Metodi matematici per l'informatica

Corso del professore Carlucci
https://sites.google.com/uniroma1.it/mmi2223/home

Lugini Andrea

February 3, 2023

Contents

0.1 Tecniche di conteggio: Matematica combinatoria

La matematica combinatoria è la branca della matematica che si occupa dei problemi di conteggio.
Ad esempio il problema del numero di targe automobilistiche disponibili al mondo ricade in questo ambito.

0.1.1 Principio Moltiplicativo

Se scelgo un primo oggetto fra m_1, un secondo oggetto tra m_2, ..., un t-esimo oggetto fra m_t oggetti ho $m_1 \cdot m_2 \cdot ... \cdot m_t$ soluzioni.

0.1.2 Disposizioni

Le disposizioni sono sequenze nelle quali l'ordine conta.

Disposizioni con ripetizione di ordine k di n oggetti

$$D'_{n,k} = n^k$$

Disposizioni semplici di ordine k di n oggetti

$$C.E. = 1 \leq k \leq n$$

$$D_{n,k} = \frac{n!}{(n-k)!}$$

Nel caso $k = n$, parliamo di permutazioni e abbiamo: $P_n = n!$.

Permutazioni con ripetizioni

Presi n elementi, che si **ripetono rispettivamente** $k_1, ..., k_n$ volte, le possibili permutazioni sono:

$$P_n^{k_1,...,k_n} = \frac{n!}{k_1! \cdot ... \cdot k_n!}$$

Permutazioni di n oggetti con q vincoli

$$\frac{P_n}{q!}$$

0.1.3 Combinazioni

Le combinazioni sono sequenze nel quale l'ordine non conta

Combinazioni semplici

$$C_{n,k} = \frac{D_{n,k}}{P_k} = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Combinazioni con ripetizione

Risolvono il problema della **scritture additive** e della distribuzione di k oggetti identici tra n insiemi

$$C'_{n,k} = \binom{n+k-1}{k-1}$$

0.1.4 Proprietà del coefficiente binomiale

$$\binom{n}{k} = \binom{n}{n-k}$$

Dimostrazione per **doppio conteggio**: con $\binom{n}{k}$ scelgo k oggetti su n, lasciando fuori $n-k$ oggetti. E' quindi equivalente scegliere gli $n-k$ oggetti da lasciare fuori, ovvero $\binom{n}{n-k}$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Dimostrazione per **partizioni**: dato un insieme N di cardinalità n nel quale vogliamo scegliere k oggetti sappiamo che il numero di possibili soluzioni sono $\binom{n}{k}$. Se vogliamo inserire vincoli specifici di scelta, ovvero scegliere k oggetti, tra i quali un oggetto x, nell'insieme n, la totalità dei sottoinsiemi che contengono x è data dalla scelta fissa $x\cdot$ le **combinazioni** dei restanti $k-1$ oggetti fra $n-1$ elementi, ovvero $\binom{n-1}{k-1}$. Se invece vogliamo vedere il problema al contrario, ovvero scegliere k oggetti, tra i quali **non vogliamo x**, dobbiamo scegliere k oggetti su $n-1$ elementi, quindi $\binom{n-1}{k}$. Per partizione abbiamo quindi che la totalità delle scelte è data dall'unione delle scelte che includono x e quelle che non includono x, insiemi **disgiunti**, è quindi è dimostrata la formula.

$$\binom{n}{m} \cdot \binom{m}{k} = \binom{n}{k} \cdot \binom{n-k}{m-k}$$

Dimostrazione per **doppio conteggio**: il primo termine a sinistra sveglie m oggetti su n elementi, e il secondo mi fa scegliere k oggetti fra gli m scelti prima. A destra scegliamo k oggetti su n, e poi scegliamo $m-k$ oggetti sui restanti $n-k$.
Esempio:
Vogliamo fare una squadra di calcio con 3 portieri e 10 giocatori di movimento, scegliendo fra 30 bambini.
A sinistra scegliamo prima i 13 bambini che giocheranno a calcio e poi sceglieremo i 3 fra questi 13 che faranno i portieri.
A destra invece scegliamo prima i 3 portieri fra i 30 bambini, e poi sceglieremo i 10 giocatori di movimento fra i restanti 30 tolti i 3 portieri bambini.

0.1.5 Principio additivo

Il principio additivo ci permette di risolvere un problema di conteggio **sommando le numerosità** di n sottoinsiemi, detti **partizioni** dell'insieme da contare, se e solo se i sottoinsieme suddividono la collezione in gruppi **esclusivi ed esaustivi**. E' esprimibile come:

$$\forall i \in \{1, ..., n\} : A_i \subseteq A \wedge$$

$$\forall i, j \in \{1, ..., n\} \text{ con } i \neq j : A_i \cap A_j = \emptyset \wedge$$

$$\forall a \in A : \exists i \in \{1, ..., n\} \text{ t.c. } a \in A_i$$

$$\implies \#A = \Sigma_{i=1}^{n} \#A_i$$

Metodo inverso

Il principio additivo ci permette di dimostrare il metodo inverso.
Infatti, preso un sottoinsieme A di T ed il suo complementare $\overline{A}$ in T, definito come $\forall x \in T$ t.c. $x \notin A$, per i quali valgono quindi le proprietà $A \cup \overline{A} = T$ e $A \cap \overline{A} = \emptyset$, è dimostrato quindi il principio additivo, che ci permette di calcolare $\#T$ come $\#A + \#\overline{A}$, che implica

$$\#A = \#T - \#\overline{A}$$

.

0.1.6 Insieme potenza

$$P(A) = \{S | S \subseteq A\}$$

$$\#P(A) = \Sigma_{k=0}^{\#A} \binom{\#A}{k} = 2 \cdot \Sigma_{k=0}^{\#A/2} \binom{\#A}{k}$$

Dimostriamo ora per **buona traduzione** che $\#P(A) = 2^{\#A}$:
prendiamo due linguaggi, L_1, che rappresenta tutti $S \in P(A)$, ed L_2, che rappresenta tutte le possibili **stringhe binarie** di lunghezza $= \#A$; se costruiamo queste stringhe ponendo in posizione i 1 se $e \in S$ e 0 in caso contrario, possiamo notare che, poichè ogni $S \in P(A)$ è distinto, anche le corrispondenti stringhe saranno distinte.
Quindi, $\#P(A) =$ #stringhe binarie con l $= \#A$, ed è banale contare quante stringhe sono presenti in L_2: 2 possibili valori, 0 ed 1, per $\#A$ posizioni, ovvero $2^{\#A}$, esattamente quello che volevamo dimostrare.
Possiamo inoltre notare che $\binom{n}{k} =$ #stringhe binarie con l $= \#A$ con esattamente k "1".

0.1.7 PIE: Principio di inclusione ed esclusione

L'insieme Q dato da tutti gli elementi distinti degli insiemi A e B è esprimibile come $(A \cup B) \cap \overline{A \cap B}$.
Quindi:

$$\#(A \cup B) = \#A + \#B - \#(A \cap B)$$

Più genericamente,

$$\begin{gathered}\#(A \cup B \cup ... \cup Z) = \\ \#A + \#B + ... + \#Z \\ -\#(A \cap B) - \#(A \cap Z) - (B \cap Z) - ... \\ +\#(A \cap B \cap Z) + ...\end{gathered}$$

0.1.8 Metodo di riduzione

Il metodo di riduzione consiste nel trasformare un problema in un problema più semplice.

0.2 Funzioni

$$f : I \longrightarrow O$$

0.2.1 Definizione

Una funzione è una legge che, preso l'insieme di partenza I detto dominio, e l'insieme di arrivo O detto codominio, $\exists! y$ t.c. $y = f(x)$.

0.2.2 Immagine e pre-immagine

$y \in O$ t.c. $y = f(x \in I)$ è detta immagine di x via f.
$x \in I$ t.c. $y \in O = f(x)$ è detta pre-immagine di y via f

0.2.3 Definizione insiemistica

Presi I e O, $f : I \longrightarrow O \subseteq (I \cdot O)$ t.c. $\forall x \in I \exists! y \in O$ t.c. $(x, y) \in f$

0.2.4 Funzioni a più argomenti

Una funzione a più argomenti può essere vista come una funzione che ha

$$I = I_1 \cdot I_2 \cdot ...$$

ed e quindi formata da **n-tuple ordinate**.
La notazione usata in questo caso è:

$$f : I^n \longrightarrow O$$

0.2.5 Iniettività, Suriettività e Biettività

Iniettiva: $\forall x, y$ t.c. $x \neq y \Longrightarrow f(x) \neq f(y)$
Suriettiva: $\forall y \in O \exists x \in I$ t.c. $y = f(x)$
Biettiva: Iniettiva $\wedge$ suriettiva.

Proprietà dell'iniettiva

$$f : X \longrightarrow Y, f \text{ iniettiva } \Longrightarrow \exists g : Y \longrightarrow X \text{ t.c. } (g \circ f)(x) = x$$

La dimostrazione è alquanto semplice.
Se $y \in f(X) \Longrightarrow \exists! x \in X$ t.c. $f(x) = y$ in quanto f iniettiva.
Se invece $y \notin f(X)$ allora non ci interessa il comportamento di $g(y)$.

Implicazione dell'esistenza di g

$$\exists g : Y \longrightarrow X \, (g \circ f)(x) = x \Longrightarrow f \text{ iniettiva}$$

. Procediamo per assurdo, ipotizzando che f non sia iniettiva.
Allora esisterebbero due valori $x_0, x_1 \in X, x_0 \neq x_1$ t.c. $f(x_0) = f(x_1)$. Sappiamo inoltre che $(g \circ f)(x_0) = x_0$ e $(g \circ f)(x_1) = x_1$. In quanto g l'inversa di f e $f(x_0) = f(x_1)$ allora

$$(g \circ f)(x_0) = (g \circ f)(x_1) \Longrightarrow x_0 = x_1$$

Situazione impossibile per ipotesi.

Corollario

$$f \text{ iniettiva} \iff \exists g \text{ t.c. } (g \circ f)(x) = x$$

Proprietà della suriettività

$$f : X \longrightarrow Y, f \text{ suriettiva} \implies \exists g : Y \longrightarrow X \text{ t.c. } (f \circ g)(y) = y$$

Anche qui la dimostrazione è alquanto banale.
Infatti, prendendo un qualunque $y \in Y$ basta prendere x t.c. $f(x) = y$, la cui esistenza è garantita dalla suriettività di f.
Potrebbero esserci diverse $x \in X$ che soddisfano questa relazione, ma non è importanti quali scegliamo.

Implicazione dell'esistenza di g

$$\exists g : Y \longrightarrow X \text{ t.c. } (f \circ g)(y) = y \Longrightarrow f \text{ suriettiva}$$

Procediamo per assurdo, ipotizzando che f non sia suriettiva. Questo implica che $\exists y \in Y$ t.c. $\nexists x \in X$ t.c. $y = f(x)$. Però per ipotesi $f(g(y)) = y \Longrightarrow \exists x \in X$ t.c. $y = f(x)$, in contraddizione con quanto definito prima.

Corollario

$$f \text{ suriettiva} \iff \exists g \text{ t.c. } (f \circ g)(x) = x$$

0.2.6 Proprietà insiemistiche delle funzioni

Presi $A, B \subseteq I$:

$$f \text{ iniettiva} \implies f(A \cap B) = f(A) \cap f(B)$$

$$f(A \cup B) = f(A) \cup f(B)$$

0.2.7 Composizione di funzioni

Prese $f : X \longrightarrow Y$ e $g : Y \longrightarrow Z$, $g \circ f = h : X \longrightarrow Z$ **definita come** $h(x) = g(f(x))$
La composizione di funzione **non è commutativa** ma è **associativa**

0.2.8 Iniettività, Suriettività e Biettività

La composizione di 2 funzioni iniettive/suriettive/biettive è iniettiva/suriettiva/biettiva.

0.2.9 Funzione inversa

La funzione inversa f^{-1} è quella funzione per il quale vale:

$$x = I(x) = \begin{Bmatrix} \left(f^{-1} \circ f\right)(x) \\ \left(f \circ f^{-1}\right)(x) \end{Bmatrix}$$

$$f : X \longrightarrow Y$$

$$f^{-1} : Y \longrightarrow X$$

Per i corollari definiti nella sezione su iniettiva e suriettiva, la prima condizione implica che f sia iniettiva, mentre la seconda implica che f sia suriettiva. E di conseguenza implicato che

$$\exists f^{-1} \Longleftrightarrow f \text{ biettiva}$$

0.2.10 Immagine inversa

$$f : X \longrightarrow Y,\ A \subseteq Y \Longrightarrow$$

$$\exists f^{-1} : Y \longrightarrow \mathcal{P}(X) \text{ t.c. } \forall a \in A\, f(a) = \{x \in X : f(x) = a\}$$

La pre-immagine non implica l'esistenza della funzione inversa.
Basti pensare ad una funzione f non iniettiva. Possiamo comunque definire le pre-immagini degli elementi del suo dominio, ma non una funzione inversa in quanto f non è biettiva.

0.3 Cardinalità degli insiemi

0.3.1 Relazione

Presi due insiemi finiti A, B, se $\exists f$:

- **iniettiva** $\implies \#A \leq \#B$
- **suriezione** $\implies \#A \geq \#B$
- **biezione** $\implies \#A = \#B$

Nell'ultimo caso si parla di **equicardinalità**, proprietà **riflessiva, simmetrica, transitiva**

0.3.2 Definizione insiemistica insieme N

Metodo usato da Peano per definire N:

- **0**: classe degli insiemi in biezione con $A = \emptyset$
- **1**: classe degli insiemi in biezione con $A = \{\emptyset\}$
- **2**: Classe degli insiemi in biezione con $A = \{\emptyset, \{\emptyset\}\}$
- **...**: ...

0.3.3 Teorema di Cantor-Bernstein-Schroder

$$\exists f \text{ iniettiva } A \longrightarrow B \wedge \exists g \text{ iniettiva } B \longrightarrow A \implies \#A = \#B$$

Dimostrazione

La dimostrazione a parole è abbastanza semplice, in quanto l'iniettività da A a B implica che $\#B \geq \#A$, e l'iniettività da B ad A implica che $\#A \geq \#B$, e di conseguenza $\#A = \#B$

Corollario I

$$\#A \leq \#B \iff \exists \text{ iniezione } f : A \longrightarrow B$$

Corollario II

$$\#A < \#B \iff \exists \text{ iniezione } f : A \longrightarrow B \wedge \nexists \text{ iniezione } g : B \longrightarrow A$$

0.3.4 Teorema di Cantor

$$\#A < \#\mathcal{P}(A)$$

Dimostrazione

Ipotizziamo che esista una suriezione $f : A \to \mathcal{P}(A)$, quindi deve esistere un $x \in A$ t.c. $f(x) = B$, con

$$B = \{\forall a \in A \text{ t.c. } a \notin f(a)\}$$

Per tale costruzione, possiamo dire che $x \in B \vee x \notin B$
Ora abbiamo 2 situazioni:

- $x \in B \Longrightarrow x \in f(x) \Longrightarrow x \notin B \Longrightarrow$ contraddizione
- $x \notin B \Longrightarrow x \notin f(x) \Longrightarrow x \in B \Longrightarrow$ contraddizione

f non può essere quindi suriettiva, di conseguenza $\#\mathcal{P}(A) > \#A$.

0.3.5 Insiemi infiniti numerabili

Un insieme **infinito numerabile** è un insieme in **biezione** con **N**
Alcuni esempi di insiemi infiniti numerabili sono l'insieme **Q**, l'insieme $\forall n \geq 0, N^n$.

Dimostrazione della numerabilità di Z

Definiamo $f : N \longrightarrow Z$ biettiva, dove R è la funzione resto.

$$f(n) = \left[\lfloor \frac{n}{2} \rfloor + \frac{1-(-1)^n}{2}\right] \cdot (-1)^{n+1}$$

Possiamo facilmente vedere che Z è:

- iniettiva: ad ogni valore $n \in \mathbf{N}$ viene associato un valore in Z
- suriettiva: rimossi gli elementi 0, ad ogni coppia $n, n+1$ con $n = 2x$ sono associati $\lceil \frac{n}{2} \rceil, -\frac{n}{2}$.

Dimostrazione della numerabilità di $N \cdot N$

$$\begin{array}{cccc} (1,3) & (2,3) & (3,3) & ... \\ (1,2) & (2,2) & (3,2) & ... \\ (1,1) & (2,1) & (3,1) & ... \end{array}$$

Ora percorriamo la matrice ottenuta nel seguente modo:

- Prima diagonale: $(1,1)$
- Seconda diagonale: $(1,2), (2,2)$
- ... diagonale: ....

Possiamo notare come ogni elemento venga iterato una ed una sola volta.
Un alto modo per dimostrare che esiste una relazione biettiva è

$$f(h,m) = h_0 m_0 h_1 m_1 ...$$

Questa relazione associa ad ogni coppia (h,m) un numero $x \in \{n > 10, \forall n \in N\}$.
Ma poichè possiamo facilmente dimostrare che $\{n > 10, \forall n \in N\}$ è un insieme infinito numerabile, ne deduciamo che lo è anche $N \cdot N$.
Questa dimostrazione può essere estesa per ogni $N^n, \forall n > 1 \in N$.

Proprietà

Presi A insieme numerabile, B insieme finito o numerabile, $A \cup B$ è sempre numerabile.
Ogni sottoinsieme di un insieme numerabile è a sua volta numerabile.

0.3.6 Insiemi infiniti non numerabili

Sequenze binarie infinite

Prendiamo l'insieme SBI, fatto da sequenze di 0 ed 1 infinite, e ipotizziamo che sia enumerabile. Prendiamo ora una qualuque diagonale che contiene un carattere di ognuna di queste stringhe, e ora invertiamo gli 1 con gli 0.
Ci accorgiamo che è una stringa dove il bit in posizione k è "flippato" rispetto al bit in posizione k della stringa k. Di conseguenza è una stringa che ha almeno un carattere diverso da ogni altra stringa, e che quindi non fa parte delle stringhe "contate".
L'insieme è quindi non enumerabile.

Argomento diagonale di Cantor

La dimostrazione usata per le SBI è detta **argomento diagonale di Cantor**, che il matematico usò per dimostrare che l'insieme dei numeri **I** non è enumerabile (a rendere questo insieme non enumerabile sono in realtà gli irrazionali trascendentali, in quanto gli irrazionali algebrici sono per definizione in biezione con **N**)

0.3.7 Cardinalità del continuo

Un insieme ha **cardinalità del continuo** se è in biezione con **R**.

Insieme potenza

Per il principio della buona traduzione, sappiamo che preso un insieme A con $\#A = n$ esiste una relazione di biezione tra i sottoinsiemi di A e le stringhe binarie di lunghezza n.

Questo è applicabile per qualsiasi sottoinsieme di $\mathbf{N}$, che può essere anche infinito, che viene associato ad una stringa detta **sequenza caratteristica**.
Di conseguenza abbiamo che

$$\forall S \subseteq \mathbf{N}\ \exists! SB(S) \iff \#SBI = \#\mathcal{P}(N)$$

dove $\mathcal{P}$ è l'insieme potenza (l'insieme di tutti i sottoinsiemi)

$$\implies \exists h \text{ biettiva } A \longrightarrow B$$

Insiemi equicardinali di R

$$\#\mathbf{R} = \#\mathcal{P}(N) = \#SBI$$

Dimostriamolo:
poichè sappiamo che $\#\mathbf{R} = \#[0,1) \implies (\#\mathcal{P}(N) = \#[0,1) \implies \#\mathcal{P}(N) = \#\mathbf{R})$.
Definiamo ora due iniezioni fra $[0,1)$ e $\mathcal{P}(N)$. La prima, f, è definita così: prendiamo la forma decimale espansa di $r \in [0,1)$, e costruiamo il sottinsieme $S \in \mathcal{P}(N)$ come

$$r = 0.d_1d_2d_3... \to S = \{10 \cdot d_1, 10^2 \cdot d_2, 10^3 \cdot d_3, ...\}$$

.
Possiamo facilmente definire l'iniezione g che funziona al contrario: preso il sottoinsieme $S \in \mathcal{P}(N)$, definiamo

$$S = \{d_1, d_2, d_3, ...\} \to r = 0.d_1d_2d_3...$$

Per il teorema di CBS $\#\mathbf{R} = \#\mathcal{P}(N)$

0.3.8 Numeri transfiniti

Sono numeri usati per indicare la **cardinalità di un insieme infinito**, e non condividono le proprietà degli altri numeri.

- $\aleph_0 = \#\mathbf{N}$
- $\aleph_1 = \#\mathcal{P}(N)$
- ...

0.4 Relazioni

Presi due insiemi A, B, una relazione R fra A, B è un sottoinsieme $S \subseteq A \cdot B$.
Osserviamo che:

- Può $\exists a \in A$ t.c. $\#R(a) \in [0, +\infty)$.
  Questa proprietà esprime la differenza fra relazione e funzione.
- Può esistere $R = (A, A)$, detta **relazione binaria**
- Ogni R può essere visto come una relazione su un solo insieme.
  Infatti $R(A, B) \implies R(A \cup B)$

0.4.1 Metodi di rappresentazione

Grafi diretti

Rappresetazione che collega tramite archi gli elementi $a \in A$ agli elementi $b \in B \iff (a, b) \in R(A, B)$
Nel caso si tratti di una relazione su un solo insieme possiamo rappresentare una sola volta gli elementi di A e collegare gli elementi $a_0, a_1 \in A \iff (a_0, a_1) \in R(A)$

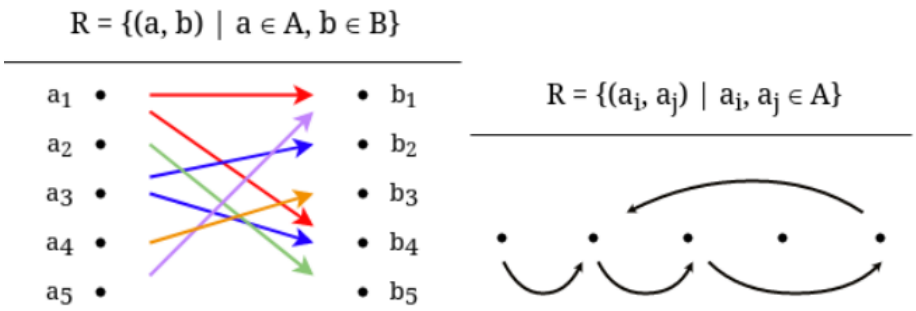

Figure 1: Dx: Bigrafo, Sx: Digrafo

Matrice binaria

Definiamo una matrice M_R dove

$$M_{i,j} = \begin{cases} 1 & (a_i, b_j) \in R(A, B) \\ 0 & (a_i, b_j) \notin R(A, B) \end{cases}$$

0.4.2 Relazione inversa

Data una relazione, **esiste sempre** l'inversa

$$R^{-1} = \{(b,a) \forall (a,b) \in R\}$$

Quando $R^{-1} = R$ si parla di **relazione simmetrica**.

$$R\,(A,B) \;\textbf{simmetrica} \iff (a,b) = (b,a)$$

Corrispondenza con la trasposizione

Questa operazione corrisponde con la trasposizione della matrice M_R

$$M_{R^{-1}} = {M_R}^T$$

Possiamo inoltre facilmente dedurre che

$$R \text{ simmetrica} \iff M_{R^{-1}} = M_R$$

0.4.3 Composizione di relazioni

$$R \subseteq A \cdot B, S \subseteq B \cdot C \implies R \circ S = (a,c) \iff \exists\,(a,b) \wedge \exists\,(b,c)$$

Nei casi di $R \circ R$ parliamo di **iterazione**

Composizione di relazioni come prodotto fra matrici

$$M_{R,S} = M_R \cdot M_S$$

Dove si usano la somma ed il prodotto booleano

Associatività

$$R \circ (S \circ D) = (R \circ S) \circ D$$

In quanto la moltiplicazione fra matrici è associativa, possiamo dedurre che lo è anche la composizione di relazioni in quanto operazioni equivalenti

Commutatività

$$R \circ S \circ D \neq R \circ D \circ S$$

Come prima, possiamo dedurlo dal fatto che il prodotto fra matrici non è commutativo

0.4.4 Relazioni transitive

$$R \subseteq A \cdot A \text{ transitiva} \iff$$

$$(\forall a,b,c \in A,\; aRb \wedge bRc \implies aRc)$$

Chiusura transitiva

E' detta **chiusura transitiva** di R **la più piccola relazione transitiva** R^T tale che:

$$R \subseteq R^T \wedge R^T \text{ transitiva } \wedge R \subseteq S, \big(\text{S transitiva} \Longrightarrow R^T \subseteq S\big)$$

Cammino

$$R \subseteq A \cdot A, \exists x_0, x_1, ... \text{ t.c. } aRx_0Rx_1R...Rb$$
$$\Longleftrightarrow \exists \text{ cammino } a \to b \text{ di lunghezza } l \geq 1$$

0.4.5 Relazione di equivalenza

- Riflessiva: $\forall a \in A \, \exists aRa$
- Simmetrica: $\forall a, b \in A, \, aRb \Longrightarrow bRa$
- Transitiva: $\forall a, b, c \in A, \, aRb \wedge bRc \Longrightarrow aRc$

Classi di equivalenza

Preso $a \in A$, possiamo definire l'insieme

$$[a]_R = \{b \in A \mid aRb\}$$

. Questo insieme è detto **classe di equivalenza** Possiamo inoltre dire che:

- per la riflessività, $\forall a \in A \, [a]_R \neq \emptyset$
- per la simmetria e la transitività, $\forall a, b \in A \, [a]_R \cap [b]_R = \emptyset \vee [a]_R = [b]_R$

Partizioni

Una partizione di un insieme A è la famiglia $\{C_i \mid i \in I\}$ tali che

- $C_i \subseteq A$
- $C_i \neq \emptyset$
- $\forall a \in A \exists i \in I \text{ t.c. } a \in C_i$
- $\forall i, j \in I, i \neq j \Longrightarrow C_i \cap C_j = \emptyset$
- $\bigcup_{i \in I} C_i = A$

Possiamo quindi dire che

$\{C_i \mid i \in I\}$ partizione $A, R(A), (aRb \Longleftrightarrow \exists i \in I \text{ t.c. } a, b \in C_i) \Longrightarrow R(A)$ relazione di equivalenza

0.4.6 Relazioni d'ordine

Relazione binaria che gode di alcune proprietà della relazione $\leq$ ($\mathbf{N}$)

Relazione d'ordine totale

- Riflessiva: $\forall a \in A \, \exists aRa$
- Anti-simmetrica: $\forall a, b \in A$, $aRb \wedge bRa \Longrightarrow a = b$
- Transitiva: $\forall a, b, c \in A$, $aRb \wedge bRc \Longrightarrow aRc$
- Totale: $\forall a, b \in A, a \leq b \vee b \leq a$. Se questa proprietà non sussiste si parla di **ordine parziale**

$\emptyset$ e una qualunque $R(\emptyset)$ sono relazioni d'ordine.

Cicli

$$\forall R(A) \text{ ordine } \Longrightarrow \text{ lunghezza massimo ciclo } = 1$$

Dimostrazione
Ipotizziamo per assurdo che esista un ciclo di lunghezza > 1, ovvero tale che

$$a_1 R a_2 R ... R a_1, \text{ t.c. } \forall i, j \, i \neq j \Longrightarrow a_i \neq a_j$$

Per transitività ripetuta abbiamo che $a_1 R a_i$, ma anche che $a_i R a_1, \forall i \neq 1$.
Per antisimmetria ciò implica che $a_i = a_1$, ovvero che tutti gli elementi del ciclo sono lo stesso elemento. Ne consegue che il ciclo si può ridurre a $a_1 R a_1$, di lunghezza 1.

Minimo e massimo di un ordine

$$a \in A \text{ t.c. } \forall b \in A \exists aRb / bRa \Longrightarrow a \text{ è minimo/massimo di } R(A)$$

Non è garantita l'esistenza di questi elementi.

Minimali e massimale di un ordine

E' detto **minimale** $a \in R(A)$ t.c. $\forall b \in A, b \neq a, \nexists bRa$.
Analogamente, è detto **massimale** $a \in R(A)$ t.c. $\forall b \in A, b \neq a, \nexists aRb$
Inoltre, $\forall R(A), A$ finito $\exists a \in A$ minimale $\wedge \exists b \in A$ massimale

Dimostrazione
Prendiamo il percorso P più lungo $a_1 R a_2 R ... R a_n$, dove a_1 minimale.
Se $\exists a \in A, a \notin P$, non può valere aRa_1, in quanto esisterebbe il percorso $aRa_1 R a_2 R ... R a_n$, di lunghezza maggiore di P, impossibile per ipotesi.
Se invece $\exists a \in A, a \in P$ ne consegue che esiste un ciclo in P, impossibile in quanto siamo in un ordine parziale.
Ne segue che a_1 è il minimale di $R(A)$

Immersioni tra ordini

Tutti gli ordini sono inclusioni insiemistiche, ovvero:

$$\begin{gathered}\leq (X) \text{ ordine parziale }, \leq^{*} (X^{*}) \text{ ordine parziale} \\ \Longrightarrow \exists f : X \to X^{*} \text{ iniettiva t.c. } (x \leq y \Longleftrightarrow f(x) \leq^{*} f(y))\end{gathered}$$

Immersione nell'insieme potenza

$$\exists \leq (X) \Longrightarrow \exists \text{ immersione } \subseteq (\mathcal{P}(X))$$

Dimostrazione
Definiamo

$$f : X \to \mathcal{P}(X), f(x) = \{z \in X \mid z \leq x\}$$

Verifichiamo l'iniettività per assurdo:

$$\begin{gathered}\forall x, y \in X, y \neq x, f(x) = f(y), x \leq x, y \leq y \\ \Longrightarrow x \in f(x) \wedge y \in f(y) \Longrightarrow x \in f(y) \wedge y \in f(x) \\ \Longrightarrow x \leq y \wedge y \leq x \Longrightarrow y = x \text{ per anti-simmetria} \\ \Longrightarrow \text{ contraddizione}\end{gathered}$$

Verifichiamo che $x \leq y \Longrightarrow f(x) \subseteq f(y)$:

$$\begin{gathered}x = y \Longrightarrow f(x) = f(y) \Longrightarrow f(x) \subseteq f(y) \\ x < y \Longrightarrow x \in f(y), y \notin f(x) \\ \text{Inoltre, per transitività } \forall z \in f(x), z \leq x < y \Longrightarrow z < y \Longrightarrow z \in f(y) \\ \Longrightarrow \forall z \in f(x), z \in f(y) \wedge x \in f(y) \wedge y \notin f(x) \\ \Longrightarrow f(x) \subset f(y)\end{gathered}$$

Verifichiamo anche l'implicazione opposta:

$$x \in f(x), f(x) \subseteq f(y) \Longrightarrow x \in f(y) \Longrightarrow x \leq y$$

Estensioni totali di ordini parziali

$$\begin{gathered}A = \{a_1, ..., a_n\}, R(A) \text{ ordine parziale } \Longrightarrow \\ \exists R^{*}(A) \text{ ordine totale t.c. } R \subseteq R^{*} \\ \Downarrow \\ \forall a, b \in A, R(A) \text{ ordine parziale}, \nexists aRb \\ \Longrightarrow \exists R^{'}(A) \supseteq R \text{ t.c. } \exists aR^{'}b\end{gathered}$$

Dimostrazione per casi

$(a,b) \in A \times A$, $X = \{x \in A \mid xRa\}(x \leq a)$, $Y = \{y \in A \mid bRx\}(x \geq b)$
$R^{'} = R \cup (X \times Y)$
$\nexists aRb \Longrightarrow \nexists x \in X$ t.c. $xRa \wedge bRx \Longrightarrow X \cap Y = \emptyset$

R riflessiva $\Longrightarrow R^{'}$ riflessiva

Dimostriamo l'antisimmetria:
Ipotizziamo $\forall x \in X, y \in Y \; \exists xR^{'}y \wedge \exists yR^{'}x$
$\Longrightarrow (xRy \vee (x,y) \in X \times Y) \wedge (yRx \vee (y,x) \in X \times Y)$
Ne consegue per casi:
$(x,y), (y,x) \Longrightarrow x \in X \cap Y \Longrightarrow$ impossibile
$(x,y), yRx \Longrightarrow xRa \Longrightarrow yRa \Longrightarrow y \in X \Longrightarrow y \in X \cap Y \Longrightarrow$ impossibile
$xRy, (y,x) \Longrightarrow bRx \Longrightarrow bRy \Longrightarrow y \in Y \Longrightarrow y \in X \cap Y \Longrightarrow$ impossibile
$xRy, yRx \Longrightarrow y = x$ per antisimmetria

Dimostriamo la transitività:
Ipotizziamo $\forall x, y, z \in X, \exists xR^{'}y \wedge \exists yR^{'}z$
$\Longrightarrow (xRy \vee (x,y) \in X \times Y) \wedge (yRz \vee (y,z) \in X \times Y)$
Ne consegue per casi:
$(x,y), (y,z) \Longrightarrow y \in X \wedge y \in Y \Longrightarrow y \in X \cap Y \Longleftrightarrow$ impossibile
$(x,y), yRz \Longrightarrow y \in Y \Longrightarrow bRy \Longrightarrow bRz \Longrightarrow z \in Y \Longrightarrow (x,z) \in X \times Y \Longrightarrow xR^{'}z$
$xRy, (y,z) \Longrightarrow y \in X \Longrightarrow \exists yRa \Longrightarrow xRa \Longrightarrow x \in X \Longrightarrow (x,z) \in X \times Y \Longrightarrow xR^{'}z$
$xRy, yRz \Longrightarrow xRz \Longrightarrow xR^{'}z$

Dimostrazione per induzione
Consideriamo il problema nel caso $A = a$. Banale il fatto che R parziale sia anche totale.
Consideriamo ora un generico caso $A = a_1, ..., a_n$, dove abbiamo che $\exists a, b \in A$ t.c. $\nexists aRb \wedge \nexists bRa$.
Sappiamo che $\exists a \in A$ minimale di R, ed escludiamolo da A. Nell'insieme $R(A \backslash \{a\})$ abbiamo due casi:

- $R(A \backslash \{a\})$ totale: basta definire un nuovo ordine

$$R_T = R(A \backslash \{a\}) \cup \{aRx \, \forall x \in R(A \backslash \{a\})\}$$

- $R(A \backslash \{a\})$ parziale: ripetiamo lo stesso procedimento definito sopra finchè non trovaimo un $R(A \backslash \{a_{i_1}, ..., a_{i_n}\})$ totale.
  Sappiamo che suddetto caso esiste in quanto al limite si arriva a un caso dove $A = a$ che sappiamo essere totale.

Di conseguenza, per un qualunque n sappiamo risolvere il caso $n-1$, ed avendo risolto $n-1$ sappiamo risolvere n

Sottosuccessioni

$$A, \exists S_A \iff \exists j \in [i, i + \#S] \text{ t.c. } S_{j-i} = A_j \, \forall j$$

Sottosuccessioni monotone ed ordini totali

$\forall n \geq 1$, $A = \{a_1, ..., a_{n^2+1}\}$ t.c. $R(A)$ ordine totale $\implies \exists S_A = \{a_i, ..., a_{i+n+1}\}$ monotona

Dimostrazione
Ipotizziamo per assurdo che questa successione non esista.
Consideriamo $f : \left[1, n^2 + 1\right] [1, n], f(x) = \ell_{\max} S_A = \{a_i, ..., a_x\}$ monotona
Dato che $\frac{n^2+1}{n} = n$ resto $1 \implies \exists \{i_1 < ... < i_{n+1}\}$ t.c. $f(i_1) = ... = f(i_{n+1}) = l$
Consideriamo quindi gli elementi $a_{i_1}, ..., a_{i_{n+1}}$ che sappiamo avere lo stesso $\ell_{\max}$.
Preso una qualunque coppia adiacente $a_{i_k}, a_{i_{k+1}}$, abbiamo due casi:

- $a_{i_k} < a_{i_{k+1}} \implies S_{A_{a_{i_k}}} = \{S_{A_{a_{i_k}}} < a_{i_{k+1}}\} \implies k < (k+1) \implies$ impossibile
- $a_{i_k} > a_{i_{k+1}}$

Ne consegue che

$\forall k \in [1, n+1) \implies a_{i_k} > a_{i_{k+1}} \implies \exists S^* = \{x_{i_1} > ... > x_{i_{n+1}}\} \implies \#S^* = n+1 \implies$ contraddizione

Ergo l'ipotesi è falsa

0.5 Induzione

L'idea base del principio di induzione è dimostrare che

$$P(n) \forall n \in X \subseteq \mathbf{N}$$

E' composta da due parti fondamentali:

- **Caso base**: dimostrare che $\exists n_0 \in N$ t.c. $P(n)$ Solitamente $n_0 = 0$ o 1
- **Passo induttivo**: dimostrare che $\forall n \in N, n \geq n_0, P(n) \implies P(n+1)$. L'ipotesi $P(n)$ è detta **ipotesi induttiva**

0.5.1 Principio di Induzione: versione insiemistica

$X \subseteq \mathbf{N}$
$n_0 \in X$
$\forall n \in \mathbf{N}, n \geq n_0, n \in X \implies n+1 \in X$

$$\implies \mathbf{N} - \{0, ..., n_0 - 1\} \subset X \implies X = \mathbf{N} - \{0, ..., n_0 - 1\}$$

0.5.2 Dimostrazione col Principio del Minimo Numero

Il principio del minimo numero ci dice che

$$\forall X \subseteq \mathbf{N}, X \neq \emptyset \implies \exists m \in X$$

Prendiamo le condizioni della versione insiemistica, ed ipotizziamo per assurdo che l'induzione insiemistica non sia valida, ovvero che

$$A = \mathbf{N} - \{0, ..., n_0 - 1\} - X, A \neq \emptyset$$

Per il principio del minimo numero $\exists m \in A > n_0$ in quanto $n_0 \in X$, ovvero $m - 1 \geq n_0$, e poichè è $m \in A \implies m - 1 \in X$, ma poichè $\forall n \geq n_0, n \in X \implies n+1 \in X$ allora $m - 1 \in X \implies m \in X$, in contraddizione col fatto che $m \notin X$. Ne segue che l'induzione insiemistica è vera.
La maggior parte delle dimostrazioni per PMN sono dimostrazioni per assurdo.

0.5.3 Mettere in evidenza il caso base

Il passaggio fondamentale nel processo di dimostrazione per induzione è mettere in evidenza il caso n, ovvero mostrare il caso n sia incluso nel caso $n+1$.

0.5.4 Principio di induzione forte

Il principio di induzione è una versione del principio di induzione dove nel passo induttivo, oltre a considerare $P(n)$ vero, sfruttiamo il fatto che $\forall x \in [n_0, n] P(n)$ vera

0.6 Logica proposizionale

Un linguaggio proposizionale è un insieme L di simboli contenente:

- **Connettiviti logici**: $\implies$, $\iff$, $\neg, \vee, \wedge$
- **Parentesi**: ()
- **Variabili proposizionali**: Insieme VAR_L di simboli diversi da connettivi e parentesi. Data una proposizione F, sono anche dette **parti atomiche** di F

L'insieme delle **proposizioni** (PROP_L) di L è il minimo insieme X di stringhe finite di simboli in L t.c.:

- $\mathrm{VAR}_L \subset X$
- $A \in X \implies \neg A \in X$
- $A, B \in X \implies A \vee / \wedge / \implies / \iff B \in X$

0.6.1 Connettivi logici nell'algebra booleana

- $\neg A = \overline{A}$
- $A \wedge B = A \cdot B$
- $A \vee B = A \vee B$
- $A \implies B = \overline{A \cdot \overline{B}}$
- $A \iff B = AB + \overline{A}\overline{B}$

Valgono di conseguenza le leggi e i metodi di rappresentazione dell'algebra booleana.

0.6.2 Sottoformule

$$A, B \in \mathrm{PROP}_L, B\text{sottostringa di } A \implies B \text{ sottoformula } A$$

0.6.3 Semantica della Logica proposizionale

Assegnamento

$$\alpha : \mathrm{VAR} \to \{0, 1\}$$

$0, 1$ sono detti **valori di verità**. Il concetto è estensibilie alle proposizioni, dove $\alpha\,(F)$, detta anche F sotto α, è l'insieme degli assegnamenti alle atomiche

Soddisfacibile, Insoddisfacibile e Tautologica

$$\exists \alpha \in A \text{ t.c. } \alpha(F) = 1 \iff F \in \text{ SAT}$$
$$\forall \alpha \in A, \alpha(F) = 1 \iff F \in \text{ TAUT}$$
$$\neg A \in \text{ TAUT} \iff A \in \text{ UNSAT}$$

Conseguenza logica

$$\forall \alpha \in A, [1 = \alpha(F_1) = ... = \alpha(F_n) \implies \alpha(F) = 1] \implies F_1, ..., F_n \models F$$

F è detta **conseguenza logica** di $F_1, ..., F_n$
Il contrario è

$$\exists \alpha \in A, [1 = \alpha(F_1) = ... = \alpha(F_n) \wedge \alpha(F) = 0] \implies F_1, ..., F_n \not\models F$$

Conseguenza logica come espressione booleana

$$\forall \alpha \in A, [F_1 \cdot ... \cdot F_n \cdot F] = 1 \implies F_1, ..., F_n \models F_1$$
$$\exists \alpha \in A, [F_1 \cdot ... \cdot F_n \cdot \neg F] = 1 \implies F_1, ..., F_n \not\models F_1$$

Conseguenza logica come UNSAT e TAUT

$$F_1, ..., F_n \models F \iff [F_1 \wedge ... \wedge F_n \implies F] \in \text{ TAUT} \iff [F_1 \wedge ... \wedge F_n \wedge F] \in \text{ UNSAT}$$

Forma Normale Congiunta

La **CNF**, sempre possibile, sarebbe un modo di scrivere la formula F nella forma

$$F = \bigwedge_{i=1}^{n} C_i = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{j_i}$$

Facile notare come sia la POS
La CNF è reinscrivibile in forma insiemistica come

$$\{\{l_{1_1}, ..., l_{1_m}\}, ..., \{l_{n_1}, l_{n_m}\}\}$$

Metodo di risoluzione

Il metodo di risoluzione è un modo per scoprire se F è Insoddisfacibile o meno.
Il metodo si basa sul fatto che, in una F in CNF:

$$\exists C_1, C_2 \in F \text{ t.c. } \exists l_1 \in C_1, l_2 \in C_2 \text{ t.c. } l_1 = \neg l_2$$

L'algoritmo è il seguente:

$$l_1 \in C_1, \neg l_1 \in C_2 \implies C_1, C_2 \models \text{RIS}(C_1, C_2) = C_1 \cup C_2 - \{l_1, \neg l_1\}$$

E' possibile quindi sostituire $C_1 \wedge C_2$ con la loro risoluzione.
Il processo finisce quando $\text{RIS}(C_1, C_2) = \{\} = \square$.
Dimostriamo ora che $\square \in F \iff F \in \text{UNSAT}$

Dimostrazione *"da sinistra"*
Facile notare come $\text{RIS}(C_1, C_2)$ si ottiene solamente quando $C_1 = \{p\} \wedge C_2 = \{\neg p\}$, ovvero $p \times \neg p$, che sappiamo essere un'espressione UNSAT

Dimostrazione *"da destra"*
Dimostriamolo per induzione:

- Caso base: $n = 0 \implies F = \{\square\} \vee F = \emptyset, F \in \text{ UNSAT} \implies F = \{\square\}$
- Passo Induttivo: Abbiamo due casi anche qui:
  Consideriamo i tre insiemi:

  $$F_p = \{C \in F \mid p \in C\}, F_{\neg p} = \{C \in F \mid \neg p \in C\}, F^- = F - F_p - F_{\neg p}$$

  $$\text{RIS}\left(F_p, F_{\neg p}\right) = \left(D = F_p - \{p\}\right) \cup \left(E = F_{\neg p} - \{\neg p\}\right)$$

  $R = D \cup E \cup F^-$ (questo processo è equivalente al metodo di risoluzione) $= F^- \times D \times E$

  Dimostriamo per assurdo che R è UNSAT:
  $\exists \alpha$ t.c. $\alpha\left(R\right) = 1 \implies \alpha\left(D \times E\right) = 1$. Definiamo $\alpha_1 = \alpha, \alpha\left(p\right) = 1$ e $\alpha_0 = \alpha, \alpha\left(p\right) = 0$

  - $\alpha_1\left(F\right) = 0 \implies \forall C_p \in F_p : \alpha_1\left(C_p\right) = 1 \implies \exists C_{\neg p} \in F_{\neg p} : \alpha_1\left(C_{\neg p}\right) = 0$
    In quanto possiamo ignorare $\neg p$ in quanto $= 0$, ne consegue che $\alpha_1\left(C_{\neg p} - \{\neg p\}\right) = 0 \implies \alpha\left(C_{\neg p} - \{\neg p\}\right) = 0$
    Quest'ultima osservazione implica per costruzione $\alpha\left(E\right) = 0$
  - Analogamente per α_0 e $C_p - \{p\}$. Concludiamo che $\alpha\left(D\right) = 0$

  $\alpha\left(D \times E\right) = 1 \implies \alpha\left(D\right) = 1$, contraddizione e di conseguenza cade l'argomento.
  Abbiamo quindi dimostrato che R è UNSAT, e quindi che $\square \in \text{RIS}\left(R\right)$, ottenuta applicando il metodo di risoluzione. Q.E.D