SAPIENZA
UNIVERSITÀ DI ROMA

UNIVERSITÀ "SAPIENZA" DI ROMA
FACOLTÀ DI INFORMATICA

Metodi Matematici per l'Informatica

Appunti integrati con il libro "Discrete Mathematics, an Open Introduction", Oscar Levin

Author
Simone Bianco

25 dicembre 2021

Indice

Capitolo 0

Introduzione

0.1 Cos'è la matematica discreta?

La **matematica discreta**, a volte chiamata matematica finita, è la branca della matematica che studia le **strutture matematiche discrete**, ossia strutture individualmente separate, dunque che non supportano o richiedono né il concetto di continuità né quello di densità. Al contrario dell'algebra o dell'analisi matematica, nella matematica discreta il concetto di intervallo non sussiste, poichè non comprende un *insieme discreto* di oggetti.

Per comprendere meglio ciò che viene trattato nell'ambito della matematica discreta, possiamo prendere in considerazione l'esempio più semplice di struttura discreta, ossia un **insieme finito** di valori interi: considerando l'ipotetica funzione matematica che restituisca il numero di penne possedute da chi sta leggendo questi appunti, potremmo dire che l'intervallo di valori sia 0, 1, 2, o addirittura anche 3. Tuttavia, una cosa è sicura: la quantità non sarà mai 1,32419 penne, poichè questo valore non è *discreto*.

Due tipici semplici problemi che possono essere affrontati con la matematica discreta sono i seguenti:

- Un ristorante offre un menù a scelta tra 5 primi piatti, 4 secondi piatti e 7 dessert. Considerando un pasto completo come menu formato da un primo, un secondo e un dessert, quanti pasti completi è possibile consumare?
- Una targa italiana di un'auto è costituita da 2 lettere, 3 cifre e 2 lettere. Quante targhe è possibile comporre?

Il concetto di matematica discreta, quindi, incapsula al suo interno un grande numero di argomenti. Gli argomenti principali che verranno affrontati in questo corso prevedono quattro concetti fondamentali: il **calcolo combinatorio**, le **sequenze**, la **logica simbolica** e la **teoria dei grafi**.

Capitolo 1

Calcolo combinatorio

1.1 Tecniche di conteggio

Alla base della matematica discreta vi sono degli importanti principi che definiscono il modo in cui è possibile contare grandi collezioni di oggetti in modo veloce e preciso.

Consideriamo il seguente problema elementare: in pasticceria ci sono 14 tipi di ciambelle e 16 tipi di muffin e Marco vuole comprare o una ciambella o un muffin. Quante opzioni ha Marco? La risposta è molto semplice: $14 + 16 = 30$. In questo caso abbiamo applicato la più semplice delle tecniche di conteggio: il **principio additivo**.

Principio Additivo e Moltiplicativo

Theorem 1. Principio additivo

Il principio additivo afferma che se un evento A può accadere in m_1 modi e un evento B può accadere in m_2 modi, allora l'evento $A \vee B$ può accadere in $m_1 + m_2$ modi

Affinchè ciò sia valido, è importante che gli eventi siano **disgiunti**, ossia diversi in ogni modo (es. deve essere impossibile che A e B possano accadere allo stesso tempo). Nel caso in cui considerassimo un mazzo di 52 carte contenente 26 carte rosse e 12 facce e volessimo sapere le combinazioni possibili affinchè esca una faccia rossa non potremmo applicare il principio additivo, dunque $26 + 12 = 38$, poichè ci sono 6 carte che sono sia rosse che facce.

L'esistenza del principio additivo in matematica discreta implica naturalmente anche l'esistenza del **principio moltiplicativo**.

Theorem 2. Principio moltiplicativo

Il principio moltiplicativo afferma che se un evento A può accadere in m_1 modi e un evento B può accadere in m_2 modi, allora l'evento $A \wedge B$ può accadere in $m_1 \cdot m_2$ modi

Riprendendo i due esempio fatti nel capitolo introduttivo, possiamo risolvere entrambi i quesiti applicando il principio moltiplivativo:

- Un ristorante offre un menù a scelta tra 5 primi piatti, 4 secondi piatti e 7 dessert. Considerando un pasto completo come menu formato da un primo, un secondo e un dessert, quanti pasti completi è possibile consumare?

$$A \wedge B = 5 \cdot 4 \cdot 7$$

- Una targa italiana di un'auto è costituita da 2 lettere, 3 cifre e 2 lettere. Quante targhe è possibile comporre?

$$A \wedge B \wedge C = 26^2 \cdot 10^3 \cdot 26^2$$

Questi esempi, tuttavia, sono *statici*, dunque possiedono a priori una quantità conosciuta di elementi appartenenti ad ogni evento. Nella maggior parte dei casi in cui sia necessario applicare il Principio Moltiplicativo, tali informazioni vanno ricavate attenendosi alla situazione proposta, facendo attenzione ai dati forniti dal problema. Il Principio Moltiplicativo, quindi, può essere applicato anche in casi in cui ci siano dei *vincoli*.

Il caso tipico è quello di scelte consecutive di elementi in uno stesso insieme: se l'insieme di partenza ha n elementi avrò $m_1 = n$ possibilità per la prima scelta, $m_2 = n - 1$ per la seconda, $m_2 = n - 3$ per la terza, e così via.

Per comprendere meglio le applicazioni del Principio Moltiplicativo in presenza di vincoli, consideriamo il seguente esempio e le casistiche proposte:

- Formando una parola, dunque una successione, di 5 lettere scelte tra A, B, C, D, E, F, G, H, I e J:
  - quante sono le parole che non iniziano con H? $\Rightarrow 9 \cdot 10^4$
  - quante sono le parole che non iniziano con H e non finiscono con A? $\Rightarrow 9 \cdot 10^3 \cdot 9$
  - quante sono le parole che iniziano per A? $\Rightarrow 1 \cdot 10^4$
  - quante sono le parole che iniziano con H e hanno B in terza posizione? $\Rightarrow 1 \cdot 10 \cdot 1 \ \cdot 10 \cdot 10 = 10^3$
  - quante sono le parole che non contencono 2 lettere consecutive identiche? $\Rightarrow 10 \cdot 9^4$
  - quante sono le aprole che non iniziano con J e non contengono 2 lettere consecutive identiche? $\Rightarrow 9 \cdot 9^4$

Una volta compresi i due principi, è necessario affrontare le casistiche in cui sia necessario impiegare entrambi i principi al fine di poter ottenere la soluzione richiesta.

Riprendendo il precedente esempio, consideriamo questa ulteriore casistica:

- Quante sono le targhe che contengono una unica P (indipendentemente dalla posizione)?

Per poter ottenere una soluzione valida, è necessario scomporre la richiesta in dei *tipi* (o *categorie*) **mutualmente esclusivi**, ossia disgiunti, ed **esaustivi**, ossia contenenti tutte le casistiche possibili appartenenti alla richiesta originale.

Possiamo, quindi, individuare i seguenti tipi di cui possiamo facilmente calcolare la quantità applicando il Principio Moltiplicativo:

1. Tipo 1: Targhe con P in *prima* posizione $\Rightarrow 1 \cdot 25 \cdot 10^3 \cdot 25^2 = 10^3 \cdot 25^3$
2. Tipo 2: Targhe con P in *seconda* posizione $\Rightarrow 25 \cdot 1 \cdot 10^3 \cdot 25^2 = 10^3 \cdot 25^3$
3. Tipo 3: Targhe con P in *terza* posizione $\Rightarrow 25^2 \cdot 10^3 \cdot 1 \cdot 25 = 10^3 \cdot 25^3$
4. Tipo 4: Targhe con P in *quarta* posizione $\Rightarrow 25 \cdot 10^3 \cdot 25 \cdot 1 = 10^3 \cdot 25^3$

Una volta calcolate le quantità dei singoli tipi, possiamo applicare il Principio Additivo per poter soddisfare la richiesta iniziale:

$$T_1 + T_2 + T_3 + T_4 = 10^3 \cdot 25^3 + 10^3 \cdot 25^3 + 10^3 \cdot 25^3 + 10^3 \cdot 25^3 = 4 \cdot 10^3 \cdot 25^3$$

Come è facilmente intuibile, il concetto sopra espresso è facilmente riconducibile in termini di **insiemi**, dove ognuno dei tipi è un *sottoinsieme* di A, ossia l'insieme che soddisfa la richiesta:

$$T_1 \subseteq A, T_2 \subseteq A, T_3 \subseteq A, T_4 \subseteq A$$

$$A = T_1 \cup T_2 \cup T_3 \cup T_4$$

Anche la condizione di mutua esclusività può essere rappresentata in termini di insiemi, affermando che gli insiemi T_1, T_2, T_3, T_4 sono *due a due disgiunti*, ossia la loro intersezione corrisponde ad un *insieme vuoto*:

$$T_1 \cap T_2 = \emptyset, T_1 \cap T_3 = \emptyset, T_1 \cap T_4 = \emptyset, T_2 \cap T_3 = \emptyset, T_3 \cap T_4 = \emptyset$$

Per semplificare la scrittura, d'ora in poi, nel caso in cui A sia un insieme, useremo la notazione #A per indicare il numero di elementi di A (o *cardinalità* di A).

1.1.1 Principio di Esclusione e Inclusione

Immaginiamo di dover contare quante siano le targhe contenenti almeno una T e almeno un 9 al loro interno. Effettuare una tipizzazione disambigua e completa di questo insieme sarebbe molto laborioso, dunque possiamo effettuare un *passaggio al complemento*, escludendo l'insieme contenente le targhe **senza nessuna T o senza nessun 9** dall'insieme totale delle targhe.

- A = insieme totale delle targhe
- S = insieme delle targhe contenenti almeno una T e almeno un 9 (il nostro obiettivo)
- $A \setminus S$ = insieme complementare di S in A

Tuttavia, rimane il problema del dover tipizzare questo insieme complementare. Possiamo provare a dividerlo in questi due tipi:

- K = insieme delle targhe che non contengono una T $\Rightarrow$
- J = insieme delle targhe che non contengono un 9 $\Rightarrow 26^2 \cdot 9^3 \cdot 26^2$

Abbiamo quindi descritto $A \setminus S$ come $K \cup J$. Rimane però un problema: nell'insieme K vengono contate anche le targhe **sia senza T sia senza 9** e lo stesso accade anche nell'insieme J. Dunque, stiamo contando **due volte** tutte le targhe sia senza T sia senza 9.

Poiché entrambi i due insiemi K e J condividono questa tipologia di targhe, possiamo dire che $K \cap J$ viene contato due volte, quindi per "aggiustare il tiro" è necessario **escludere** gli elementi dell'intersezione dalla somma degli elementi di K e J:

$$\#(A \setminus S) = \#(K \cup J) = \#K + \#J - \#(K \cap J)$$

Una volta identificato l'insieme complementare, possiamo calcolare la quantità richiesta #S dal quesito stilando una lista delle varie quantità impiegate ed utilizzando il principio additivo tra di esse:

- #A = $26^2 \cdot 10^3 \cdot 26^2$
- #K = $25^2 \cdot 10^3 \cdot 25^2$
- #J = $26^2 \cdot 9^3 \cdot 26^2$
- $\#(K \cap J) = 25^2 \cdot 9^3 \cdot 25^2$
- $\#(K \cup J)$ = #K + #J - $\#(K \cap J)$

$$\#S = \#A - \#(A \setminus S) = \#A - (\#K + \#J - \#(K \cap J))$$

$$\#S = 26^2 \cdot 10^3 \cdot 26^2 - (25^2 \cdot 10^3 \cdot 25^2 + 26^2 \cdot 9^3 \cdot 26^2 - 25^2 \cdot 9^3 \cdot 25^2)$$

Vediamo ora un caso più complesso dove sia necessario applicare anche il principio di inclusione oltre a quello di esclusione:

Consideriamo un caso in cui i nostri dati sono divisi in 3 tipi. Consideriamo una classe di 41 studenti sottoposti a tre test di valutazione: Combinatoria (C), Induzione (I) e Logica (L). I risultati dei test a nostra disposizione sono i seguenti:

- 12 studenti superano I
- 5 studenti superano L
- 8 studenti superano C
- 2 studenti superano sia I che L
- 6 studenti superano sia I che C
- 3 studenti superano sia L che C
- 1 studente supera sia I che L che C

Quanti studenti hanno superato almeno un test?

Per rispondere alla domanda, possiamo contare gli elementi appartenenti all'unione $I \cup L \cup C$, in modo da ricoprire tutti i casi possibili. Tuttavia, come nel caso precedente, esistono alcuni casi in cui vengono ripetuti dei conteggi (ad esempio, sia l'insieme I che l'insieme L condividono $I \cap L$, dunque essa verrebbe contata due volte nell'unione $I \cup L$)

Procedendo in modo analogo all'esempio precedente, potremmo calcolare la quantità di studenti che ha superato almeno un test come:

$$\#I + \#L + \#C - \#(I \cap L) - \#(L \cap C) - \#(C \cap I)$$

Tuttavia, **escludendo** le tre intersezioni abbiamo generato un altro problema: tutti e tre gli insiemi I, L e C contengono l'intersezione $I \cap L \cap C$ e allo stesso modo anche i tre insiemi $I \cap L$, $L \cap C$ e $C \cap I$ contengono tale intersezione. Abbiamo, dunque, sia **incluso tre volte** questa intersezione sia **escluso tre volte**, finendo con il non conteggiare tale intersezione. Per aggiustare ancora una volta il tiro, dobbiamo **re-includere** questa intersezione nel conteggio finale, ottenendo che:

$$\#S = \#I + \#L + \#C - \#(I \cap L) - \#(L \cap C) - \#(C \cap I) + \#(I \cap L \cap C)$$

$$\#S = 12 + 5 + 8 - 2 - 3 - 6 + 1 = 15$$

1.2 Figure della combinatoria

Una volta compresi i due principi alla base del calcolo combinatorio, di seguito vedremo anche quelle che sono le *figure fondamentali* ed estremamente ricorrenti nel calcolo combinatorio.

1.2.1 Disposizioni con ripetizione

Le **disposizioni con ripetizione** sono una generalizzazione dei casi in cui, nell'applicazione del PM, il fattore moltiplicativo sia costante.

Per comprendere meglio di cosa si tratta, analizziamo il seguente problema:

- Consideriamo l'insieme A = a, b, c. Vogliamo contare le sequenze ordinate di lunghezza 2 di elementi scelti in A con possibili ripetizioni.

In questo caso, le sequenze ordinate ricavabili sono: aa, ab, ac, ba, bb, bc, ca, cb, cc. Poichè abbiamo 3 scelte per il primo elemento e 3 scelte per il secondo, possiamo applicare il PM e ricavare la quantità: $3 \cdot 3 = 9$.

Generalizzando questa casistica, possiamo definire le disposizioni con ripetizione come:

Theorem 3. Disposizioni con ripetizione

Definiamo come **disposizione con ripetizione** di *ordine k* di *n oggetti* una sequenza ordinata $(x_1, x_2, ..., x_k)$ di k oggetti scelti tra gli n totali

$$D'_{n,k} = n \cdot n \cdot ... \cdot n = n^k$$

1.2.2 Disposizioni semplici

Le **disposizioni semplici** sono una generalizzazione dei casi in cui, nell'applicazione del PM, il fattore moltiplicativo decresca di 1 ad ogni passo.

Per comprendere meglio di cosa si tratta, analizziamo il seguente problema:

- Consideriamo l'insieme A = a, b, c. Vogliamo contare le sequenze ordinate di lunghezza 1, 2 e 3.

In questo caso, le sequenze di lunghezza 1 sono tre (a, b, c), quelle di lunghezza 2 sono sei (ab, ac, ba, bc, ca, cb) e quelle di lunghezza 3 sono ancora sei (abc, acb, bac, bca, cab, cba).

Utilizzando il PM per contarle, nel caso in cui la lunghezza sia 2 allora avremo 3 possibilità per la prima lettera e 2 per la seconda ($3 \cdot 2$), emntre nel caso in cui la lunghezza sia 3 allora avremo 3 possibilità per la prima lettera, 2 per la seconda e 1 per la terza ($3 \cdot 2 \cdot 1 = 6$).

Possiamo generalizzare entrambi i casi nel concetto di disposizione semplice:

Theorem 4. Disposizioni semplici

Sia $1 \leq k \leq n$. Definiamo come **disposizione semplice** di *ordine* k di n *oggetti* una sequenza ordinata $(x_1, x_2, ..., x_k)$ di k oggetti distinti tra loro scelti tra gli n totali

$$D_{n,k} = n \cdot (n-1) \cdot ... \cdot (n-(k-1))$$

Possiamo notare come l'equazione che descrive le disposizioni semplici corrisponda facilmente al *fattoriale di n* troncato da un certo termine in poi. Più precisamente, tale concetto corrisponde a dire che dal fattoriale di n venga troncata la coda $(n-k) \cdot (n-(k+1)) \cdot ... \cdot 2 \cdot 1$, la quale corrisponde esattamente al fattoriale di (n - k).

Possiamo dunque riscrivere l'equazione definente le disposizioni semplici come:

$$D'_{n,k} = \frac{n!}{(n-k)!}$$

Nel caso in cui n e k coincidano, allora indicheremo questa particolare disposizione con il termine *permutazione*. Poichè in questo caso il fattoriale di (n - k) corrisponderebbe al fattoriale di 0, dunque 1, le permutazioni corrispondono al fattoriale di n:

$$n = k, P_n = D'_{n,k} = \frac{n!}{(n-k)!} = \frac{n!}{0!} = n!$$

Per approfondire il concetto, di seguito vedremo due esempi in cui è possibile applicare le due tipologie di disposizioni:

- Quanti sono i possibili ordini di arrivo (non simultanei) in una gara con 10 partecipanti (assumendo che tutti gli atleti arrivino al traguardo)?

  Ci troviamo in una casistica in cui ad ogni arrivo la quantità di possibili arrivi diminuisca: 10 atleti potranno arrivare primi, 9 potranno arrivare secondi e così via. Poichè non è necessario effettuare alcun troncamento, ci troviamo dinnanzi ad una permutazione di numero 10.

  $$P_{10} = 10!$$

- Se a un torneo partecipano 8 squadre scelte tra 15 e l'ordine di partenza è a sorte, quanti sono i possibili schieramenti di partenza?

  In questo caso, invece, ci troviamo in una situazione dove ad una permutazione di 15 vengono troncati tutti i possibili ordini di partenza successivi all'ottavo ordine, poichè le squadre partecipanti potranno essere solo 8 su 15. Il risultato, quindi, corrisponderà ad una disposizione semplice di ordine 8 di numero 15.

  $$D_{15,8} = \frac{15!}{(15-8)!} = \frac{15!}{7!}$$

1.2.3 Anagrammi

Gli **anagrammi** sono un caso particolare di disposizione. Per capire in modo diretto di cosa tratta, vediamo i seguenti esempi:

- Quanti sono gli anagrammi della parola NONNA?

  Nel caso in cui considerassimo ognuna delle lettere ripetute come una lettera diversa (quindi come se la parola in questione fosse $N_1ON_2N_3A$), potremmo identificare la risposta come una semplice permutazione di tutte le lettere disponibili, quindi $P_5 = 5! = 120$.

  Nel caso in cui invece considerassimo le lettere ripetute come la stessa, avremmo degli anagrammi uguali tra loro poichè le tre N sono intercambiabili tra loro. In questo caso, quindi, sarà necessario dividere il numero di permutazioni originali per il numero di permutazioni della quantità di lettere N ripetute, che in questo esempio chiameremo r.

$$\#A = \frac{P_n}{P_{n_1}} = \frac{P_5}{P_3} = \frac{5!}{3!} = 20$$

- Quanti sono gli anagrammi della parola NONNO?

  In questo caso ci troviamo in una situazione molto simile alla precedente, tuttavia le tipologie di lettere ripetute sono due, N e O. Per soddisfare la domanda, possiamo procedere con lo stesso metodo, dividendo il numero delle permutazioni originali (5!) per il numero delle permutazioni della quantità di lettere N ripetute e di lettere O ripetute, che chiameremo rispettivamente n_1 e n_2.

$$\#A = \frac{P_n}{P_{n_1} \cdot P_{n_2}} = \frac{P_5}{P_3 \cdot P_2} = \frac{5!}{3! \cdot 2!} = 10$$

Ricapitolando, per ottenere il numero di anagrammi di una parola formata da n *occorrenze* di lettere di cui n_1 sono identiche, allora avremo $\frac{n!}{n_1!}$ possibilità. Nel caso in cui ci siano n_1 lettere identiche di un tipo e n_2 di un altro tipo, allora avremo $\frac{n!}{n_1! \cdot n_2!}$ possibilità.

In generale, quindi, gli anagrammi di una parola lunga n lettere, in cui compaiono t gruppi di $n_1, n_2, ..., n_t$ lettere ripetute, sono:

$$\#A = \frac{n!}{n_1! \cdot n_2! \cdot ... \cdot n_t!}$$

Il calcolo degli anagrammi, tuttavia, non si limita ad essere applicato solo nel caso in cui sia lavori con parole, bensì in qualsiasi *caso analogo* dove ogni tipologia di elemento può "corrispondere" ad una lettera:

- Quanti sono gli ordinamenti di 14 frutti di cui 7 mele e 3 pere e 4 pesche se mi interessa soltanto distinguere tra mele, pere e pesche?

$$\#A = \frac{n!}{n_1! \cdot n_2! \cdot n_3!} = \frac{14!}{7! \cdot 3! \cdot 4!} = 120120$$

1.2.4 Combinazioni semplici

Fino ad ora, abbiamo visto problemi in cui veniva sempre considerato l'*ordine* in cui gli elementi si presentavano gli elementi di un dato insieme (permutazioni e disposizioni). Nell'ambito delle **combinazioni**, invece, l'ordine non ha alcuna importanza. Per capire meglio di cosa si tratta, vediamo il seguente esempio:

- Consideriamo l'insieme A = a, b, c, d. Vogliamo contare quanti sono i sottinsiemi di 3 elementi.

Poichè si tratta di sottoinsiemi possibili e non *sequenze ordinate*, tutti i sottoinsiemi dove gli stessi tre elementi sono in ordine diverso, corrispondono tutti ad una singola possibile combinazione:

$$\{a, b, c\} = \{b, c, a\} = \{b, a, c\} = ...$$

Possiamo quindi facilmente contare manualmente quanti siano i sottoinsiemi possibli: {a, b, c}, {a, b, d}, {a, c, d}, {b, c, d}.

Per poter calcolare le combinazioni possibili in modo matematico, invece, possiamo ricavare il concetto partendo dalle disposizioni semplici, in questo caso di ordine 3:

$$D_{4,3} = \frac{4!}{1!} = 16$$

$$\overbrace{abc, acb, bac, bca, cab, cba \Rightarrow 3!}$$

$$abd, adb, bad, bda, dab, dba \Rightarrow 3!$$

$$adc, acd, dac, dca, cad, cda \Rightarrow 3!$$

$$dbc, dcb, bdc, bcd, cdb, cbd \Rightarrow 3!$$

Una volta enumerate tutte le possibili disposizioni semplici, possiamo notare come, considerando il caso in cui l'ordine non sia importante, ogni "fila" corrisponda allo *stesso sottoinsieme*. Per ottenere la quantità di combinazioni semplici, dunque, sarà necessario considerare solo **1 disposizione** per "fila".

Per tradurre in formula questo concetto, quindi, sarà necessario dividere la disposizione semplice $D_{n,k}$ per k!, ossia il numero di elementi in ogni "fila":

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

Questa formula è molto importante nella Combinatoria e perciò viene definita come **coefficiente binomiale** (che vedremo in seguito) e viene indicato con la seguente notazione specifica, che si legge "n scegli k":

$$C_{n,k} \Rightarrow \binom{n}{k}$$

Di seguito vedremo alcuni esercizi in cui sia possibile applicare il concetto di combinazione semplice per ricavare una soluzione:

- In un gruppo di 80 individui vogliamo scegliere un gruppo di 4 rappresentanti. In quanti modi posso farlo?

  Questo è un tipico esempio di applicazione diretta del concetto di combinazione semplice, poichè non ci interessa l'ordine dei rappresentanti della delegazione.

$$\#A = \binom{80}{4} = \frac{80!}{(80-4)! \cdot 4!}$$

- Quante sono invece le delegazioni con 2 individui per gruppo?

  In questo caso, possiamo calcolare le totali combinazioni possibili calcolando prima le combinazioni possibili per scegliere i due componenti femminili, successivamente le combinazioni per scegliere quelli maschili e calcolare il prodotto di entrambe applicando il PM.

$$\#A = \binom{40}{2} \cdot \binom{40}{2}$$

- Quante sono invece le delegazioni con *almeno* un rappresentante per ogni genere?

  La parola chiave *almeno* indica la possibilità di ottenere la risposta attraverso un *passaggio al complemento*, ossia l'ottenimento della soluzione attraverso l'**esclusione** del numero di combinazioni *vincolate* dal numero di combinazioni totali possibili.

  In questo caso, le categorie di combinazioni vincolate sono due: le combinazioni con solo rappresentanti maschi $\binom{40}{4}$ e quelle con solo rappresentati femminili $\binom{40}{4}$.

$$\#A = \binom{80}{4} - \binom{40}{4} - \binom{40}{4}$$

  In alternativa, potremmo soddisfare la domanda con una *tipizzazione* in tre categorie esaustive:

  1. T_1 = solo un maschio e tre femmine $\Rightarrow \binom{40}{1} \cdot \binom{40}{3}$
  2. T_2 = solo una femmina e tre maschi $\Rightarrow \binom{40}{1} \cdot \binom{40}{3}$
  3. T_3 = due maschi e due femmine $\Rightarrow \binom{40}{2} \cdot \binom{40}{2}$

$$\#A = \#T_1 + \#T_2 + \#T_3 = \binom{40}{1}\binom{40}{3} + \binom{40}{1}\binom{40}{3} + \binom{40}{2}\binom{40}{2} = 2\binom{40}{1}\binom{40}{3} + 2\binom{40}{2}$$

- Quanti modi abbiamo di scegliere una delegazione di 4 rappresentanti in cui un membro assume il ruolo di portavoce?

  In questo caso, possiamo soddisfare la domanda procedendo in due modi: scegliere prima i 4 rappresentanti e successivamente 1 portavoce tra di loro, oppure scegliere prima il portavoce e successivamente gli altri 3 rappresentanti

  $$\#A = \binom{80}{4}\binom{4}{1} \quad \text{oppure} \quad \#A = \binom{80}{1}\binom{79}{3}$$

  Entrambi i procedimenti coincidono con lo stesso valore, dunque possiamo affermare che:

  $$\binom{80}{4}\binom{4}{1} = \binom{80}{1}\binom{79}{3}$$

  Generalizzando questa situazione, possiamo dire che scegliendo m elementi, dove sia importante l'ordine di un solo elemento tra essi, tra n totali, allora:

  $$\binom{n}{m}\binom{m}{1} = \binom{n}{1}\binom{n-1}{m-1} \Rightarrow \binom{n}{m}m = n\binom{n-1}{m-1}$$

- Consideriamo una elezione cui si presentano 15 liste politiche ciascuna delle quali presenta 10 candidati. Il sistema di voto consiste nello scegliere una lista e nell'esprimere al massimo 2 preferenze tra i candidati di quella lista. Vogliamo sapere quanti sono i possibili esiti del voto.

  Possiamo tipizzare il problema in tre categorie:

  1. T_1 = Voti con 0 preferenze $\Rightarrow \binom{10}{0}$, poichè devo contare l'*insieme vuoto*
  2. T_2 = Voti con 1 preferenze $\Rightarrow \binom{10}{1}$
  3. T_3 = Voti con 2 preferenze $\Rightarrow \binom{10}{2}$

  Successivamente sarà necessario applicare il PA tra i tre tipi individuati, per poi moltiplicare il risultato per il numero di liste totali:

  $$15\left(\binom{10}{0} + \binom{10}{1} + \binom{10}{2}\right) \Rightarrow 15 \cdot \sum_{i=1}^{2}\binom{10}{i}$$

1.3 Tecniche di dimostrazione

1.3.1 Dimostrazione per doppio conteggio

Abbiamo osservato come la seguente identità possa essere dimostrata per doppio conteggio

$$\binom{n}{m}\binom{m}{1} = \binom{n}{1}\binom{n-1}{m-1}$$

Tuttavia, essa è valida solo nel caso in cui si vada a scegliere **solo una persona** appartenente alla sotto-delegazione. Possiamo, dunque, generalizzare l'espressione sostituendo 1 con un valore **k**, mantenendola vera **solo** nel caso in cui $0 < k \leq m \leq n$:

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

In questo modo, la parte sinistra dell'espressione conterà i modi di scegliere una delegazione di **m elementi** tra **n elementi**, tra cui vengono poi scelti **k elementi** che possano comporre una sotto-delegazione, mentre la parte destra dell'espressione conterà prima i modi di scegliere una sotto-delegazione di **k elementi** scelti tra **n elementi**, per poi scegliere **m-k elementi** tra **n-k elementi** (ossia tutti gli elementi rimanenti una volta sottratti quelli appartenenti alla sotto-delegazione) con cui formare la normale delegazione.

Sappiamo quindi che $\binom{n}{k}$ ci permette di contare la quantità di sottoinsiemi di k elementi scelti tra n elementi. Tuttavia, esiste anche **un altro modo** di contare la stessa quantità che può tornare utile nel caso in cui k sia un numero molto vicino ad n.

Considerando l'insieme A come l'insieme composto da n elementi, vogliamo contare la quantità di sottoinsiemi contenenti k elementi. Nel fare ciò, ogni volta che viene considerato un sottoinsieme di A contenente k elementi (che chiameremo S), viene **scartato** un sottoinsieme di n - k elementi. Questo sottoinsieme contente gli "scarti" è quindi il **complementare del sottoinsieme di k elementi in A** e viene identificato dalla notazione $\mathbf{A \backslash S}$. Visto che dall'esistenza della prima tipologia di sottoinsieme deriva anche l'esistenza dell'altra, possiamo dire che contare la **quantità di sottoinsiemi complementari** di n - k elementi equivale a contare la **quantità dei sottoinsiemi** di k elementi che si vuole realmente contare:

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

Immaginando di trovarci in un caso in cui bisogni contare i sottoinsiemi di 98 elementi scelti tra 100 elementi, dunque $\binom{100}{98}$ possiamo applicare il ragionamento descritto precedentemente e contare $\binom{100}{2}$ sottoinsiemi, ottenendo la stessa quantità.

1.3.2 Dimostrazione per traduzione

Per convalidare l'effettiva correttezza della precedente dimostrazione, possiamo traslare il concetto precedente nel concetto di **traduzione** da un insieme all'altro, dove l'insieme (o **lingua**) di partenza è quello dei sottoinsiemi di A di k elementi, che chiameremo L_1, e l'insieme (o **lingua)** di arrivo è quello dei sottoinsiemi di A di n - k elementi, che chiameremo L_2.

Stiamo quindi effettuando una traduzione tra i due insiemi, dove ad ogni elemento del primo viene **associato** un elemento dell'altro. Quindi, ad ogni sottoinsieme S di A viene associato il suo complementare in A:

$$S \mapsto A \setminus S$$

Per sostenere che si tratti di una **buona traduzione**, e dunque che L_2 ha lo stesso numero di elementi di L_1 dobbiamo assicurarci che la traduzione rispetti le seguenti proprietà:

1. Ogni elemento di L_1 viene tradotto in **uno e un solo** elemento di L_2
2. Ogni elemento di L_2 è la traduzione di **almeno** un elemento di L_1
3. Non si dà il caso che due elementi distinti di L_1 vengano tradotti nello stesso elemento di L_2

Poiché ad ogni elemento di una lingua è associato un elemento di un'altra, dunque abbiamo una buona traduzione tra i due insiemi A e B, possiamo affermare che i due insiemi hanno **lo stesso numero di elementi**.

Esercizio con dimostrazione per traduzione

Immaginiamo di dover distribuire una quantità t di giocattoli a m bambini. Vogliamo sapere quanti siano i possibili modi per effettuare tale distribuzione.

Per risolvere il quesito, possiamo assegnare dei valori piccoli e comodi alle due variabili, in modo da poter studiare e ricavare una possibile regola di conteggio **generica**.

Scegliamo quindi di dover distribuire 3 giocattoli a 2 bambini, che chiameremo Irene e Marco. Poiché si tratta di numeri piccoli, possiamo calcolare manualmente i possibili modi di distribuzione enumerandoli:

Giorgio	Marco
3	0
2	1
1	2
0	3

Possiamo quindi dire che i modi possibili sono solo **4**. Ma avremmo potuto utilizzare un altro metodo per calcolare questa quantità?

Possiamo provare a risolvere il problema effettuando una **traduzione**, dove i numeri vengono riscritti come **pallini**:

Giorgio	Marco
3	0
2	1
1	2
0	3

$\Rightarrow$

Giorgio	Marco
●●●	
●●	●
●	●●
	●●●

Volendo astrarre ulteriormente, possiamo riscrivere la barra separatrice tra i due bambini come una **stanghetta**:

Giorgio	Marco
●●●	
●●	●
●	●●
	●●●

$\Rightarrow$

●●● |
●● | ●
● | ●●
| ●●●

Queste traduzioni rispettano le caratteristiche tipiche di una **buona traduzione**, dunque possiamo affermare che contare la quantità di modi di poter scrivere una stringa contenente **3 pallini** ed **1 stanghetta** corrisponde a contare i modi di poter distribuire **3 giocattoli** a **2 bambini**.

Per poter contare i modi di poter scrivere la stringa di pallini e stanghette, possiamo calcolare la quantità di sottoinsiemi in cui compaiono *solo i tre pallini* o la quantità di sottoinsiemi in cui compare *solo la stanghetta* (poiché sono **complementari**).

La prima quantità può essere calcolata come un **sottoinsieme di 3** elementi in un insieme di **4 elementi** (ossia i tre pallini e la stanghetta), mentre la seconda quantità può analogamente essere calcolata come un **sottoinsieme di 1** elemento in un insieme di **4 elementi**. Poiché complementari, i due conteggi corrispondono alla stessa quantità:

$$\binom{4}{3} = \binom{4}{1} \Longrightarrow 4$$

Volendo **generalizzare** questo conteggio, notiamo come 4 corrisponda al numero di giocattoli sommato al numero di bambini meno 1 $(m + t - 1)$, 3 corrisponda al numero di giocattoli e 1 al numero di bambini meno 1 $(t-1)$. Possiamo quindi affermare la seguente **regola di conteggio**:

$$\binom{m+t-1}{m} = \binom{m+t-1}{t-1}$$

Per confermare la validità di questa regola, possiamo provare a calcolare i modi per poter distribuire 7 giocattoli a 6 bambini, sostituendo i nuovi valori a quelli precedenti:

$$\binom{7+6-1}{7} = \binom{7+6-1}{6-1} \Longrightarrow \binom{12}{7} = \binom{12}{5}$$

Seconda soluzione

Poiché tramite la traduzione abbiamo trovato un modo per astrarre il problema trasformandolo nel calcolare i modi di scrivere una stringa, è facilmente intuibile come sia possibile, in entrambi i casi mostrati, utilizzare anche gli **anagrammi** per poter calcolare le stesse quantità (ripasso: sezione 1.2.3):

$$\#A = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_t!}$$

- Quanti sono gli anagrammi di una parola formata da tre pallini ed una stanghetta?
  - "Lettere" totali: 4
  - Ripetizioni della "lettera" $\bullet$: 3
  - Ripetizioni della "lettera" $|$: 1

$$\#A_1 = \frac{3!}{3! \cdot 1!} = \binom{3}{1}$$

- Quanti sono gli anagrammi di una parola formata da sette pallini e cinque stanghette?
  - "Lettere" totali: 12
  - Ripetizioni della "lettera" $\bullet$: 7
  - Ripetizioni della "lettera" $|$: 5

$$\#A_2 = \frac{12!}{7! \cdot 5!} = \binom{12}{5}$$

1.3.3 Combinazioni semplici e sottoinsiemi

Ora che abbiamo compreso come contare i sottoinsiemi di k elementi scelti tra n elementi di un insieme A utilizzando vari metodi, vogliamo trovare un modo per poter contare la quantità di **tutti i sottoinsiemi possibili** di un insieme A.

In linguaggio insiemistico, l'insieme contenente tutti i sottoinsiemi possibili di un altro insieme viene definito come **insieme potenza**, e viene identificato come:

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

Per poter contare il numero di elementi presenti nell'insieme potenza di A, possiamo applicare il principio additivo su tutte le combinazioni semplici di n elementi partendo da 0 fino ad n stesso:

$$\#P(A) = \#S_{tot} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n}$$

Tuttavia, contare questa quantità può risultare estremamente laborioso. Possiamo cercare quindi un modo più semplice per poterli contare:

- Consideriamo la collezione di lettere B, M, Q, T, U, Z di cui vogliamo contare tutti i modi possibili per selezionare una sotto-collezione, ossia scegliere alcune lettere e altre no, senza tenere conto dell'ordine degli elementi (ossia non distinguo tra una scelta M, Q, Z e Q, M, Z).

  Per semplificare il conteggio, possiamo effettuare una traduzione dalle lettere che compongono la collezione ad una stringa di numeri binari, dove ad ogni lettera può corrispondere un 1 o uno 0 a seconda della sua presenza o meno all'interno del sottoinsieme descritto.

  Nel caso in cui volessimo rappresentare il sottoinsieme M, Q, T, potremmo riscrivere questo sottoinsieme come 011100, poiché B, U e Z non sono presenti (e dunque vengono sostituite con uno 0). Di conseguenza, all'insieme vuoto corrisponderà a 000000, mentre all'insieme di tutte le lettere corrisponderà a 111111.

  Poiché si tratta di una buona traduzione, per rispondere alla domanda possiamo contare direttamente la quantità di disposizioni semplici di 6 cifre scelte tra 0 ed 1 ($D_{6,2}$), corrispondenti alle possibili disposizioni della stringa binaria, ossia 2^6. Nel caso in cui aggiungessimo A e C alla collezione di lettere, il risultato diventerebbe 2^8.

Possiamo quindi dedurre che un **insieme di n elementi** possiede 2^n sottoinsiemi e di conseguenza:

$$\#P(A) = \#S_{tot} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

Capitolo 2

Funzioni

2.1 Definizioni di funzione

In informatica, così come in molte altri ambiti matematici, una **funzione** è l'**associazione** di un input di vario genere (dunque numeri, caratteri, ecc) a un output anch'esso di vario genere. Affinché si possa parlare di funzione però, bisogna assicurarsi che ad ogni input corrisponda **ad un solo** output. Possiamo quindi dare la seguente definizione di funzione:

Definition 1. Funzione

Una **funzione** è una associazione tra elementi di un insieme I (detto **dominio**) ad elementi di un insieme O (detto **codominio**), in modo tale che ogni elemento del dominio venga associato un **unico** elemento del codominio.

Denotiamo una funzione da un dominio I a un codominio O come

$$f : I \to O$$

dove I e O sono due insiemi arbitrari. Ogni elemento $x \in I$ viene associato (o mappato) da f in un unico elemento $y \in O$.

$$x \mapsto y$$

Normalmente, scriviamo che $f(x) = y$ e diciamo che y è **immagine** di x via f e che che x è **pre-immagine** di y via f.

È necessario puntualizzare come secondo la definizione proposta una funzione **non** è identificabile semplicemente come una *regola di associazione* di elementi di un insieme a elementi di un altro insieme. Per definire una funzione è necessario specificarne il **dominio** e il **codominio**.

Due funzioni possono quindi, essere **diverse** anche se la regola che le definisce è la stessa, ad esempio non possiamo considerare le due funzioni $f(x) = x^2$ definita in $f : \mathbb{N} \to \mathbb{N}$ e $g(x) = x^2$ definita in $g : \mathbb{R} \to \mathbb{R}$ come **uguali** poiché i loro domini e codomini sono diversi.

Funzioni come insiemi

Nella Matematica moderna è abituale identificare una funzione come un **insieme di tutti i punti** del suo grafico. Abbiamo visto come una funzione $f : I \to O$ associa a ogni elemento $x \in I$ (ossia l'argomento) un unico elemento $y \in O$ (il valore). Possiamo quindi rappresentare tale associazione come la coppia ordinata (x, y).

Possiamo quindi affermare che f corrisponda all'**insieme di tutte le coppie ordinate (x, y)**:

$$f = \{(x, y) : x \in I, y \in O, f(x) = y\}$$

In termini più generali, dati due insiemi **A** e **B**, denotiamo con $\mathbf{A} \times \mathbf{B}$ il suo **prodotto cartesiano**, ossia l'insieme delle coppie ordinate di tipo (a, b) con $a \in A$ e $b \in B$. Tecnicamente, dunque, una funzione $f : I \to O$ non è altro che un **sottoinsieme** di $I \times O$.

Possiamo dare quindi un'altra definizione di funzione:

Definition 2. Funzione (in insiemistica)

Una funzione $f : I \to O$ è un **sottoinsieme del prodotto cartesiano** $I \times O$ tale che per ogni $x \in I$ esiste uno e un solo $y \in O$ tale che $(x, y) \in f$

$$f = \{(x, y) : x \in I, y \in O, f(x) = y\}$$
$$f \subseteq I \times O$$

2.2 Funzioni iniettive, suriettive e biettive

Generalmente, nell'ambito delle funzioni è possibile individuare **due particolari tipi** di quest'ultime in base alle **caratteristiche** assunte dalle loro associazioni.

Immaginiamo di star associando ad ogni persona il proprio codice fiscale tramite una funzione. In questo caso possiamo affermare che ad ogni elemento del **codominio** (l'insieme dei codici fiscali) viene associato **un solo** elemento del **dominio** (l'insieme delle persone). Dunque, nel caso in cui prendessimo due elementi scelti a caso x_1 e x_2 dal dominio, le loro **immagini** $f(x_1)$ e $f(x_2)$ saranno **sempre diverse tra loro**. Una funzione di questo tipo viene chiamata **funzione iniettiva**.

Definition 3. Funzione iniettiva

Una funzione f è detta **iniettiva** se a elementi distinti x_1 e x_2 appartenenti al dominio sono associate immagini distinte $f(x_1)$ e $f(x_2)$ nel codominio, dunque **non esistono alcun** x_1 e x_2 per cui $f(x_1) = f(x_2)$

$$f : I \to O$$
$$f \text{ è iniettiva se } \nexists x_1, x_2 \in I;\ x_1 \neq x_2 \,|\, f(x_1) = f(x_2)$$

Consideriamo ora invece la funzione $f(x) = x^2$ dove $f : \mathbb{Z} \to \mathbb{Z}$, rappresentabile graficamente come una parabola. Notiamo facilmente come ad **ogni** elemento del codominio $y \in \mathbb{Z}$ è **immagine** di **almeno** un elemento del dominio $x \in \mathbb{Z}$ (es: $y = 4$ è immagine sia di $x_1 = 2$ sia di $x_2 = -2$). Una funzione di questo tipo viene chiamata **funzione suriettiva**.

Definition 4. Funzione suriettiva

Una funzione f è detta **suriettiva** se **ogni** elemento appartenente al codominio è **immagine di almeno un** elemento appartenente al dominio.

$$f : I \to O$$

$$f \text{ è suriettiva se } \forall y \in O \exists x \in I \mid f(x) = y$$

Nel caso in cui una funzione è **sia iniettiva che suriettiva**, essa viene definita **biettiva**. Dunque, poiché possiede entrambe le caratteristiche delle due tipologie, ossia ogni elemento del codominio $y \in O$ è **immagine di esattamente un** elemento del dominio $x \in I$.

Definition 5. Funzione biettiva

Una funzione f viene detta **biettiva** se è **sia iniettiva che suriettiva**.

Esempio di analisi di una funzione

- La funzione $f : \mathbb{Z} \to \mathbb{Z}^+$ con $f(x) = x^2$, è effettivamente una funzione valida? Se sì, è biettiva?
  - ***f* è una funzione valida**, poiché per ogni elemento del dominio $x \in \mathbb{Z}$ esiste un solo elemento del codominio $y \in \mathbb{Z}^+$ tale che $(x, y) \in f$, dove f è un sottoinsieme del prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}^+$

    $$f = \{(x, y) : x \in \mathbb{Z}, y \in \mathbb{Z}^+, f(x) = y\}$$

    $$f \subseteq \mathbb{Z} \times \mathbb{Z}^+$$

  - ***f* non è biettiva** poiché essa è solo suriettiva ma non iniettiva:
    - Ogni elemento del codominio è immagine di almeno un elemento del dominio, dunque la funzione **è suriettiva**
    - Considerando i due elementi appartenenti al dominio $x_1 = 3$ e $x_2 = -3$, non è vero che $f(x_1) \neq f(x_2)$, dunque la funzione **non è iniettiva**

2.3 Funzioni ed operatori insiemistici

Una volta definita una funzione e le sue tipologie principali, vediamo come essa interagisce con gli **operatori insiemistici**.

Analizziamo le due seguenti inclusioni:

$$f(A \cap B) \subseteq f(A) \cap f(B) \quad e \quad f(A) \cap f(B) \subseteq f(A \cap B)$$

Consideriamo un elemento $z \in f(A \cap B)$. Per definizione di immagine di $A \cap B$ via f, possiamo dire che esiste un elemento $w \in A \cap B \,|\, f(w) = z$. Tuttavia, ciò implica che esista anche un elemento $w \in A \,|\, f(w) = z$ e un elemento $w' \in B \,|\, f(w') = z$ (basterebbe scegliere lo stesso elemento per entrambi). Abbiamo quindi dimostrato che anche la proposizione $z \in f(A) \cap f(B)$ è **vera**.

Consideriamo ora, invece, un elemento $z \in f(A) \cap f(B)$. Avremo dunque che $z \in f(A)$ e $z \in f(B)$, da cui deduciamo che esiste un elemento $w \in A \,|\, f(w) = z$ e un elemento $w' \in B \,|\, f(w') = z$. A questo punto, però, non possiamo ancora affermare con certezza che $w = w'$, a meno che la funzione non sia **iniettiva**, poiché l'unico modo in cui venga esplicitamente affermato che $f(w) = z = f(w')$. Dunque, abbiamo dimostrato che anche la proposizione $z \in f(A \cap B)$ è **vera** se la funzione è **iniettiva**.

Proposition 5

Sia $f : I \to O$ una funzione e siano $A, B \subseteq I$ due sottoinsiemi del dominio. Se f è iniettiva, allora

$$f(A \cap B) \subseteq f(A) \cap f(B) \quad e \quad f(A) \cap f(B) \subseteq f(A \cap B)$$

da cui deduciamo che

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

Proviamo invece ora a dimostrare il contrario. Sia $f : I \to O$ una funzione e siano $A, B \in O$ due sottoinsiemi del codominio. Possiamo affermare che $f(A \cup B) = f(A) \cup f(B)$?
f deve essere comunque iniettiva?

Procedendo analogamente alla dimostrazione precedente, consideriamo l'inclusione $f(A \cup B) \subseteq f(A) \cup f(B)$, definendo per esteso i vari insiemi coinvolti:

- $f(A \cup B) = \{z \in O : \exists x \in A \cup B \in I \,|\, f(x) = z\}$
- $f(A) = \{z \in O : \exists x \in A \,|\, f(x) = z\}$
- $f(B) = \{z \in O : \exists x \in B \,|\, f(x) = z\}$
- $f(A) \cup f(B) = \{z \in O : (\exists x \in A \,|\, f(x) = z) \vee (\exists x \in B \,|\, f(x) = z)\}$

Consideriamo dunque un elemento $z \in f(A \cup B)$. Per sua definizione, esiste un elemento $x \in A \cup B \in I \,|\, f(x) = z$, che implica a sua volta che $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$.

Se esiste un elemento $x \in A \,|\, f(x) = z$, sicuramente $x \in A \cup B$, poiché sarà incluso da A, dunque $z \in f(A) \cup f(B)$ Allo stesso modo, se esiste un elemento $x \in B \,|\, f(x) = z$, sicuramente $x \in A \cup B$, poiché sarà incluso da B, dunque $z \in f(A) \cup f(B)$.

Poiché abbiamo dimostrato che in entrambi i casi $z \in f(A) \cup f(B)$, possiamo dire che $f(A \cup B) \subseteq f(A) \cup f(B)$ è **vera**.

Consideriamo ora l'inclusione $f(A) \cup f(B) \subseteq f(A \cup B)$ con un elemento $z \in f(A) \cup f(B)$. Per definizione, significa che $z \in f(A) \vee z \in f(B)$. Anche questa volta abbiamo un ragionamento per casi:

Se $z \in f(A)$ allora esiste un elemento $x \in A \,|\, f(x) = z$, dunque $x \in A \cup B \,|\, f(x) = z$, poiché incluso da A. Allo stesso modo, Se $z \in f(B)$ allora esiste un elemento $x \in B \,|\, f(x) = z$, dunque $x \in A \cup B \,|\, f(x) = z$, poiché incluso da B.

Poiché abbiamo dimostrato che in entrambi i casi $z \in f(A \cup B)$, possiamo dire che $f(A) \cup f(B) \subseteq f(A \cup B)$ è **vera**, ricavando che:

Proposition 6

Sia $f : I \to O$ una funzione e siano $A, B \subseteq O$ due sottoinsiemi del codominio. Se f è iniettiva, allora

$$f(A \cup B) \subseteq f(A) \cup f(B) \quad e \quad f(A) \cup f(B) \subseteq f(A \cup B)$$

da cui deduciamo che

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

2.4 Composizioni di funzioni

Comporre funzioni significa **applicarle in sequenza**. Ad esempio, comporre la funzione $f : n \mapsto n + 1$ alla funzione $g : n \mapsto n^2$ significa ricavare ricavare la **funzione composta** $h : n \mapsto n + 1 \mapsto (n + 1)^2$, che viene riscritta come $h : n \mapsto (n + 1)^2$. Affinché ciò sia possibile, è necessario che il **codominio** della funzione f **rientri nel dominio** della funzione g

Definition 6. Funzione composta

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. La funzione composta di f e g è la funzione $h : X \to Z$, definita come $x \in X$, $h(x) = g(f(x))$. Per indicare l'avvenuta composizione, la funzione composta h viene denotata come $(g \circ f)$

Riprendendo l'esempio iniziale, possiamo notare come l'**ordine di composizione** sia estremamente importante:

- $g \circ f : n \mapsto (n + 1)^2$
- $f \circ g : n \mapsto n^2 + 1$

La composizione di funzioni, dunque, **non è commutativa**.

Considerando invece le tre funzioni $f : X \to Y$, $g : Y \to Z$ e $h : Z \to W$, possiamo notare come la loro composizione sia **associativa**, dunque $(h \circ (g \circ f)) = ((h \circ g) \circ f)$

- $(g \circ f) : X \to Z$, dunque può essere composta con $h : Z \to W$ per ottenere $(h \circ (g \circ f)) : X \to W$
- $f : X \to Y$, dunque può essere composta con $(h \circ g) : Y \to W$ per ottenere $((h \circ g) \circ f) : X \to W$

Considerando sempre le due funzioni $f : X \to Y$ e $g : Y \to Z$, possiamo provare ad affermare che:

- Se f e g sono **iniettive** allora $(g \circ f)$ è iniettiva.
- Se f e g sono **suriettive** allora $(g \circ f)$ è suriettiva.
- Se f e g sono **biettive** allora $(g \circ f)$ è biettiva.

Dimostrazione della conservazione dell'iniettività

Supponiamo per assurdo che esista un elemento del codominio $z \in Z$ tale che esistono **due distinti element**i del dominio $x \neq x' \in X$ dove $(g \circ f)(x) = z = (g \circ f)(x')$, dunque che la funzione composta **non sia iniettiva**.

Poiché $(g \circ f)(x) = z = (g \circ f)(x')$ equivale a dire che $g(f(x)) = z = g(f(x'))$ e dato che g è **iniettiva per ipotesi**, se g mappa gli elementi $f(x)$ e $f(x')$ allo stesso elemento z, allora obbligatoriamente $f(x) = f(x')$.

Tuttavia, poiché anche f è **iniettiva per ipotesi**, l'unico modo in cui $f(x) = f(x')$ è se $x = x'$, dunque la supposizione per assurdo iniziale viene **contraddetta**, dunque l'iniettività viene **conservata**.

Dimostrazione della conservazione della suriettività

Scegliamo un arbitrario elemento $z \in Z$. Dato che g è **suriettiva per ipotesi**, esiste un elemento $y \in Y \mid g(y) = z$. Dato che anche f è **suriettiva per ipotesi**, esiste un elemento $x \in X \mid f(g(y)) = z$. Abbiamo dunque dimostrato che esiste un $x \in X$ tale che $(g \circ f)(x) = z$, dunque la funzione composta **conserva** la suriettività.

2.5 Funzione inversa e immagine inversa

La nozione di **funzione inversa** è piuttosto naturale nella pratica matematica: sappiamo cosa vuol dire che $x \mapsto x - 1$ è l'inversa di $x \mapsto x + 1$ o che $n \mapsto \frac{n}{2}$ è l'inversa di $n \mapsto 2n$. In generale, abbiamo la seguente definizione di funzione inversa:

Definition 7. Funzione inversa

Sia $f : X \to Y$ una funzione. La funzione $g : Y \to X$ si dice inversa di f se e solo se $(g \circ f)$ è l'identità su X e $(f \circ g)$ è l'identità su Y.

La funzione inversa di f viene denominata come f^{-1}, dove f è una funzione invertibile solo è **biettiva** ed **esiste** una funzione f^{-1}.

Consideriamo ora la funzione $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ definita come segue:

$$f(1) = a,\ f(2) = a,\ f(3) = a,\ f(4) = b,\ f(5) = b$$

Abbiamo dunque che $f^{-1}(\{a, b, c\}) = \{1, 2, 3, 4, 5\}$. Notiamo come l'elemento a ha 3 pre-immagini, l'elemento b ha 2 pre-immagini e l'elemento c non ha alcuna pre-immagine.

Dunque, non abbiamo un modo univoco per leggere f all'inverso associando uno e un unico elemento di 1, 2, 3, 4, 5 a ogni elemento di a, b, c. Risulta quindi naturale considerare l'**insieme delle pre-immagini** di un elemento del codominio come un **sottoinsieme del dominio** di una funzione.

Definition 8. Immagine inversa

Sia $f : X \to Y$ e sia $A \subseteq Y$. Definiamo $f^{-1}(A)$ come l'**insieme** che contiene **tutte e sole** le pre-immagini via f di elementi di A

$$f^{-1}(A) = \{x \in X : f(x) \in A\}$$

ATTENZIONE: Il simbolo f^{-1} in questo caso **non indica** necessariamente una funzione, bensì solo un'associazione tra sottoinsiemi del codominio O e sottoinsiemi del dominio I ma non si tratta in generale di una funzione O a I.

Quando f^{-1} esiste come funzione, la notazione introdotta $f^{-1}(A)$ per la **pre-immagine di A via f** coincide con la notazione $f^{-1}(A)$ intesa come **immagine dell'insieme A via $\mathbf{f^{-1}}$** (sostanzialmente, $f^{-1}(A)$ corrisponde sia alla pre-immagine di f sia all'immagine di f^{-1})

Inoltre, data una funzione $f : I \to O$ possiamo senz'altro definire sempre una funzione pre-immagine di tipo:

$$\pi : O \to \mathcal{P}(I)$$

associando a ogni elemento del codominio di f l'**insieme delle sue pre-immagini** (indicato con $\mathcal{P}(I)$). Si noti che in questo caso è ammesso associare l'insieme vuoto come insieme delle pre-immagini, poiché ciò accade ogni volta che consideriamo un elemento del codominio che non possiede pre-immagini.

Capitolo 3

Relazioni

3.1 Definizione di relazione

Il concetto di relazione è fondamentale una **generalizzazione** del concetto di funzione. Come modelli intuitivi di relazione, prendiamo per esempio: *"a è padre di b"*, dove a e b sono due esseri umani; oppure: *"n è minore di m"* dove n e m sono numeri naturali.

Si vede facilmente che, a differenza delle funzioni, **una relazione non è ovunque definita** e può "far corrispondere" allo stesso 'input' (a, ossia il padre) più di un 'output' ($b_1, b_2, ...$, ossia i suoi figli). Possiamo formalizzare questo concetto in termini insiemistici, dando la seguente definizione di relazione:

Definition 9. Relazione

Siano A e B due insiemi. Una relazione R tra A e B è un sottoinsieme del prodotto cartesiano $A \times B$, ossia un insieme di **coppie ordinate** (a, b) con $a \in A$ e $b \in B$, **senza ulteriori vincoli**. Una relazione tra A e B può essere indicata come $R(a, b)$ o aRb.

$$R \subseteq A \times B$$

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

Notiamo come dalla definizione appena data risultino **quattro fondamentali osservazioni** sulle relazioni:

1. Possono esistere elementi $a \in A$ tale che non esistano coppie di tipo (a, b) nella relazione (alcuni elementi di A possono non essere in relazione con **nessun elemento** di B)
2. Possono esistere elementi $a \in A$ tale che esista più di una coppia di tipo $(a, \cdot)$ nella relazione (alcuni elementi di A possono essere in relazione con **più elementi** di B)
3. Nel caso in cui $A = B$, dunque $R \subseteq A \times B = R \subseteq A \times A$, diciamo che R è una relazione su A (**relazione binaria**). Infatti, ogni relazione può essere vista come una **relazione su un singolo insieme** (ad esempio: Se $R \subseteq A \times B$, allora è anche vero che $R \subseteq (A \cup B) \times (A \cup B)$, dunque è una relazione su $C = A \cup B$)

Esempi:

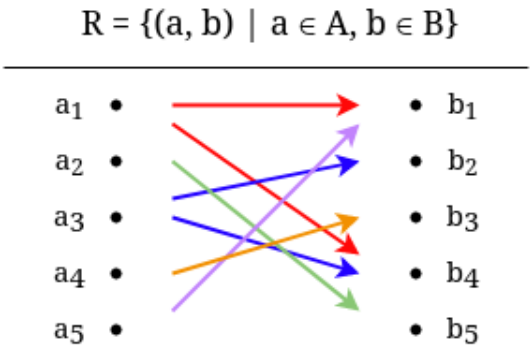
- Sia A l'insieme dei cani e B l'insieme degli esseri umani. La relazione *"a è il cane di b"* corrisponde a:
$$R = \{(a, b) \mid a \in A, b \in B\}$$
- Siano $n \in \mathbb{N}$ e $m \in \mathbb{N}$. La relazione *"$n < m$"* corrisponde a:
$$R = \{(n, n) \mid n, m \in \mathbb{N} \ e \ n < m\}$$

3.2 Rappresentazioni di relazioni

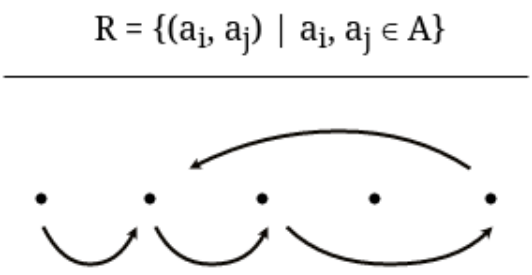
Oltre alla rappresentazione in termini insiemistici, è possibile rappresentare una relazione in **due modi**:

Grafi diretti

Per rappresentare una **relazione tra A e B** rappresentiamo a sinistra gli elementi di A e a destra quelli di B (**grafo bipartito**). Disegniamo una freccia da $a \in A$ a $b \in B$ se e solo se $(a, b) \in R$.



Nel caso di una relazione **su un singolo insieme A** (dunque $R \subseteq A \times A$), possiamo disegnare una volta sola gli elementi di A (**digrafo**) e disegnare una freccia tra ogni coppia (a_1, a_2) di elementi di A per cui vale $(a_1, a_2) \in R$.



Matrici

Se R è una relazione tra $A = a_1, a_2, ..., a_m$ e $B = b_1, b_2, ..., b_m$, la **matrice di R**, denotata $\mathbf{M_R}$, è una matrice $n \times m$ definita come:

$$M_R = \begin{cases} 1 & se\ (a_i, b_j) \in R \\ 0 & se\ (a_i, b_j) \notin R \end{cases}$$

Dalla sua definizione, notiamo come la matrice risulti in una tabella di **righe**, corrispondenti agli elementi di A, e **colonne**, corrispondenti agli elementi di B, contenente degli **1 e 0** a seconda dell'esistenza o non della coppia ordinata (a, b).

Questa rappresentazione è particolarmente importante, poiché usata per rappresentare relazioni nei **calcolatori elettronici** e ne permette una manipolazione abbastanza efficiente.

Esempio:

- Sia $A = \{1, 2, 3, 4\}$ e $R = \{(1, 2), (2, 4), (3, 2), (4, 2), (4, 4)\}$, dunque $R \subseteq A \times A$:

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad \Longrightarrow \quad \begin{array}{c|cccc} & a_1 & a_2 & a_3 & a_4 \\ \hline a_1 & 0 & 1 & 0 & 0 \\ a_2 & 0 & 0 & 0 & 1 \\ a_3 & 0 & 1 & 0 & 0 \\ a_4 & 0 & 1 & 0 & 1 \end{array}$$

3.3 Relazione inversa

Come per le funzioni, è naturale considerare l'**inversione** di una relazione, ad esempio l'inversa della relazione *"a è padre di b"* è la relazione *"b è figlio di a"*. Tuttavia, a differenza di quanto accade con le funzioni, una relazione **possiede sempre un'inversa**.

Definition 10. Relazione inversa

Se $R \subseteq A \times B$, denotiamo con R^{-1} la sua relazione inversa, corrispondente al sottoinsieme di $B \times A$, definito come:

$$R^{-1} \subseteq B \times A$$
$$R^{-1} = \{(b, a) \mid b \in B, a \in A, (a, b) \in R\}$$

Quando una relazione inversa coincide esattamente con la relazione originale stessa, allora tale relazione viene definita **simmetrica**. Più formalmente una relazione $R \subseteq A \times B$ viene detta simmetrica se e solo se per ogni $a \in A$ e per ogni $b \in B$, vale che $(a, b) \in R$ e $(b, a) \in R$.

Ricavare l'inversa di una relazione

Calcolare l'inversa di una relazione in **forma insiemistica** risulta estremamente semplice, poiché basta **invertire le coppie** di R:

$$R = \{(2,2),(2,6),(2,8),(3,6),(4,8)\}$$

$$R^{-1} = \{(2,2),(6,2),(8,2),(6,3),(8,4)\}$$

Nel caso in cui volessimo calcolare R^{-1} partendo dal **grafo** di una relazione, ci basterebbe **invertire la direzione delle frecce**:

$R = \{(a_i, a_j) \mid a_i, a_j \in A\}$

$R^{-1} = \{(a_j, a_i) \mid a_i, a_j \in A, (a_i, a_j) \in R\}$

Infine, nel caso in cui volessimo calcolare R^{-1} partendo dalla **matrice** di una relazione, ci basterebbe **invertire le righe con le colonne**:

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad M_{R^{-1}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

ATTENZIONE: i tre esempi riportati sopra sono l'uno indipendente dall'altro, dunque non rappresentano tutti e tre le stesse relazioni e relazioni inverse.

3.4 Relazioni composte

Così come per le funzioni, risulta naturale considerare la **composizione di relazioni**. Ad esempio, se **R** è la relazione tale che $R(a,b)$ se solo se *"a è padre di b"* e **S** è la relazione tale che $S(c,d)$ se e solo se *"c è marito di d"*, allora viene naturale considerare la relazione composta **T** tale che $T(a,d)$ se e solo se *"a è suocero di d"*.

Definition 11. Relazione composta

Se $R \subseteq A \times B$ e $S \subseteq B \times C$, la **relazione composta** di R e S è la relazione tra A e C che sussiste tra $a \in A$ e $c \in C$ se e solo se esiste un $b \in B$ tale che **R(a,b)** e S**(b, c)** La relazione composta viene denotata **(S ∘ B)**.

Quando una relazione viene **composta con se stessa**, parliamo di **iterazione**. Per esempio, l'iterazione della relazione P *"a è padre di b"* corrisponde alla relazione **(P ∘ P)** *"a è nonno di b"*. Iterando nuovamente, otteniamo la relazione P ∘ (P ∘ P) *"a è bisnonno di b"* e così via.

Ricavare la composizione tra relazioni

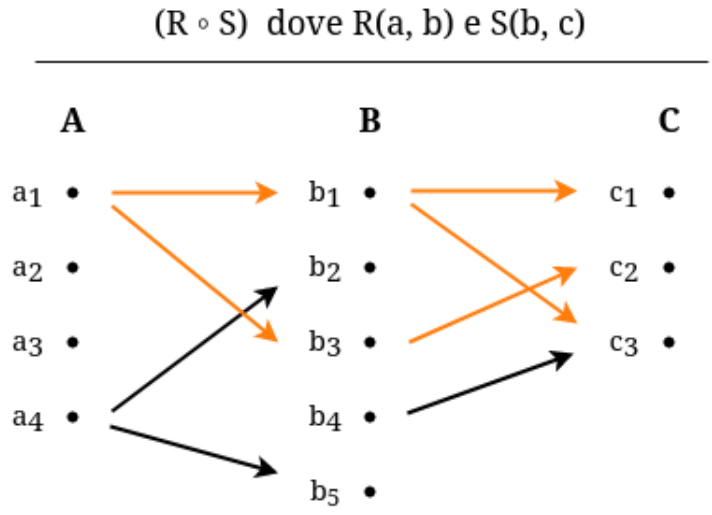
Così come per le relazioni inverse, le relazioni composte possono essere facilmente calcolare nelle tre forme di rappresentazione.

Tuttavia, calcolare le composizioni tra relazioni in **forma insiemistica**, risulta *più complesso*. Consideriamo il seguente esempio: sia $R = \{(a,b),(b,b),(b,d),(c,a),(d,a)\}$ e $S = \{(a,d),(a,b),(b,c),(d,b)\}$. Per ricavare la composta $(S \circ R)$, **partiamo dal primo elemento di R**, ossia (a,b) e **cerchiamo in S una coppia** (b,x), dove x può essere un qualsiasi elemento di C ($x \in C$). Per ogni coppia di questo tipo, sappiamo che (a,x) è nella relazione composta $(S \in R)$

- $(a,c) \in (S \circ R)$ poiché $R(a,b)$ e $S(b,c)$
- $(b,c) \in (S \circ R)$ poiché $R(b,b)$ e $S(b,c)$
- $(b,b) \in (S \circ R)$ poiché $R(b,d)$ e $S(d,b)$
- $(c,b) \in (S \circ R)$ poiché $R(c,a)$ e $S(a,b)$
- $(c,d) \in (S \circ R)$ poiché $R(c,a)$ e $S(a,d)$
- $(a,b) \in (S \circ R)$ poiché $R(d,a)$ e $S(a,b)$
- $(d,d) \in (S \circ R)$ poiché $R(d,a)$ e $S(a,c)$

Ricaviamo quindi che $(R \circ S) = \{(a,c),(b,c),(b,b),(c,b),(c,d),(a,b),(d,d)\}$

Il calcolo di una composizione tra relazioni in **forma grafica**, risulta la *più intuitiva e diretta* tra le tre:



$$(R \circ S) = \{(a_1,c_1),(a_1,c_2),(a_1,c_3)\}$$

Infine, il calcolo di una composizione tra relazioni in **forma matriciale** risulta come il prodotto tra righe della prima matrice e le colonne della seconda matrice, dunque un normale **prodotto tra matrici**

$$M_{(R \circ S)} = M_R \times M_S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

3.5 Relazioni transitive

Una relazione viene detta **transitiva** quando, considerando **tre elementi** a, b e c appartenenti $A \times A$, esiste una relazione tra a ed b, dunque $R(a, b)$, ed una relazione tra b ed c, dunque $R(b, c)$, da cui possiamo dedurre logicamente che esista anche la relazione $R(a, c)$.

Definition 12

Una relazione $R \subseteq A \times A$ viene detta transitiva se per ogni $a, b, c \in A$ vale che se $R(a, b)$ e $R(b, c)$ allora $R(a, c)$

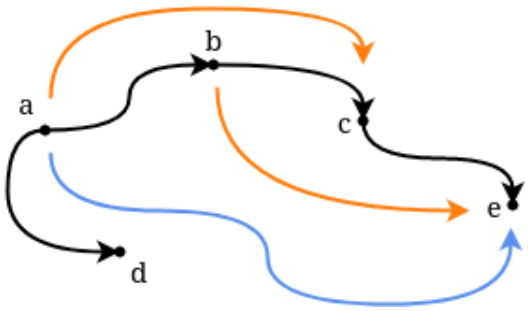
Esempi:

- La relazione $R(a, b)$ se e solo se *"a è padre b"* non è transitiva (es: se Marco è padre di Irene e Andrea è padre di Marco, non è vero che Andrea è padre di Irene)
- La relazione $n < m$ dove $n, m \in \mathbb{N}$ è transitiva (es: se $3 < 5$ e $5 < 18$, è vero che $3 < 18$)
- La relazione di successore $R = \{(n, n+1) \mid n \in \mathbb{N}\}$ non è transitiva (es: se $R(4, 5)$ e $R(5, 6)$, non è vero che $R(4, 6)$.
- La relazione $R = \{(1, 2), (1, 3), (2, 2), (2, 5), (5, 2), (3, 4)\}$ su $A = \{1, 2, 3, 4, 5\}$ non è transitiva (es: con $a = 1$, $b = 3$ e $c = 4$ esiste $(1, 3)$, $(3, 4)$ ma non $(1, 4)$)

ATTENZIONE: è necessario sottolineare che la definizione di transitività è espressa con un **quantificatore universale** (dunque deve valere **per ogni** $a, b, c \in A$) seguito da un condizionale (se x, allora y). Tuttavia, questa definizione **non richiede** che una relazione R soddisfi che per ogni $a, b, c \in A$ valgano $R(a, b)$ e $R(b, c)$, bensì è richiesto che **se** valgono sia $R(a, b)$ e $R(b, c)$, allora deve valere anche $R(a, c)$.

3.6 Chiusura transitiva

La relazione R^1 rappresentata con **frecce NERE** nel digrafo seguente **non è transitiva**: valgono $R^1(a,b)$ e $R^1(b,c)$, ma non vale $R(a,c)$ ed analogamente $R^1(b,c)$ e $R^1(c,e)$, ma non vale $R(b,e)$. Si noti che il fatto che valga $R^1(a,d)$ ma non ci siano frecce uscenti da d **sia ininfluente** per determinare se la relazione sia transitiva o non (ricordiamo che si cerca la transitività solo se valgono sia $R^1(a,d)$ sia una relazione $R^1(d,x) \,|\, x \in A \times A$ affinché si possa andare a verificare se valga $R^1(a,x)$)



Consideriamo ora la relazione R^2 rappresentata dalla **righe NERE** e dalla **righe ARANCIONI**, ottenuta cercando di rimediare ai due controesempi precedenti all transività di R^1. Tuttavia, anche questa relazione **non è transitiva**: valgono sia $R^2(a,c)$ (freccia arancione) che $R^2(c,e)$ ma non vale $R^2(a,e)$ (nè frecce nere, nè frecce arancioni).

La relazione R^3 rappresentata dalle frecce **NERE, ARANCIONI e AZZURRE**, al contrario di R^1 e R^2, **è transitiva**. Infatti, essa viene ricavata rimediando al controesempio visto sopra alla transività di R^2, poiché ora valgono sia $R^3(a,c)$ (freccia arancione), sia $R^3(c,e)$ (freccia nera) e sia $R^3(a,e)$ (freccia azzurra).

Con R^3 abbiamo ottenuto un'**estensione della relazione iniziale**, nel senso che $R^1 \subseteq R^3$, che ha la caratteristica di essere anche transitiva. Inoltre, la relazione R^3 è **la più piccola relazione transitiva che estende $\mathbf{R^1}$** (dunque ottenuta "aggiungendo il minor numero di frecce"). Questa tipologia di estenzione viene chiamata **chiusura transitiva** di una relazione:

Definition 13. Chiusura transitiva di una relazione

Chiamiamo **chiusura transitiva di R** la più piccola relazione transitiva che estende R, ossia la relazione R^T tale che:

- $R \subseteq R^T$
- R^T è transitiva
- Se S estende R ed è transitiva, allora $R^T \subseteq S$

Esempi:

- Data una mappa di strade a senso unico che collegano città ($R(a,b)$ se e solo se c'è una strada che parte dalla città a e arriva alla città b), la chiusura transitiva contiene tutte e sole le coppie di città (x,y) tali che esiste un itinerario che porta da x a y.

Consideriamo ora una relazione R su A, dove $a, b \in A$. Diciamo che esiste un **cammino** di lunghezza $\ell \geq 1$ da a verso b se esistono elementi $x_1, x_2, ..., x_{l-1}$ in A tali che $R(a, x_1), R(x_1, x_2), ..., R(x_{\ell-1}, b)$. Ciò include anche il **caso particolare** in cui due punti a e b tali che $R(a, b)$, dunque sono già in relazione tra loro. In questo caso, si può correttamente affermare che **esiste** un cammino di lunghezza $\ell = 1$ da a verso b e la condizione "esistono $x_1, x_2, ..., x_{\ell-1}$" è **vera a vuoto**.

Definition 14. Relazione di raggiungibilità

Data $R \subseteq A \times A$ consideriamo la **relazione di raggiungibilità** (anche detta *connettività*), definita come:

$$R^c = \{(a, b) \in A \times A \mid \textit{esiste un cammino di lunghezza } \ell \geq 1 \textit{ da } a \textit{ verso } b\}$$

Esempio:

- Consideriamo la relazione $R = \{(1, 2), (2, 3), (3, 4)\}$ su $A = \{1, 2, 3, 4\}$. Proviamo a **estendere** R in modo da ottenere una relazione transitiva. Dato che $(1, 2) \in R$ e $(2, 3) \in R$, devo aggiungere la coppia $(1, 3)$. Dato che $(2, 3) \in R$ e $(3, 4) \in R$, devo aggiungere la coppia $(2, 4)$. Chiamiamo R^{++} la relazione ottenuta aggiungendo queste coppie, ossia $R^{++} = R \cup \{(1, 3), (2, 4)\}$. Tuttavia, R^{++} **non è transitiva**: infatti $(1, 3) \in R^{++}$ e $(3, 4) \in R^{++}$ ma $(1, 4) \notin R^{+}$.

  Aggiungiamo la coppia $(1, 4)$. Chiamiamo R^{+++} la relazione così ottenuta, ossia $R^{+++} = R \cup R^{++} \cup \{(1, 4)\}$. R^{+++} **è transitiva**: per tutti i possibili casi in cui si verifica la pre-condizione della definizione di transività è vera anche la conclusione.

  Ripercorrendo quanto appena fatto, osserviamo che $\mathbf{R^{++} = R \cup (R \circ R)}$. Infatti, per definizione, $(R \circ R)$ contiene tutte e sole le coppie (a, c) tali che esiste un $b \in A$ tale che $(a, b), (b, c) \in R$. Questo è il caso per la coppia $(1, 3)$ (poiché esistono $(1, 2)$ e $(2, 3)$ in R) e per la coppia $(2, 4)$ (poiché esistono $(2, 3)$ e $(3, 4)$ in R).

  Analogamente, $\mathbf{R^{+++} = R \cup (R \circ R) \cup (R \circ (R \circ R))}$. Sappiamo che, per definizione stessa, $(x, y) \in (R \circ R) \circ R$ se e solo se esiste $z \in A$ tale che $(x, z) \in (R \circ R)$ e $(z, y) \in R$. Questo è il caso solo per la coppia $(1, 4)$: infatti $(1, 3) \in R \circ R$ e $(3, 4) \in R$.

In base all'esempio precedente, notiamo che la chiusura transiva di una relazione R è **strettamente collegata** con le relazioni ottenute **componendo R con se stessa**. Data R, definiamo quindi una **successione di relazioni** come

$$R^1 = R \textit{ e } R^{n+1} = R^n \circ R \textit{ con } n \geq 1$$

Volendo considerare anche l'**unione di tutte le $\mathbf{R^n}$**, possiamo considerare l'unione

$$R^\infty = \bigcup_{n \in \mathbb{N}} R^n$$

Si ricorda che una coppia (x, y) appartiene all'**unione infinita** precedente se e solo se esiste un $n \in N$ tale che $(x, y) \in R^n$. Nelle sezioni successive, dimostreremo che R^c e R^∞ **coincidono entrambi** con la **chiusura transitiva di R**.

3.7 Relazioni di equivalenza e partizioni

Una **relazione di equivalenza** è una **generalizzazione** di alcune proprietà fondamentali della relazione di identità. Consideriamo la relazione di identità numerica su N. Ovviamente gode delle seguenti proprietà:

- Per ogni $n \in N$ abbiamo $n = n$
- Per ogni $n, m \in N$ abbiamo che se $n = m$ allora $m = n$
- Per ogni $n, m, q \in N$ abbiamo che se $n = m$ e $m = q$ allora $n = q$

Notiamo come queste tre caratteristiche corrispondono esattamente alle tre proprietà delle relazioni precedentemente viste

Definition 15. Relazione di equivalenza

Una relazione R su un insieme A viene detta **relazione di equivalenza** se e solo se gode delle seguenti tre proprietà:

- **Riflessività**: per ogni $a \in A$ esiste $R(a, a)$
- **Simmetria**: per ogni $a, b \in A$ se $R(a, b)$ allora $R(b, a)$
- **Transitività**: per ogni $a, b, c \in A$ se $R(a, b)$ e $R(b, c)$ allora $R(a, c)$

Classi di equivalenza

Consideriamo gli interi N e stabiliamo $R(a, b)$ se e solo se a e b hanno lo stesso resto nella divisione per 2. Per esempio $R(-4, 18)$, poiché entrambi hanno resto 0 nella divisione per 2, mentre $(-8, 3) \notin R$ poiché hanno resto 1. Possiamo facilmente verificare come si tratti di una **relazione di equivalenza**, poiché rispetta tutte e tre le proprietà necessarie.

Dato che i possibili resti della divisione per 2 di un intero sono 0 e 1, è facile osservare che **ogni intero** sarà in relazione R con 0 oppure con 1! Possiamo quindi definire un intero arbitrario p considerando l'**insieme degli interi in relazione R con p**:

$$[p]_R = \{q \in N \mid R(p, q)\}$$

Questa viene detta la **classe di equivalenza di p modulo R**. Osserviamo facilmente che per ogni intero p, si ha $p \in [0]_R$ oppure $p \in [1]_R$ a seconda che p sia **pari** o **dispari**, dunque a seconda se abbia resto 0 od 1 una volta diviso per 2.

Visto in un altro modo, possiamo dire che presi due interi p e q, le loro classi di equivalenza o **coincidono** oppure sono completamente **disgiunte**.

- Se p e q sono **pari**, allora $[p]_R = [q]_R = [0]_R$
- Se p e q sono **dispari**, allora $[p]_R = [q]_R = [1]_R$,
- Se p e q sono uno pari e l'altro dispari, allora $[p]_R \cap [q]_R = \emptyset$

Definiamo quindi il seguente teorema:

Theorem 7. Classe di equivalenza

Sia $R \subseteq A \times A$ una relazione di equivalenza. Per $a \in A$ definiamo la **classe di equivalenza di A** come

$$[a]_R = \{b \in N \mid R(a,b)\}$$

Dove:

- Per ogni $a \in A$ abbiamo $[a]_R \neq \emptyset$
- Per ogni $a, b \in A$ abbiamo che $[a]_R \cap [b]_R = \emptyset$ oppure $[a]_R = [b]_R$

Partizioni

Definiamo ora R sugli interi N ponendo $R(a,b)$ se e solo se a e b hanno lo stesso resto nella divisione per 3. Come sopra si dimostra che è un **relazione di equivalenza**. In questo caso i resti possibili sono tre: 0, 1, 2. Come per l'esempio precedente, si osserva facilmente che per ogni intero p si ha $R(p,0)$, $R(p,1)$ o $R(p,2)$ In termini di classi di equivalenza questo significa che esistono solo le **tre classi di equivalenza**: $[0]_R$, $[1]_R$, $[2]_R$ contenenti.

La costruzione si generalizza facilmente fissando un intero n qualunque e ponendo $R(a,b)$ se e solo se a e b hanno lo stesso resto nella divisione per n. In questo caso abbiamo **classi di equivalenza** e determinano una **partizione di N**.

Definition 16. Partizione

Una **partizione** di un insieme A è una famiglia $\{C_i \mid i \in I\}$ di **insiemi non vuoti** $C_i \subseteq A$, dove I è un **insieme di indici qualunque**, tali che:

- Per ogni $a \in A$ esiste un $i \in I$ tale che $a \in C_i$
- Per $i, j \in I$ se $i \neq j$ allora $C_i \cap C_j = \emptyset$ (ossia le classi in I sono due a due disgiunte)

Si osserva che $\bigcup_{i \in I} C_i \subseteq A$ dato che ogni C_i è sottoinsieme di A, mentre dal primo punto della definizione di partizione notiamo che invece che $A \subseteq \bigcup_{i \in I} C_i$. Di conseguenza possiamo affermare che $A = \bigcup_{i \in I} C_i$

Theorem 8

Se $\{C_i : i \in I\}$ una partizione di A, allora la relazione $R \subseteq A \times A$ definita ponendo $R(a,b)$ se e solo se esiste un $i \in I$ tale che $a, b \in C_i$ è una relazione di equivalenza su A.

3.8 Relazioni d'ordine

Una **relazione d'ordine** è una relazione che gode di alcune proprietà fondamentali della relazione di ordine numerico minore o uguale applicata sull'insieme dei naturali ($\leq \mathbb{N}$). Ovviamente, tale relazione gode delle seguenti proprietà:

- Per ogni $n \in N$, $n \leq n$
- Per ogni $n, m \in N$ se $n \leq m$ e $m \leq n$, allora $m = n$
- Per ogni $n, m, q \in N$ se $n \leq m$ e $m \leq q$, allora $n \leq q$
- Per ogni $n, m \in N$ vale $n \leq m$ oppure $m \leq n$

Notiamo come queste quattro caratteristiche corrispondono esattamente a quattro proprietà delle relazioni precedentemente viste

Definition 17. Relazione di ordine totale

Una relazione R su un insieme A viene detta **relazione di ordine totale** se e solo se gode delle seguenti quattro proprietà:

- **Riflessività**: Per ogni $a \in A$ esiste $R(a, a)$
- **Anti-simmetria**: Per ogni $a, b \in A$ se $R(a, b)$ e $R(b, a)$ allora $a = b$
- **Transitività**: Per ogni $a, b, c \in A$ se $R(a, b)$ e $R(b, c)$ allora $R(a, c)$
- **Totalità**: Per ogni $a, b \in A$ vale $a \leq b$ oppure $b \leq a$. Se questa proprietà non è valida ma le altre tre si, allora si tratta di un **ordine parziale**

Esempio con dimostrazione

Poniamo $R(a, b)$ se e solo se a è **identico** a b ***oppure*** a è **padre** di b. Si tratta di una relazione d'ordine?

- **Verifica della riflessività**

  Considerando un essere umano a, vale $R(a, a)$ poiché a è identico a se stesso

- **Verifica dell'anti-simmetria**

  Considerando due esseri umani a e b, supponiamo valga che $R(a, b)$ e $R(b, a)$

  - **Caso 1**: Se abbiamo che $R(a, b)$ perché $a = b$ e $R(b, a)$ perché $b = a$, la prima condizione è soddisfatta poiché a è identico a b, dunque vale l'anti-simmetria
  - **Caso 2**: Se abbiamo che $R(a, b)$ perché $a = b$ e $R(b, a)$ perché b è padre di a, otteniamo un caso impossibile, poiché b dovrebbe essere padre di se stesso
  - **Caso 3**: Se abbiamo che $R(a, b)$ perché a è padre di b e $R(b, a)$ perché $a = b$, otteniamo un caso impossibile, poiché a dovrebbe essere padre di se stesso
  - **Caso 4**: Se abbiamo che $R(a, b)$ perché a è padre di b e $R(b, a)$ perché b è padre di a, otteniamo un caso impossibile, poiché a dovrebbe essere padre di se stesso

- **Verifica della trasitività**

  Considerando tre esseri umani a, b e c, supponiamo valga che $R(a,b)$, $R(b,c)$

  - **Caso 1**: Se abbiamo che $R(a,b)$ perché $a = b$ e $R(b,c)$ perché $b = c$, allora vale $R(a,c)$ poiché $a = c$
  - **Caso 2**: Se abbiamo che $R(a,b)$ perché $a = b$ e $R(b,c)$ perché b è padre di a, allora vale $R(a,c)$ poiché a è padre di c
  - **Caso 3**: Se abbiamo che $R(a,b)$ perché a è padre di b e $R(b,c)$ perché $b = c$, allora vale $R(a,c)$ poiché a è padre di c
  - **Caso 4**: Se abbiamo che $R(a,b)$ perché a è padre di b e $R(b,c)$ perché b è padre di c, otteniamo che a è nonno di c, dunque la transitività non persiste poiché a non è padre di c

Possiamo concludere, dunque, che **non** si tratti di una relazione d'ordine. Nel caso in cui, invece, la seconda condizione imposta fosse stata "a è antenato di b" allora avremmo potuto definire tale relazione come relazione d'ordine

Immersioni tra ordini

Tutti gli ordini sono inclusioni insiemistiche: è possibile mappare ogni elemento di un **primo ordine** in un elemento del **secondo** in modo tale che elementi distinti siano mappati in elementi distinti (iniettività) e in modo tale da preservare le relazioni d'ordine tra gli elementi. Dunque, se un elemento precede l'altro nel primo ordine la sua immagine deve precedere l'immagine dell'altro nel secondo ordine.

Definition 18. Immersione tra ordini

Sia $\leq$ un ordine parziale su un insieme X e sia $\leq^*$ un ordine parziale su un insieme X^*. Definiamo la funzione $f : X \to X^*$ come **immersione** di $(X, \leq)$ in $(X^*, \leq^*)$ se:

- È iniettiva
- Vale $f(x) \leq^* f(y)$ se e solo se $x \leq y$

Inoltre, possiamo definire il seguente teorema:

Theorem 9

Sia X un insieme e $\leq$ una relazione d'ordine su X. Esiste una immersione in $\mathcal{P}(X)$ ordinato da $\subseteq$

Dimostrazione

Definiamo la funzione $f : X \to \mathcal{P}(X)$ come $f = \{y \in X \mid y \leq x\}$

- **Verifica dell'iniettività**

  Siano $x, y \in X$ tali che $f(x) = f(y)$. Dato che $x \leq x$ e $y \leq x$ abbiamo che $x \in f(x)$ e $y \in f(y)$. Dunque, $x \in f(y)$ e di conseguenza $x \leq y$, mentre $y \in f(x)$ e di conseguenza $y \leq x$. Per anti-simmetria, otteniamo che $x = y$.

- **Verifica dell'immersione** Sia $x \leq y$. Se $z \in f(x)$ allora $z \leq x$ e per transitività abbiamo che $z \leq y$, dunque $z \in f(y)$. Questo dimostra $f(x) \subseteq f(y)$. Supponiamo ora che $f(x) \subseteq f(y)$ e dimostriamo che $x \leq y$. Dato che $x \in f(x)$, per riflessività di $\leq$, abbiamo che $x \in f(y)$ e dunque $x \leq y$.

Abbiamo dunque dimostrato che gli ordini di tipo $(\mathcal{P}(X), \subseteq)$ contengono una coppia di **qualsiasi insieme ordinato**

3.9 Estenzioni totali di ordini parziali

Gli **ordni totali** permettono di **confrontare** gli elementi di un insieme finito in modo del tutto *lineare*, partendo dal minimo e procedendo seguendo l'ordine. Al contrario, gli **ordini parziali** sono più complicati poiché è necessario seguire i diversi **"percorsi" ramificati** che collegano i punti. Risulta dunque interessante osservare che **è sempre possibile estendere un ordine parziale a un ordine totale** sullo stesso insieme.

Theorem 10. Estenzione totale di un ordine parziale

Sia $A = \{a_1, a_2, ..., a_n\}$ un insieme finito ordinato da una relazione R di **ordine parziale**. Allora esiste una relazione $R^* \subseteq A \times A$ che è un **ordine totale** ed estende R, ossia $\forall a, b \in A$, se $R(a, b)$ allora $R^*(a, b)$.

Dunque, sia $A = \{a_1, a_2, ..., a_n\}$ relazione di ordine parziale. Siano $a, b \in A$ due elementi **incomparabili** relativamente a R, ossia tali che $(a, b) \notin R$ e $(b, a) \notin R$. Esiste una relazione $R' \subseteq A \times A$ tale che:

- $R \subseteq R'$
- $(a, b) \in R'$

Dimostrazione

Definiamo la relazione R' aggiungendo la coppia (a, b) e tutte le coppie (x, y) per x, y tale che $R(x, a)$ e $R(b, y)$. Stiamo quindi considerando **tutti gli elementi minori o uguali ad a** e vogliamo **imporre** che essi (nella nuova relazione R') siano **tutti minori o uguali** a **tutti gli elementi maggiori o uguali a b**.

In termini insiemistici poniamo:

$$X = \{x \in A \,|\, R(x, a)\} \texttt{ ossia tutti i minori o uguali ad a}$$
$$Y = \{y \in A \,|\, R(b, y)\} \texttt{ ossia tutti i maggiori o uguali a b}$$

Andiamo quindi a definire $R' : R \cup (X \times Y)$ e proviamo a dimostrare che R' è un ordine parziale su A.

Possiamo facilmente affermare che $X \cap Y = \emptyset$, poiché altrimenti avremmo un elemento $x \in X \cap Y$ per cui varrebbe sia $R(x, a)$ sia $R(b, x)$ (ossia un elemento sia inferiore o uguale ad a sia maggiore o uguale a b) dunque transitivamente varrebbe $R(a, b)$, cosa che non può accadere poiché a e b sono **incomparabili**. Inoltre, possiamo affermare che R' sia riflessiva poiché R è riflessiva.

Supponendo che $R'(x,y)$ e $R'(y,x)$, possiamo affermare che ciò possa accadere solo se $x = y$. Possiamo dire ciò poiché da $R'(x,y)$ otteniamo che $R(x,y)$ oppure che $(x,y) \in X \times Y$, mentre da $R'(y,x)$ otteniamo che $R(y,x)$ oppure che $(y,x) \in X \times Y$. A questo punto avremmo quattro casi possibili:

- **Caso 1**: se $(x,y) \in X \times Y$ e $(y,x) \in X \times Y$ allora avremmo che $x \in X \cap Y$, cosa che come abbiamo stabilito non può accadere
- **Caso 2**: se $R(x,y)$ e $(y,x) \in X \times Y$ allora avremmo che $y \in X$ e dunque $R(y,a)$. L'esistenza di questa relazione, però, implicherebbe anche l'esistenza di $R(x,a)$, da cui consegue che $x \in X$. La condizione $(y,x) \in X \times Y$ implica anche che $x \in Y$, dunque avremmo $x \in X \cap Y$, cosa che come abbiamo stabilito non può accadere.
- **Caso 3**: se $(x,y) \in X \times Y$ e $R(y,x)$, avremmo che da $x \in X$ segue $R(x,a)$, mentre da $y \in Y$ segue $R(b,y)$. Tuttavia, da $R(x,a)$, $R(b,y$ e $R(y,x)$ seguirebbe per transitività che $R(b,a)$, cosa che non può accadere poichè a e b devono essere non comparabili.
- **Caso 4**: se $R(x,y)$ e $R(y,x)$ allora abbiamo che $x = y$, poiché R è antisimmetrica

  Cerchiamo ora, invece, di dimostrare la transitività di R'. Supponiamo che $R'(x,y)$ e $R'(y,z)$, da cui otteniamo che $R(x,y)$ oppure $(x,y) \in X \times Y$ e che $R(y,x)$ oppure $(y,x) \in X \times Y$. Ancora una volta, quindi, abbiamo quattro casi da analizzare:

  - **Caso 1**: se $(x,y) \in X \times Y$ e $(y,z) \in X \times Y$ allora abbiamo che $y \in X \cap Y$, cosa che abbiamo stabilito non può accadere.
  - **Caso 2**: se $(x,y) \in X \times Y$ e $R(y,z)$ allora abbiamo che $y \in Y$, dunque $R(b,y)$. Tuttavia, da $R(y,z)$ abbiamo anche che $y \in X$, dunque $y \in X \times Y$, cosa che non può accadere.
  - **Caso 3**: se $R(x,y)$ e $(y,z) \in X \times Y$ allora abbiamo che $y \in X$, dunque $R(y,a)$. Per transitività, avremmo anche che $R(x,a)$, dunque $(x,z) \in X \times Y$ e dunque $x \in X$, contraddicendo $X \cap Y = \emptyset$
  - **Caso 4**: se $R(x,y)$ e $R(y,z)$ allora abbiamo $R(x,z)$ per transitività di R, dunque abbiamo anche $R'(x,z)$ perchè $R' \subseteq R$

3.10 Ordini totali e successioni monotone

Supponiamo di scegliere a caso una sequenza di k numeri interi distinti, in **ordine arbitrario** $(a_1, ..., a_k)$. Siamo sicuri di trovare in essa un numero a_i tale che esiste un successivo a_j (quindi $i < j$) che è maggiore di a_i oppure minore di a_j . Siamo **sicuri** di poter trovare $1 \leq i < j < h \leq k$ tali che $a_i < a_j < a_h$ oppure $a_i > a_j > a_h$ o di poter trovare una successione di questo tipo di lunghezza maggiore?

In generale, ci stiamo quindi chiedendo se possiamo trovare "sotto-successioni" strettamente crescenti o strettamente decrescenti all'interno della successione casuale di partenza.

Il seguente teorema ci dice che se vogliamo essere **sicuri** di trovare, all'interno di una successione arbitraria di numeri naturali, sotto-successioni crescenti o decrescenti lunghe $n + 1$, è sufficiente scegliere $n^2 + 1$ numeri.

Theorem 11. Successioni monotone

Sia $n \leq 1$ e sia $(x_1, ..., x_{n^2+1})$ una **successione di elementi distinti** scelti in insieme X su cui $\preceq$ è un ordine totale. Allora esiste una sotto-successione strettamente crescente o strettamente decrescente lunga $n + 1$.

N.B.: X non è necessariamente un insieme di numeri ma è un insieme arbitrario, mentre la relazione denotata con $\preceq$ è un arbitrario ordine totale su X e le sotto-successioni sono ordinate rispetto ad esso.

Denotiamo con $\prec$ l'**ordine stretto** ottenuto da $\preceq$ (infatti $x \prec y$ se e solo se $x \preceq y$ ma $x \neq y$). Una **sotto-successione strettamente crescente** di lunghezza $l \leq n^2 + 1$ è una sequenza $(x_{a1}, x_{a2}, ..., x_{al})$ con $x_{a1} \prec x_{a2} \prec ... \prec x_{al}$, per qualche $a_1 < ... < a_l$ in $\{1, ..., n^2 + 1\}$. Analogamente, una **sotto-successione strettamente decrescente** di lunghezza $l \leq n^2 + 1$ è una sequenza $(x_{a1}, x_{a2}, ..., x_{al})$ con $x_{al} \prec x_{al-1} \prec ... \prec x_{a1}$, per qualche $a_1 < ... < a_l$ in $\{1, ..., n^2 + 1\}$.

3.11 Cicli ed elementi minimali di un ordine

Considerando un **ordine parziale** R su un insieme A, possiamo affermare con certezza che **R non ha cicli** eccetto quelli di tipo $R(a, a)$. Ricordiamo che un **ciclo** è un cammino che inizia e finisce nello stesso punto, ossia:

$$R(a_1, a_2), R(a_2, a_3), ..., R(a_{m-1}, a_m), R(a_m, a_1)$$

o scritto più comodamente con il modo alternativo di scrivere una relazione:

$$a_1 R a_2 R a_3 R ... R a_{m-1} R a_m R a_1$$

Per transitività di R, abbiamo che $R(a_1, a_2)$ e $R(a_2, a_3)$ implicano che $R(a_1, a_3)$. Analogamente, l'esistenza di $R(a_3, a_4)$ implica che $R(a_1, a_4)$. Percorrendo l'intero ciclo, dunque, otterremo che $R(a_1, a_m)$ e sappiamo inoltre che $R(a_m, a_1)$. Per anti-simmetria di R, questo indica che $a_1 = a_m$, cosa che ci permette di affermare con certezza che **non esistono cicli** di lunghezza $m > 1$ (i cicli di lunghezza 1 esistono poiché R è riflessiva, dunque esiste $R(a, a)$ per ogni $a \in A$).

Proposition 12

In un ordine (parziale) esistono **solo cicli di lunghezza 1**, ossia di tipo (a, a).

Inoltre, possiamo dire che in un ordine parziale su un insieme finito **non esiste necessariamente un elemento minimo**, inteso come un elemento $a \in A$ tale che per ogni $b \in A$ vale $R(a, b)$.

Consideriamo la relazione R su 1, 2, 3, 4, 5 definita come segue:

$$\{(1,3), (3,4), (4,5), (1,4), (1,5), (2,3), (2,4), (2,5), (1,1), (2,2), (3,3), (4,4), (5,5)\}$$

Nell'ordine qui sopra **non esistono elementi minimi**, ma esistono elementi **"quasi minimi"**, nel senso che non esistono altri elementi più piccoli di loro. Ciò vale per gli elementi 1 e 2, dato che in R non c'"e nessuna coppia di tipo $(x, 1)$ con $x \neq 1$ o di tipo $(x, 2)$ con $x \neq 2$.

Proposition 13

Un ordine (parziale) non ha necessariamente un **elemento minimo**.

Invece, ogni ordine parziale su un insieme finito ha un **elemento minimale**, definito come un elemento $a \in A$ per cui per ogni $b \in A\{a\}$ **non** vale $R(b, a)$. Consideriamo un **cammino di lunghezza massima in A**, ossia una scelta di elementi $a_1, ..., a_m$ in A tali che $a_1 R a_2 R ... R a_{m-1} R a_m$ e non esista un cammino di lunghezza più grande.

Si osserva allora facilmente che, prendendo un $a \in A$ diverso da tutti gli $a_1, ..., a_m$, non può valere $R(a, a_1)$, altrimenti **avremmo un cammino più lungo** di quello scelto sopra, ossia $aRa_1Ra_2R...Ra_{m-1}Ra_m$.

Inoltre, notiamo che prendendo un a_i con $2 \leq i \leq m$ non può valere $R(a_i, a_1)$. Se valesse, avremmo che il cammino contiene un **ciclo**, cosa che abbiamo detto essere **impossibile** se non di lunghezza 1.

Proposition 14

Un ordine (parziale) ha necessariamente (almeno) un elemento minimale.

3.12 Dimostrazione per induzione

Siamo ora pronti a dare una **dimostrazione alternativa** dell'estendibilità di ogni ordine parziale su un insieme finito a un ordine totale.

La nostra tesi è: Ogni ordine parziale su un insieme finito si può estendere a un ordine totale sullo stesso insieme. Riformulandola in termini più espliciti, possiamo dire che:

Proposition 15

Per ogni possibile cardinalità n, per ogni insieme A di cardinalità n, per ogni ordine parziale R su A, esiste un ordine totale R^* tale che $R \subseteq R^*$

Proponiamo il seguente argomento per stabilire la tesi:

- **Caso Base**: Dimostriamo che la tesi vale per insiemi di cardinalità $n = 1$. Consideriamo un insieme generico di questo tipo, ossia $A = a$. L'**unico ordine parziale** R su un insieme di questo tipo è $R = \{(a, a)\}$, che corrisponde anche ad un **ordine totale**. La tesi quindi è vera per $n = 1$, dove l'estensione totale di R (ossia R') è **R stessa**.

- **Passo induttivo**: Assumiamo ora che la tesi sia vera fino a insiemi di cardinalità n, dove n è un **generico intero maggiore di 1**. Dimostriamo che in questo caso possiamo stabilire la tesi anche per insiemi di cardinalità $n + 1$.

  A questo scopo consideriamo un generico insieme A con $n + 1$ elementi. Come osservato precedentemente, A contiene **almeno un elemento minimale**. Sia a un tale minimale. Escludendo a dall'insieme A, otteniamo l'insieme $A \backslash a$ composto da n elementi. Inoltre la relazione R^- su $A \setminus a$, ottenuta cancellando da R tutte le coppie che contengono a, è un **ordine parziale**.

  Tuttavia, abbiamo assunto di saper dimostrare la tesi per insiemi di cardinalità n. In particolare possiamo farlo per l'ordine R^- sull'insieme $A \setminus a$. Esiste dunque un **ordine totale** R_R^- su $A \setminus a$ che **estende** R^-. Definiamo quindi un ordine R_T su A come:

  $$R_T = R_T^- \cup \{(a, x) : a \in A\}$$

  Poiché è facilmente dimostrabile che R_T sia un ordine totale su A che estende R, possiamo affermare che **la tesi vale** per ogni cardinalità $n \geq 1$

Capitolo 4

Induzione

Come abbiamo visto alla fine del capitolo precedente, una **dimostrazione per induzione** è composta da Come abbiamo visto una dimostrazione per induzione consta di due parti fondamentali:

Definition 19. Principio di Induzione

Per stabilire una tesi di tipo **universale**, ossia che per ogni $n \geq 1$ vale una certa proprietà $P(n)$, è sufficiente stabilire **i due punti seguenti**:

1. **Caso base**: Verifichiamo/dimostriamo che la proprietà P vale per $n = 1$.
2. **Passo induttivo**: Consideriamo un generico $n \geq 1$ e, dando per assunto che la proprietà P valga per n, dimostriamo che vale per $n + 1$. Dunque, dimostriamo che vale l'implicazione:

$$\texttt{Se } P(n) \texttt{ allora } P(n+1)$$

Il **Principio di Induzione** ammette anche una **formulazione insiemistica**, che otteniamo considerando un sottoinsieme X **non vuoto** di $N = \{1, 2, 3, 4, ...\}$

Definition 20. Principio di Induzione (in Insiemistica)

Se X soddisfa le due seguenti proprietà:

- $1 \in X$
- Per un generico $n \geq 1$ vale $n \in X$ allora vale anche $n + 1 \in X$

è possibile concludere che $\mathbb{N} \subseteq X$, ossia X contiene tutti i numeri naturali

Il Principio di Induzione può "giustificarsi" un po' più rigorosamente ricorrendo a un principio decisamente più intuitivo. Consideriamo un arbitrario $A \subseteq N$ **non vuoto** da cui possiamo intuire abbastanza facilmente che A possiede un **elemento minimo** (ricordiamo che per elemento minimo si intende un $a \in A$ tale che per ogni altro $b \in A$, non vale $b < a$).

Chiamiamo questo principio il **Principio del Minimo Numero (o Principio del Buon Ordinamento)**. Tale principio ci permette (per comodità di formulazione insiemistica) di giustificare il Principio di Induzione.

Definition 21. Principio del Minimo Numero

Ogni sottoinsieme non vuoto dei numeri naturali ha **un minimo**.

Consideriamo un insieme $X \subseteq N$ che soddisfa le due proprietà, ossia $1 \in X$ e, per un generico $n \geq 1$, se $n \in X$ allora $n+1 \in X$.

Supponiamo per assurdo che non valga la conclusione del Principio di Induzione: ossia supponiamo che non è vero che $N \subseteq X$. Dunque l'insieme $A = (N \setminus X)$ è un **sottoinsieme non-vuoto di N**. Per il Principio del Minimo Numero, A contiene un minimo, che chiameremo m. Tale m non può essere 1, dato che $1 \in X$ e $m \notin X$. Dunque, $m > 1$ e pertanto $m-1 \geq 1$ (dunque m è ancora un numero naturale). Inoltre dato che m è scelto come **il minimo in N ma non in X**, necessariamente $m-1 \in X$.

Tuttavia, X soddisfa la seconda proprietà, dunque se $m-1 \in X$ allora $m \in X$ (poiché $m-1+1 \in X$). Abbiamo raggiunto una contraddizione: $m \in X$ e $m \notin X$, dimostrando quindi la validità del Principio di Induzione.

Possiamo quindi generalizzare la precedente definizione di principio di induzione in modo che valga per un qualsiasi caso a partire da un valore k fino ad un valore n

Definition 22. Principio di Induzione da k

Per stabilire una tesi di tipo **universale**, ossia che per ogni $n \geq k$ vale una certa proprietà $P(n)$, è sufficiente stabilire **i due punti seguenti**:

1. **Caso base**: La proprietà P vale k
2. **Passo induttivo**: Consideriamo un generico $n \geq k$ e, dando per assunto che la proprietà P valga per n, dimostriamo che vale per $n+1$. Dunque, dimostriamo che vale l'implicazione:

$$\texttt{Se } P(n) \texttt{ allora } P(n+1)$$

4.1 Esempi di induzione

Esempio 1

Dimostrare che per $n \geq 1$ vale la seguente proprietà:

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

- **Caso Base**: $1 = \frac{1(1+1)}{2}$ è vera, non serve dimostrarlo

- **Passo induttivo**: Dando per vera

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

per principio di induzione affermiamo che

$$1 + 2 + 3 + ... + n + (n+1) = \frac{(n+1)((n+1)+1)}{2}$$

Notiamo che il caso $n+1$ **racchiude al suo interno** il caso n.

$$\underbrace{1 + 2 + 3 + ... + n}_{\textbf{Caso n}} + (n+1)$$

Possiamo quindi applicare l'**ipotesi induttiva** a questo caso, sostituendo parte della forma estesa con la proprietà di n:

$$\underbrace{1 + 2 + 3 + ... + n}_{\textbf{Caso n}} + (n+1) = \underbrace{\frac{n(n+1)}{2}}_{\textbf{Caso n}} + (n+1)$$

A questo punto otteniamo un'equazione verificabile applicando semplici regole di manipolazione algebrica, dunque possiamo dire che **la proprietà è vera per n $\geq$ 1**:

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)((n+1)+1)}{2}$$

Esempio 2

Considerando la somma dei primi n **numeri pari**, ossia $2 + 4 + 6 + ... + 2n$, dimostriamo che per ogni $n \geq 1$ vale:

$$2 + 4 + 6 + ... + 2n = n(n+1)$$

- **Caso base**: $2 = 1(1+1)$ è vero, non serve dimostrarlo
- **Passo induttivo**: considerando per vero che

$$2 + 4 + 6 + ... + 2n = n(n+1)$$

affermiamo per induzione che

$$2 + 4 + 6 + ... + 2n + 2(n+1) = (n+1)((n+1)+1)$$

da cui sostituiamo il caso n presente nel caso $n+1$ con la sua proprietà

$$\underbrace{2 + 4 + 6 + ... + 2n}_{\textbf{Caso n}} + 2(n+1) = \underbrace{n(n+1)}_{\textbf{Caso n}} + 2(n+1)$$

ottenendo anche in questo esempio un'equazione verificabile algebricamente, **confermando** quindi la tesi iniziale

$$n(n+1) + 2(n+1) = (n+1)((n+1)+1)$$

Generalizzazione di casi algebrici

In casi come i due esempi precedenti, è comune utilizzare il **simbolo di sommatoria** per abbreviare le somme e avere maggior rigore.

Per esempio, la somma $1 + 2 + 3 + ... + n$ si abbrevia come

$$\sum_{i=1}^{n} = 1 + 2 + 3 + ... + n$$

AIUTO: per chi se ne intendesse di programmazione, questa espressione può essere letta come un **ciclo for**: per ogni valore di i da 1 (poiché inizialmente $i = 1$) a n, effettuo $+i$.

$$\sum_{i=1}^{1} i = 1 \qquad \sum_{i=1}^{2} i = 1 + 2 \qquad \sum_{i=1}^{3} i = 1 + 2 + 3$$

Nei casi in cui andiamo ad effettuare un'**ipotesi induttiva**, possiamo effettuare il seguente passaggio:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} \right) i + (n+1)$$

Analogamente, il caso del secondo esempio in cui avevamo $2 + 4 + 6 + ... + 2n$ può essere abbreviato come

$$\sum_{i=1}^{n} 2 \cdot i = 2 + 4 + 6 + ... + 2n$$

Dunque, in linea più generale, possiamo generalizzare come

$$\sum_{i=1}^{n} f(i) = f(1) + f(2) + f(3) + ... + f(n)$$

N.B.: per abbreviare una **serie di prodotti**, piuttosto che una **serie di somme**, viene utilizzato il simbolo $\prod$

Esempio 3

Dimostrare per induzione che per ogni $n \geq 0$ vale $n < 2^n$

- **Caso base**: $0 < 2^0$ è vero, non serve dimostrare
- **Passo induttivo**: dando per vero che $n < 2^n$, affermiamo che $n + 1 < 2^{(n+1)}$. Evidenziando il caso n all'interno del caso $n + 1$, otteniamo che

$$\underbrace{n}_{\textbf{Caso n}} + 1 = \underbrace{2^n}_{Cason} + 1$$

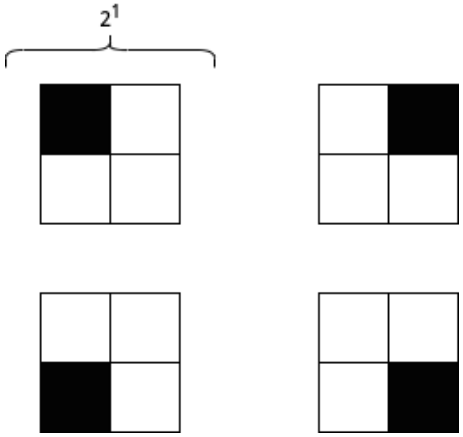
  Sappiamo inoltre che $n < n + 1$, che $2^{n-1} = 2 \cdot 2^n = 2^n + 2^n$ e che, per ipotesi induttiva, $n + 1 < 2^n + 1$ (dovuta a $n < 2^n$), per cui possiamo affermare che $n < n + 1 < 2^n + 1 \leq 2^n + 2^n$

Esempio 4

Consideriamo il seguente problema: Abbiamo un pavimento quadrato composto di $2^n \times 2^n$ quadrati e vogliamo ricoprirlo di **piastrelle bianche a forma di L** rispettando il vincolo seguente: vogliamo mettere una **piastrella nera quadrata** in una delle **posizioni centrali del pavimento**; ossia in uno dei quattro quadrati che hanno un angolo nel centro del pavimento.

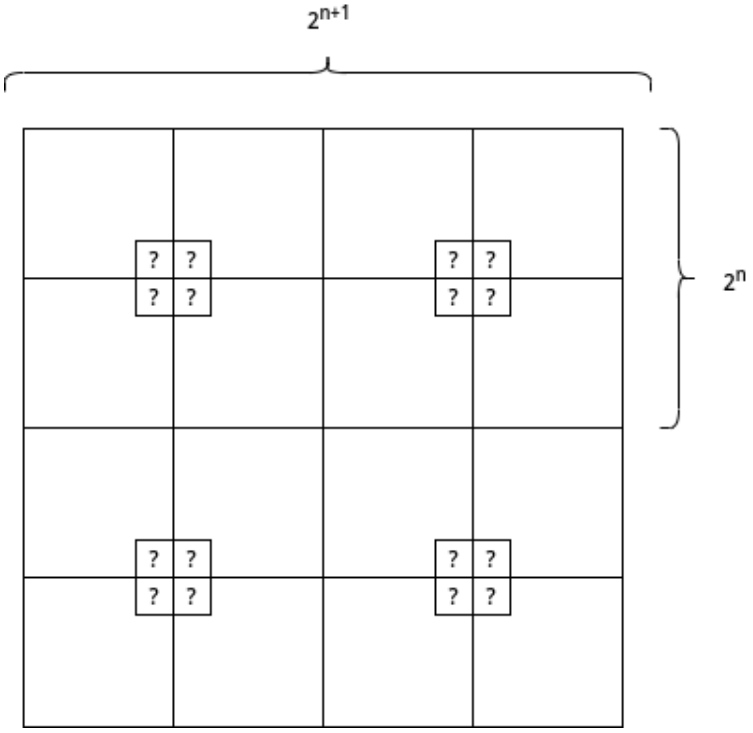
L'arredatore ci assicura che è possibile farlo per ogni $n \geq 1$. Non siamo molto convinti e vogliamo dimostrarlo. Proviamo per induzione.

- **Caso base**: con $n = 1$ abbiamo un pavimento di $2^1 \times 2^1$ piastrelle quadrate, dunque ogni modo di posizionare una piastrella a L lascia libero un quadrato centrale in cui mettere la piastrella nera.



***ATTENZIONE**: per comodità la piastrella ad L viene rappresentata come composta da 3 piastrelle bianche, tuttavia è necessario ricordare che si tratta di **una piastrella unica**.*

- **Passo induttivo**: consideriamo ora il caso $n+1$, in cui abbiamo un pavimento $2^{n+1} \times 2^{n+1}$. Poiché a livello matematico $2^{n+1} = 2 \cdot 2^n$, è facilmente intuibile come un pavimento di lato 2^{n+1} sia **scomponibile in quattro pavimenti** di lato 2^n. Per via della nostra **ipotesi induttiva**, ciascuno di questi quattro pavimenti può essere riempito dalle piastrelle bianche ad L lasciando libero uno **spazio centrale per una piastrella nera**.



La nostra ipotesi induttiva afferma che è possibile riempire anche il pavimento 2^{n+1} lasciando lo spazio centrale per una sola piastrella nera. Poiché il pavimento 2^{n+1} è composto dai **4 pavimenti** 2^n, è facilmente intuibile che sarebbe possibile lasciare **4 spazi liberi per una piastrella nera**. 3 di questi spazi potrebbero essere riempiti da un'altra piastrella bianca ad L, lasciando quindi come richiesto solo uno spazio centrale per la piastrella nera anche nel pavimento 2^{n+1}. Dunque, esiste una piastrella nera P che esiste sia in uno dei pavimenti 2^n sia nel pavimento 2^{n+1}.

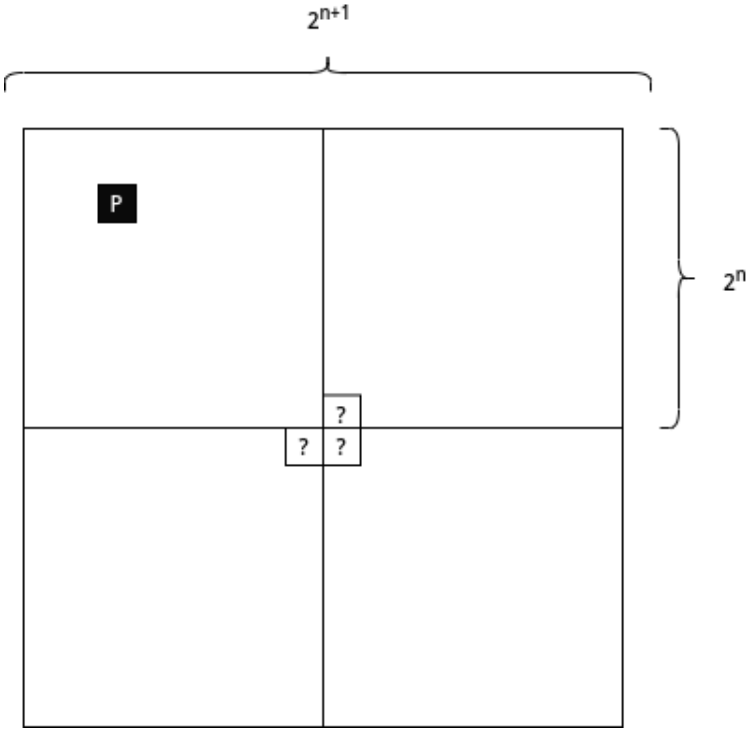
Tuttavia, come possiamo facilmente notare dall'immagine precedente, tale piastrella P **non è situata al centro del pavimento $\mathbf{2^{n+1}}$**. Possiamo quindi **rinforzare la nostra ipotesi induttiva**:

Hypothesis 1. Nuova ipotesi induttiva

E possibile pavimentare un pavimento di $2^n \times 2^n$ con piastrelle bianche a L lasciando spazio per un piastrella nera quadrata in **una qualsiasi posizione del pavimento.** (dunque non più solo centrale)

Poiché la nostra nuova ipotesi afferma che la piastrella nera possa essere in **qualsiasi posizione**, possiamo scegliere **un pavimento arbitrario** tra i quattro (sceglieremo quello in alto a sinistra per comodità) che contenga la **piastrella P in una qualsiasi posizione**, mentre le possibili piastrelle nere degli altri tre pavimenti 2^n saranno posizionate **al centro** del pavimento 2^{n+1}, in modo che possano essere riempiti da una piastrella bianca ad L.

L'ipotesi dell'arredatore è quindi **giusta**.



4.2 Errori di induzione

Vogliamo dimostrare che per ogni $n \geq 1$ esiste un gruppo di n tifosi esiste una squadra S tale che tutti i tifosi tifano quella squadra, implicando ovviamente che tutti i tifosi tifano la stessa unica squadra.

- **Caso base**: $n = 1$, dunque abbiamo un insieme $T = \{t_1\}$ di tifosi che verifica la tesi proposta
- **Passo induttivo**: consideriamo il caso in cui abbiamo un insieme $n + 1$ di tifosi $T = \{t_1, t_2, t_3, ..., t_n, t_{n+1}\}$. All'interno di questo insieme, possiamo individuare due sottoinsiemi di n tifosi: $\{t_1, t_2, t_3, ..., t_n\}$ e $\{t_2, t_3, ..., t_n, t_{n+1}\}$. Essendo due sottoinsiemi di n tifosi, essi corrispondono ad una squadra per cui tutti gli n tifosi tifano. Chiameremo tali squadre rispettivamente S e S'.

  Notiamo inoltre che esistono dei tifosi che **tifano per entrambe le squadre**. Tuttavia, ricordiamo che **tutti i tifosi tifano la stessa unica squadra**, dunque l'unico caso in cui ciò è possibile è se $S = S'$, da cui deduciamo quindi che esiste una squadra per cui l'insieme di $n + 1$ tifosi tifa.

La dimostrazione proposta presenta però una falla: nel caso in cui $n = 1$ abbiamo un insieme $T = \{t_1, t_2\}$, in cui è possibile individuare le due squadre $\{t_1\}$ e $\{t_2\}$. Tuttavia, notiamo facilmente che tali squadre **non hanno tifosi in comune**, dunque non possiamo dire che $S = S'$ e di conseguenza possiamo affermare che per $n = 2$ non esiste una squadra tifata da $n + 1$ tifosi.

- Il caso $P(1) \to P(2)$ è quindi **invalido**, rendendo quindi la dimostrazione **falsa**.

4.3 Principio di Induzione Forte

In matematica, esiste il seguente teorema:

Theorem 16

Ogni numero naturale n, dove $n \geq 2$, può scriversi come prodotto di numeri primi.

e noi vogliamo provare a dimostrarlo per induzione.

- **Caso base**: per $n = 2$ abbiamo che n è composto da se stesso, poiché 2 è un numero primo
- **Passo induttivo**: la nostra ipotesi afferma che ogni n possa essere scritto come un prodotto di k numeri primi (che chiameremo p_i), dunque

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k$$

Analogamente, possiamo scrivere $n+1$ sia come un prodotto di h fattori primi (che chiameremo q_i) sia come il prodotto dei fattori primi componenti n sommato ad 1

$$n + 1 = q_1 \cdot q_2 \cdot ... \cdot q_h$$

oppure

$$n + 1 = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$$

Tuttavia, queste scritture non ci aiutano molto nel confermare la nostra ipotesi. Possiamo provare quindi un altro approccio.

Per assurdo, supponiamo che la tesi non sia vera. Esiste quindi il seguente insieme **non vuoto**:

$$C = \{n : n \geq 2 \texttt{ e non è fattorizzabile in primi}\}$$

Per il **principio del minimo numero**, questo insieme C contiene un minimo, che chiameremo m. Questo numero **non può né essere 2 né essere primo**, poiché altrimenti sarebbe scrivibile come un prodotto di primi (dunque $m \notin C$). Dato che m non è primo, possiamo scriverlo come un prodotto tra due numeri a e b:

$$m = a \cdot b$$

dove

$$2 \leq a, b \leq m$$

poiché $2 < m$, dato che m non può essere 2, e $a, b < m$, dato che $m = a \cdot b$.

Poiché $a, b \notin C$ (perché ammettono una fattorizzazione in primi, non perché $a, b \leq 2$), possiamo scriverli come un prodotto tra primi

$$a = p_1 \cdot p_2 \cdot ... \cdot p_k$$

$$b = q_1 \cdot q_2 \cdot ... \cdot q_j$$

da cui deduciamo che

$$m = p_1 \cdot p_2 \cdot ... \cdot p_k \cdot q_1 \cdot q_2 \cdot ... \cdot q_j$$

Abbiamo raggiunto una **contraddizione**: $m \in C$, perché m non è scrivibile come un prodotto tra primi, ma anche $m \notin C$, poiché scrivibile come un prodotto tra primi. L'ipotesi iniziale è quindi **vera**.

Nell'argomento di sopra ci siamo ritrovati a ragionare su due elementi più piccoli del minimo dei controesempi, ossia i due fattori a, b tali che $m = a \cdot b$.

In termini di induzione questo significa supporre che l'Ipotesi Induttiva vale non soltanto per il predecessore immediato del numero che stiamo considerando, ma per **tutti i numeri più piccoli di esso**. In base a queste considerazioni formuliamo il seguente **Principio di Induzione Forte**:

Definition 23. Principio di Induzione Forte

Sia P una proprietà di interi non-negativi e sia k un intero non-negativo.

Se per un $n > k$ arbitrario valgono i seguenti punti:

- **Caso base**: P vale per k
- **Passo induttivo**: P vale per $k, k+1, k+2, ..., n-1$ allora vale anche per n

allora possiamo concludere che per ogni $n \geq k$ vale $P(n)$

Capitolo 5

Logica proposizionale

La Logica Proposizionale si occupa di studiare le proprietà di alcuni **costrutti logici** utilizzati nel linguaggio naturale e nella pratica scientifica e matematica, quali il *non* **(negazione)**, l'*oppure* **(disgiunzione)**, l'*e* **(congiunzione)**, il *se ... allora* **(implicazione)** o il *se e solo se* **(equivalenza, doppia implicazione)**.

Consideriamo le tre proposizioni aritmetiche:

- Se $a = 0$ o $b = 0$ allora $a \cdot b = 0$
- $a \cdot b \neq 0$
- $a \neq 0$ e $b \neq 0$

Per formalizzare tali proposizioni, è necessario prima individuare quali siano le **parti atomiche**, ossia quei costrutti logici che non sono scomponibili in altre parti, dunque che possono essere **solo vere o false**. In questo caso, tali parti atomiche corrispondono a $a = 0$, $b = 0$ e $a \cdot b = 0$.

Associamo quindi a ciascuna parte atomica una **lettera** che la identifichi: $a = 0$ diventa **A**, $b = 0$ diventa **B** e $a \cdot b = 0$ diventa **C**. Possiamo quindi riscrivere le tre proposizioni in **termini formali**, sostituendo le parti atomiche con le loro lettere, per poi sostituire i **costrutti linguistici** con dei **simboli**: il ***"non"*** come $\neg$, le ***"o"*** come $\vee$, le ***"e"*** come $\wedge$, i ***"se"*** come $\rightarrow$ e i ***"se e solo se"*** come $\leftrightarrow$.

- $(A \vee B) \rightarrow C$
- $\neg C$
- $\neg A \wedge \neg B$

Utilizzare un linguaggio di questo tipo ci permette di formalizzare ogni costrutto logico, dunque anche costrutti non matematici.

Consideriamo le seguenti proposizioni:

- Se il padre è alto o la madre è alta allora il figlio è alto
- Il figlio è basso
- Il padre è basso e la madre è bassa

Possono essere riscritte formalmente allo stesso modo dell'esempio precedente, dove per A intendiamo *"il padre è alto"*, per B intendiamo *"la madre è alta"* e per C intendiamo *"il figlio è alto"*.

- $(A \vee B) \rightarrow C$
- $\neg C$
- $\neg A \wedge \neg B$

A differenza dell'esempio precedente però, la proposizione *"Se il padre è alto o la madre è alta allora il figlio è alto"* è **empiricamente falsa**, mentre la proposizione *Se* $a = 0$ *o* $b = 0$ *allora* $a \cdot b = 0$ è **matematicamente vera**. Tuttavia, ciò non ci interessa, poiché riconosciamo che entrambe le **proposizioni sono corrette**, inteso come **valide**: **se** le premesse (ossia le parti) sono **vere**, **allora** la conclusione è **vera**.

5.1 Linguaggio e proposizioni formali

Di seguito vengono elencate una serie di definizioni, necessarie per le sezioni successive:

Definition 24. Linguaggio proposizionale

Un linguaggio proposizionale è un insieme $\mathcal{L}$ di simboli contenente

- I seguenti simboli, detti **connettivi logici**: $\neg$, $\vee$, $\wedge$, $\rightarrow$ e $\leftrightarrow$
- Le**parentesi tonde chiuse e aperte**
- Una quantità finita o infinita numerabile di simboli (distinti dai connettivi e dalle parentesi) detti **variabili proposizionali**, il cui insieme viene indicato con $VAR_{\mathcal{L}}$

Definition 25. Proposizioni

Sia L un linguaggio proposizionale. L'insieme delle **proposizioni** (o formule ben formate) in $\mathcal{L}$ è il minimo insieme X di stringhe finite di simboli in $\mathcal{L}$ tale che:

- **Tutte le variabili proposizionali** di $\mathcal{L}$ sono in X
- Se A è in X allora $(\neg A)$ è in X
- Se A e B sono in X allora $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ sono in X

Denotiamo con $PROP_{\mathcal{L}}$ (o $FML_{\mathcal{L}}$) l'insieme delle proposizioni (o formule) nel linguaggio L. Se L è chiaro dal contesto, scriviamo PROP.

Definition 26. Sotto-formula

Una proposizione B è una sotto-formula di una proposizione A se è verificato uno dei seguenti casi:

1. A è identica a B
2. A è $(\neg C)$ e B è sotto-formula di C
3. A è $(C \blacksquare D)$ e B è sotto-formula di C oppure è sotto-formula di D

A è $(\neg C)$, C è detta **sotto-formula immediata** di A. Se A è $(C \blacksquare D)$, C e D sono dette **sotto-formule immediate** di A, dove il simbolo ■ rappresenta un **segnaposto** per i **connettivi logici** ($\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$)

5.2 Semantica della logica proposizionale

Definition 27

Un **assegnamento** è una funzione di tipo

$$v : VAR \rightarrow \{1, 0\}$$

I numeri **1 e 0** vengono detti valori di **verità**, e sono intuitivamente da identificarsi come **Vero (1)** e **Falso (0)**.

Vogliamo estendere un qualunque assegnamento $v : VAR\{1, 0\}$ a una **funzione**

$$v' : PROP \rightarrow \{0, 1\}$$

Lo facciamo dando delle regole per calcolare **ricorsivamente** il valore di v' su una proposizione A come funzione dei valori di v' sulle sotto-formule immediate di A. Per alleggerire la notazione, la funzione v assume le seguenti regole:

$$v((\neg A)) = \begin{cases} 1 & se\ v(A) = 0 \\ 0 & se\ v(A) = 1 \end{cases}$$

$$v((A \vee B)) = \begin{cases} 0 & se\ v(A) = v(B) = 0 \\ 1 & altrimenti \end{cases}$$

$$v((A \wedge B)) = \begin{cases} 1 & se\ v(A) = v(B) = 1 \\ 0 & altrimenti \end{cases}$$

$$v((A \rightarrow B)) = \begin{cases} 0 & se\ v(A) = 0\ e\ v(B) = 0 \\ 1 & altrimenti \end{cases}$$

$$v((A \leftrightarrow B)) = \begin{cases} 1 & se\ v(A) = v(B) \\ 0 & altrimenti \end{cases}$$

Queste regole possono essere anche rappresentate attraverso delle **tavole della verità**, dove per ogni combinazione viene stabilita la sua veridicità, ad esempio:

A	$\neg A$
0	1
1	0

A	B	$(A \vee B)$
0	0	0
0	1	1
1	0	1
1	1	1

A	B	$(A \to B)$
0	0	1
0	1	1
1	0	0
1	1	1

Vediamo ora un esempio di **proposizione complessa** e la sua conseguente **tabella della verità**:

$$A = ((P \vee Q) \to (R \vee (R \to Q)))$$

P	Q	R	$(R \to Q)$	$(R \vee (R \to Q))$	$(P \vee Q)$	A
0	0	0	1	1	0	1
0	0	1	0	1	0	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	1	1	1
1	0	1	0	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Possiamo costruire (meccanicamente) la tavola di verità di una **qualunque proposizione A**. Se la proposizione contiene **n variabili proposizionali**, la sua tavola di verità avrà $\mathbf{2^n}$ **righe**. **Ogni assegnamento di valori** di verità alle variabili proposizionali di A **corrisponde ad una riga** della tavola di verità di A, e viceversa.

5.3 Soddisfacibilità, Conseguenza e Validità logica

Vediamo altre definizioni relative alle proposizioni logiche:

Definition 28. Proposizione soddisfacibile

Un assegnamento v soddisfa una proposizione A se $v(A) = 1$. Si dice anche che v è un modello di A.

A è **soddisfacibile** se esiste un assegnamento che la soddisfa, altrimenti viene detta **insoddisfacibile**. Indichiamo con SAT l'insieme delle proposizioni soddisfacibili e con $UNSAT$ l'insieme delle proposizioni insoddisfacibili.

Definition 29. Conseguenza logica

Siano $\mathcal{F} = \{A_1, ..., A_n\}$ un insieme di proposizioni e sia A una proposizione. Diciamo che A **è conseguenza logica di** $\mathcal{F}$ se ogni assegnamento che **soddisfa tutti gli elementi di F soddisfa anche A**.

Scriviamo in tal caso $A_1, ..., A_n \models A$ e diciamo che le premesse $A_1, ..., A_n$ implicano logicamente la conclusione A.

Se $\mathcal{F}$ è l'**insieme vuoto**, scriviamo $\emptyset \models A$. In questo caso la definizione dice che **A è soddisfatta da tutti gli assegnamenti**. Infatti, per qualunque v è vero che v soddisfa tutti gli elementi dell'insieme $\emptyset$ (poiché ovviamente non contiene proposizioni).

Definition 30. Tautologia (o Verità logica)

Una proposizione A è una **tautologia (o verità logica)** se per ogni assegnamento v vale $v(A) = 1$. Indichiamo con $TAUT$ l'insieme delle tautologie.

Una volta enunciate le seguenti tre definizioni, possiamo definire anche un teorema strettamente derivante da esse:

Theorem 17

Siano $A_1, ..., A_n, A$ delle proposizioni. Allora i seguenti punti sono equivalenti:

- $A_1, ..., A_n \models A$
- $((A_1 \wedge ... \wedge A_n) \rightarrow A) \in TAUT$
- $(A_1 \wedge ... \wedge A_n \wedge \neg A) \in UNSAT$

5.4 Espressività della logica proposizionale

Vogliamo usare la logica proposizionale per giudicare in modo rigoroso della **valitdità** di argomenti e della **verità** di proposizioni. Abbiamo definito la nozione fondamentale di **conseguenza logic**a di una proposizione da un numero finito di premesse:

$$A_1, ..., A_n \models A$$

La **validità di un argomento formalizzato** come questo può essere, con gli strumenti attuali, verificata in **tre modi**:

- Verificando se un assegnamento α soddisfa tutte le premesse $A_1, ..., A_n$, allora α soddisfa la conclusione A, secondo la definizione di $\models$
- Verificando che la formula $(A_1 \wedge ... \wedge A_n) \rightarrow A$ è in $TAUT$ (usando la tavola di verità).
- Verificando che la formula $(A_1 \wedge ... \wedge A_n \wedge (\neg A)$ è in $UNSAT$ (usando la tavola di verità).

Esempio 1 - Argomenti verbali

Semplici argomenti verbali. La logica proposizionale si presta bene anche a a formalizzare argomenti verbali:

1. Se studi e sei intelligente allora superi l'esame.
2. Se sei intelligente allora studi.
3. Non superi l'esame.
4. Sei scemo.

Possiamo formalizzarlo in:

1. $(A \wedge B) \rightarrow C$
2. $B \rightarrow A$
3. $\neg C$
4. $\neg B$

Per poi provare a verificarne la validità attraverso i tre modi individuati precedentemente:

- Verificare se esiste un assegnamento α che soddisfa tutte e quattro le proposizioni descritte (ossia $(A \wedge B) \rightarrow C$, $B \rightarrow A$, $\neg C$ e $\neg B$
- Verificare se la proposizione $((A \wedge B) \rightarrow C \wedge (B \rightarrow A) \wedge \neg C) \rightarrow \neg B$ è una tautologia (dunque è in $TAUT$)
- Verificare se la proposizione $((A \wedge B) \rightarrow C \wedge (B \rightarrow A) \wedge \neg C \wedge \neg\neg B)$ è insoddisfacibile (dunque è in $UNSAT$)

Tutti e tre i casi sono risolvibili attraverso delle **tabelle della verità**, tuttavia è anche possibile giungere alla conclusione di veridicità osservando bene il **senso logico di ogni proposizione** e il modo in cui si **relaziona** alle altre (si lascia il compito al lettore, potrebbe essere d'aiuto)

Suggerimento: si guardi il secondo caso, dove si cerca di vedere se sia una tautologia

Esempio 2

Consideriamo la seguente cartina. Vogliamo riuscire a colorare l'Italia, l'Austria e l'Ungheria di **rosso** o di **blu**, in modo che ogni stato non abbia lo stesso colore di un'altro stato ad esso **adiacente**.

Dichiariamo il seguente linguaggio proposizionale: le variabili proposizionali sono I_R, I_B, A_R, A_B, U_R, U_B e il loro significato intuitivo è: I_R = *l'Italia è rossa*, mentre I_B = *l'Italia è blu* e così via.

Quindi, esprimiamo formalmente i tre vincoli definiti dal problema:

- Ogni stato riceve un colore

$$(I_R \vee I_B) \wedge (A_R \vee A_B) \wedge (U_R \vee U_B)$$

- Se uno stato è rosso, allora non è blu

$$(I_R \to \neg I_B) \wedge (A_R \to \neg A_B) \wedge (U_R \to \neg U_B)$$

- Se uno stato è di un colore, allora il suo adiacente non potrà avere quello stesso colore

$$(I_R \to \neg A_R) \wedge (I_B \to \neg A_B) \wedge (A_R \to \neg U_R) \wedge (A_B \to \neg U_B)$$

I tre stati saranno quindi colorabili nel modo richiesto **se e solo se** l'insieme delle proposizioni descritte è dentro SAT.

Supponiamo che i tre stati siano colorabili come richiesto. Allora esiste un assegnamento che **soddisfa le proposizioni**. Questo assegnamento è facilmente intuibile e verificabile nei tre modi individuati precedentemente, ossia: $v(I_R) = 1$, $v(I_B) = 0$, $v(A_R) = 1$, $v(A_B) = 0$, $v(U_R) = 1$, $v(U_B) = 0$.

***Attenzione**: intuitivamente possiamo trovare anche un altro assegnamento che soddisfi le proposizioni, ossia $v(I_R) = 0$, $v(I_B) = 1$, $v(A_R) = 0$, $v(A_B) = 1$, $v(U_R) = 0$, $v(U_B) = 1$, tuttavia ricordiamo che è necessario trovare **un solo assegnamento valido** affinché possa essere considerata verificata*

5.5 Equivalenza logica e verità notevoli

Abbiamo ora gli strumenti per dare la seguente definizione di Equivalenza logica:

Definition 31

Due formule A, B si dicono **logicamente equivalenti** se per ogni assegnamento α, $\alpha(A) = \alpha(B)$. In questo caso scriviamo $A \equiv B$.

Si osserva facilmente che $A \equiv B$ se e solo se $\models (A \leftrightarrow B)$ e che la relazione di equivalenza logica è invece una relazione di equivalenza sull'insieme delle proposizioni.

- $A \equiv A$
- Se $A \equiv B$ e $B \equiv C$, allora $A \equiv C$
- Se $A \equiv B$, allora $B \equiv A$

Una volta definita l'equivalenza booleana, possiamo enunciare anche quelle che vengono considerate **verità notevoli**, ossia delle equivalenze logiche "rapide" (si pensi ai *limiti notevoli* della normale matematica):

Nome	**Teorema**	**Duale**
Identità	$B \wedge 1 = B$	$B \vee 0 = 0$
Elemento nullo	$B \wedge 0 = 0$	$B \vee 1 = 1$
Idem-potenza	$B \wedge B = B$	$B \vee B = B$
Involuzione	$\overline{B} = B$	$\overline{B} = B$
Complementare	$\overline{B} \wedge B = 0$	$\overline{B} \vee B = 1$
P. Commutativa	$B \wedge C = C \wedge B$	$B \vee C = C \vee B$
P. Associativa	$(B \wedge C) \wedge D = B \wedge (C \wedge D)$	$(B \vee C) \vee D = B \vee (C \vee D)$
P. Distributiva	$B \wedge (C \vee D) = (B \wedge C) \vee (B \wedge D)$	$B \vee (C \wedge D) = (B \vee C)(B \vee D)$
1° T. Assorbimento	$B \wedge (B \vee C) = B$	$B \vee (B \wedge C) = B$
2° T. Assorbimento	$(B \wedge C) \vee (B \wedge C) = B$	$(B \vee C) \wedge (B \vee C) = B$
T. di DeMorgan	$\overline{B_0 \wedge B_1 \wedge B_2 ...} = \overline{B_0} \vee \overline{B_1} \vee \overline{B_2} ...$	$\overline{B_0 \vee B_1 \vee B_2 ...} = \overline{B_0} \wedge \overline{B_1} \wedge \overline{B_2} ...$

Utilizzando le precedenti verità notevoli, possiamo individuare anche delle **regole di traduzione** dei vari **connettivi logici**:

- $(A \leftrightarrow B) \equiv ((A \rightarrow B) \wedge (B \rightarrow A))$
- $(A \rightarrow B) \equiv (\neg A \vee B)$
- $(A \vee B) \equiv (\neg A \rightarrow B)$
- $(A \vee B) \equiv \neg(\neg A \wedge \neg B)$
- $(A \wedge B) \equiv \neg(\neg A \vee \neg B)$

Esempio 1 Dimostriamo che $\models (A \to (B \to C) \leftrightarrow ((A \wedge B) \to C)$

$$A \to (B \to C) \equiv (\neg A \vee (\neg B \vee C) \equiv (\neg A \vee \neg B) \vee C) \equiv \neg(A \wedge B) \vee C \equiv (A \vee B) \to C$$

Esempio 2 Dimostriamo che $\models (A \to B) \leftrightarrow (\neg B \to \neg A)$

$$(\neg B \to \neg A) \equiv (\neg\neg B \vee \neg A) \equiv (B \vee \neg A) \equiv (\neg A \vee B) \equiv (A \to B)$$

5.6 Forma Normale Congiuntiva

Definiamo col termine **"letterale"** una variabile proposizionale o una negazione di una variabile proposizionale. Se L è un letterale, definiamo $\overline{L}$ il suo complementare.

Diciamo che A è in **Forma Normale Congiuntiva (CNF)** se A è una **congiunzione di disgiunzioni di letterali**, ossia è della forma seguente, dove gli $L_{i,j}$ sono letterali:

$$(L_{1,1} \vee L_{1,2} \vee ... \vee L_{1,m_1}) \wedge (L_{2,1} \vee L_{2,2} \vee ... \vee L_{2,m_2}) \wedge ... \wedge (L_{n,1} \vee L_{n,2} \vee ... \vee L_{n,m_n})$$

Che abbreviamo con la seguente forma:

$$\bigwedge_{i \leq n} \bigvee_{j \leq m_i} L_{i,j}$$

Theorem 18. Forma Normale Congiuntiva (CNF)

Per ogni A esiste A^{CNF} tale che A^{CNF} è una **Forma Normale Congiuntiva** e vale

$$A \equiv A^{CNF}$$

Osservazione: Una CNF è una **tautologia** se e soltanto se tutti i suoi congiunti sono **tautologie**.

Fissiamo una rappresentazione agile e compatta per **formule in CNF**. Una formula F in CNF la seguente forma:

$$C_1 \wedge C_2 \wedge ... \wedge C_n$$

dove ogni C_i (detta **clausola**) è una disgiunzione (OR) di letterali.

Rappresentiamo una clausola $C = L_1 \vee ... \vee L_k$ come l'**insieme dei suoi letterali**

$$\{L_1, ..., L_k\}$$

e rappresentiamo una formula $F = C_1 \wedge ... \wedge C_n$ come l'**insieme delle sue clausole**

$$\{C_1, ..., C_n\}$$

5.7 Risoluzione

Siano C_1 e C_2 due clausole e L un letterale, tale che $L \in C_1$ e $\overline{L} \in C_2$. Definiamo

$$RES_L(C_1, C_2) = (C_1 - L) \cup (C_2 - \overline{L})$$

dove anche $Res_L(C_1, C_2)$ è una clausola e viene detta **risolvente di C_1 e C_2 rispetto a L**. La **Regola di Risoluzione** ci permette di passare dalle clausole C_1 e C_2 al loro risolvente.

Theorem 19. Lemma di Risoluzione

Sia L un letterale tale che $L \in C_1$ e $\overline{L} \in C_2$. Allora vale che

$$C_1, C_2 \models RES_L(C_1, C_2)$$

Il Lemma, inoltre, ci dice che se, partendo da una formula $F = \{C_1, ..., C_n\}$ in CNF, siamo in grado di ottenere la **clausola vuota** $\square$ applicando la regola di Risoluzione, allora la formula di partenza è **insoddisfacibile**.

Theorem 20. Correttezza

Sia $F = \{C_1, ..., C_n\}$ una formula in CNF. Se, applicando la Regola di Risoluzione un numero finito di volte alle clausole in F e ai risultanti risolventi, ottengo la clausola vuota $\square$, allora F è insoddisfacibile.

Esempio 1

Consideriamo la formula $F = \{\{\neg q, p\}, \{r, p\}, \{\neg p, \neg q\}, \{\neg p, s\}, \{q, \neg r\}, \{q, \neg r\}, \{q, \neg s\}\}$

- Applicando la risoluzione a $\{\neg q, p\}$ e $\{\neg p, \neg q\}$ (sul letterale p) ottengo

$$\{\neg q\}$$

- Applicando la risoluzione a $\{\neg q\}$ e $\{q, \neg r\}$ ottengo

$$\{\neg r\}$$

- Applicando la risoluzione a $\{\neg r\}$ e $\{r, p\}$ ottengo

$$\{p\}$$

- Applicando la risoluzione a $\{p\}$ e $\{\neg p, s\}$ ottengo

$$\{s\}$$

- Applicando la risoluzione a $\{s\}$ e $\{q, \neg s\}$ ottengo

$$\{q\}$$

- Infine, applicando la risoluzione a $\{q\}$ e $\{\neg q\}$ ottengo

$$\square$$

Concludiamo così che $F \in UNSAT$.

Esempio 2

Consideriamo la seguente formula F in CNF:

$$F = \{\{\neg p, \neg q, r\}, \{\neg p, \neg q, s\}, \{\neg p_1, \neg q1, r_1\}, \{\neg r_1, \neg s, s_1\}, \{p\}, \{q\}, \{q1\}, \{p_1\}, \{\neg s_1\}\}$$

- Possiamo applicare la risoluzione di clausole partendo dall'insieme di clausole F, scegliendo ogni volta una **coppia di clausole** a cui è possibile applicare la risoluzione.

  Otteniamo una sequenza finita di clausole come segue:

$$\{\neg p, \neg q, s\}, \{\neg r_1, \neg s, s_1\}, \{\neg p, \neg q, \neg r_1, s_1\}, \{p\}, \{\neg q, \neg r_1, s_1\}, \{q\}, \{\neg r_1, s_1\},$$
$$\{\neg s_1\}, \{\neg r_1\}, \{\neg p_1, \neg q1, r_1\}, \{\neg p_1, \neg q1\}, \{q1\}, \{\neg p_1\}, \{p_1\}, \square$$

- Dal fatto che l'ultima clausola è una **clausola vuota**, che è insoddisfacibile, e dalla proprietà sopra dimostrata che il risolvente è **conseguenza logica delle due clausole premesse**, possiamo concludere che F è insoddisfacibile.

Consideriamo la domanda opposta: se $F \in UNSAT$, è vero che posso certificarlo, applicando iterativamente la regola di risoluzione di clausole, partendo dalle clausole di F e raggiungendo la clausola vuota?

Questa proprietà, se vale, è detta **completezza** (del metodo di Risoluzione): il metodo è capace di certificare tutti i casi di $F \in UNSAT$. Inoltre, è opportuno introdurre un concetto formale di **derivazione in Risoluzione** di una clausola C da una formula F, che renda **rigorosa** l'idea di "applicare iterativamente la regola di Risoluzione a partire da un insieme di clausole".

Definition 32. Derivazione/Refutazione in Risoluzione

Sia $F = \{C_1, ..., C_{n-1}\}$ una formula. Una sequenza ordinata di clausole

$$D_1, D_2, ..., D_{k-1}, D_k$$

è una **derivazione in Risoluzione della clausola** D_k se, per ogni $i \in [1, k]$, abbiamo che $D_i \in F$ oppure esistono $j, h < i$ tali che $D_i = RES_L(D_j, D_h)$, per qualche letterale L.

In altre parole, ogni clausola Di ha un **certificato** per appartenere alla sequenza/derivazione: può essere una clausola di F **oppure** derivare da due clausole precedenti per applicazione di risoluzione.

Se esiste una derivazione della clausola C dalla formula $F = \{C_1, ..., C_n\}$ scriviamo $C_1, ..., C_n \vdash_{RES} \square$ o $F \vdash_{RES} C$ Se $D_n = \square$ diciamo che la derivazione è detta una **refutazione di F** (in simboli: $F \vdash_{RES} \square$).

5.7.1 Algoritmo di decisione per $F \in UNSAT$

Dai risultati visti finora possiamo definire un **algoritmo** per testare se $F \in UNSAT$, dove F è una formula in CNF.

L'input dell'algoritmo è una formula F in CNF, ossia $F = \{C_1, ..., C_n\}$ dove le C_i sono clausole. L'algoritmo procede come segue, usando F come variabile:

Definition 33

while esistono clausole C_i, C_j in F tali che il loro risolvente R non è già in F

do $F = F \cup \{R\}$.

L'algoritmo termina in n**umero finito di passi** perché esiste solo un numero finito di clausole su un dato insieme di variabili proposizionali.

Dall'algoritmo ricaviamo quindi il seguente teorema:

Theorem 21

$F \in UNSAT$ se e soltanto se una clausola vuota $\square$ è nella formula F al termine dell'algoritmo.