1️⃣

Metodi matematici per l'informatica

1-Combinatoria

La combinatoria permette di capire quanti accoppiamenti si possono fare con delle caratteristiche ben precise.

Esempi:

Ci sono 5 volpi e 4 gatti, quanti accoppiamenti si possono fare?

Quante targhe di auto esistono con il formato italiano?

1.1-Principio moltiplicativo

Se dobbiamo scegliere un oggetto da un gruppo N_1 e un oggetto da un gruppo N_2 ecc...

Il numero di combinazioni possibili è $N_1 \cdot N_2 \cdot N_3 \cdot ... \cdot N_N$

Esempio:

Quanti menù completi si possono fare con 5 antipasti, 6 primi, 7 secondi e 5 dolci?

Risultato = $5 \cdot 6 \cdot 7 \cdot 5$

1.2-Disposizioni

Se abbiamo n elementi da ordinare (con ripetizioni) in k posti il numero di combinazioni è:

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

> ' indica che ci sono ripetizioni

Esempio:

Quanti numeri binari si possono scrivere con 7 cifre?

$D'_{2,7} = 2^7$

Se abbiamo n elementi da ordinare (senza ripetizioni) in k posti il numero di combinazioni è:

$D_{n,k} = \frac{n!}{(n-k)!} = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-(k-1))$

Esempio:

Quanti possibili podi ci possono essere se ad una gara partecipano 8 atleti?

$D_{8,3} = \frac{8!}{(8-3)!} = \frac{8!}{5!} = 8 \cdot 7 \cdot 6$

> Se k = n si chiamano **Permutazioni**

Esempio:

Quanti ordini si arrivo ci possono essere se ad una gara partecipano 7 atleti?

$D_{7,7} = \frac{7!}{(7-7)!} = \frac{7!}{0!} = 7!$

> Da ricordare: 0! = 1

Se negli elementi da ordinare alcuni si ripetono più di una volta bisognerà dividere per il numero di disposizioni possibili di quegli elementi, cioè r!

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

Esempio:

Quanti anagrammi della parola NONNA sono possibili?

$D_{5,5} = \frac{5!}{3!}$

Se c'è più di una ripetizione bisogna dividere per tutte

Esempio:

Quanti anagrammi della parola NONNO sono possibili?

$D_{5,5} = \frac{5!}{3! \cdot 2!}$

1.3-Principio additivo

Il numero totale delle combinazioni A è dato dalla somma del numero delle combinazioni dei sottoinsiemi B.

Questi insiemi devono essere disgiunti, cioè non devono avere nessun elemento in comune. Devono essere anche esaustivi, cioè qualsiasi elemento di A deve appartenere a uno dei sottoinsiemi B. Si chiama "partizione di A" la somma dei sottoinsiemi che hanno queste caratteristiche.

Esempio:

Quante targhe esistono che contengano una sola C?

A (numero di targhe con C) = B1 (numero di targhe con C al primo posto) + B2 (numero di targhe con C al secondo posto) + B3 (numero di targhe con C al sesto posto) + B4 (numero di targhe con C al settimo posto)

$$B1 = B2 = B3 = B4 = 25^3 \cdot 10^3 \implies A = 25^3 \cdot 10^3 \cdot 4$$

1.4-Rapporti tra insiemi

Scrittura	Descrizione
A = B	Uguaglianza: A e B hanno gli stessi elementi, implica anche che A ⊆B e B⊆A
A ⊆ B	Sottoinsieme: ogni elemento di A appartiene anche a B
A ∩ B	Intersezione: insieme formato dagli elementi comuni ad A e B
A ∪ B	Unione: insieme formato dagli elementi di A e da quelli di B
A∩B = ∅	Disgiunzione: nessun elemento di A appartiene anche a B
	Insieme vuoto: insieme senza elementi
x ∈A	Appartenenza: l'elemento x fa parte dell'insieme A
x ∉A	Non appartenenza: l'elemento x non fa parte di A
#A o |A| o $\overline{A}$	Numero di oggetti nell'insieme A

1.5-Metodo inverso

Se dobbiamo trovare il numero di elementi di un insieme A e conosciamo un insieme C più grande possiamo sottrarre a questo insieme C il complementare di A (B).

#A = #C - #B

A⊆C, B⊆C

A∩B = ∅

C = A∪B

Esempio:

Quante targhe contengono almeno una P?

B = targhe senza P = $25^4 \cdot 10^3$

C = totale targhe = $26^4 \cdot 10^3$

A = C – B = $(26^4 \cdot 10^3) - (25^4 \cdot 10^3) = 10^3(26^4 - 25^4)$

1.6-Combinazioni

Le combinazioni sono disposizioni di n elementi in k posti in cui non conta l'ordine. Contano i sottoinsiemi di k elementi di un insieme di n elementi.

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

Esempi:

Ci sono 80 studenti, 40 maschi e 40 femmine, quanti gruppi di 4 rappresentanti possono esserci?

$$C_{80,4} = \frac{80!}{76! \cdot 4!}$$

Se i rappresentanti devono essere 2 maschi e 2 femmine?

$$C_{40,2} \cdot C_{40,2} = \left(\frac{40!}{38! \cdot 2!}\right)^2$$

Se uno dei rappresentanti è più importante?

$80 \cdot C_{79,3} = 80 \cdot \frac{79!}{76! \cdot 3!} = \left(\frac{80!}{76! \cdot 4!}\right) \cdot 4$

1.6.1-Insieme potenza:

Il numero totale di sottoinsieme di un insieme di n elementi cioè la partizione $S t.c. S \subseteq A$si chiama insieme delle parti o insieme potenza di a

$$P(a) = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

1.6.2-Combinazioni con ripetizioni:

Quanti modi di distribuire n caramelle a k bambini?

Le combinazioni sono tante quante le parole di n+k-1 lettere con n pallini uguali e k-1 stanghette uguali.

$$C'_{n,k} = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = \frac{(n+k-1)!}{n! \cdot (k-1)!}$$

1.6.3-Scritture additive:

Quanti modi ci sono di sommare 6 numeri per ottenere 7?

n = 7

k = 6

$$C'_{n,k} = \binom{n+k-1}{n} = \binom{7+6-1}{7} = \binom{7+6-1}{6-1}$$

1.7-Principio di inclusione-esclusione

2 termini:

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

3 termini:

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

#$(A \cap B \cap C)$

n termini:

#$(A1 \cup A2 \cup \ldots \cup An)$ = #A1 + #A2 +...+ #An - #$(Ai \cap Aj)$ + #$(Ai \cap Aj \cap Ak)$ =>

=> sommo gli elementi dei singoli insiemi, tolgo le intersezioni pari e sommo quelle dispari.

2-Funzioni

Una funzione è un'associazione di elementi di un insieme(dominio) agli elementi di un altro insieme(codominio), tale che ad ogni elemento del dominio sia associato un unico elemento del codominio.

f: A → B

se X⊆A => f: X → B

se Y ⊇B => f: A → Y

Si può identificare una funzioni dal suo grafico insiemistico, cioè l'insieme delle coppie (argomento, valore).

2.1-Def. Insiemistica

A x B = insieme delle coppie ordinate (a, b) con $a \in A$ e $b \in B$

x = prodotto cartesiano

$$f \subseteq AxB \text{ t.c. } \forall a \in A \ \exists! b \in B \text{ t.c. } (a, b) \in f$$

f = grafico = {(arg, val),…} = estensione = insieme di elementi

2.1.1-Unione di funzioni

$f(A \cup B) \ \subseteq \ f(A) \ \cup \ f(B) \implies \forall y \in f(A \cup B) \ \exists x \in A \cup B$ t.c. $y \in f(A) \cup f(B)$

$f(A \cap B) \subseteq f(A) \cap f(B)$=> sempre vero

Non è sempre vero che $f(A \cap B) \supseteq f(A) \cap f(B)$, è verificata solo se f è iniettiva

2.2-Composizione di funzioni

f: x → y

g: y → z

g(f(x)) definisce una funzione da x → z

La composizione di funzioni non è commutativa, cioè f(g(x))≠g(f(x))

Se f e g sono iniettive allora $f_o g$ è iniettiva.

Se f e g sono suriettiva allora $f_o g$ è suriettiva.

2.3-Funzioni biettive

f: x → y è iniettiva se $\exists g : y \rightarrow x$ t.c. $(f_o g) : y \rightarrow y$ è identità su y $\implies \forall n \in y \implies f_o g(n) = n$

f: x → y è suriettiva se $\exists g : y \rightarrow x$ t.c. $(g_o f) : x \rightarrow x$ è identità su x $\implies \forall n \in x \implies g_o f(n) = n$

f: x → y è biettiva se $\exists g : y \rightarrow x$ t.c. $(g_o f) : x \rightarrow x$ è identità su x e $(f_o g) : y \rightarrow y$ è identità su y

2.4-Dimostrare la non biettività

2.4.1-Metodo diagonale:

S = {sequenze binarie infinite}

Per assurdo poniamo S come biettiva $\implies \exists f : N \rightarrow S$

S = f(0), f(1), f(2)…

F(0) =	b_0^1	b_0^2	b_0^3
F(1) =	b_1^1	b_1^2	b_1^3
F(2) =	b_2^1	b_2^2	b_2^3

ϕ = diagonale flippata

$\varphi \in S, \varphi \notin f(0), f(1), f(2)... \implies \forall n \in N \implies \varphi \neq f(n)$

2.4.2-Metodo canonico:

Ci sono degli invitati e vogliamo avere una foto di tutti i possibili gruppi di persone, più una dello sfondo senza persone. Ogni invitato può portare a casa una foto.

Sicuramente alcune foto resteranno escluse perché una foto che non verrà scelta è la foto con tutti le persone che hanno scelto una foto che non li ritrae.

Quindi:

f: A → P(A) = potenza di A

non è suriettiva

#A < #P(A)

3-Relazioni

f: A → B è una funzione se da ogni punto di A parte una sola freccia.

Le relazioni non hanno questo vincolo quindi da ogni punto di A possono partire più frecce.

Una relazione binaria è un sottoinsieme di AxB.

R è una relazione tra A e B con $a \in A$ e $b \in B$, si scrive aRb o $(a,b) \in R$ o R(a,b).

3.1-Matrici

A = {$a_1, a_2, a_3, ..., a_n$}

B = {$b_1, b_2, b_3, ..., b_n$}

M_R = matrice di R

	b_1	b_2	b_3
a_1	$m_{i,j}$	//	//
a_2	//	//	//
a_3	//	//	//

$$m_{i,j} = \begin{cases} 0 & m_{i,j} \notin R \\ 1 & m_{i,j} \in R \end{cases}$$

Esempio:

R = {(1,2),(2,4),(3,2),(4,2),(4,4)}

$$\begin{Bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{Bmatrix}$$

3.1.1-Inversione

Se $R \subseteq AxB$, l'inversa è $R^{-1} \subseteq BxA$

Basta invertire l'ordine delle coppie.

Esempio:

R = {(1,a),(1,0),(1,c),(2,b)}

R^{-1} = {(a,1),(0,1),(c,1),(b,2)}

3.2-Composizione di relazione

$R \subseteq AxB$

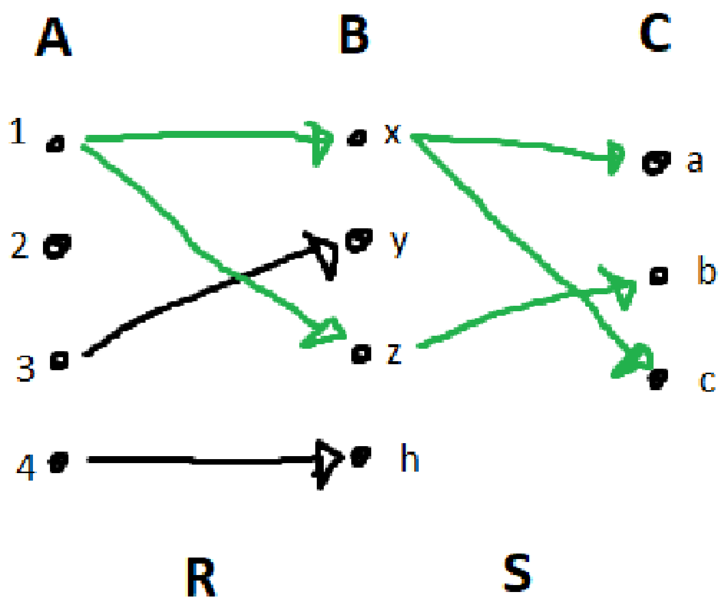
$S \subseteq BxC$

La loro composta è la relazione tra A e C, che esiste tra $a \in A$ e $c \in C$ solo se esiste $b \in B$ tale che aRb e bSc. Si scrive S_oR.

R = {(1,x),(1,z),(3,y),(4,h)}

S = {(x,a),(x,c),(z,b)}

La composta S_oR = {(1,a),(1,c),(1,b)}



3.2.1-Matrici composte

R = {(1,2),(2,2),(2,4),(3,1),(4,1)}

S = {(1,2),(1,4),(2,3),(4,2)}

$$M_R = \begin{Bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{Bmatrix}$$

$$M_S = \begin{Bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Bmatrix}$$

$S_o R$ = {(1,3),(2,2),(2,3),(3,2),(3,4),(4,2),(4,4)}

$$M_{S_o R} = \begin{Bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{Bmatrix}$$

3.2.2-Moltiplicazione tra matrici

$$M_1 = \begin{Bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{Bmatrix}$$

$$M_2 = \begin{Bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{Bmatrix}$$

$$M_1 \cdot M_2 = \begin{Bmatrix} M_{1,1} = 1 & M_{1,2} = 0 & M_{1,3} = 1 \\ M_{2,1} = 1 & M_{2,2} = 0 & M_{2,3} = 1 \\ M_{3,1} = 0 & M_{3,2} = 1 & M_{3,3} = 1 \end{Bmatrix}$$

$$M_{i,j} = M1_{i,1} \cdot M2_{1,j} + M1_{1,2} \cdot M2_{1,j} + ...$$

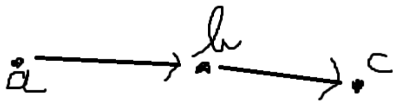
$$M_{3,2} = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 1$$

3.3-Relazioni transitive

Definizione: una relazione $R \subseteq AxA$ è transitiva se $\forall a, b, c \in A$ se $\exists aRb, bRc \implies aRc$

Transitiva:

Non transitiva perché aRb e bRc ma non aRc:



3.3.1-Trasformare una funzione non transitiva in transitiva

1. vedere i controesempi di R, se non ci sono è transitiva
2. aggiungere le frecce mancanti ottenendo una nuova relazione
3. ricominciare da 1

3.3.2-Chiusura transitiva

Presa una relazione R, la chiusura transitiva di R è la più piccola relazione che estende R ed è transitiva.

Definizione:

Cammino: $R \subseteq AxA$ con $a, b \in A$, un cammino di lunghezza $l \geq 1$ da a verso b è una sequenza $x_1, x_2, ..., x_{l-1} \in A$ t.c. $aRx_1Rx_2R...Rx_{l-1}Rb$.

La chiusura transitiva di una relazione R è collegata alla relazione ottenuta componendo R con se stessa varie volte.

Quindi se $R^1 = R$ allora $R^2 = R_oR$ e $R^{n+1} = R^n{}_oR$

Se uniamo tutte le R^n otteniamo $R^\infty \underset{n \in N}{=} R^n$, questi sono due modi diversi che coincidono con la chiusura transitiva di R.

3.4-Intersezione e unione tra relazioni

Se R è transitiva e S è transitiva:

$R \cup S \subseteq$ AxA → $\{(a,b) t.c. (a,b) \in R o (a,b) \in S\}$è transitiva

$R \cap S \subseteq$ AxA → $\{(a,b) t.c. (a,b) \in R e (a,b) \in S\}$è transitiva

3.5-Relazioni di equivalenza

Una relazione $R \subseteq AxA$:

1. È riflessiva se $\forall a \in A \implies aRa$
2. È simmetrica se $\forall a, b \in A$ se $aRb \implies bRa$
3. È transitiva se $\forall a, b, c \in A$ se aRb e $bRa \implies aRc$

3.5.1-Relazione totale

Una relazione $R \subseteq AxA$ è totale se prendendo una qualsiasi coppia di elementi a, b $\exists aRb$ oppure bRa

Deve essere:

- Riflessiva:$\forall a \in A \implies aRa$
- Antisimmetrica:$\forall a, b \in A$ se aRb e $bRa \implies a = b$
- Transitiva: $\forall a, b, c \in A$ se aRb e $bRc \implies aRc$
- Totale:$\forall a, b \in R \implies aRb \text{ oppure } bRa$

3.5.2-Relazione parziale

Una relazione $R \subseteq AxA$ è parziale se solo alcuni elementi sono confrontabili tra loro.

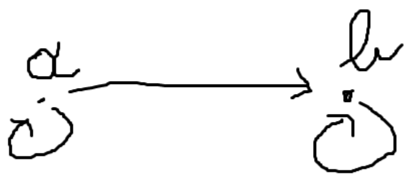
Deve essere:

- Riflessiva:$\forall a \in A \implies aRa$
- Antisimmetrica:$\forall a, b \in A$ se aRb e $bRa \implies a = b$
- Transitiva: $\forall a, b, c \in A$ se aRb e $bRc \implies aRc$

3.5.3-Passare da un ordine parziale ad un ordine totale

Relazione di ordine parziale

Per passare ad una relazione totale bisogna aggiungere almeno una linea per ogni coppia di elementi



Ci sono più relazioni di ordine totale partendo da una singola relazione di ordine parziale.

4-Induzione

Dimostrazione per induzione:

$\forall n \in N$ vale P(n) (proprietà generica in N)

1. Dimostrare che vale per n=1
2. Assumendo P(n) vera per un n generico maggiore di 1, dimostrare che vale la proprietà per n+1

Induzione insiemistica:

Se un insieme X soddisfa le seguenti proprietà:

1. $1 \in X$
2. $\forall N \geq 1$ se $n \in X \implies n + 1 \in X$

Allora S = N

4.1-Principio del minimo numero

$\forall S \subseteq \ N$ con $S \neq ∅ \implies$ S ha un minimo

Dimostrazione per induzione:

Per assurdo S soddisfa 1 e 2 ma $S \neq N \implies \frac{N}{S} \neq \varnothing = X$

X ha un minimo $m > 1 \implies m-1 \notin X \implies m-1 \in N \implies m-1 \in S \implies m-1\ +\ 1 = m \in S \implies m \notin X \implies$ Contraddizione

Esempio:

La somma dei primi n numeri positivi vale $\frac{n(n+1)}{2}$

1. $n = 1 \implies \frac{1(1+1)}{2} = 1$
2. assumo P(n) vera per $n \geq 1$ e dimostro P(n+1):

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

5-Logica Proporzionale

Un argomento logico è formato da 3 proposizioni:

1. argomento iniziale: premessa → conclusione
2. negazione della conclusione
3. negazione della premessa

La 3 è una derivazione delle prime 2.

5.1-Simboli usati

¬ = not

V = or

⋀ = and

→ = allora

↔ = se e solo se

A, B , C = variabili

Esempio:

1. se a = 0 o b = 0 allora ab = 0
2. $ab \neq 0$
3. $a \neq 0$ e $b \neq 0$

Formalizzata usando la logica proporzionale diventa:

1. A V B → C (A = (a = 0), B = (b=0), C = (ab = 0))
2. ¬C
3. ¬A ⋀ ¬B

5.2-Assegnamento

L’assegnamento è una funzione del tipo:

v: VAR → {0,1}

0 vuol dire falso, 1 vuol dire vero.

Regole:

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

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

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

v(A → B) = $\begin{cases} 0 & v(A) = 1, v(B) = 0 \\ 1 & \text{altrimenti} \end{cases}$

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

Possiamo scrivere le funzioni composte secondo queste regole in una tabella della verità.

Esempio:

A = ((P V Q) → (R V (R → Q)))

P	Q	R	R → Q	R V (R → Q)	P V 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

5.3-Soddisfacibilità

Una proposizione A è soddisfacibile se esiste almeno un assegnamento che la soddisfa.

SAT è l'insieme delle proposizioni soddisfacibili($A \in SAT$ se ha almeno una soluzione)

UNSAT è l'insieme delle proposizioni non soddisfacibili($A \in UNSAT$ se non ha soluzioni)

$B \models A$ vuol dire che se un assegnamento soddisfa B allora soddisfa pure A

Se A è vero sempre allora A è una tautologia($A \in TAUT, \neg A \in UNSAT, \varnothing \models A$)