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.

N	naturali	Q	razionali relativi
N^+	naturali positivi	Q^+	razionali positivi
		Q^-	razionali negativi
Z	interi relativi		
Z^+	interi positivi	R	reali
Z^-	interi negativi	R^+	reali positivi
		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) + som(i) = (n+1)+ ((n+1)n)/2 (per il passo base) = (2n+2+n^2+n)/2

base:

Sottoinsiemi e insiemi uguali

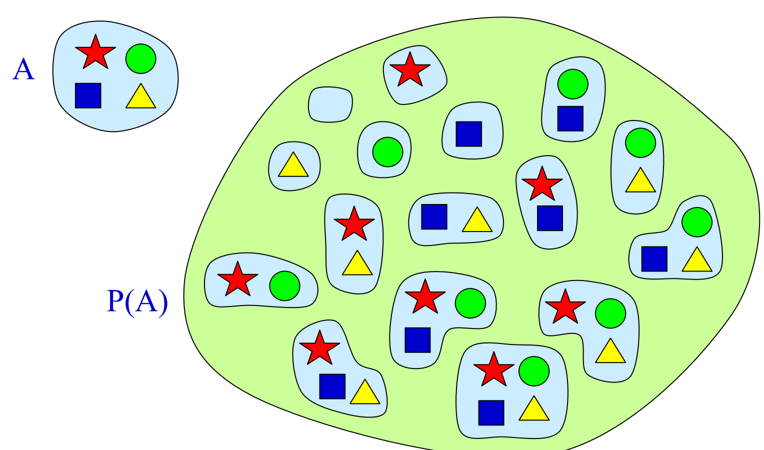
- dati due insiemi A e B, se
  $x \in B \Rightarrow x \in A$
  allora B è *sottoinsieme* di A, e si scrive $B \subseteq A$
- ogni insieme è sottoinsieme di se stesso
- l'insieme vuoto $\varnothing$ è sottoinsieme di ogni insieme
- se A e B sono finiti, allora $B \subseteq A \Rightarrow |B| \leq |A|$
- 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 $|P(A)| = 2^n$

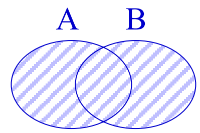


l'insieme delle parti include tutti i possibili sottoinsiemi di A

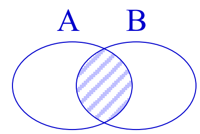
6

Operazioni tra insiemi

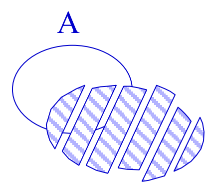
- *unione* $C = A \cup B$
  - se A e B sono finiti $|C| \leq |A|+|B|$
  - commutativa e associativa



- *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



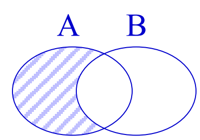
- *partizione* di A
  - insieme di n sottoinsiemi di A tali che
    $A_1 \cup A_2 \cup \ldots \cup A_n = A$
    $i \neq j \Rightarrow A_i \cap A_j = \varnothing$



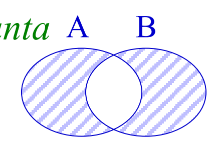
7

Operazioni tra insiemi

- *complemento* di B rispetto ad A
  $C = A\text{-}B = \{x|\ x \in A \wedge x \notin B\}$



- *differenza simmetrica* o *somma disgiunta*
  $A+B=A \cup B-(A \cap B)$



- *prodotto cartesiano* $C=A \times B$
  $C= \{<x,y>|\ x \in A \wedge y \in B\}$
  - insieme di tutte le possibili coppie ordinate
  - il prodotto cartesiano è associativo ma non commutativo

    (AxB)xC = Ax(BxC)

8

Relazioni

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

$$A_1 \times A_2 \times \ldots \times A_n$$

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

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

esempio:

- la relazione "minore di" definita sui naturali è l'insieme $R \subseteq N \times N = N^2$, dove $R=\{<x,y>| x<y\}$

9

Relazione d'ordine

- $R \subseteq A^2 = A \times A$ è una *relazione d'ordine* se valgono le seguenti proprietà:
  1. *riflessività*
     $<x,x> \in R$
  2. *antisimmetria*
     $<x,y> \in R \wedge <y,x> \in R \Rightarrow x=y$
  3. *transitività*
     $<x,y> \in R \wedge <y,z> \in R \Rightarrow <x,z> \in R$

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 N

10

Relazione d'ordine totale

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

esempio:

la relazione "≤" è una relazione d'ordine totale su N
$1 \leq 2 \leq 3 \leq 4 \leq 5 \leq 6 \leq 7 \leq 8 \ldots$

11

Relazione di equivalenza

- $R \subseteq A^2 = A \times A$ è una *relazione di equivalenza* se valgono le seguenti proprietà:
  1. *riflessività*
     $<x,x> \in R$
  2. *simmetria*
     $<x,y> \in R \Rightarrow <y,x> \in R$
  3. *transitività*
     $<x,y> \in R \wedge <y,z> \in R \Rightarrow <x,z> \in R$

esempio: la relazione "=" è una relazione di equivalenza su 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 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

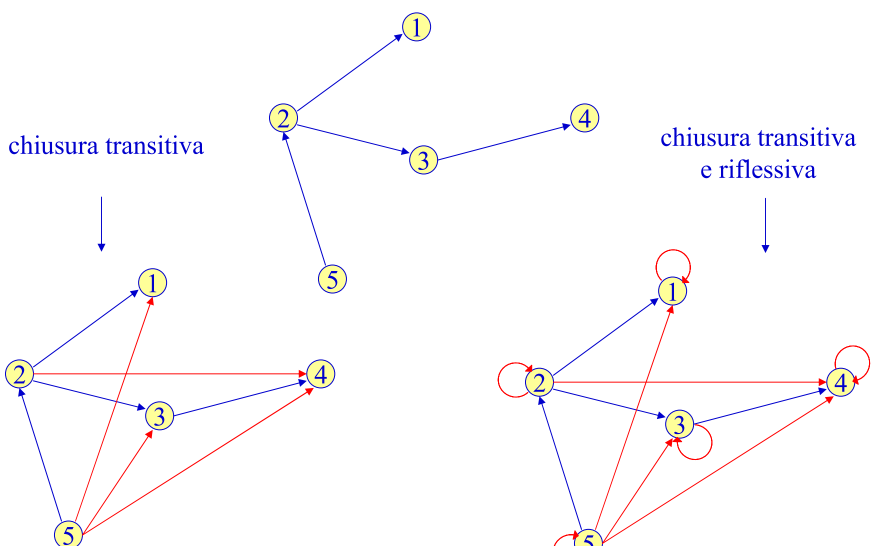
Operazioni su relazioni

- *unione*
  $R_1 \cup R_2 = \{<x,y> \mid <x,y> \in R_1 \vee <x,y> \in R_2\}$
- *complementazione*
  $\underline{R} = \{<x,y> \mid <x,y> \notin R\}$
- *chiusura transitiva*
  $R^+ = \{<x,y> \mid \exists y_1, \ldots, y_n \in A,\ n \geq 2,\ y_1 = x,\ y_n = y$ tali che $<y_i, y_{i+1}> \in R,\ i = 1, \ldots, n-1\}$
- *chiusura transitiva e riflessiva*
  $R^* = R^+ \cup \{<x,x> \mid x \in A\}$

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

$$R \subseteq X_1 \times \ldots \times X_n$$

è una *relazione funzionale* se

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

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

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

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

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

$$f\colon X_1 \times \ldots \times X_{n-1} \to X_n$$

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

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

17

Funzioni: dominio codominio

dom(f) = *dominio* di f

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

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

cod(f) = *codominio* di f

sottoinsieme di X_n

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

18

Funzioni: fibra

dato un x_n

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

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

$f^{-1}(x_n) = \{<x_1, \ldots, x_{n-1}> \in X_1 \times \ldots \times X_{n-1} \mid$

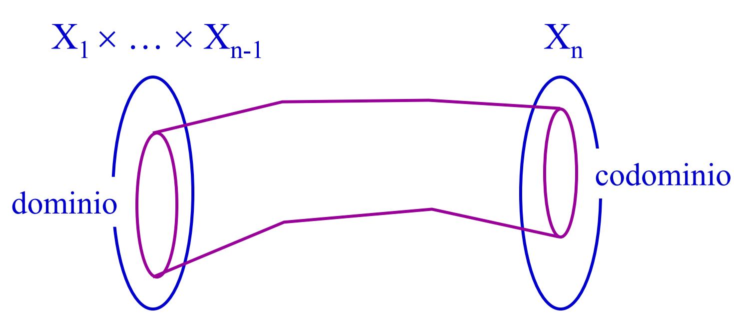
$<x_1, \ldots, x_{n-1}> \in dom(f)$

$\wedge$

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

19

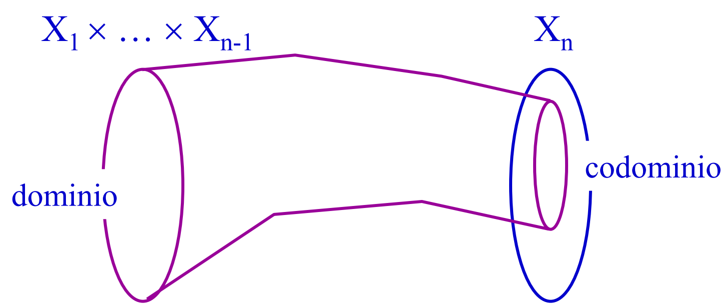
Funzione



20

Funzione totale

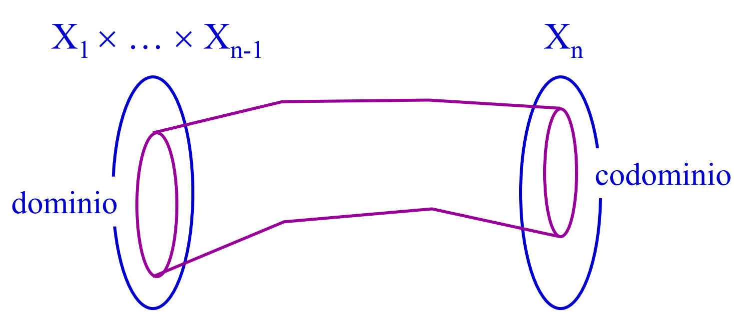
- una funzione f è *totale* se dom(f) = $X_1, \ldots, X_{n-1}$



21

Funzione parziale

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

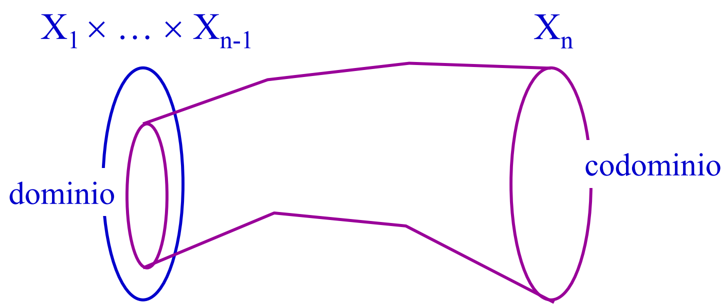


- tutte le funzioni sono parziali

22

Funzione suriettiva

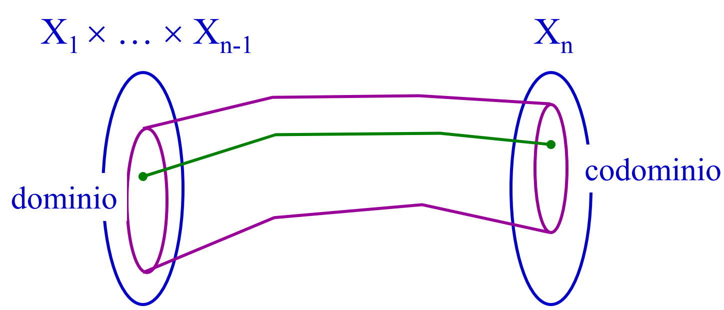
- una funzione f è *suriettiva* se cod(f) = X_n



23

Funzione iniettiva

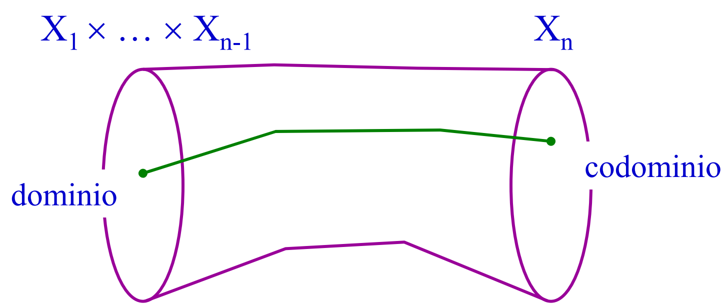
- una funzione f è *iniettiva* se $|f^{-1}(x_n)|=1$



24

Funzione biiettiva

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



25

tutti gli elementi di A corrispondono a tutti gli elementi di B. Quindi anche nel senso inverso (f^-1) sarà totale, iniettiva e suriettiva.

Pidgeonhole principle

teorema:

dati due insiemi A e B tali che

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

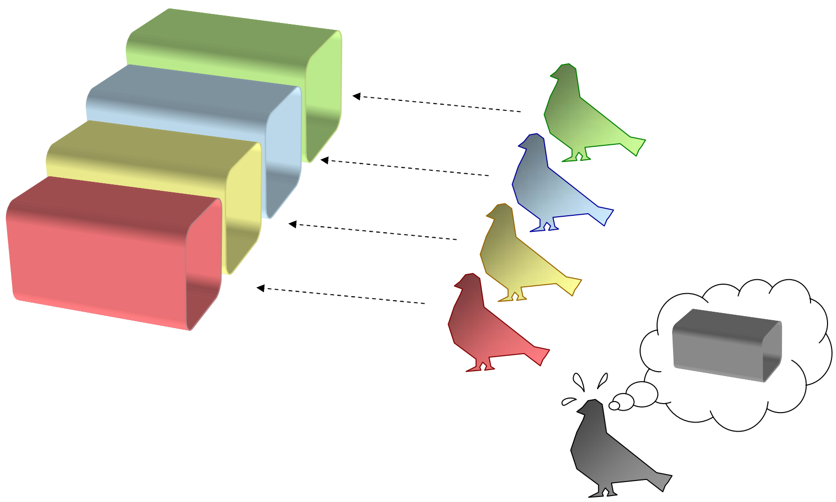
non esiste una funzione f: $A \rightarrow B$ che sia totale e iniettiva

dimostrazione:

basata sulla cardinalità di B e per induzione

26

Pidgeonhole principle



27

Dimostrazione (pidgeonhole principle)

- dimostrazione per induzione
  - passo base: |B|=1
  - passo induttivo: |B|>1

non esiste una funzione iniettiva e totale A->B se la cardinalità di B è minore della cardinalità di A

- 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

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

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

  applichiamo l'ipotesi induttiva $\Rightarrow$ contraddizione

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)

f^-1(b) = controimmagine o fibra

29

la cardinalità ci indica quali funzioni posso applicare su due insiemi

Cardinalità di insiemi infiniti

Questi 2 insiemi possono essere 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:

  $|A|=0$ se $A=\emptyset$

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

biiezione: iniettiva, suriettiva e totale

è lo stesso procedimento che si esegue quando si contano gli elementi di un insieme

30

l'insieme vuoto non ha caratterizzazione (non puo' esserci un insieme vuoto di mele)

Numerabilità

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

31

ovvero che esiste una biiezione con N

Numerabilità degli interi relativi

teorema:

l'insieme Z degli interi relativi è numerabile

dimostrazione:

biiezione con N

Z:	0	1	-1	2	-2	3	-3	4	-4	…
N:	0	1	2	3	4	5	6	7	8	…

32

ad ogni elemento di Z posso far corrispondere un elemento di N. if (x>0) { y = 2x−1} else { y = 2x}

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	…

y= x/2

33

Numerabilità

alef zero * alef zero = alef zero

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				

data una coppia di naturali ottengo un altro naturale. Questo vale anche per triple, quadruple etc.

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:

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

anche qui posso trovare un numero che corrisponde a qualsiasi elemento dell'unione, usando le diagonali

35

Insiemi non numerabili

hanno più elementi dei numerabili

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

teorema:

R non è numerabile

I naturali sono contenuti nei reali ma questo non implica che i reali siano numerabili!

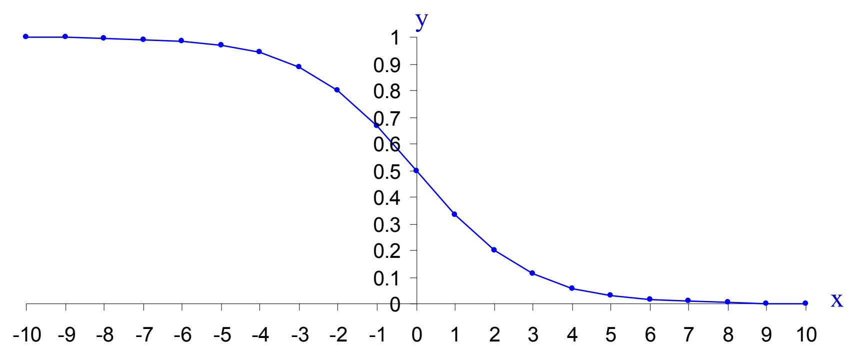
dimostrazione:

1. dimostriamo che R è equinumeroso a (0,1)
2. dimostriamo che (0,1) non è numerabile

36

Insiemi non numerabili

(0,1) e 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'iesimo elemento di (0,1)
- consideriamo $r \in (0,1)$ che ha come i-esima cifra della mantissa (i=1, 2, …) un valore diverso da 0, da 9, e dal valore della i-esima cifra di Φ_i

l'iesimo di (0,1) che corrisponde al naturale

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 è un reale ma NON ha un corrispondente naturale, perchè se fosse nella posizione k sarebbe diverso da se stesso (la sua k-esima cifra)

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

P(N) = insieme dei sottoinsiemi (insieme delle parti)

teorema:

P(N) non è numerabile

dimostrazione:

supponiamo per assurdo che lo sia

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

a ciascun P_i associamo la sequenza

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

$$b_{ij}=0 \text{ se } j \notin P_i$$
$$b_{ij}=1 \text{ se } j \in P_i$$

costruisco una sorta di firma per determinare se l'elemento appartiene a Pi

40

Insiemi non numerabili

costruiamo ora l'insieme P (diagonale) con sequenza $p_0, p_1, \ldots, p_k, \ldots$ 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 $\aleph_0$

usiamo la stessa tecnica per determinare la non numerabilità dei reali (mediante l'elemento r che dovrebbe essere diverso da se stesso)

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

come le firme 0 o 1 usate nella dimostrazione precedente

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

transfinito e infinito
sono lo stesso concetto

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*

2^alef zero è uguale a alef uno? (ovvero è la cardinalità successiva ad alef zero?) Non si può negare, ma non si può neanche affermare

43

Cardinalità delle funzioni totali intere

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

una relazione funzionale è un sottoinsieme dell'insieme delle parti del prodotto cartesiano

44

Cardinalità transfinite

teorema:

R è equinumeroso a P(N) ed è quindi continuo

dimostrazione:

è sufficiente mostrare che la proprietà vale per i reali in (0,1), vista la biiezione tra 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: $\aleph_0$, $2^{\aleph_0}$, $22^{\aleph_0}$, …)

Cantor ha dimostrato che esistono infiniti cardinali transfiniti

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