

Appunti di Lezione: Strutture Discrete

Parte I: Logica Proposizionale, Insiemi e relazioni

V. Cutello

Contenuti

1 Logica Proposizionale

- La Logica Proposizionale
- Forme Normali

2 Insiemi

- Il concetto di insieme e le proprietà di base
- Insiemi ed operazioni tra di essi
- Dimostrazione diretta
- Esercizi su Insiemi
- Famiglie di insiemi
- Insieme prodotto
- Paradossi

3 Relazioni e Funzioni

- Relazioni binarie e funzioni
- Relazioni di Equivalenza
- Relazioni d'ordine
- Rappresentazione di insiemi finiti
- Esercizi e Problemi su Relazioni e Famiglie di Insiemi
- Il Problema del "Hitting Set"

4 Insiemi chiusi e famiglie chiuse di insiemi

- Caso Studio: la congettura Union-Closed

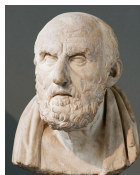
STRUTTURE DISCRETE

PARTE 1: LOGICA PROPOSIZIONALE, INSIEMI E RELAZIONI

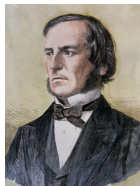
1: LOGICA PROPOSIZIONALE

La Logica Proposizionale

La logica proposizionale viene sviluppata nel III secolo A.C. dalla scuola degli Stoici ed in particolare Crisippo.



Gran parte del lavoro e degli scritti originali furono perduti. Solo tanti secoli dopo il lavoro prima di Leibnitz e poi di Boole e De Morgan formalizzò in maniera definitiva il campo.



La Logica Proposizionale è, anche per questo, conosciuta come Logica Booleana.

Il linguaggio della logica

- Le logiche sono linguaggi formali per rappresentare informazioni da cui trarre conclusioni
- Ogni linguaggio è la composizione di due parti fondamentali: Sintassi e Semantica
 - La sintassi definisce le frasi (formule) del linguaggio
 - La semantica definisce il significato delle frasi ovvero, per quanto riguarda le formule la loro veridicità di una formula, ossia se sono vere o false.

Tipi di Logiche

- Le logiche sono caratterizzate da quello che assumono come primitive
- Assunzioni ontologiche: cosa esiste ?
 - fatti, oggetti, tempo, credenze
- Valori di verità

Linguaggio	Assunzioni ontologiche	Valori di verità
Logica Proposizionale	Fatti	Vero/Falso
Logica del primo ordine	Fatti e relazioni su oggetti	Vero/Falso
Logica Temporale	Fatti, tempo e relazioni su oggetti	Vero/Falso
Logica Probabilistica	Fatti, tempo e relazioni su oggetti	Grado di credenza

Logica proposizionale

- La logica proposizionale è la logica più semplice
- Inerentemente connessa al mondo binario 0/1 dei calcolatori
- Si occupa di fatti, proposizioni o affermazioni e della loro veridicità
- Una proposizione è un'affermazione che è vera oppure falsa, ma non entrambe.
- La costruzione sintattica di una formula avviene usando regole semplici e operatori fondamentali

Logica proporzionale: Sintassi

- Il vocabolario consiste di un insieme di variabili proposizionali \mathcal{P} di solito denotate con p, q, r, \dots con eventuale numerazione sottoscritta, ovvero p_1, p_2 etc.
- Le variabili proposizionali possono assumere solo 2 valori: 1 o anche vero (true in inglese e abbreviato con T) oppure 0 o anche falso (abbreviato con F)
- Ogni variabile proposizionale è, già da sé, una "formula" proposizionale
- Formule più complesse, si possono costruire, a partire dalle variabili proposizionali, utilizzando degli operatori, detti connettivi logici:
 - \neg negazione: si legge "non"
 - \vee disgiunzione logica: si legge "o"
 - \wedge congiunzione logica: si legge "e"
 - \Rightarrow implicazione logica: si legge "se ... allora ..." oppure "implica"
 - \Leftrightarrow coimplicazione logica: si legge "se e solo se " oppure "implica e co-implica"

Formule proposizionali

- Vediamo come costruire formule della logica proposizionale sintatticamente corrette
- Se P e Q sono formule, allora
 - $\neg P$ oppure $\neg Q$ sono formule
 - $P \vee Q$ è una formula
 - $P \wedge Q$ è una formula
 - $P \Rightarrow Q$ è una formula
 - $P \Leftrightarrow Q$ è una formula

Formule proposizionali

- Nelle espressioni logiche, o formule, l'ordine degli operatori segue regole di precedenza e può essere aggiustato usando le parentesi.
- La negazione \neg ha la precedenza maggiore, mentre i connettivi \wedge e \vee hanno la stessa precedenza e, quindi, si applicano da sinistra verso destra, anche se, per evitare ambiguità è utile utilizzare le parentesi.
- Vediamo degli esempi
 - $\neg p \vee q$ (leggi: "non p o q ") è la formula dove la negazione si applica solo a p
 - $\neg(p \vee q)$ (leggi: "non p o q ") è la formula dove la negazione si applica alla disgiunzione $p \vee q$

Semantica: Interpretazione

- Una interpretazione I su \mathcal{P} è una funzione $I : \mathcal{P} \rightarrow \{0, 1\}$ o, equivalentemente, $I : \mathcal{P} \rightarrow \{T, F\}$
- Date due formule P_1 e P_2 e data una interpretazione I che assegna un valore di verità alle variabili proposizionali presenti nella formula, si calcola il valore di verità di tutta la formula $I(P_1)$ o $I(P_2)$ come segue
 - $I(\neg P_1)$ è vera se e solo se $I(P_1)$ è falsa
 - $I(P_1 \vee P_2)$ è vera se e solo se almeno una tra $I(P_1)$ e $I(P_2)$ è vera
 - $I(P_1 \wedge P_2)$ è vera se e solo se $I(P_1)$ e $I(P_2)$ sono entrambe vere
 - $I(P_1 \Rightarrow P_2)$ è vera se $I(P_1)$ è falsa oppure se $I(P_2)$ è vera
 - $I(P_1 \Leftrightarrow P_2)$ è vera se e solo se $I(P_1 \Rightarrow P_2)$ è vera e $I(P_2 \Rightarrow P_1)$ è pure vera

Esempi

Tabella: Esempi di proposizioni e negazioni

Proposizioni Vere	Proposizioni False
Roma è la capitale d'Italia	Catania è la capitale d'Italia
$3 > 2$	$2 > 3$
Non è vero che Catania è la capitale d'Italia	Non è vero che Roma è la capitale d'Italia
Non è vero che $2 > 3$	Non è vero che $3 > 2$

Esempi

Tabella: Esempi di proposizioni e congiunzioni

<i>P1</i>	<i>P2</i>	<i>P1 e P2</i>
Roma è la capitale d'Italia	Catania è il capoluogo della Sicilia	Falso
Roma è la capitale d'Italia	Palermo è il capoluogo della Sicilia	Vero
Milano è la capitale d'Italia	Non è vero che Catania è il capoluogo della Sicilia	Falso
Milano è la capitale d'Italia	Catania è il capoluogo della Sicilia	Falso

Tavole della verità

- Generalizziamo quanto visto utilizzando le tabelle, o tavole della verità per i connettivi logici

Negazione

p	$\neg p$
T	F
F	T

Congiunzione

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

Disgiunzione

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

Implicazione

p	q	$p \Rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

Implicazione doppia

p	q	$p \Leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

Soddisfacibilità

- Data una formula P diremo che la formula è **soddisfacibile** se esiste una interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, tale che $I(P)$ è vera.
- Data una formula P diremo che la formula è **insoddisfacibile** se non esiste una interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, tale che $I(P)$ è vera.
- Una formula P si dice **tautologia** o **valida** se per ogni interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, la formula risulta vera.

Si noti che una formula è valida se e solo se la sua negazione è insoddisfacibile.
Vediamo degli esempi

- $p \wedge (q \vee \neg p)$ è soddisfacibile
- $p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p)$ è insoddisfacibile
- $p \rightarrow (\neg p \rightarrow q)$ è una tautologia

Lo dimostriamo utilizzando le tavole di verità.

Soddisfacibilità: Esempi

Esempio Soddisfacibile

p	q	$q \vee \neg p$	$p \wedge (q \vee \neg p)$
F	F	T	F
F	T	T	F
T	F	F	F
T	T	T	T

Esempio Tautologia

p	q	$\neg p \Rightarrow q$	$p \Rightarrow (\neg p \Rightarrow q)$
F	F	F	T
F	T	T	T
T	F	T	T
T	T	T	T

Esempio Insoddisfacibile

p	q	$q \vee \neg p$	$\neg q \vee \neg p$	$p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p)$
F	F	T	T	F
F	T	T	T	F
T	F	F	T	F
T	T	T	F	F

Principi fondamentali della logica

- Due formule particolari ci danno i 2 principi fondamentali della logica proposizionale, per ogni proposizione p si ha
 - **Principio del terzo escluso**
 $p \vee \neg p$ è una tautologia, ossia sempre vera
 - **Principio di non contraddizione**
 $p \wedge \neg p$ è insoddisfacibile, ossia sempre falsa:

Equivalenza logica e proprietà

- Due formule aventi le stesse variabili proposizionali, P e Q si dicono equivalenti, $P \equiv Q$ se comunque assegniamo un valore alle variabili, P risulta vera se e solo se Q risulta vera.
- Abbiamo allora le seguenti proprietà dei connettivi logici
 - $p \vee q \equiv q \vee p$ (commutatività della disgiunzione)
 - $p \wedge q \equiv q \wedge p$ (commutatività della congiunzione)
 - $p \vee (q \vee r) \equiv (p \vee q) \vee r$ (associatività della disgiunzione)
 - $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ (associatività della congiunzione)

Si dimostrano facilmente utilizzando le tavole della verità (Esercizio)

Altre equivalenze logiche

- $\neg(\neg p) \equiv p$ (doppia negazione)
- $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ (contrapposizione)
- $p \Rightarrow q \equiv \neg p \vee q$ (Eliminazione implicazione)
- $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (Eliminazione doppia implicazione)
- Leggi di De Morgan
 - $\neg(p \vee q) \equiv \neg p \wedge \neg q$ ovvero, la negazione della disgiunzione è equivalente alla congiunzione delle negazioni
 - $\neg(p \wedge q) \equiv \neg p \vee \neg q$ ovvero, la negazione della congiunzione è equivalente alla disgiunzione delle negazioni
- Distributività
 - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ distributività della congiunzione sulla disgiunzione
 - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ distributività della disgiunzione sulla congiunzione

Anche queste si dimostrano facilmente utilizzando le tavole della verità (Esercizio)

Tavole di verità: Esercizi

- Costruisci le Tavole di Verità delle seguenti formule

- $p \wedge q \wedge (r \vee s)$
- $p \vee q \vee (r \wedge s)$
- $p \wedge (q \vee (s \wedge (\neg p \vee \neg q)))$
- $((p \vee \neg q \vee r) \wedge s) \vee t$

Esercizi

- Verificare che se si considerano i valori numerici 1 per vero e 0 per falso, e assegnati tali valori numerici alle variabili proposizionali p e q abbiamo che
 - $\neg p \equiv 1 - p$
 - $p \vee q \equiv \max(p, q)$
 - $p \wedge q \equiv \min(p, q)$
 - $p \Rightarrow q \equiv \max(1 - p, q)$
 - $p \Leftrightarrow q \equiv \min(\max(1 - p, q), \max(p, 1 - q))$

Giustificazione o Conseguenza Logica

- Sia \mathcal{P} un insieme di proposizioni (formule) e P una proposizione.
- Diciamo che \mathcal{P} giustifica P o, equivalentemente, che P è una conseguenza logica di \mathcal{P} e lo denotiamo con

$$\mathcal{P} \models P$$

se ogni interpretazione I che soddisfa tutte le formule di \mathcal{P} soddisfa anche P .

- Vediamo un esempio, sia $\mathcal{P} = \{p, p \Rightarrow q\}$ ossia l'insieme formato da 2 formule: p e $p \rightarrow q$.
- Allora $\mathcal{P} \models q$ e lo dimostriamo con la tavola di verità

Esempio Giustificazione Logica

p	q	$p \rightarrow q$	q	
F	F	T	F	p falsa
F	T	T	T	p falsa
T	F	F	F	$p \Rightarrow q$ falsa
T	T	T	T	✓

- Notiamo che se P è vero, non deve necessariamente essere vero che tutte le proposizioni di \mathcal{P} siano vere.

Giustificazione o Conseguenza Logica: Esempio

- Dimostriamo che se $\mathcal{P} = \{p \vee r, q \vee \neg r\}$ allora $\mathcal{P} \models p \vee q$

Esempio Giustificazione Logica

p	q	r	$p \vee r$	$q \vee \neg r$	$p \vee q$
F	F	F	F	T	F
F	F	T	T	F	F
F	T	F	F	T	T
F	T	T	T	T	$T \checkmark$
T	F	F	T	T	$T \checkmark$
T	F	T	T	F	T
T	T	F	T	T	$T \checkmark$
T	T	T	T	T	$T \checkmark$

Forme Normali

- Nelle applicazioni informatiche in cui si usano formule del calcolo proposizionale, si trasformano spesso le formule in forme standardizzate, ovvero in una delle due seguenti forme normali
- **Forma Normale Congiuntiva**
 - Una formula p è in Forma Normale Congiuntiva (CNF) se è scritta come congiunzione di disgiunzioni. Per esempio
 - $(p \vee q) \wedge (\neg p \vee \neg r \vee s)$
- **Forma Normale Disgiuntiva**
 - Una formula p è in Forma Normale Disgiuntiva (DNF) se è scritta come disgiunzione di congiunzioni. Per esempio
 - $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$

Forme Normali

- Una qualunque formula P si può trasformare in una delle due forme normali, attraverso un semplice procedimento algoritmico.
- **Algoritmo di Trasformazione in Forma Normale**
 - (Fase 1) Elimina le doppie implicazioni $p \Leftrightarrow q$ dalla formula sostituendole con $(p \Rightarrow q) \wedge (q \Rightarrow p)$
 - (Fase 2) Elimina le implicazioni $p \Rightarrow q$ dalla formula sostituendole con $\neg p \vee q$
 - (Fase 3) Sposta le negazioni \neg a ridosso delle variabili proposizionali, utilizzando le regole di De Morgan, ed eliminando le doppie negazioni.
Per esempio

$$\neg(\neg p \vee \neg r \vee s) \text{ diventa } (p \wedge r \wedge \neg s)$$

Forme Normali

● Algoritmo di Trasformazione in Forma Normale

(Fase 4-a) Per costruire una CNF distribuire la congiunzione sulla disgiunzione ed eliminare tautologie. Per esempio $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$ è una formula in DNF che vogliamo trasformare in CNF. Abbiamo

$$\begin{aligned} (p \vee (\neg p \wedge \neg r \wedge s)) \wedge (q \vee (\neg p \wedge \neg r \wedge s)) &\equiv \\ (p \vee \neg p) \wedge (p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s) &\equiv \\ (p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s) \end{aligned}$$

● Esercizio: Dimostrare, utilizzando le tavole di verità, che

$$(p \wedge q) \vee (\neg p \wedge \neg r \wedge s) \equiv (p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s)$$

Forme Normali

- **Algoritmo di Trasformazione in Forma Normale**

(Fase 4-b) Per costruire una DNF distribuire la disgiunzione sulla congiunzione ed eliminare disgiunti insoddisfacibili e ripetizioni.

Per esempio, $(p \vee q) \wedge (\neg p \vee \neg r)$ è una formula in CNF che vogliamo trasformare in DNF. Abbiamo

$$\begin{aligned}(p \wedge \neg p) \vee (p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r) &\equiv \\ (p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r)\end{aligned}$$

- **Esercizio:** Dimostrare, utilizzando le tavole di verità, che

$$(p \vee q) \wedge (\neg p \vee \neg r) \equiv (p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r)$$

Forme Normali: Esercizio

- Trasformiamo $p \Rightarrow (q \wedge (r \vee s))$ in CNF e in DNF
- CNF
 - Eliminiamo \Rightarrow : $\neg p \vee (q \wedge (r \vee s))$
 - Distribuiamo \wedge su \vee : $(\neg p \vee q) \wedge (\neg p \vee r \vee s)$
 - Verifichiamo la correttezza utilizzando la tavola di verità, ma prima notiamo che se p è falsa allora $p \Rightarrow (q \wedge (r \vee s))$ è vera ma anche la congiunzione $(\neg p \vee q) \wedge (\neg p \vee r \vee s)$ è vera. Quindi, per semplicità limitiamoci al caso p vera e agli 8 casi rimanenti

Tavola di verità con p vera

q	r	s	$p \Rightarrow (q \wedge (r \vee s))$	$(\neg p \vee q) \wedge (\neg p \vee r \vee s)$
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	F	F
T	F	F	F	F
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Forme Normali: Esercizio

- Trasformiamo $p \Rightarrow (q \wedge (r \vee s))$ in CNF e in DNF
- DNF
 - Eliminiamo \Rightarrow : $\neg p \vee (q \wedge (r \vee s))$
 - Distribuiamo \vee su \wedge : $\neg p \vee (q \wedge r) \vee (q \wedge s)$
 - Verifichiamo la correttezza utilizzando la tavola di verità, ma anche in questo caso notiamo che se p è falsa allora $p \Rightarrow (q \wedge (r \vee s))$ è vera ma anche la disgiunzione $\neg p \vee (q \wedge r) \vee (q \wedge s)$ è vera. Quindi, di nuovo, per semplicità limitiamoci al caso p vera e agli 8 casi rimanenti

Tavola di verità con p vera

q	r	s	$p \Rightarrow (q \wedge (r \vee s))$	$\neg p \vee (q \wedge r) \vee (q \wedge s)$
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	F	F
T	F	F	F	F
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Forme Normali: Esercizi

- Trasforma le seguenti formule in CNF e in DNF
 - $\neg(p \Rightarrow (q \wedge (r \vee s)))$
 - $(q \wedge (r \vee s)) \Rightarrow p$
 - $p \wedge (q \vee (s \wedge (\neg p \vee \neg q)))$
 - $((p \vee \neg q \vee r) \wedge s) \vee t$

STRUTTURE DISCRETE

PARTE 1: LOGICA PROPOSIZIONALE, INSIEMI E RELAZIONI

2: Insiemi

Il concetto di insieme

I nostri discorsi futuri si baseranno sul concetto intuitivo di insieme, che assumiamo come "nozione primitiva", anche se deve essere soggetto ad alcuni vincoli per non cadere in paradossi.

La Teoria assiomatica degli Insiemi, ovvero la teoria assiomatica di Zermelo-Fraenkel, si preoccupa di dare un assetto formalmente rigoroso al campo, ma esula dai nostri discorsi.



Ernst F. F. Zermelo (1871–1953)
logico e matematico tedesco



Abraham Fraenkel (1891–1965)
logico e matematico israeliano

Il concetto di insieme

Noi seguiremo qui la linea espositiva della cosiddetta "Teoria ingenua degli Insiemi", considerandoli come collezione ben definita di oggetti (con sinonimi possibili: aggregato, classe, famiglia, etc.) piuttosto che "oggetti" che verificano determinati assiomi, ma nel contempo ricorderemo anche alcuni degli assiomi che caratterizzano la teoria assiomatica di Zermelo-Fraenkel.

Fu il matematico tedesco Georg Cantor (1845-1918) a dare origine alla Teoria degli Insiemi ed a dimostrare, tra le altre cose, che gli insiemi infiniti possono avere diverse grandezze.



Caratterizzazione di un insieme

- E' importante chiarire cosa si intende per "collezione ben definita" di oggetti.
- Un insieme è univocamente caratterizzato dal suo contenuto, ovvero dagli elementi che gli appartengono. Formalizziamo il concetto di appartenenza.

Appartenenza

Se T è un insieme, l'espressione $x \in T$ si legge: "x appartiene all'insieme T " oppure "x è un elemento di T ."

Non Appartenenza

Scriveremo invece $x \notin T$ per negare l'espressione precedente, cioè per affermare che x non appartiene all'insieme T .

Assioma di estensionalità

Dal momento che un insieme è univocamente caratterizzato dal suo contenuto, due insiemi che contengono gli stessi elementi, sono lo stesso insieme. Abbiamo, quindi, una prima proprietà fondamentale che viene anche denominata "Assioma di Estensionalità":

Definizione (Uguaglianza tra insiemi)

Due insiemi A e B sono uguali se hanno gli stessi elementi. In simboli:

$$A = B \Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B)$$

Descrizione di un insieme

- Quando è possibile, per specificare un insieme sarà sufficiente elencarne gli elementi. Per convenzione generale, gli elementi di un insieme vengono elencati tra parentesi graffe. Ad esempio
 - $\{1, 2, 3\}$ indica l'insieme i cui elementi sono appunto i numeri 1, 2, 3.

Singoleto

La notazione $\{a\}$ indica l'insieme costituito dal solo elemento a , detto insieme singoletto.

Insieme vuoto

Con il simbolo \emptyset indicheremo un insieme speciale, detto insieme vuoto, che è l'insieme che non contiene alcun elemento.

Definizione di un insieme

- Dalla definizione di uguaglianza, ne deduciamo immediatamente che gli insiemi $A = \{1, 2, 3\}$ e $B = \{2, 3, 1, 2, 3\}$ sono uguali perché contengono gli stessi elementi.
- Per lo stesso motivo, anche gli insiemi $A = \{1, 2, 3\}$ e $B = \{3, 1, 2\}$ sono uguali.
- Quindi, ogni insieme è caratterizzato dal fatto che i suoi elementi appaiono in esso una sola volta e non importa in quale ordine essi sono elencati.
- Più in generale, possiamo specificare un insieme esplicitando la proprietà che caratterizza i suoi elementi. Formalmente, se P è una proprietà ben definita, possiamo allora definire l'insieme $\{x : \text{la proprietà } P \text{ è vera per } x\} \equiv \{x : P(x)\}$

Definizione di un insieme

- Cosa vuol dire che P è una proprietà ben definita? Vuol dire che per ogni valore di x , $P(x)$ può assumere sempre solo i 2 valori vero o falso (anche se non sappiamo quale).

Esempi di insiemi

- Supponiamo P sia la proprietà di essere nato il primo o l'ultimo giorno del mese, allora $\{x : P(x)\}$ è un insieme.
- Supponiamo P sia la proprietà di essere un divisore di $10^{1000} + 1$, allora $\{x : P(x)\}$ è un insieme, anche se non conosciamo i divisori di tale numero enorme.

Esempio di non insieme

Supponiamo P sia la proprietà di essere "alti", allora $\{x : P(x)\}$ non è un insieme.

Cardinalità

Ad ogni insieme possiamo associare un'importante caratterizzazione: la quantità di elementi che gli appartengono.

Definizione (Cardinalità)

Dato un insieme A , il numero di elementi che lo costituisce è denominato cardinalità dell'insieme ed è denotata con $|A|$. Se $|A|$ è un numero intero l'insieme si dice finito, altrimenti infinito.

Esempio

- La cardinalità dell'insieme vuoto è quindi zero, $|\emptyset| = 0$, mentre $|\{1, 2, 3\}| = 3$ e $|\{a\}| = 1$.
- La cardinalità dell'insieme costituito dai numeri pari è invece infinita, $|\{x : x \text{ è un numero pari}\}| = +\infty$

Insiemi discreti

Diamo una definizione intuitiva di insieme discreto, evitando di ricorrere ai concetti classici di topologia

Definizione (Insieme discreto)

Un insieme A si dice discreto se è possibile ordinare i suoi elementi in maniera tale che tra un qualunque elemento ed il successivo nell'ordinamento dato, non vi sono altri elementi dell'insieme. Quindi, è un insieme composto da elementi "isolati".

Esempio

Ogni insieme finito è discreto. In particolare, anche l'insieme vuoto \emptyset è discreto.

Insiemi numerici

Ricordiamo che

- $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$
- $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$
- $\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}\}$
- $\mathbb{R} = \{x : x \text{ razionale o irrazionale} \}$
- $\mathbb{C} = \{x : x \text{ reale o immaginario} \}$

Quindi

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

Insiemi numerici

Abbiamo

Tabella: Tabella Insiemi Numerici

\mathbb{N}	insieme dei numeri naturali	discreto
\mathbb{Z}	insieme degli interi relativi	discreto
\mathbb{Q}	insieme dei numeri razionali	né discreto né continuo
\mathbb{R}	insieme dei numeri reali	continuo
\mathbb{C}	insieme dei numeri complessi	continuo

La costruzione di nuovi insiemi

- Abbiamo detto che un insieme è una collezione ben definita di oggetti.
- Questo ci permette di definire, utilizzando specifiche chiare, procedimenti che, partendo da insiemi assegnati, ci forniscono nuovi insiemi.

Relazione di Inclusione

Se abbiamo due insiemi A e B e tutti gli elementi di A sono anche elementi di B allora diciamo che A è incluso in B , ovvero che A è un sottoinsieme di B .

Definizione (Inclusione)

A è un sottoinsieme di B , denotato con $A \subseteq B$ se

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B)$$

Se A è un sottoinsieme di B allora B è un sovrainsieme di A ed in questo caso lo denotiamo con $B \supseteq A$.

Relazione di Inclusione

- Notiamo che la relazione $A \subseteq B$ è verificata nel caso in cui $A = B$.
- Per esprimere il fatto che $A \subseteq B$ ma A è diverso da B , cioè esistono elementi di B che non sono elementi di A , scriviamo $A \subset B$ o equivalentemente $B \supset A$. In questo caso diciamo che A è un sottoinsieme proprio di B , ovvero A è propriamente contenuto in B .
- Possiamo specificare un sottoinsieme di un dato insieme elencandone gli elementi, quando possibile, oppure utilizzare una proprietà ben definita. Più in dettaglio, supponiamo che T sia un insieme e che $P(x)$ sia una proprietà che ha senso per gli elementi di T . Scriviamo allora $\{x : x \in T \text{ e } P(x)\}$ per indicare il sottoinsieme di T formato dagli elementi per cui $P(x)$ è vera.

Relazione di Inclusione

Esempio

Supponiamo T sia l'insieme di tutti i numeri interi positivi da 1 a 100, ovvero

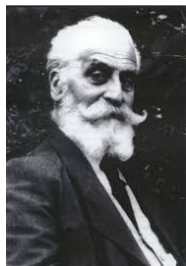
$$T = \{1, 2, 3, 4, \dots, 98, 99, 100\}$$

e supponiamo che la proprietà $P(x)$ sia quella di essere un multiplo di 10. Allora

$$\{x : x \in T \text{ e } P(x)\} = \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100\}.$$

Operazioni tra insiemi

Introduciamo adesso le operazioni fondamentali tra insiemi, a cominciare da unione ed intersezione, i cui simboli \cup , \cap , oltre al simbolo di appartenenza \in , furono introdotti dal matematico e logico piemontese Giuseppe Peano (1858-1932) a fine '800.



Unione di due insiemi

L'unione di due insiemi A e B è l'insieme formato da quegli elementi che appartengono ad almeno uno dei due insiemi A e B .

La notazione per indicare l'unione è $A \cup B$ e quindi

$$A \cup B = \{x : x \in A \text{ oppure } x \in B.\}$$

Esempio

Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora

$$A \cup B = \{1, 2, 3, 4, 5\}$$

e, notiamo che l'elemento 3, presente in entrambi gli insiemi, è ovviamente presente nell'unione una sola volta, come da definizione di insieme.

Unione di due insiemi

L'unione di due insiemi A e B è commutativa ed associativa, ovvero

- $A \cup B = B \cup A$ (commutatività)
- $A \cup (B \cup C) = (A \cup B) \cup C$ (associatività)

Intersezione di due insiemi

L'intersezione di due insiemi A e B è l'insieme formato da quegli elementi che appartengono ad entrambi gli insiemi A e B .

La notazione per indicare l'unione è $A \cap B$ e quindi

$$A \cap B = \{x : x \in A \text{ e } x \in B.\}$$

Esempio

Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora

$$A \cap B = \{3\}$$

e, notiamo che l'elemento 3, è l'unico presente in entrambi gli insiemi

Intersezione di due insiemi

L'Intersezione di due insiemi A e B è commutativa ed associativa, ovvero

- $A \cap B = B \cap A$ (commutatività)
- $A \cap (B \cap C) = (A \cap B) \cap C$ (associatività)

Cardinalità dell'unione

Se A e B sono insiemi finiti allora

$$|A \cup B| = |A| + |B| - |A \cap B|$$

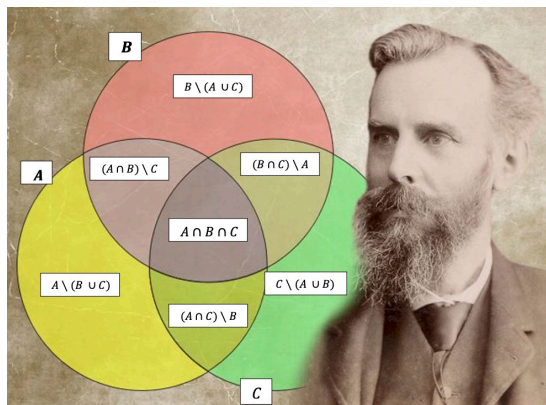
ovvero la cardinalità dell'unione dei due insiemi è la somma delle cardinalità meno la cardinalità dell'intersezione.

Se gli insiemi A e B sono disgiunti allora

$$|A \cup B| = |A| + |B|$$

Diagrammi di Venn

Dati due insiemi A e B , se li rappresentiamo sul piano, la loro relazione può essere caratterizzata da disegni, detti diagrammi di Venn, dal nome del matematico inglese John Venn (1834-1923).



Proprietà formali di unione ed intersezione

Abbiamo già detto che unione ed intersezione sono commutative ed associative. Ecco altre proprietà importanti

- $A \cap A = A$ e $A \cup A = A$ (idempotenza)
- Proprietà Distributiva
 - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (l'intersezione si distribuisce sull'unione)
 - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (l'unione si distribuisce sull'intersezione)
- Proprietà di Assorbimento
 - $A \cap (A \cup B) = A$ (l'intersezione tra un insieme con uno che lo contiene produce l'insieme dato)
 - $A \cup (A \cap B) = A$ (l'unione tra un insieme ed un suo sottoinsieme produce l'insieme dato)

Differenza di due insiemi

La differenza di due insiemi A e B denotata con $A \setminus B$ è l'insieme formato da quegli elementi del primo insieme A in che non appartengono al secondo insieme B . Quindi

$$A \setminus B = \{x : x \in A \text{ e } x \notin B.\}$$

Esempio

Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora $A \setminus B = \{1, 2\}$, l'elemento 3, che è l'unico presente in entrambi gli insiemi, è sottratto da A .

Cardinalità della differenza

Se A e B sono insiemi finiti allora

$$|A \setminus B| = |A| - |A \cap B|$$

ovvero la cardinalità della differenza è la cardinalità di A meno la cardinalità della intersezione di A con B .

Complemento di un insieme

Se assumiamo di trattare con insiemi che siano tutti sottoinsiemi di un insieme "universo" U , allora dato $A \subseteq U$ l'insieme $U \setminus A$ viene detto complemento di A . Quindi, il complemento di un insieme A è l'insieme di tutti gli elementi che non appartengono ad A . Ci sono diverse notazioni per indicare il complemento di un insieme, le più comuni sono

- $U \setminus A = A^C$
- $U \setminus A = \bar{A}$

Esempio

Se $A = \{1, 2, 3\}$ e $U = \{1, 2, 3, \dots, 10\}$ allora

$$A^C = \{4, 5, \dots, 10\}$$

Proprietà del complemento

Elenchiamo le 3 proprietà fondamentali del complemento

- 1 $(A^C)^C = A$ (il complemento del complemento di un insieme è l'insieme stesso)
- 2 $(A \cap B)^C = A^C \cup B^C$ (De Morgan: il complemento dell'intersezione è l'unione dei complementi)
- 3 $(A \cup B)^C = A^C \cap B^C$ (De Morgan: il complemento dell'unione è l'intersezione dei complementi)

Cardinalità del complemento

Se U è finito e $A \subseteq U$ allora $|A^C| = |U| - |A|$.

Differenza simmetrica di due insiemi

La differenza simmetrica di due insiemi A e B è l'unione delle 2 differenze, ovvero $(A \setminus B) \cup (B \setminus A)$, quindi è l'insieme formato da quegli elementi del primo o del secondo insieme che non appartengono ad entrambi.

La notazione per indicare la differenza simmetrica è Δ e quindi

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Esempio

Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora

$$A \Delta B = \{1, 2, 4, 5\}$$

Quindi, l'elemento 3, che è l'unico presente in entrambi gli insiemi, è sottratto dall'unione $A \cup B$.

Differenza simmetrica di due insiemi

La differenza simmetrica di due insiemi A e B è commutativa ed associativa, ovvero

- $A \Delta B = B \Delta A$ (commutatività)
- $A \Delta (B \Delta C) = (A \Delta B) \Delta C$ (associatività)

Inoltre, vale la seguente uguaglianza

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Cardinalità della differenza simmetrica

Se A e B sono finiti allora allora

$$\begin{aligned} |A \Delta B| &= |(A \setminus B) \cup (B \setminus A)| = |A \setminus B| + |B \setminus A| = \\ &= |A| - |A \cap B| + |B| - |B \cap A| = |A| + |B| - 2|A \cap B|. \end{aligned}$$

Dimostrazione diretta

Tutte le dimostrazioni di proprietà e le soluzioni di esercizi su insiemi includeranno dimostrazioni del tipo

- dimostra che $A \subseteq B$ o, equivalentemente, $B \supseteq A$, oppure
- dimostra che $A = B$ oppure
- dimostra che $A = \emptyset$

Per dimostrare che $A \subseteq B$ si considera un elemento generico $x \in A$ e si dimostra che $x \in B$.

Per dimostrare che $A = B$, per l'assioma di estensionalità dobbiamo dimostrare che hanno gli stessi elementi. Quindi si dimostra che $A \subseteq B$ e $B \subseteq A$.

Per dimostrare che $A = \emptyset$ si fa vedere che la definizione di appartenenza ad A porta ad una contraddizione.

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

Dimostriamo prima che $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$

Sia x un elemento generico tale che $x \in (A \setminus B) \cup (B \setminus A)$.

Due casi sono possibili

C1 $x \in (A \setminus B)$ e quindi $x \in A$ e $x \notin B$ perché $A \setminus B$ è l'insieme di tutti gli elementi di A che non appartengono a B . Dal fatto che $x \in A$ ne deduciamo che $x \in A \cup B$ perché $A \cup B$ contiene tutti gli elementi di A e tutti gli elementi di B . Inoltre, dal fatto che $x \notin B$ ne deduciamo che $x \notin A \cap B$ perché non appartenendo a B non può appartenere a $A \cap B$. Quindi, ricapitolando, $x \in A \cup B$ e $x \notin A \cap B$ e quindi appartiene a $(A \cup B) \setminus (A \cap B)$.

C2 $x \in (B \setminus A)$ e quindi $x \in B$ e $x \notin A$. Dal momento che $x \in B$ ne deduciamo che $x \in A \cup B$. Infine, $x \notin A$ implica che $x \notin A \cap B$ e quindi, come nel caso 1, $x \in (A \cup B) \setminus (A \cap B)$.

Abbiamo allora dimostrato che $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$

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

Dimostriamo adesso che $(A \setminus B) \cup (B \setminus A) \supseteq (A \cup B) \setminus (A \cap B)$

Sia allora x un elemento generico tale che $x \in (A \cup B) \setminus (A \cap B)$.

Quindi $x \in A \cup B$ ma $x \notin A \cap B$. Allora x appartiene ad uno solo dei due insiemi A e B .

Due casi sono possibili

C1 $x \in A$ e $x \notin B$: quindi $x \in A \setminus B$. Possiamo allora dedurre che $x \in (A \setminus B) \cup (B \setminus A)$.

C2 $x \in B$ e $x \notin A$: e quindi, $x \in B \setminus A$. Come nel caso 1, allora dedurre che $x \in (A \setminus B) \cup (B \setminus A)$.

Abbiamo allora dimostrato che $(A \setminus B) \cup (B \setminus A) \supseteq (A \cup B) \setminus (A \cap B)$

Risulta, infine, dimostrato che $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

Esercizi

Dimostrare che

$$\mathbf{E1} \quad (A \setminus B) \cup (C \setminus B) = (A \cup C) \setminus B$$

$$\mathbf{E2} \quad (A \setminus B) \cap (C \setminus B) = (A \cap C) \setminus B$$

$$\mathbf{E3} \quad (A \setminus B) \setminus C = A \setminus (B \cup C)$$

$$\mathbf{E4} \quad A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap B \cap C)$$

$$\mathbf{E5} \quad (A \setminus C) \cap (B \setminus C) \cap (A \setminus B) = \emptyset$$

$$\mathbf{E6} \quad (A \cap B)^C = A^C \cup B^C \text{ (De Morgan)}$$

$$\mathbf{E7} \quad (A \cup B)^C = A^C \cap B^C \text{ (De Morgan)}$$

$$\mathbf{E8} \quad A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

$$\mathbf{E9} \quad (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

$$\mathbf{E10} \quad (A \cup B) \setminus (A \Delta B) = A \cap B$$

Insieme delle parti

Dato un insieme T , consideriamo un insieme i cui elementi sono tutte le parti o sottoinsiemi di T . Questo insieme sarà detto Insieme delle parti di T , o anche insieme potenza di T , e si indicherà con il simbolo $\mathcal{P}(T)$ oppure il simbolo $pow(T)$.

Esempio

Sia $T = \{1, 2, 3\}$ allora

$$\mathcal{P}(T) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Un insieme di insiemi, come ad esempio l'insieme delle parti, è anche detto "famiglia di insiemi".

Cardinalità dell'Insieme delle parti

Sia T un insieme finito, quanti sono gli elementi di $\mathcal{P}(T)$?

- Se $T = \emptyset$ ha un solo sottoinsieme, ovvero \emptyset . Quindi $\mathcal{P}(T) = \{\emptyset\}$ e $|\mathcal{P}(T)| = 1$.
- Se $|T| = 1$, quindi $T = \{a\}$, ha due sottoinsiemi, ovvero \emptyset e se stesso. Quindi $\mathcal{P}(T) = \{\emptyset, T\}$ e $|\mathcal{P}(T)| = 2$.
- Se $|T| = 2$, quindi $T = \{a, b\}$ i suoi sottoinsiemi sono \emptyset , $\{a\}$, $\{b\}$, e $\{a, b\}$. Quindi $\mathcal{P}(T) = \{\emptyset, \{a\}, \{b\}, T\}$ e quindi $|\mathcal{P}(T)| = 4$.
- Se $|T| = 3$, come abbiamo visto nell'esempio precedente, $\mathcal{P}(T)$ contiene 8 elementi, ovvero $|\mathcal{P}(T)| = 8$.

Notiamo allora che ogni volta che aumentiamo di una unità il numero di elementi, il numero di elementi dell'insieme delle parti raddoppia. Questo ci fa concludere, intuitivamente, che se $|T| = n$ allora

$$|\mathcal{P}(T)| = 2^n.$$

Dimostreremo in maniera rigorosa che $|\mathcal{P}(T)| = 2^{|T|}$ quando introdurremo il principio di induzione.

Esempi e proprietà

Vediamo alcuni esempi

$$\mathbf{E1} \quad \mathcal{P}(\emptyset) = \{\emptyset\}$$

$$\mathbf{E2} \quad \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

$$\mathbf{E3} \quad \mathcal{P}(\{a, \{a, b\}\}) = \{\emptyset, \{a\}, \{\{a, b\}\}, \{a, \{a, b\}\}\}$$

ed alcune proprietà

$$\mathbf{P1} \quad \mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$$

$$\mathbf{P2} \quad \mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$$

Dimostrazione P1

Dimostriamo la proprietà P1

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$$

Caso \subset : Supponiamo $X \in \mathcal{P}(A \cap B)$, allora $X \subset A \cap B$ quindi $X \subset A$ e $X \subset B$. Possiamo allora concludere che $X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$ da cui $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$

Caso \supset : Viceversa, supponiamo adesso che $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$, allora $X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$. Quindi, $X \subseteq A$ e $X \subseteq B$ ovvero $X \subseteq A \cap B$ che implica $X \in \mathcal{P}(A \cap B)$.

Dimostrazione P2

Dimostriamo la proprietà P2

$$\mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$$

Dobbiamo allora dimostrare che $\mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$ ed inoltre trovare un elemento $X \in \mathcal{P}(A \cup B)$ tale che $X \notin \mathcal{P}(A) \cup \mathcal{P}(B)$ per qualche insieme A e B .

Caso \supset : Supponiamo che $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$, allora $X \in \mathcal{P}(A)$ oppure $X \in \mathcal{P}(B)$. Nel primo caso $X \subseteq A$ mentre nel secondo caso $X \subseteq B$. In entrambi i casi, quindi, $X \subseteq A \cup B$ da cui $X \in \mathcal{P}(A \cup B)$.

Caso \neq : Sia $A = \{1, 2\}$ e $B = \{1, 3\}$. L'insieme $A \cup B = \{1, 2, 3\}$ appartiene a $\mathcal{P}(A \cup B)$ ma non appartiene a $\mathcal{P}(A) \cup \mathcal{P}(B)$.

Famiglie infinite

Una famiglia di insiemi che ha un numero infinito di elementi è una famiglia infinita. Se invece ha un numero finito di elementi allora è una famiglia finita. Si noti che la definizione appena data non riguarda la cardinalità (finita o infinita) degli elementi della famiglia.

Esempio 1

Sia $\mathcal{F} = \{P, D\}$ dove P è l'insieme dei numeri pari (infinito) e D è l'insieme dei numeri dispari (infinito). La famiglia \mathcal{F} è una famiglia finita di insiemi.

Esempio 2

Sia $\mathcal{F} = \{P_1, P_2, P_3, \dots\}$ dove $P_i = \{2^1, \dots, 2^i\}$. La famiglia è infinita, ma tutti i suoi elementi sono insiemi finiti.

Unione di famiglie infinite

Le operazioni di unione ed intersezione si possono estendere al caso di famiglie infinite di insiemi. Sia \mathcal{F} una famiglia qualunque di insiemi, possibilmente infinita. Si indica con

$$\bigcup_{X \in \mathcal{F}} X$$

l'insieme costituito dagli elementi che appartengono a qualcuno degli insiemi $X \in \mathcal{F}$ e viene detto insieme unione della famiglia \mathcal{F} . Quindi,

$$\bigcup_{X \in \mathcal{F}} X = \{x : \exists X, X \in \mathcal{F} \text{ e } x \in X\}$$

Intersezione di famiglie infinite

Analogamente, se \mathcal{F} è una famiglia qualunque di insiemi, possibilmente infinita, si indica con

$$\bigcap_{X \in \mathcal{F}} X$$

l'insieme costituito dagli elementi che appartengono a tutti gli insiemi $X \in \mathcal{F}$ e viene detto insieme intersezione della famiglia \mathcal{F} . Quindi,

$$\bigcap_{X \in \mathcal{F}} X = \{x : \forall X \in \mathcal{F}, x \in X\}$$

Definizione di partizione

Una famiglia di insiemi \mathcal{F} è una partizione dell'insieme U se gli elementi di \mathcal{F} sono sottoinsiemi di U , dette anche parti, classi o blocchi della partizione, che "coprono" U senza sovrapporsi. Formalmente,

- Per ogni $X \in \mathcal{F}$ si ha che $X \subseteq U$;
- $\bigcup_{X \in \mathcal{F}} X = U$
- per ogni $X, Y \in \mathcal{F}, X \neq Y$ si ha $X \cap Y = \emptyset$.

Esempio

Sia $U = \{1, 2, 3, \dots, 12\}$ l'insieme numerico che rappresenta i mesi dell'anno. Allora

$$\mathcal{F} = \{\{1, 3, 5, 7, 8, 10, 12\}, \{2\}, \{4, 6, 9, 11\}\}$$

è una partizione dei mesi dell'anno, nello specifico mesi con 31 giorni, mesi con 30 giorni e mesi con meno di 30 giorni.

Copie ordinate

Consideriamo due elementi, non necessariamente distinti, x e y . Creiamo una coppia ordinata dove il primo elemento è x ed il secondo elemento è y . Denotiamo tale coppia con (x, y) . Si noti che:

- la coppia (x, y) è diversa dalla coppia (y, x) (a meno che $x = y$).
- $(x, y) = (x', y')$ se e solo se $x = x'$ e $y = y'$.

Caveat: la coppia (x, y) è diversa dall'insieme $\{x, y\}$ costituito dagli elementi x e y .

Definizione di insieme prodotto

Siano dati due insiemi non vuoti A e B .

Diremo insieme prodotto di A per B , e lo indicheremo con $A \times B$, l'insieme di tutte le coppie ordinate (x, y) con $x \in A$ e $y \in B$. Quindi,

$$A \times B = \{(x, y) : x \in A \text{ e } y \in B\}.$$

Esempio di insieme prodotto

Esempio di prodotto è il piano cartesiano $\mathbb{R} \times \mathbb{R}$, dove \mathbb{R} indica la retta reale. Così, il piano può essere rappresentato mediante l'insieme di tutte le coppie ordinate di numeri reali, cioè mediante $\mathbb{R} \times \mathbb{R}$. Il piano cartesiano è di solito indicato con \mathbb{R}^2 .

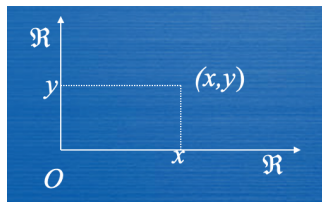


Figura: Piano cartesiano \mathbb{R}^2

Definizione estesa di insieme prodotto

Dati, in un certo ordine, tre insiemi A, B, C , si chiama loro prodotto, e si indica con $A \times B \times C$ l'insieme di tutte le terne ordinate (x, y, z) con $x \in A, y \in B, z \in C$.

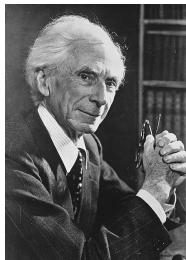
La definizione si estende in modo ovvio al caso di un numero finito qualsiasi di insiemi, A_1, A_2, \dots, A_n .

Ad esempio si indica con \mathbb{R}^n l'insieme di tutte le n -uple ordinate (x_1, x_2, \dots, x_n) di numeri reali.

Paradosso di Russell

Stiamo basando tutti i nostri discorsi sul concetto intuitivo di insieme, assunto come "nozione primitiva", ma sin dall'inizio abbiamo sottolineato che bisogna usare tale concetto intuitivo con attenzione per evitare di cadere in paradossi.

Il più famoso di tali paradossi è dovuto a Bertrand Russell (1872-1970), matematico, filosofo, logico inglese.



Paradosso di Russell

Agli inizi del XX secolo, i matematici teorizzavano la possibilità di fondare tutta la matematica sulla teoria degli insiemi. Ma Russell scoprì un paradosso che sembrava assestare un colpo "mortale" a tale speranza.

Partendo dal concetto intuitivo di insieme e dagli esempi che abbiamo visto, deduciamo che in generale un insieme non appartiene a se stesso. Però, possiamo anche immaginare la possibilità di un insieme che appartiene a se stesso. Per esempio, l'insieme di tutti gli insiemi che hanno un numero infinito di elementi, di sicuro appartiene a se stesso.

Se, quindi, assumiamo che una qualunque "proprietà" possa definire un insieme, possiamo anche costruire l'insieme di tutti gli insiemi che non appartengono a se stessi, ovvero

$$S = \{A : A \text{ è un insieme, e } A \notin A\}$$

Paradosso di Russell

Domanda

$$S \in S \quad ???$$

- Se rispondiamo "SI" $S \in S$, allora dalla definizione di S ne dobbiamo dedurre che $S \notin S$.
- Se rispondiamo "NO", $S \notin S$, allora dalla definizione di S ne dobbiamo dedurre che $S \in S$.

Quindi, entrambe le risposte portano ad una contraddizione.

Come evitare la contraddizione?

Una possibilità è quella di imporre che la definizione di insieme, per esempio usando un predicato che lo definisce, deve implicitamente includere che tale insieme sia anche sottoinsieme di un insieme conosciuto.

Tale definizione non si applica all'insieme delle parti che comunque è definito da un assioma.

Avremo allora che

$$S = \{A : A \subseteq U, A \notin A\}$$

dove U è un insieme "universo" conosciuto. Avremo ancora la contraddizione che $S \in S$ allora $S \notin S$, ma se $S \notin S$ allora o $S \notin U$ oppure $S \in S$. E quindi la contraddizione si può evitare assumendo che $S \notin U$.

STRUTTURE DISCRETE**PARTE 1: INSIEMI E RELAZIONI****2: Relazioni e Funzioni**

Relazione Binaria

Siano U un insieme non vuoto. Con il termine relazione (binaria) indichiamo un predicato in 2 variabili definito sugli elementi di U , ovvero un insieme

$$R \subseteq U \times U$$

Sia ora R una relazione. Consideriamo l'insieme

$$\{(x, y) : (x, y) \in A \times B \text{ e } R(x, y)\},$$

cioè il sottoinsieme di $A \times B$ costituito da tutte le coppie per cui la relazione è verificata. Esso viene detto grafico della relazione.

Da un punto di vista di notazioni, scriveremo indifferentemente $R(x, y)$ oppure $(x, y) \in R$ per denotare che x e y verificano la relazione R .

Funzione

Una relazione f definita in $A \times B$ si dice funzione di A (dominio) in B (codominio), se per ogni $x \in A$ esiste uno ed uno solo $y \in B$ tale che $(x, y) \in f$.

La notazione classica $f : A \rightarrow B$ mette in evidenza il dominio e il codominio di f . Per ogni $x \in A$ l'unico elemento $y \in B$ tale che $(x, y) \in f$ si indica con $f(x)$ e si dice valore assunto dalla funzione f in x .

Funzioni particolari

Alcune funzioni particolari

- Dato un qualunque insieme A , l'applicazione $f : A \rightarrow A$ tale che per ogni x $f(x) = x$ si dice applicazione identica di A e si indica con I_A .
- Dati due insiemi qualunque A e B , l'applicazione $f : A \times B \rightarrow A$ tale che per ogni (x, y) $f(x, y) = x$ si dice proiezione canonica su A .
- Similmente, l'applicazione $f : A \times B \rightarrow B$ tale che per ogni (x, y) $f(x, y) = y$ si dice proiezione canonica su B .

Sulle funzioni

Data un'applicazione $f : A \rightarrow B$ e dato un sottoinsieme X di A si dice immagine di X il sottoinsieme di B costituito dagli elementi che provengono da qualche elemento di X . Questo sottoinsieme viene indicato con $f(X)$. Pertanto:

$$f(X) = \{y : y \in B \text{ e } (\exists x \in X) | f(x) = y\}.$$

In particolare, l'insieme $f(A)$ si dirà immagine dell'applicazione f . Se l'immagine di f è un insieme che ha un solo elemento, allora la f è una funzione costante, ovvero

$$\forall x, y \in A, f(x) = f(y).$$

Funzione surgettiva

Data un'applicazione $f : A \rightarrow B$ se l'immagine $f(A) = B$ allora la funzione si dice surgettiva.

Esempi

- L'applicazione identica in un qualunque insieme;
- le proiezioni canoniche su un prodotto $X \times Y$.

Funzione iniettiva

Data un'applicazione $f : A \rightarrow B$ se porta punti distinti su punti distinti allora la funzione si dice iniettiva. Formalmente

$$\forall x, y \in A, \text{ se } x \neq y, \text{ allora } f(x) \neq f(y).$$

Esempi

- L'applicazione identica in un qualunque insieme;
- la funzione successore sui numeri naturali, ossia la funzione $f(n) = n + 1$.

Funzione biiettiva

Un'applicazione $f : A \rightarrow B$ si dice biiettiva (o anche corrispondenza biunivoca) se è sia iniettiva che surgettiva.

Esempi

- L'applicazione identica in un qualunque insieme;
- la funzione dall'insieme dei numeri naturali all'insieme dei numeri naturali pari, che associa ad ogni numero il suo doppio. Ossia la funzione $f(n) = 2n$.

Esempi di funzioni

Siano \mathbb{R} l'insieme dei numeri reali e \mathbb{R}^+ l'insieme dei numeri reali positivi, allora la funzione $x \rightarrow x^2$

- non è iniettiva né surgettiva se definita $\mathbb{R} \rightarrow \mathbb{R}$
- è iniettiva se definita $\mathbb{R}^+ \rightarrow \mathbb{R}$
- è surgettiva se definita $\mathbb{R} \rightarrow \mathbb{R}^+$
- è una biiezione se definita $\mathbb{R}^+ \rightarrow \mathbb{R}^+$

Cardinalità di un insieme

Abbiamo già detto che la cardinalità di un insieme è il numero di elementi che appartengono all'insieme.

La nozione di biiezione o corrispondenza biunivoca sta alla base della nozione di numero: contare significa stabilire una corrispondenza biunivoca tra un insieme di oggetti ed un insieme "campione". In particolare sia n un numero naturale maggiore di 0 e sia

$I_n = \{0, 1, 2, \dots, n-1\}$ l'insieme degli interi che precedono n

- si dice che un insieme X è finito se esiste un $n \in \mathbb{N}$ tale che X si possa mettere in corrispondenza biunivoca con I_n ;
- in questo caso si dice che X ha numero cardinale n e si scrive $c(X) = n$ oppure $|X| = n$.
- Se non esiste alcun n per cui questo è possibile, si dice che X è infinito.

Cardinalità di un insieme

Dimostriamo il seguente

Teorema

Se A e B sono due insiemi finiti ed esiste una funzione iniettiva $f : A \rightarrow B$ allora $|A| \leq |B|$.

Dimostrazione

Consideriamo l'immagine $f(A)$. Sappiamo che $f(A) \subseteq B$ e sappiamo che ogni elemento di $f(A)$ è l'immagine di uno ed un solo elemento di A poiché la funzione f è iniettiva. Quindi in $f(A)$ ci sono tanti elementi quanti ce ne sono in A . Ne concludiamo che $|A| = |f(A)| \leq |B|$.

△

Cardinalità di un insieme

Se X e Y sono insiemi finiti disgiunti si ha

$$c(X \cup Y) = c(X) + c(Y)$$

Più in generale

$$c(X \cup Y) = c(X) + c(Y) - c(X \cap Y).$$

Se X e Y sono insiemi finiti

$$c(X \times Y) = c(X) * c(Y)$$

Proprietà delle relazioni

Sia dato un insieme U . Diremo che una relazione $R(x, y)$ definita in $U \times U$ è:

- **Riflessiva** : se $\forall x \in U$ risulta vero $R(x, x)$.
- **Simmetrica**: se $\forall x, y \in U$ se $R(x, y)$ è vero allora anche $R(y, x)$ è vero;
- **Transitiva**: se $\forall x, y, z \in U$ se $R(x, y)$ e $R(y, z)$ sono vere, allora $R(x, z)$ è vero

Una relazione che sia riflessiva, simmetrica e transitiva si dice relazione di **equivalenza**.

Cardinalità di un insieme

Dati due insiemi, si dice che essi hanno lo stesso numero cardinale se essi possono essere posti in corrispondenza biunivoca. Se due insiemi X e Y hanno lo stesso numero cardinale scriveremo $c(X) = c(Y)$.
Avere lo stesso numero cardinale è una relazione riflessiva, simmetrica e transitiva, e quindi una relazione di equivalenza.

Proprietà delle relazioni di equivalenza

Indicheremo una relazione di equivalenza tra x e y con

$$x \approx y.$$

Data una relazione di equivalenza in un insieme U e preso un $x \in U$, indichiamo con $[x]$ l'insieme di tutti gli elementi di U equivalenti a x ovvero

$$[x] = \{y \in U : x \approx y\}$$

Chiamiamo $[x]$ la **classe di equivalenza** di x .

Proprietà delle classi di equivalenza

Vale il seguente

Teorema

Due classi di equivalenza o sono disgiunte o coincidono.

Dimostrazione

Siano $[x]$ e $[z]$ due classi di equivalenza e supponiamo che esse abbiano un elemento w in comune: pertanto è $w \approx x$ e $w \approx z$. Allora, per la proprietà transitiva è $x \approx z$.

Sia ora $y \in [x]$, cioè $y \approx x$. Per la proprietà transitiva è $y \approx z$, cioè $y \in [z]$. Quindi, $[x] \subseteq [z]$.

Analogamente si dimostra che $[z] \subseteq [x]$.

△

Classi di equivalenza e partizioni

Data una relazione di equivalenza R su un insieme U , consideriamo ora la famiglia di insiemi \mathcal{F} costituita da tutte le classi di equivalenza. Per costruzione, \mathcal{F} è un sottoinsieme di $\text{pow}(U)$ tale che:

- Per ogni $X \in \mathcal{F}$ si ha che $X \neq \emptyset$, e $\bigcup_{X \in \mathcal{F}} X = U$, infatti per ogni $x \in U$, $x \in [x]$;
- per ogni $X, Y \in \mathcal{F}$, $X \neq Y$ si ha $X \cap Y = \emptyset$ (vedi teorema precedente)

Quindi, una relazione di equivalenza R individua una partizione \mathcal{F} su U che viene detta **Insieme Quoziente** di U rispetto alla relazione R e viene indicata col simbolo U/R .

Relazioni di Equivalenza e applicazioni surgettive

Reciprocamente, data una partizione \mathcal{F} di un insieme U , è subito individuata in modo unico una relazione R tale che

$$\mathcal{F} = U/R.$$

La relazione R sarà ovviamente la seguente: $x \approx y$ se e solo se x e y appartengono ad un medesimo elemento di \mathcal{F} .

Data in U una relazione R risulta individuata l'applicazione $U \rightarrow U/R$ che porta ogni $x \in U$ nella sua classe di equivalenza $[x]$. Si tratta di un'applicazione surgettiva che viene detta **applicazione canonica sul quoziente**.

Relazioni di pre-ordine

Definizione

Si dice preordinamento (o preordine) una relazione binaria assegnata in un insieme che goda della proprietà riflessiva e transitiva.

Se R è un preordinamento occorre tener presente che, non essendo più assicurata la proprietà simmetrica se è vero che $R(x, y)$ non è più necessariamente vero che $R(y, x)$.

Esempi

- Ogni relazione di equivalenza è un pre-ordinamento.
- La relazione $x \leq y$ nell'ambito degli interi (o razionali, o reali) è un pre-ordinamento.
- Sia E un insieme qualunque; la relazione $X \subseteq Y$ è un pre-ordinamento in $\text{pow}(U)$.

Relazioni d'ordine

Definizione

Si dice che una relazione binaria R in un insieme U è antisimmetrica se:

$$\forall x, \forall y \in U \text{ si ha che : } (R(x, y) \text{ e } R(y, x)) \rightarrow x = y.$$

In altre parole il sussistere di entrambe le relazioni $R(x, y)$ e $R(y, x)$ è possibile solo quando x e y coincidono.

Definizione

Si dice ordinamento un preordinamento che goda anche della proprietà antisimmetrica. Pertanto un ordinamento è una relazione che gode della proprietà riflessiva, antisimmetrica e transitiva.

Insiemi ordinati

Definizione

Un insieme U su cui è definita un relazione di pre-ordine si dice pre-ordinato.

Un insieme U su cui è definita un relazione d'ordine si dice ordinato.

Dato un pre-ordinamento oppure un ordinamento (rappresentato dal simbolo \leq) in un insieme U , si pone

$$x < y \text{ se } x \leq y \text{ e } x \neq y.$$

Massimi e minimi

Definizione

- *Massimi e Massimali:*

- *Un elemento M di un insieme ordinato U si dice massimo se per ogni $x \in U$ si ha $x \leq M$.*
- *Si dice invece massimale se non vi è alcun elemento di U che lo supera.*

- *Minimi e minimali*

- *Un elemento m di un insieme ordinato U si dice minimo se per ogni $x \in U$ si ha $m \leq x$.*
- *Si dice invece minimale se non vi è alcun elemento di U ad esso inferiore*

Massimi e minimi

- Evidentemente ogni elemento che sia massimo (minimo) è anche massimale (minimale) ma non viceversa.
- Un insieme ordinato può avere più elementi massimali (minimali) ma non può avere più di un massimo (minimo).
- In un insieme ordinato non sempre accade che due elementi x e y siano fra loro confrontabili, cioè sussista una delle due relazioni $x \leq y$ o $y \leq x$.

Esempi

- Sia U un insieme qualunque; la relazione $X \subseteq Y$ è un ordinamento in $\text{pow}(U)$. Se l'insieme U ha più di un elemento si possono trovare coppie X e Y di sottoinsiemi di U tali che $X \not\subseteq Y$ e $Y \not\subseteq X$.
- La relazione $x \leq y$ nell'ambito degli interi (o razionali, o reali) è un ordinamento. In questo caso tutti gli elementi sono confrontabili

Insiemi totalmente ordinati

Definizione

Un ordinamento \leq definito in un insieme U si dice totale o lineare se per ogni coppia (x, y) di elementi di U si ha $x \leq y$ oppure $y \leq x$. Altrimenti si dirà parziale.

Un sottoinsieme T di un insieme ordinato U risulta anch'esso ordinato con l'ordinamento che gli viene subordinato da U .

Strutture dati per insiemi di interi

Sia $A \subseteq \mathbb{N}$ un insieme finito e non vuoto, e quindi $c(A) = n$ per qualche $n \geq 1$. Dal momento che U è finito, possiamo dire che $A \subseteq I_m$ per qualche intero m . Ricordiamo che $I_m = \{0, 1, 2, \dots, m-1\}$.

Possiamo utilizzare diverse rappresentazioni per gli insiemi finiti di interi, tenendo conto dell'utilizzo che vogliamo farne. Per esempio

- verificare se $x \in A$;
- dati A e B calcolare $A \cup B$ e $A \cap B$
- dati A e B verificare se $A \subseteq B$

Strutture dati per insiemi di interi

Rappresentazione binaria

La struttura dati più semplice ed immediata per rappresentare $A \subseteq I_m$ è un'array binaria X di m elementi, tale che

- $X[i] = 1$ se $i \in A$
- $X[i] = 0$ se $i \notin A$

Rappresentazione estesa

In alternativa si può utilizzare un'array di interi (o una lista concatenata) Y con $|A| = n$ elementi, tale che se $A = \{x_0, x_1, \dots, x_{n-1}\}$ allora per ogni $0 \leq i \leq n-1$

$$Y[i] = x_i$$

Strutture dati per insiemi di interi

Se utilizziamo la rappresentazione binaria, verificare che un elemento $i \in A$ prende tempo costante.

Se utilizziamo la rappresentazione estesa, invece, ed A non è ordinato, dobbiamo scorrere tutta l'array e quindi tempo lineare. Se l'array è ordinata invece si può fare in tempo logaritmico.

D'altro canto, se utilizziamo la rappresentazione binaria, per l'insieme $A = \{10, 3, 99\}$ serve un'array di dimensione 100, mentre, se utilizziamo la rappresentazione estesa, serve un'array di dimensione 3.

Strutture dati per insiemi di interi

Se $U = I_n$ ovvero $U = \{0, 1, 2, \dots, n-1\}$ la rappresentazione binaria di ogni suo sottoinsieme è una sequenza di n bits.

Quindi, tutti i suoi sottoinsiemi sono rappresentabili usando n bits.

Possiamo di nuovo rispondere alla domanda: quanti sono gli elementi di $\text{pow}(U)$?

Questa volta lo facciamo dicendo che gli elementi di $\text{pow}(U)$ sono tanti quanti sono i numeri binari esprimibili con $|U|$ bits. Quindi $2^{|U|}$.

Esercizi

Ricordiamo che una relazione (binaria) R su un insieme U è definita come $R \subseteq U \times U$. Si assuma che R ed S sono relazioni su un insieme U .

E1 Se R ed S sono riflessive,

(E1.1) $R \cap S$ è riflessiva?

(E1.2) $R \cup S$ è riflessiva?

E2 Se R ed S sono simmetriche

(E2.1) $R \cap S$ è simmetrica?

(E2.2) $R \cup S$ è simmetrica?

E3 Se R ed S sono transitive

(E2.1) $R \cap S$ è transitiva?

(E2.2) $R \cup S$ è transitiva?

Nota bene: dimostrare le risposte "positive", giustificare le risposte negative per mezzo di un controesempio.

Esercizi

Per le seguenti relazioni, dimostrare se sono riflessive, simmetriche o transitive.

- E4** U è l'insieme dei cittadini italiani e $R(x, y)$ la relazione x vive a meno di 10Km da y
- E5** U un insieme finito, $P(U)$ l'insieme potenza e $R(X, Y)$ la relazione X e Y sono disgiunti
- E6** U un insieme finito, $P(U)$ l'insieme potenza e $R(X, Y)$ la relazione X e Y hanno intersezione non vuota
- E7** U un insieme finito, $P(U)$ l'insieme potenza e $R(X, Y)$ la relazione $|X \setminus Y| \geq |Y \setminus X|$

Nota bene: dimostrare le risposte "positive", giustificare le risposte negative per mezzo di un controesempio.

Il Problema del "Hitting Set"

Un problema matematicamente, ma soprattutto **computazionalmente** interessante è quello di trovare un hitting set minimo per una famiglia di insiemi. Diamo la definizione di Hitting Set (HS).

Definizione (Hitting Set)

Siano U un insieme finito, $H \subseteq U$, e sia \mathcal{A} una famiglia di sottoinsiemi di U tutti diversi dall'insieme vuoto.

Diciamo che H è un hitting set (HS) per \mathcal{A} se e solo se per ogni $A \in \mathcal{A}$ si ha $A \cap H \neq \emptyset$.

Esempio

Sia $U = \{a, b, c, d, e\}$ e sia

$$\mathcal{A} = \{\{a, b, c\}, \{a, d, e\}, \{b, c, d\}, \{c, d, e\}\}.$$

L'insieme $\{a, b, c\}$ è un HS per \mathcal{A} mentre $\{b, c\}$ o $\{d, e\}$ non lo sono.

Il Problema del "Hitting Set"

Definizione (Hitting Set Minimo)

Siano U un insieme finito, $H \subseteq U$, e sia \mathcal{A} una famiglia di sottoinsiemi di U tutti diversi dall'insieme vuoto.

Se H è un hitting set e per ogni $x \in H$ l'insieme $H \setminus \{x\}$ non è un hitting set, diciamo che H è un hitting set minimale.

Se H è un hitting set tale che $|H| = \min\{|K| : K \text{ è un hitting set } \mathcal{A}\}$ allora H è un hitting set minimo

Esempio

Sia $U = \{a, b, c, d, e\}$ e sia

$$\mathcal{A} = \{\{a, b, c\}, \{a, d, e\}, \{b, c, d\}, \{c, d, e\}\}.$$

L'insieme $\{a, b, c\}$ è un HS ma non è minimale poiché $\{a, c\}$ è un HS.

$\{a, c\}$ è anche minimo, visto che nessun elemento da solo è presente in tutti gli insiemi di \mathcal{A} .

Come trovare un HS minimo?

- Il problema di trovare un HS minimo per una famiglia di insiemi è facilmente risolvibile: basta provare per tutti i sottoinsiemi di U .
- Sfortunatamente, questo vorrebbe dire che il numero di operazioni da fare è esponenziale in $|U|$ visto che i sottoinsiemi non vuoti di U sono esattamente $2^{|U|} - 1$.
- Se $|U| = 100$ il numero totale di operazioni sarebbe dell'ordine di $1,26 \cdot 10^{30}$. Anche avendo un computer in grado di generare e controllare un miliardo di sottoinsiemi di U al secondo, servirebbero $1,26 \cdot 10^{21}$ secondi, ossia circa $3,5 \cdot 10^{17}$ ore. Quindi, in totale, $1,4510^{16}$ giorni, che equivalgono a circa 40 mila miliardi di anni.
- Conviene senz'altro assumere che non si abbia tutto questo tempo a disposizione.
- Cosa fare allora?

Come trovare un HS minimo?

- Possiamo fare di meglio che controllare tutti i sottoinsiemi di U ?
- Risposta: **non si sa!** Nessuno sa se esiste un algoritmo o un'idea migliore.
- Il problema del minimo HS appartiene ad una classe di problemi (sono tanti), chiamati \mathcal{NP} -hard o anche intrattabili, per i quali non si conoscono soluzioni veloci, ossia soluzioni dove il numero delle operazioni cresce in maniera polinomiale e non esponenziale al crescere della dimensione del problema.
- In genere, per questo tipo di problemi, si studiano casi particolari e si danno soluzioni che producono soluzioni "buone" ma non ottime per il caso generale.

Casi particolari per il problema HS minimo

- Un primo caso particolare è quello in cui gli insiemi della famiglia \mathcal{A} sono tutti disgiunti. Tale è il caso, se per esempio \mathcal{A} è una partizione di U . In questo caso, si prende un elemento a caso in ogni insieme di \mathcal{A} e si ottiene velocemente un HS minimo.
- Il caso di cui sopra, ci dice, in particolare, che se \mathcal{A} possiede n elementi ognuno disgiunto da tutti gli altri (per esempio n insiemi singoletto) allora ogni HS deve contenere almeno un elemento da ognuno di questi insiemi.

Esempio

Sia $U = \{a, b, c, d, e\}$ e sia

$$\mathcal{A} = \{\{a, b, c\}, \{a, d, e\}, \{c, d\}, \{c, d, e\}, \{d\}, \{e\}\}.$$

Allora d, e devono appartenere ad ogni HS, e quindi, in questo esempio un HS minimo è per esempio $\{a, d, e\}$.

$\{d, e\}$ non è un HS, visto che non interseca $\{a, b, c\}$.

Algoritmi "golosi" (o greedy)

- Un modo per cercare di risolvere i problemi \mathcal{NP} -hard e, quindi, in particolare anche il problema HS minimo, è quello di utilizzare un approccio cosiddetto "goloso" o "greedy", ovvero scegliere elementi che sembrano molto buoni.
- Nello specifico, potremmo prendere l'elemento x_1 di U che appartiene al maggior numero di elementi di \mathcal{A}
- Poi, per tutti gli elementi di \mathcal{A} a cui x_1 non appartiene, scegliamo l'elemento x_2 che appartiene alla maggior parte di essi, e così via.

Algoritmi "golosi" (o greedy): Esempio

Sia $U = \{a, b, c, d, e, f\}$ e sia

$$\mathcal{A} = \{\{a, b, e\}, \{a, b, f\}, \{b, d\}, \{a, c, f\}, \{a, c, e\}, \{c, e, f\}\}.$$

- L'elemento a appartiene a 4 insiemi e viene scelto. Rimangono 2 insiemi disgiunti, $\{b, d\}$ e $\{c, e, f\}$.
- Da ognuno di questi 2 insiemi disgiunti siamo costretti a scegliere un elemento, per esempio d e f e così abbiamo costruito un insieme $H = \{a, d, f\}$ che è un HS minimale ma non minimo.
- Infatti, hitting set minimo è l'insieme $\{b, c\}$.
- Un altro HS che l'algoritmo potrebbe tornare è $\{a, b, c\}$ che ovviamente non è minimale.

HS Minimo: Esercizi

Sia $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Per ognuna delle seguenti famiglie, trovare uno Hitting Set minimo.

- 1 $\mathcal{A} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8\}, \{9, 10\}, \{1, 4, 5\}, \{2, 6, 8\}, \{3, 5\}, \{1, 10\}\}$
- 2 $\mathcal{A} = \{\{1, 2\}, \{1, 3, 4\}, \{4, 5, 6\}, \{6, 7, 8\}, \{8, 9, 10\}, \{5, 8, 9\}\}$
- 3 $\mathcal{A} = \{\{1, 2\}, \{2, 3, 4\}, \{4, 5\}, \{5, 6\}, \{3, 8, 9\}, \{6, 9\}, \{7, 8\}, \{7, 10\}\}$

STRUTTURE DISCRETE

PARTE 1: INSIEMI E RELAZIONI

3: Insiemi chiusi e famiglie chiuse di insiemi

Insiemi chiusi

Sia dato un insieme U ed una operazione definita su uno o più elementi di U . Se l'operazione può essere definita o completata all'interno di U allora diciamo che U è chiuso rispetto a tale operazione.

Esempi

- Sia $U = \mathbb{N}$ se consideriamo l'operazione binaria "somma" allora \mathbb{N} è chiuso rispetto alla somma, perché la somma di due numeri interi non negativi è a sua volta un numero intero non negativo.
- Se invece consideriamo l'operazione "sottrazione" allora \mathbb{N} non è chiuso rispetto alla sottrazione perché il risultato della sottrazione potrebbe essere un numero negativo che non appartiene a \mathbb{N} .

Insiemi chiusi

Vediamo altri esempi

Esempi

- Sia $X = \{1, 2, 3\}$. Se consideriamo l'operazione binaria "minimo comune multiplo" (mcm) allora dato che $mcm(2, 3) = 6$, X non è chiuso rispetto a tale operazione.
- Se poniamo $X = \{1, 2, 3, 6\}$ allora X è chiuso rispetto all'operazione mcm .
- Se consideriamo l'insieme degli interi relativi \mathbb{Z} allora abbiamo un insieme chiuso rispetto alla sottrazione.
- Però \mathbb{Z} non è chiuso rispetto alla divisione

Chiusura rispetto ad unione ed intersezione

Definizione

Sia \mathcal{F} una famiglia di insiemi

- diciamo che \mathcal{F} è chiusa rispetto all'unione se per ogni coppia di insiemi X e Y appartenenti a \mathcal{F} anche $X \cup Y$ appartiene a \mathcal{F} .
- diciamo che \mathcal{F} è chiusa rispetto all'intersezione se per ogni coppia di insiemi X e Y appartenenti a \mathcal{F} anche $X \cap Y$ appartiene a \mathcal{F} .

Esempi

Sia $\mathcal{F} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}\}$ abbiamo che \mathcal{F} è chiuso rispetto all'unione ma non è chiuso rispetto all'intersezione, perché $\{1, 2\} \cap \{1, 3\} = \{1\} \notin \mathcal{F}$.

Chiusura rispetto ad unione ed intersezione

Sia \mathcal{F} una famiglia di insiemi, tutti sottoinsiemi di un insieme universo U . Quindi, $\mathcal{F} \subseteq \text{pow}(U)$. In particolare, per ogni $X \in \mathcal{F}$ il complemento di X rispetto ad U , ovvero $X^C = U \setminus X$ è anche un elemento di $\text{pow}(U)$. Possiamo allora definire la famiglia "complemento" rispetto ad U , e la denotiamo con \mathcal{F}^C , come segue

$$\mathcal{F}^C = \{X^C : X \in \mathcal{F}\}$$

Notiamo che

$$(\mathcal{F}^C)^C = \mathcal{F}$$

Vale il seguente

Teorema

La famiglia \mathcal{F} è chiusa rispetto all'unione (resp. intersezione) se e solo se la famiglia \mathcal{F}^C è chiusa rispetto all'intersezione (resp. unione).

Chiusura rispetto ad unione ed intersezione

Dimostriamo il teorema

Teorema

La famiglia \mathcal{F} è chiusa rispetto all'unione se e solo se la famiglia \mathcal{F}^C è chiusa rispetto all'intersezione.

Dimostrazione

Se \mathcal{F} è chiusa rispetto all'unione. Siano $X, Y \in \mathcal{F}^C$. Esistono allora $A, B \in \mathcal{F}$ tali che $X = A^C$ e $Y = B^C$. Quindi, $X \cap Y = A^C \cap B^C = (A \cup B)^C$ (De Morgan). E quindi, poiché $(A \cup B) \in \mathcal{F}$ si ha che $(A \cup B)^C \in \mathcal{F}^C$.

Viceversa sia \mathcal{F}^C chiusa rispetto all'intersezione e siano $A, B \in \mathcal{F}$. Sappiamo che $A^C, B^C, A^C \cap B^C \in \mathcal{F}^C$. Ma per De Morgan $A^C \cap B^C = (A \cup B)^C$, quindi $A \cup B \in \mathcal{F}$.

△

Chiusura rispetto ad unione ed intersezione

Sia data adesso una famiglia finita di insiemi \mathcal{F} su un insieme universo U . Sia data un'operazione $*$ binaria sugli insiemi di \mathcal{F} . Per esempio, $*$ potrebbe essere l'unione \cup oppure l'intersezione \cap . Definiamo chiusura di \mathcal{F} rispetto a $*$ la più piccola famiglia $\mathcal{F}_* \supseteq \mathcal{F}$ tale che \mathcal{F}_* è chiusa rispetto a $*$.

Quindi, la chiusura di \mathcal{F} rispetto all'operazione binaria $*$ è la famiglia che contiene tutti e soli gli insiemi di \mathcal{F} ed inoltre tutti gli elementi che si possono ottenere applicando l'operazione $*$ a 2 o più elementi di \mathcal{F} .

Quindi, per esempio, nel caso di unione e intersezione abbiamo

$$\mathcal{F}_{\cup} = \left\{ \bigcup_{X \in F'} X : F' \subseteq \mathcal{F}, F' \neq \emptyset \right\}$$

$$\mathcal{F}_{\cap} = \left\{ \bigcap_{X \in F'} X : F' \subseteq \mathcal{F}, F' \neq \emptyset \right\}$$

Esempio

- Sia data $\mathcal{F} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}\}$ famiglia non chiusa rispetto all'unione. La chiusura di \mathcal{F} è la famiglia

$$\mathcal{F}' = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{1, 2, 3, 4\}, \{1, 2, 4\}\}$$

- Si noti che anche la seguente famiglia è chiusa rispetto all'unione e contiene \mathcal{F} ma non è la chiusura di \mathcal{F}

$$\mathcal{F}'' = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{1, 2, 3, 4\}, \{1, 2, 4\}, \{1, 3, 4\}\}$$

Infatti, l'insieme $\{1, 3, 4\}$ non si può ottenere dall'unione di elementi di \mathcal{F}

Chiusura rispetto ad unione ed intersezione

Per calcolare la chiusura \mathcal{F}_\cup di una famiglia finita di insiemi \mathcal{F} definita su un insieme universo U rispetto all'unione possiamo, da definizione, tenere in considerazione tutti i sottoinsiemi di \mathcal{F} oppure usare un algoritmo iterativo che ad ogni passo calcola il risultato dell'operazione \cup ottenuto utilizzando k elementi di \mathcal{F} per $k = 1, \dots, m$ dove $m = |\mathcal{F}|$. Agiamo così

- ❶ Costruiamo la famiglia \mathcal{F}_1 mettendoci tutti gli elementi di \mathcal{F} .
- ❷ Per ogni $i = 2$ sino a m calcoliamo \mathcal{F}_i utilizzando tutte le coppie di elementi X, Y con $X \in \mathcal{F}$ e $Y \in \mathcal{F}_{i-1}$ e mettendo $X \cup Y$ in \mathcal{F}_i .
- ❸ Poniamo infine

$$\mathcal{F}_\cup = \bigcup_{i=1}^m \mathcal{F}_i$$

In maniera del tutto analoga, possiamo costruire la chiusura di una famiglia \mathcal{F} rispetto alla intersezione.

Chiusura: Esercizi

Sia $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Per ognuna delle seguenti famiglie, trovare la loro chiusura sia rispetto all'unione che rispetto all'intersezione.

- 1 $\mathcal{A} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8\}, \{9, 10\}, \{1, 4, 5\}, \{2, 6, 8\}, \{3, 5\}, \{1, 10\}\}$
- 2 $\mathcal{A} = \{\{1, 2\}, \{1, 3, 4\}, \{4, 5, 6\}, \{6, 7, 8\}, \{8, 9, 10\}, \{5, 8, 9\}\}$
- 3 $\mathcal{A} = \{\{1, 2\}, \{2, 3, 4\}, \{4, 5\}, \{5, 6\}, \{3, 8, 9\}, \{6, 9\}, \{7, 8\}, \{7, 10\}\}$

La congettura Union-Closed

Una **congettura** è una proprietà, un fatto che è sempre verificato da tutti gli esempi, ma che non si è ancora riusciti a dimostrare.

Parlando di famiglie di insiemi, una delle congetture più semplici riguarda le famiglie di insiemi chiuse rispetto all'unione.

La formulazione della congettura è molto semplice e, come spesso accade in questi casi, si è dimostrata, ad oggi, impossibile da dimostrare.

CONGETTURA (UC-Conjecture)

Sia U un insieme finito e sia \mathcal{A} una famiglia di sottoinsiemi di U non tutti vuoti. Se \mathcal{A} è chiuso rispetto all'unione esiste un elemento $x \in U$ che appartiene ad almeno la metà degli elementi di \mathcal{A} .

La congettura Union-Closed

In effetti la congettura, formulata intorno agli anni '70, nasce nella versione "complementare".

CONGETTURA (IC-Conjecture)

Sia U un insieme finito e sia \mathcal{A} una famiglia di sottoinsiemi di U non tutti vuoti. Se \mathcal{A} è chiuso rispetto all'intersezione esiste un elemento $x \in U$ che appartiene a non più della metà degli elementi di \mathcal{A} .

Le due versioni, UC-Conjecture e IC-Conjecture sono equivalenti visto che sappiamo che una famiglia \mathcal{A} è chiusa rispetto all'unione se e solo se la famiglia \mathcal{A}^C è chiusa rispetto all'intersezione, e, ovviamente per ogni $A \in \mathcal{A}$ se $x \in A$ allora $x \notin A^C$ con $A^C \in \mathcal{A}^C$.

Esempio

Sia $U = \{1, 2, 3, 4, 5, 6\}$

123456						123456			
12345	12346	12356	12456	13456	23456	12356	12346	12345	
1234	1235	1236	1456	2456	3456	1236	1235	1234	
	123	145	246	356	456	456	236	135	124
		45	46	56		56	46	45	23
			4	5	6		6	5	4
									3
									2
									1
									\emptyset
(a) Union-closed						(b) Intersection-closed			

Figura: \mathcal{A} ed il complemento \mathcal{A}^C

Entrambe le famiglie \mathcal{A} e \mathcal{A}^C contengono 25 elementi.

L'elemento 6 appare 16 volte tra gli elementi di \mathcal{A} e quindi verifica la congettura UC, ed appare 9 volte tra gli elementi di \mathcal{A}^C e quindi verifica la congettura IC.

La congettura Union-Closed

La congettura rimane non dimostrata in generale, ma è invece stata dimostrata per diversi casi speciali, tra i quali

- Quando $|U| \leq 12$ oppure $|\mathcal{A}| \leq 50$
- Se la cardinalità di \mathcal{A} è grande rispetto alla cardinalità di $|U|$ ovvero $|\mathcal{A}| \geq \frac{2}{3}2^{|U|}$. Ricordiamo che essendo $\mathcal{A} \subseteq \text{pow}(U)$ abbiamo che $|\mathcal{A}| \leq |\text{pow}(U)| = 2^{|U|}$.
- Se la cardinalità di \mathcal{A} è piccola rispetto alla cardinalità di $|U|$ ovvero $|\mathcal{A}| \leq 2|U|$.
- Se \mathcal{A} contiene un insieme di cardinalità 1 oppure di cardinalità 2.

La congettura Union-Closed

Dimostriamo il seguente

Teorema

Se \mathcal{A} contiene un insieme di cardinalità 1, $\{x\}$, allora l'elemento x verifica la congettura.

Dimostrazione

Partizioniamo \mathcal{A} in 2 sottoclassi (sottoinsiemi): $\mathcal{A}_x = \{A \in \mathcal{A} : x \in A\}$ e $\mathcal{A}'_x = \mathcal{A} \setminus \mathcal{A}_x$. Consideriamo la seguente funzione

$f : \mathcal{A}'_x \rightarrow \mathcal{A}_x$ definita come $f(A) = A \cup \{x\}$, per ogni $A \in \mathcal{A}'_x$

Dal momento che \mathcal{A} è chiuso rispetto all'unione, la funzione è ben definita e dal momento che è iniettiva ne deduciamo che

$$|\mathcal{A}'_x| \leq |\mathcal{A}_x|$$

e il teorema è dimostrato.



La congettura Union-Closed

Dimostriamo adesso il seguente

Teorema

Se \mathcal{A} contiene un insieme di cardinalità 2, $\{a, b\}$, allora almeno uno dei 2 elementi a, b verifica la congettura.

Dimostrazione

Partizioniamo \mathcal{A} in 4 sottoclassi:

- $\mathcal{A}_0 = \{A \in \mathcal{A} : a \notin A, b \notin A\},$
- $\mathcal{A}_1 = \{A \in \mathcal{A} : a \in A, b \notin A\}$
- $\mathcal{A}_2 = \{A \in \mathcal{A} : a \notin A, b \in A\},$
- $\mathcal{A}_3 = \{A \in \mathcal{A} : a \in A, b \in A\}$

Dal momento che $\{a, b\} \in \mathcal{A}$ la seguente funzione iniettiva

$$f : \mathcal{A}_0 \rightarrow \mathcal{A}_3 \text{ definita come } f(A) = A \cup \{a, b\}, \text{ per ogni } A \in \mathcal{A}_0$$

ci dice che $|\mathcal{A}_0| \leq |\mathcal{A}_3|$.

Cont.

△

Dimostrazione cont.

Dimostrazione cont.

Supponiamo, per assurdo, che né a né b verifichino la congettura. Allora avremmo

$$|\mathcal{A}_1| + |\mathcal{A}_3| < |\mathcal{A}_0| + |\mathcal{A}_2|$$

$$|\mathcal{A}_2| + |\mathcal{A}_3| < |\mathcal{A}_0| + |\mathcal{A}_1|$$

Sommando membro a membro le due disequazioni, otteniamo

$$|\mathcal{A}_1| + |\mathcal{A}_2| + 2|\mathcal{A}_3| < |\mathcal{A}_1| + |\mathcal{A}_2| + 2|\mathcal{A}_0|$$

da cui

$$|\mathcal{A}_3| < |\mathcal{A}_0|$$

che ci porta ad una contraddizione. Quindi, il teorema è dimostrato.

△

La congettura Union-Closed

Purtroppo, se \mathcal{A} contiene un insieme di cardinalità 3, non vale alcun teorema simile. Infatti, ecco un controesempio con $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(C3) $A_1 = \{1, 2, 3\}$

(C5) $A_2 = \{4, 5, 6, 7, 8\}, A_3 = \{4, 5, 6, 7, 9\}, A_4 = \{4, 5, 6, 8, 9\}, A_5 = \{4, 5, 7, 8, 9\},$
 $A_6 = \{4, 6, 7, 8, 9\}, A_7 = \{5, 6, 7, 8, 9\}$

(C6) $A_8 = \{4, 5, 6, 7, 8, 9\}, A_9 = \{1, 5, 6, 7, 8, 9\}, A_{10} = \{1, 4, 6, 7, 8, 9\},$
 $A_{11} = \{2, 4, 5, 7, 8, 9\}, A_{12} = \{2, 4, 5, 6, 8, 9\}, A_{13} = \{3, 4, 5, 6, 7, 9\},$
 $A_{14} = \{3, 4, 5, 6, 7, 8\}$

(C7) $A_{15} = \{1, 4, 5, 6, 7, 8, 9\}, A_{16} = \{2, 4, 5, 6, 7, 8, 9\}, A_{17} = \{3, 4, 5, 6, 7, 8, 9\}$

(C8) $A_{18} = \{1, 2, 3, 4, 5, 6, 7, 8\}, A_{19} = \{1, 2, 3, 4, 5, 6, 7, 9\},$
 $A_{20} = \{1, 2, 3, 4, 5, 6, 8, 9\}, A_{21} = \{1, 2, 3, 4, 5, 7, 8, 9\},$
 $A_{22} = \{1, 2, 3, 4, 6, 7, 8, 9\}, A_{23} = \{1, 2, 3, 5, 6, 7, 8, 9\},$
 $A_{24} = \{1, 2, 4, 5, 6, 7, 8, 9\}, A_{25} = \{1, 3, 4, 5, 6, 7, 8, 9\},$
 $A_{26} = \{2, 3, 4, 5, 6, 7, 8, 9\}$

(C9) $A_{27} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Gli elementi 1, 2, 3 appartengono solo a 13 dei 27 insiemi.

Chiusura: Esercizi

Sia $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Per ognuna delle seguenti famiglie, di cui abbiamo precedentemente trovato la chiusura rispetto all'unione, verificare la congettura.

- 1 $\mathcal{A} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8\}, \{9, 10\}, \{1, 4, 5\}, \{2, 6, 8\}, \{3, 5\}, \{1, 10\}\}$
- 2 $\mathcal{A} = \{\{1, 2\}, \{1, 3, 4\}, \{4, 5, 6\}, \{6, 7, 8\}, \{8, 9, 10\}, \{5, 8, 9\}\}$
- 3 $\mathcal{A} = \{\{1, 2\}, \{2, 3, 4\}, \{4, 5\}, \{5, 6\}, \{3, 8, 9\}, \{6, 9\}, \{7, 8\}, \{7, 10\}\}$

FINE PRIMA PARTE

INSIEMI e RELAZIONI