

Trasparenze del corso di

Informatica Teorica

Parte Prima

Insiemi, Relazioni, Funzioni

1

Concetti matematici di base

- Insiemi
- Relazioni
- Funzioni

2

Insiemi

- consideriamo insiemi *finiti* e insiemi *infiniti*
- $|A|$ = cardinalità dell'insieme (finito) A
- alcuni insiemi infiniti di numeri:

lo 0 è incluso nei naturali.

\mathbb{N}	naturali	\mathbb{Q}	razionali relativi
\mathbb{N}^+	naturali positivi	\mathbb{Q}^+	razionali positivi
		\mathbb{Q}^-	razionali negativi
\mathbb{Z}	interi relativi		
\mathbb{Z}^+	interi positivi	\mathbb{R}	reali
\mathbb{Z}^-	interi negativi	\mathbb{R}^+	reali positivi
		\mathbb{R}^-	reali negativi

3

Induzione matematica

per dimostrare proprietà degli elementi di insiemi infiniti
data una proposizione $P(n)$ definita sui naturali, se esiste
un naturale n_0 tale che:

(*passo base*) $P(n_0)$ è vera

(*passo induttivo*) $P(n)$ implica $P(n+1) \forall n \geq n_0$

allora P è vera $\forall n \geq n_0$

esempio:

somma dei naturali non superiori a n : $\sum_{i=1}^n i = \frac{(n+1)n}{2}$

esercizio:

dimostrare che per $n \geq 1$ $\sum_{i=0}^{n-1} 2^i = 2^n - 1$

passo base: $((1+1)*1)/2 = 1$ =sommatoria

passo ind: $(n+1) + \text{som}(i) = (n+1) + ((n+1)n)/2$ (per il passo base) $= (2n+2+n^2+n)/2$

base:

Sottoinsiemi e insiemi uguali

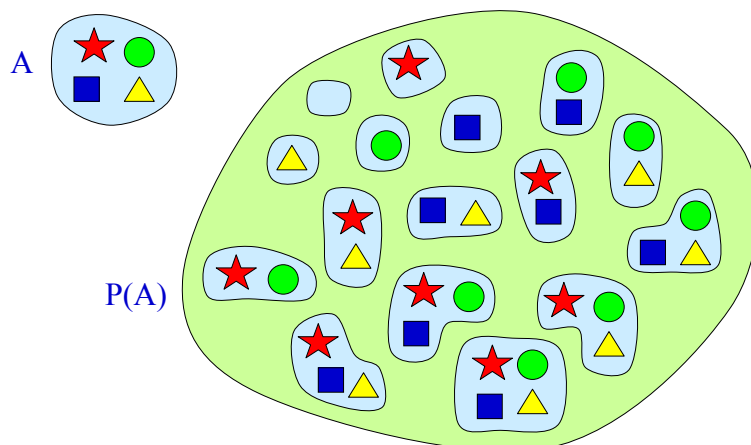
- dati due insiemi A e B, se
 $x \in B \Rightarrow x \in A$
 allora B è *sottoinsieme* di A, e si scrive $B \subseteq A$
- ogni insieme è sottoinsieme di se stesso
- l'insieme vuoto \emptyset è sottoinsieme di ogni insieme
- se A e B sono finiti, allora $B \subseteq A \Rightarrow |B| \leq |A|$
- A e B *insiemi uguali*
 $A=B \Leftrightarrow (x \in A \Leftrightarrow x \in B)$
 si può scrivere anche
 $A=B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$
- A è *sottoinsieme proprio* di B ($A \subset B$) se
 $(A \subseteq B) \wedge (A \neq B)$

5

Insieme delle parti

l'insieme dei sottoinsiemi di A è detto l'*insieme delle parti* di A e si indica con $P(A)$ o 2^A

se A è finito e $|A| = n$ allora $|P(A)| = 2^n$



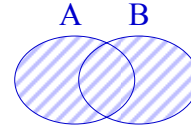
l'insieme delle parti include tutti i possibili sottoinsiemi di A

6

Operazioni tra insiemi

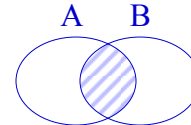
- *unione* $C = A \cup B$

- se A e B sono finiti $|C| \leq |A| + |B|$
- commutativa e associativa



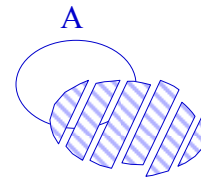
- *intersezione* $C = A \cap B$

- se A e B sono finiti $|C| \leq \min\{|A|, |B|\}$
- commutativa e associativa
- l'intersezione è distributiva rispetto all'unione



- *partizione* di A

- insieme di n sottoinsiemi di A tali che
 $A_1 \cup A_2 \cup \dots \cup A_n = A$
 $i \neq j \Rightarrow A_i \cap A_j = \emptyset$

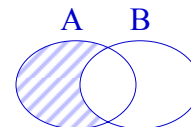


7

Operazioni tra insiemi

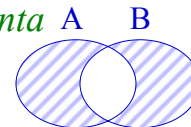
- *complemento* di B rispetto ad A

$$C = A - B = \{x \mid x \in A \wedge x \notin B\}$$



- *differenza simmetrica* o *somma disgiunta*

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



- *prodotto cartesiano* $C = A \times B$

$$C = \{ \langle x, y \rangle \mid x \in A \wedge y \in B \}$$

- insieme di tutte le possibili coppie ordinate
- il prodotto cartesiano è associativo ma non commutativo

$$(A \times B) \times C = A \times (B \times C)$$

8

Relazioni

- siano A_1, A_2, \dots, A_n n insiemi (non necessariamente distinti)
- una *relazione n -aria* è un sottoinsieme di

$$A_1 \times A_2 \times \dots \times A_n$$

$$R \subseteq A_1 \times A_2 \times \dots \times A_n$$

esistono delle n -uple che con rispettano la condizione e quindi vengono "scartate"

esempio:

- la relazione “*minore di*” definita sui naturali è l’insieme $R \subseteq \mathbb{N} \times \mathbb{N} = \mathbb{N}^2$, dove $R = \{ \langle x, y \rangle \mid x < y \}$

9

Relazione d’ordine

- $R \subseteq A^2 = A \times A$ è una *relazione d’ordine* se valgono le seguenti proprietà:

1. *riflessività*

$$\langle x, x \rangle \in R$$

2. *antisimmetria*

$$\langle x, y \rangle \in R \wedge \langle y, x \rangle \in R \Rightarrow x = y$$

3. *transitività*

$$\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \Rightarrow \langle x, z \rangle \in R$$

un insieme su cui è definita una relazione d’ordine si dice parzialmente ordinato o *poset* (“partially ordered set”)

esempio: la relazione “ \leq ” è una relazione d’ordine su \mathbb{N}

10

Relazione d'ordine totale

- una relazione d'ordine $R \subseteq A^2$ è detta *totale* se
 $\langle x, y \rangle \in A^2 \Rightarrow \langle x, y \rangle \in R \vee \langle y, x \rangle \in R$

esempio:

la relazione “ \leq ” è una relazione d'ordine totale su \mathbb{N}
 $1 \leq 2 \leq 3 \leq 4 \leq 5 \leq 6 \leq 7 \leq 8 \dots$

11

Relazione di equivalenza

- $R \subseteq A^2 = A \times A$ è una *relazione di equivalenza* se valgono le seguenti proprietà:

1. *riflessività*

$$\langle x, x \rangle \in R$$

2. *simmetria*

$$\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R$$

3. *transitività*

$$\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \Rightarrow \langle x, z \rangle \in R$$

esempio: la relazione “ $=$ ” è una relazione di equivalenza su \mathbb{R}

12

Relazione di equivalenza

- un insieme A su cui è definita una relazione di equivalenza si può partizionare in sottoinsiemi massimali di equivalenza, detti *classi di equivalenza*
- l'insieme delle classi di equivalenza di A è detto *insieme quoziente* e si denota A/R
- un elemento di A/R si denota con $[a]$
- il numero di classi di A/R si chiama *indice* di R

13

Esempio di relazione di equivalenza

- consideriamo la relazione E_k su \mathbb{N}
 $n \equiv_k m$ **n congruo m modulo k**
se esistono q, q', r (con $r < k$) tali che
 $n = qk + r$ e $m = q'k + r$
- E_k è una relazione di equivalenza
- le sue classi sono le classi resto rispetto alla divisione per k

14

Operazioni su relazioni

- unione*

$$R_1 \cup R_2 = \{ \langle x, y \rangle \mid \langle x, y \rangle \in R_1 \vee \langle x, y \rangle \in R_2 \}$$

- complementazione*

$$\underline{R} = \{ \langle x, y \rangle \mid \langle x, y \rangle \notin R \}$$

- chiusura transitiva*

$$R^+ = \{ \langle x, y \rangle \mid \exists y_1, \dots, y_n \in A, n \geq 2, y_1 = x, y_n = y \text{ tali che } \langle y_i, y_{i+1} \rangle \in R, i = 1, \dots, n-1 \}$$

- chiusura transitiva e riflessiva*

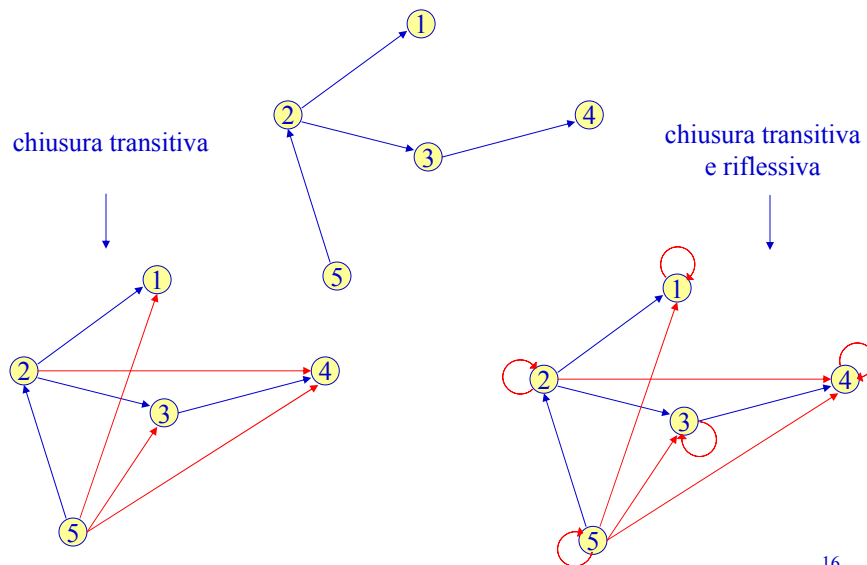
$$R^* = R^+ \cup \{ \langle x, x \rangle \mid x \in A \}$$

chiusura

transitiva: contiene (2, 5)
se conteneva (2, 3) e (3, 5)

chiusura transitiva e riflessiva:
contiene (2, 5) (2, 3) (3, 5) se
conteneva (2, 3) e (3, 5)

Chiusure di relazioni



16

Funzioni

$$R \subseteq X_1 \times \dots \times X_n$$

è una *relazione funzionale* se

$$\forall \langle x_1, \dots, x_{n-1} \rangle \in X_1 \times \dots \times X_{n-1}$$

esiste al più un elemento $x_n \in X_n$ tale che

$$\langle x_1, \dots, x_{n-1}, x_n \rangle \in R$$

si chiama *funzione* la legge che associa $\langle x_1, \dots, x_{n-1} \rangle$ ad x_n

$$f(x_1, \dots, x_{n-1}) = x_n$$

$$f: X_1 \times \dots \times X_{n-1} \rightarrow X_n$$

$X_1 \times \dots \times X_{n-1}$ è il *tipo* della funzione

la funzione trasforma gli n-1 elementi nell'elemento n

17

Funzioni: dominio codominio

$\text{dom}(f) = \text{dominio}$ di f

sottoinsieme di $X_1 \times \dots \times X_{n-1}$

$$\text{dom}(f) = \{ \langle x_1, \dots, x_{n-1} \rangle \in X_1 \times \dots \times X_{n-1} \mid \\ \exists x_n \in X_n \ f(x_1, \dots, x_{n-1}) = x_n \}$$

$\text{cod}(f) = \text{codominio}$ di f

sottoinsieme di X_n

$$\text{cod}(f) = \{ x_n \in X_n \mid \\ \exists \langle x_1, \dots, x_{n-1} \rangle \in X_1 \times \dots \times X_{n-1} \\ f(x_1, \dots, x_{n-1}) = x_n \}$$

18

Funzioni: fibra

dato un x_n

$f^{-1}(x_n) = \text{controimmagine o fibra di } x_n$

sottoinsieme di $X_1 \times \dots \times X_{n-1}$

$f^{-1}(x_n) = \{ \langle x_1, \dots, x_{n-1} \rangle \in X_1 \times \dots \times X_{n-1} \mid$

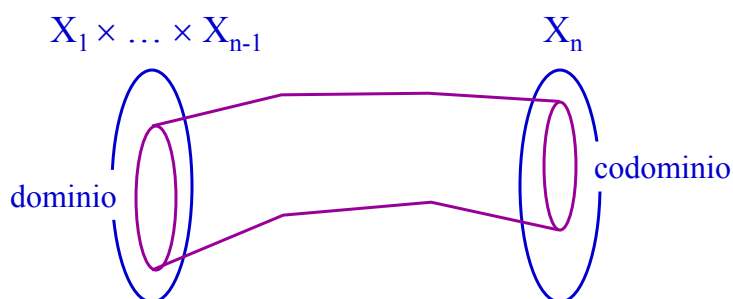
$\langle x_1, \dots, x_{n-1} \rangle \in \text{dom}(f)$

\wedge

$f(x_1, \dots, x_{n-1}) = x_n \}$

19

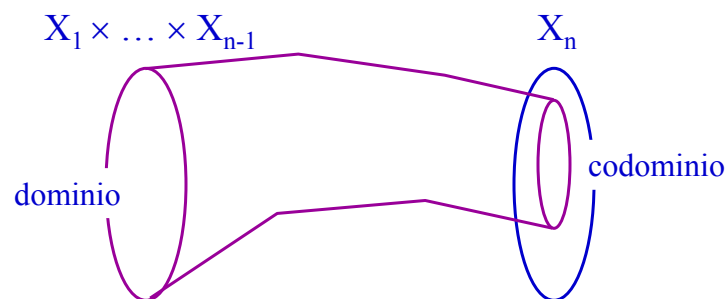
Funzione



20

Funzione totale

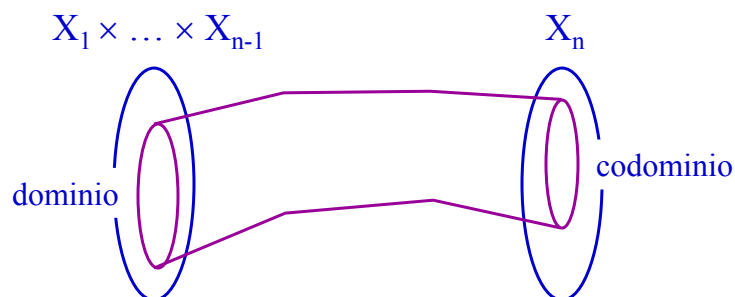
- una funzione f è *totale* se $\text{dom}(f) = X_1, \dots, X_{n-1}$



21

Funzione parziale

- una funzione f è *parziale* se $\text{dom}(f) \subseteq X_1, \dots, X_{n-1}$

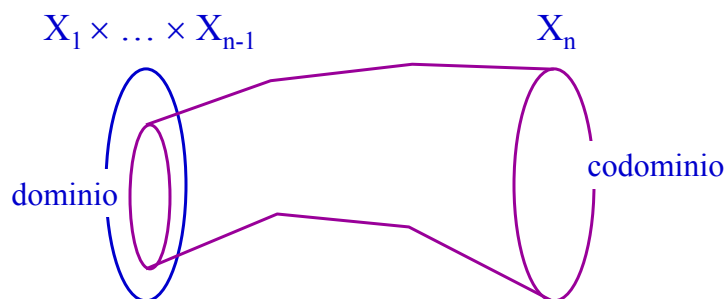


- tutte le funzioni sono parziali

22

Funzione suriettiva

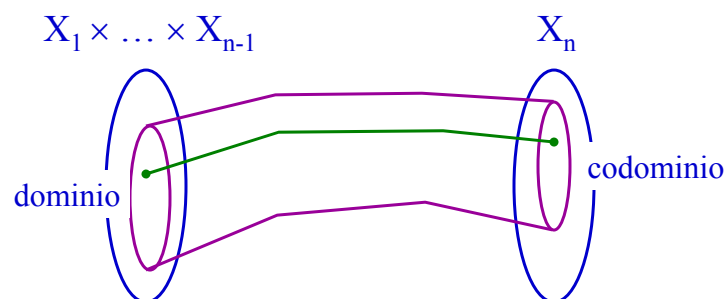
- una funzione f è *suriettiva* se $\text{cod}(f) = X_n$



23

Funzione iniettiva

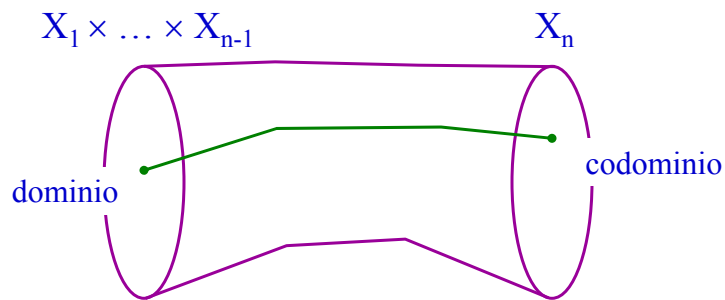
- una funzione f è *iniettiva* se $|f^{-1}(x_n)|=1$



24

Funzione biiettiva

- una funzione f è *biiettiva* (biiezione) se è iniettiva, suriettiva e totale



25

Pidgeonhole principle

teorema:

dati due insiemi A e B tali che

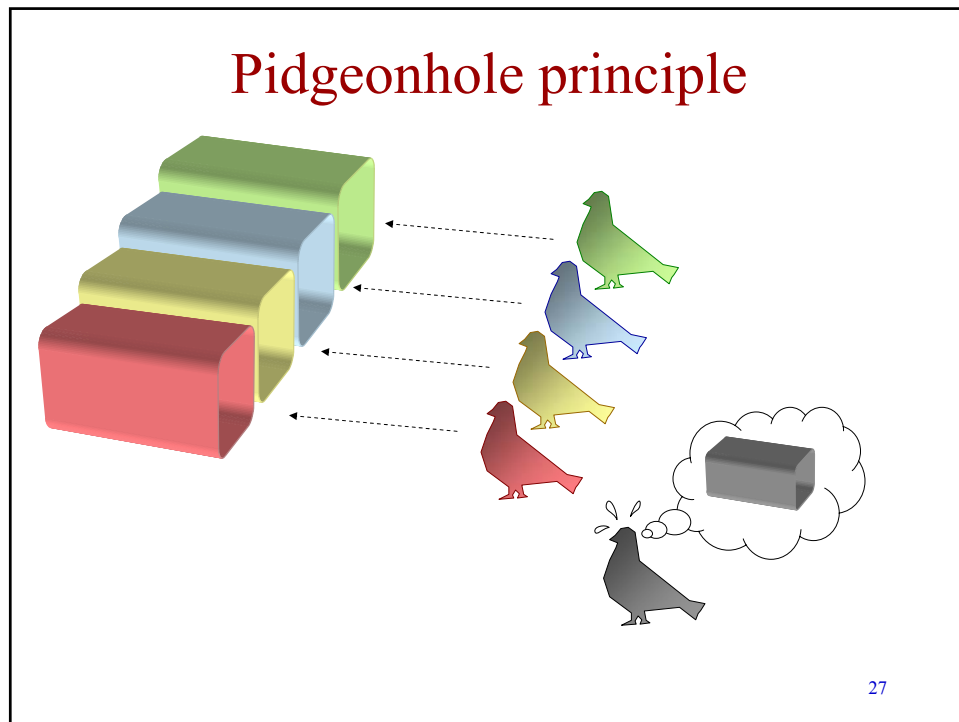
$$0 < |B| < |A| < \infty$$

non esiste una funzione $f: A \rightarrow B$ che sia totale e iniettiva

dimostrazione:

basata sulla cardinalità di B e per induzione

26



Dimostrazione (pidgeonhole principle)

- dimostrazione per induzione
 - passo base: $|B|=1$
 - passo induttivo: $|B|>1$
- passo base ($|B|=1$)
 - $B=\{b\}$, $|A|>1$, es. $A=\{a_1, a_2\}$
 - se f è totale, allora $f(a_1)=b$ e $f(a_2)=b$
 - allora f non è iniettiva perché $|f^{-1}(b)|>1$

28

Dimostrazione (pidgeonhole principle)

- **passo induttivo:** $|B| > 1$

supponiamo sia vero per $|B| = n$ ed $|A| \geq n+1$

dimostriamo che è vero per $|B| = n+1$ e $|A| \geq n+2$

ipotizziamo per assurdo che esista una funzione totale iniettiva f e scegliamo un qualunque elemento b di B

se $|f^{-1}(b)| \geq 2 \Rightarrow$ contraddizione \Rightarrow teorema dimostrato

se $|f^{-1}(b)| \leq 1$ consideriamo

$$A' = A - \{f^{-1}(b)\} \quad \text{e} \quad B' = B - \{b\}$$

$$|A'| \geq n+1 > |B'| = n$$

appliciamo l'ipotesi induttiva \Rightarrow contraddizione

la cardinalità ci indica quali funzioni posso applicare su due insiemi

procedo mano a mano eliminando dagli insiemi A e B le coppie ax e bx . Non troverò tutte le coppie quindi l'insieme finale A' avrà cardinalità diversa ($n+1 > n$)

29

Cardinalità di insiemi infiniti

- due insiemi sono *equinumerosi* se esiste una biiezione tra essi
- la relazione di equinumerosità è una relazione di equivalenza
- possiamo ora dare una definizione rigorosa di *cardinalità di un insieme finito* A :

$$|A| = 0 \text{ se } A = \emptyset$$

$$|A| = n \text{ se } A \text{ è equinumeroso a } \{0, 1, \dots, n-1\}$$

30

Numerabilità

- un insieme è *numerabile* se è equinumeroso a \mathbb{N}
- un insieme è *contabile* se è finito o numerabile
- un insieme ha cardinalità *aleph zero* (\aleph_0) se è equinumeroso a \mathbb{N} , cioè numerabile
- sottoinsiemi di insiemi contabili sono contabili
- insiemi equinumerosi ad insiemi contabili sono contabili

31

Numerabilità degli interi relativi

teorema:

l'insieme \mathbb{Z} degli interi relativi è numerabile

dimostrazione:

biiezione con \mathbb{N}

\mathbb{Z} :	0	1	-1	2	-2	3	-3	4	-4	...
\mathbb{N} :	0	1	2	3	4	5	6	7	8	...

32

Numerabilità dei numeri pari

teorema:

l'insieme P dei numeri pari è numerabile

dimostrazione:

biiezione con N

P:	0	2	4	6	8	10	12	14	16	...
N:	0	1	2	3	4	5	6	7	8	...

33

Numerabilità

teorema:

l'insieme N^2 delle coppie di naturali è numerabile

dimostrazione:

tecnica usata da Cantor per mostrare la numerabilità di Q

	0	1	2	3	4
0	0	1	3	6	10
1	2	4	7	11	
2	5	8	12		
3	9	13			
4	14				

osservazione:

per ogni $n \in N$, se A è numerabile, anche A^n è numerabile

34

Cardinalità di unioni di insiemi

teorema:

l'unione di una quantità contabile di insiemi contabili è contabile

dimostrazione:

S_0	a_{01}	a_{02}	a_{03}	a_{04}	a_{05}
S_1	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
S_2	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}
S_3	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}
S_4	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}

35

Insiemi non numerabili

per dimostrare la non numerabilità di un insieme si usa la *tecnica di diagonalizzazione* di Cantor

teorema:

\mathbb{R} non è numerabile

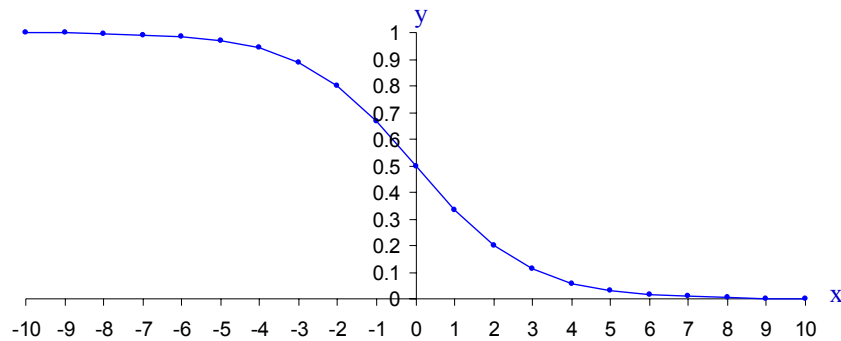
dimostrazione:

1. dimostriamo che \mathbb{R} è equinumeroso a $(0,1)$
2. dimostriamo che $(0,1)$ non è numerabile

36

Insiemi non numerabili

$(0,1)$ e \mathbb{R} sono equinumerosi: una biiezione è data, per esempio, dalla funzione $y = \frac{1}{(2^{x+1})}$



37

Insiemi non numerabili

- Supponiamo per assurdo che una enumerazione di $(0,1)$ esista, denotiamo con Φ_i l' i -esimo elemento di $(0,1)$
- consideriamo $r \in (0,1)$ che ha come i -esima cifra della mantissa ($i=1, 2, \dots$) un valore diverso da 0, da 9, e dal valore della i -esima cifra di Φ_i

38

Insiemi non numerabili

cifre delle mantisse di Φ_i :

	1	2	3	4	5	6	7	...
Φ_1	5	1	0	4	3	9	6	...
Φ_2	2	4	1	0	0	0	0	...
Φ_3	7	9	8	5	3	7	7	...
Φ_4	0	0	4	6	0	3	1	...

r	6	5	1	7
---	---	---	---	---	-----	-----	-----	-----

r , detto *elemento diagonale*, non fa parte della enumerazione, in quanto differisce da ogni elemento della enumerazione in almeno una cifra, e ciò è assurdo

39

Insiemi non numerabili

teorema:

$P(N)$ non è numerabile

dimostrazione:

supponiamo per assurdo che lo sia

sia $P_1, P_2, \dots, P_i, \dots$ una sua enumerazione

a ciascun P_i associamo la sequenza

$b_{i0}, b_{i1}, b_{i2}, \dots$, dove

$$b_{ij}=0 \text{ se } j \notin P_i$$

$$b_{ij}=1 \text{ se } j \in P_i$$

40

Insiemi non numerabili

costruiamo ora l'insieme P (diagonale) con sequenza $p_0, p_1, \dots, p_k, \dots$ dove

$$p_k = 1 - b_{kk}$$

P differisce da ogni P_i , in quanto

$$i \in P \Leftrightarrow i \notin P_i$$

osservazione: la non numerabilità di $P(N)$ vale anche per l'insieme delle parti di ogni insieme di cardinalità \aleph_0

41

Funzione caratteristica

si dice *funzione caratteristica* $f_S(x)$ di $S \subseteq N$ la funzione totale

$$f_S: N \rightarrow \{0, 1\}$$

$$f_S(x) = 0 \text{ se } x \notin S, f_S(x) = 1 \text{ se } x \in S$$

la funzione caratteristica identifica il problema del test di appartenenza ad un insieme a quello del calcolo di una funzione

teorema:

l'insieme delle funzioni caratteristiche su N non è numerabile

dimostrazione:

ovvia, considerando la biiezione tra $P(N)$ e l'insieme delle funzioni caratteristiche

42

Cardinalità transfinite – notazione aleph

- se un insieme finito ha cardinalità n , il suo insieme delle parti ha cardinalità 2^n
- analogamente, se un insieme infinito ha cardinalità \aleph_0 denotiamo con 2^{\aleph_0} la cardinalità del suo insieme delle parti
- gli insiemi con cardinalità 2^{\aleph_0} sono detti *continui*

43

Cardinalità delle funzioni totali intere

- le funzioni totali intere sono un insieme continuo
- $|\{f | f:N \rightarrow N\}| \geq 2^{\aleph_0}$
 - infatti, $\{f | f:N \rightarrow N\} \supseteq \{f | f:N \rightarrow \{0,1\}\}$, e $|\{f | f:N \rightarrow \{0,1\}\}| = 2^{\aleph_0}$
- $|\{f | f:N \rightarrow N\}| \leq 2^{\aleph_0}$
 - infatti $\{f | f:N \rightarrow N\} \subseteq P(N^2)$
 - N^2 è equinumeroso ad N
 - $|P(N^2)| = 2^{\aleph_0}$
- ne segue che $|\{f | f:N \rightarrow N\}| = 2^{\aleph_0}$

44

Cardinalità transfinita

teorema:

\mathbb{R} è equipotente a $\mathcal{P}(\mathbb{N})$ ed è quindi continuo

dimostrazione:

è sufficiente mostrare che la proprietà vale per i reali in $(0,1)$, vista la biiezione tra \mathbb{R} e $(0,1)$

uso della rappresentazione binaria della mantissa e del concetto di funzione caratteristica

i cardinali transfiniti servono a denotare la cardinalità di insiemi infiniti (es: \aleph_0 , 2^{\aleph_0} , $2^{2^{\aleph_0}}$, ...)

Cantor ha dimostrato che esistono infiniti cardinali transfiniti

vedremo come considerazioni relative alla cardinalità di insiemi infiniti daranno interessanti spunti sull'idea di calcolabilità

45