva, simmetrica e antisimmetrica però di transitiva non si parla mai di una relazione anti-transitiva?
**Risposta**: La relazione anti-transitiva è una relazione che non soddisfa la proprietà di transitività. In altre parole, una relazione $R$ è anti-transitiva se esistono $a, b, c$ tali che $aRb$ e $bRc$, ma non $aRc$. Un esempio è la relazione del successore. Tuttavia, questa proprietà non è così comune o rilevante come le altre proprietà delle relazioni, quindi non è spesso menzionata in modo specifico.

**Domanda**: Fammi esempi di funzione riflessiva, simmetrica, anti-transitiva.
**Risposta**: Un esempio di funzione riflessiva è la funzione identità, $f(x) = x$. Un esempio di funzione simmetrica è $f(x) = -x$. Un esempio di funzione anti-transitiva è $f(x) = x + 1$.

**Domanda**: È possibile avere una relazione riflessiva e antitransitiva? Se si quale.
**Risposta**: Sì, solo l'insieme vuoto.

**Domanda**: È possibile avere una relazione transitiva e antiriflessiva? Se si quale.
**Risposta**: Sì, l'insieme vuoto.

**Domanda**: Qual'è la differenza tra relazione vuota su $N \times N$ e la relazione vuota su insieme vuoto?
**Risposta**: La relazione vuota su $N \times N$ è un sottoinsieme di $N \times N$ che non contiene alcuna coppia ordinata. La relazione vuota sull'insieme vuoto è un sottoinsieme dell'insieme vuoto, che non contiene alcun elemento.

## 11.2 Cardinalità

**Domanda**:le relazioni SAS (sono le relazioni simmetriche e antisimmetriche contemporaneamente) e TAT (le relazioni transistive e antitransitiva). Son di più le relazioni SAS o TAT?
**Risposta**: Per confrontare la cardinalità delle relazioni che sono simultaneamente simmetriche e antisimmetriche (SAS) con quelle che sono sia transitive che antitransitive (TAT), consideriamo il concetto di infinità e le proprietà delle relazioni tra insiemi di numeri.

Prima di tutto, ricordiamo che un insieme di numeri primi è infinito e numerabile, mentre l'insieme delle parti di un insieme infinito numerabile, come l'insieme dei numeri primi $P$, è un'infinità non numerabile. Questo è un risultato diretto del teorema di Cantor, che afferma che l'insieme delle parti di qualsiasi insieme $A$ ha una cardinalità maggiore dell'insieme $A$ stesso.

Per dimostrare che le relazioni TAT hanno una cardinalità almeno pari all'insieme delle parti dei numeri primi, consideriamo una costruzione specifica. Prendiamo un qualsiasi sottoinsieme di numeri primi, ad esempio $\{7, 11, 13\}$, e costruiamo una relazione che includa coppie del tipo $(p, p+1)$, dove $p$ è un numero primo e $p+1$ è il suo successore immediato. Per il nostro esempio, otteniamo le coppie $(7, 8)$, $(11, 12)$, $(13, 14)$. Questa costruzione garantisce che la relazione sia antitransitiva, poiché non esistono tre elementi $a$, $b$, $c$ tali che se $(a, b)$ e $(b, c)$ appartengono alla relazione, allora $(a, c)$ dovrebbe appartenere alla relazione, il che è impossibile per la nostra costruzione.

Ogni sottoinsieme di numeri primi può essere associato univocamente a una relazione TAT mediante questa costruzione. Questo stabilisce una funzione iniettiva dall'insieme delle parti dei numeri primi all'insieme delle relazioni TAT, dimostrando che la cardinalità dell'insieme delle relazioni TAT è maggiore o uguale alla cardinalità dell'insieme delle parti dei numeri primi, che è non numerabile.

In conclusione, poiché l'insieme delle parti dei numeri primi è non numerabile e ogni sottoinsieme di numeri primi può essere associato univocamente a una relazione TAT, segue che l'insieme delle relazioni TAT è anch'esso non numerabile e, per costruzione, la sua cardinalità è almeno pari a quella dell'insieme delle parti dei numeri primi.

Questo ragionamento non si applica direttamente alle relazioni SAS, la cui cardinalità dipende da considerazioni diverse, ma suggerisce che le relazioni TAT rappresentano un insieme vasto e complesso di relazioni.

## 11.3 Sistema di Hilbert

**Domanda**: Dimostrami che $A \vdash A$
**Risposta**: Significa che $A$ è deducibile da $A, A \to ((A \to A) \to A)$ istanza del primo assioma, prendendo il secondo assioma $(A \to ((A \to A) \to A)) \to (A \to (A \to A)) \to (A \to A)$ applichiamo il modus ponens alle 2 ne deduciamo $(A \to (A \to A)) \to A \to A$ ora dobbiamo dimostrarla.
Dal primo assioma prendiamo un altra istanza $A \to (A \to A)$ ora applichiamo modus ponens e arriviamo ad $A \to A$ quindi per il teorema di deduzione sappiamo che da A si deriva A