ELEMENTI DI TEORIA DELLA COMPUTAZIONE

M.Anselmo

a.a. 2022/23

DECIDIBILITÀ E INDECIDIBILITÀ

3 maggio 2022

Obiettivo: analizzare i limiti della risoluzione dei problemi mediante algoritmi.

Studieremo: il potere computazionale degli algoritmi nella soluzione dei problemi.

Proveremo che esistono problemi che possono essere risolti mediante algoritmi e altri no.

Ricorda: Problemi di decisione

I problemi di decisione sono problemi che hanno come soluzione una risposta SI o NO.
Rappresenteremo i problemi di decisione mediante linguaggi.
Esempio.
PRIMO: Dato un numero x, x è primo?
Il linguaggio che rappresenta "PRIMO" è

$$P = \{\langle x \rangle \mid x \text{ è un numero primo}\}$$

dove $\langle x \rangle =$ "ragionevole" codifica di x mediante una stringa
Risolvere PRIMO equivale a decidere il linguaggio P

In questo modo esprimiamo un problema computazionale come un problema di riconoscimento di un linguaggio (insieme delle codifiche di istanze SI per il problema).

Problemi indecidibili

Motivazioni per lo studio di questi problemi:

- Sapere che esistono problemi non risolvibili con un computer

Problemi indecidibili

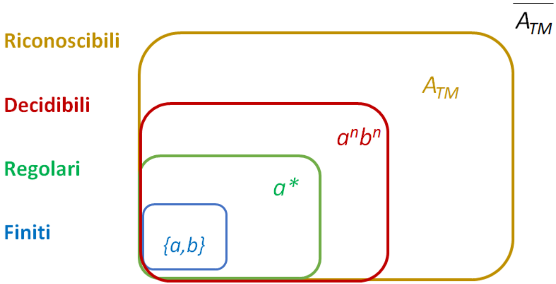
Motivazioni per lo studio di questi problemi:

- Sapere che esistono problemi non risolvibili con un computer

I problemi indecidibili sono esoterici o lontani dai problemi di interesse informatico? NO Esempi di problemi indecidibili:

- Il problema generale della verifica del software non è risolvibile mediante computer
  - Costruire un perfetto sistema di "debugging" per determinare se un programma si arresta.
  - Equivalenza di programmi: Dati due programmi essi forniscono lo stesso output?
- Compressione dati ottimale: Trovare il programma più corto per produrre una immagine data.
- Individuazione dei virus: Questo programma è un virus?

Risultati



Riconoscibili
Decidibili
Regolari
Finiti
$\overline{A_{TM}}$
A_{TM}
$a^n b^n$
$a*$
$\{a,b\}$

Strumenti

- Cardinalità di insiemi (infiniti)
- Diagonalizzazione: metodo introdotto da Cantor
- Autoreferenzialità

La dimostrazione dell'esistenza di un linguaggio non Turing riconoscibile (e di un linguaggio indecidibile) utilizza una tecnica chiamata diagonalizzazione, introdotta dal matematico Georg Cantor nel 1873.

La dimostrazione dell'esistenza di un linguaggio non Turing riconoscibile (e di un linguaggio indecidibile) utilizza una tecnica chiamata diagonalizzazione, introdotta dal matematico Georg Cantor nel 1873.
Cantor si pose il problema seguente: se abbiamo due insiemi infiniti, come possiamo dire se uno è più grande dell'altro o se hanno la stessa dimensione?

La dimostrazione dell'esistenza di un linguaggio non Turing riconoscibile (e di un linguaggio indecidibile) utilizza una tecnica chiamata diagonalizzazione, introdotta dal matematico Georg Cantor nel 1873.
Cantor si pose il problema seguente: se abbiamo due insiemi infiniti, come possiamo dire se uno è più grande dell'altro o se hanno la stessa dimensione?
Per gli insiemi finiti basta contare gli elementi dei due insiemi, ma non possiamo applicare questo metodo del conteggio agli insiemi infiniti.

La dimostrazione dell'esistenza di un linguaggio non Turing riconoscibile (e di un linguaggio indecidibile) utilizza una tecnica chiamata diagonalizzazione, introdotta dal matematico Georg Cantor nel 1873.
Cantor si pose il problema seguente: se abbiamo due insiemi infiniti, come possiamo dire se uno è più grande dell'altro o se hanno la stessa dimensione?
Per gli insiemi finiti basta contare gli elementi dei due insiemi, ma non possiamo applicare questo metodo del conteggio agli insiemi infiniti. Per esempio, prendiamo l'insieme degli interi positivi pari e l'insieme di tutte le stringhe su un alfabeto. Entrambi gli insiemi sono infiniti, ma uno dei due è più grande rispetto all'altro?

Cardinalità

Quanti numeri naturali ci sono? INFINITI!

Cardinalità

Quanti numeri naturali ci sono? INFINITI!

Quanti numeri naturali pari ci sono? INFINITI!

Cardinalità

Quanti numeri naturali ci sono? INFINITI!
Quanti numeri naturali pari ci sono? INFINITI!
Quanti numeri naturali dispari ci sono? INFINITI!

Cardinalità

Quanti numeri naturali ci sono? INFINITI!
Quanti numeri naturali pari ci sono? INFINITI!
Quanti numeri naturali dispari ci sono? INFINITI!

Quanti numeri **reali** ci sono? INFINITI!

Cardinalità

Quanti numeri naturali ci sono? INFINITI!
Quanti numeri naturali pari ci sono? INFINITI!
Quanti numeri naturali dispari ci sono? INFINITI!

Quanti numeri **reali** ci sono? INFINITI!
La quantità di numeri reali è la stessa di quella dei numeri naturali?

Come si misura la cardinalità di insiemi infiniti?

Cantor propose una soluzione interessante al problema di confrontare gli insiemi infiniti, in particolare a come stabilire se, dati due insiemi infiniti, uno sia è più grande dell'altro.

Cantor propose una soluzione interessante al problema di confrontare gli insiemi infiniti, in particolare a come stabilire se, dati due insiemi infiniti, uno sia è più grande dell'altro.

Osservò che due insiemi finiti hanno la stessa cardinalità se gli elementi dell'uno possono essere messi in corrispondenza uno a uno con quelli dell'altro.
Questo metodo confronta le dimensioni senza ricorrere al conteggio.

Cantor propose una soluzione interessante al problema di confrontare gli insiemi infiniti, in particolare a come stabilire se, dati due insiemi infiniti, uno sia è più grande dell'altro.

Osservò che due insiemi finiti hanno la stessa cardinalità se gli elementi dell'uno possono essere messi in corrispondenza uno a uno con quelli dell'altro.
Questo metodo confronta le dimensioni senza ricorrere al conteggio.

Estese questo concetto agli insiemi infiniti.

Funzioni

Definizione

Una funzione $f : X \to Y$ *è una relazione che associa ad ogni elemento* x *in* X *uno e un solo elemento* $y = f(x)$ *in* Y*.*
X *è il* **dominio** *della funzione,*
Y *è il* **codominio** *della funzione.*

Funzioni

Definizione

Una funzione $f : X \to Y$ *è una relazione che associa ad ogni elemento* x *in* X *uno e un solo elemento* $y = f(x)$ *in* Y.
X *è il* **dominio** *della funzione,*
Y *è il* **codominio** *della funzione.*

Definizione

Una funzione $f : X \to Y$ *è iniettiva se*
$\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$

Funzioni

Definizione

Una funzione $f : X \to Y$ *è una relazione che associa ad ogni elemento* x *in* X *uno e un solo elemento* $y = f(x)$ *in* Y*.*
X *è il* **dominio** *della funzione,*
Y *è il* **codominio** *della funzione.*

Definizione

Una funzione $f : X \to Y$ *è iniettiva se*
$\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$

Definizione

Una funzione $f : X \to Y$ *è suriettiva se* $\forall y \in Y$ *esiste* $x \in X$ *tale che* $y = f(x)$*.*

Funzioni

Definizione

Una funzione $f : X \to Y$ *è una relazione che associa ad ogni elemento* x *in* X *uno e un solo elemento* $y = f(x)$ *in* Y.
X *è il* **dominio** *della funzione,*
Y *è il* **codominio** *della funzione.*

Definizione

Una funzione $f : X \to Y$ *è iniettiva se*
$\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$

Definizione

Una funzione $f : X \to Y$ *è suriettiva se* $\forall y \in Y$ *esiste* $x \in X$ *tale che* $y = f(x)$.

Definizione

Una funzione $f : X \to Y$ *è una funzione biettiva di* X *su* Y *(o una biezione tra* X *e* Y*) se* f *è iniettiva e suriettiva.*

Esempi

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 2$, $f(5) = 4$ è una funzione. Non è nè iniettiva nè suriettiva.

Esempi

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 2$, $f(5) = 4$ è una funzione. Non è nè iniettiva nè suriettiva.

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7, 9\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione iniettiva ma non suriettiva.

Esempi

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 2$, $f(5) = 4$ è una funzione. Non è nè iniettiva nè suriettiva.

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7, 9\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione iniettiva ma non suriettiva.

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 2$ è una funzione suriettiva ma non iniettiva.

Esempi

Esempio $f : \{1, 2, 5\} \to \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 2$, $f(5) = 4$ è una funzione. Non è nè iniettiva nè suriettiva.

Esempio $f : \{1, 2, 5\} \to \{2, 4, 7, 9\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione iniettiva ma non suriettiva.

Esempio $f : \{1, 2, 5\} \to \{2, 4\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 2$ è una funzione suriettiva ma non iniettiva.

Esempio $f : \{1, 2, 5\} \to \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione biettiva.

Cardinalità

Definizione

Due insiemi X e Y hanno la stessa cardinalità se esiste una funzione biettiva $f : X \to Y$ di X su Y.

$$|X| = |Y| \Leftrightarrow \text{ esiste una funzione biettiva } f : X \to Y$$

.

Cardinalità

Definizione

Due insiemi X e Y hanno la stessa cardinalità se esiste una funzione biettiva $f : X \rightarrow Y$ di X su Y.

$$|X| = |Y| \Leftrightarrow \text{ esiste una funzione biettiva } f : X \rightarrow Y$$

.

Esempio $f : \{1, 2, 5\} \rightarrow \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione biettiva.

Cardinalità

Definizione

Due insiemi X e Y hanno la stessa cardinalità se esiste una funzione biettiva $f : X \to Y$ di X su Y.

$$|X| = |Y| \Leftrightarrow \text{ esiste una funzione biettiva } f : X \to Y$$

.

Esempio $f : \{1, 2, 5\} \to \{2, 4, 7\}$
dove $f(1) = 2$, $f(2) = 4$, $f(5) = 7$ è una funzione biettiva.
Esempio Sia $\mathbb{N}_P = \{2n \mid n \in \mathbb{N}\}$ l'insieme dei numeri naturali pari.
La funzione $f : \mathbb{N} \to \mathbb{N}_P$ dove $f(n) = 2n$ è una funzione biettiva e quindi $\mathbb{N}_P$ e $\mathbb{N}$ hanno la stessa cardinalità, anche se $\mathbb{N}_P \subsetneq \mathbb{N}$.

n	$f(n)$
1	2
2	4
3	6
$\vdots$	$\vdots$

Insiemi numerabili

Definizione

Un insieme è numerabile se è finito o ha la stessa cardinalità di $\mathbb{N}$.

Se A è numerabile possiamo "numerare" gli elementi di A e scrivere una lista $(a_1, a_2, \ldots)$

cioè per ogni numero naturale i, possiamo specificare l'elemento i–mo della lista.

Esempio L'insieme $\mathbb{N}_P$ dei numeri naturali pari è numerabile: l'elemento i-esimo della lista corrisponde a $2i$.

Insiemi numerabili: $\mathbb{N}^2$

Esempio. L'insieme $\mathbb{N}^2$ delle coppie di interi positivi è numerabile.

Organizziamo le coppie in una matrice infinita:

$i \backslash j$	1	2	3	4	...
1	(1,1)	(1,2)	(1,3)	(1,4)	...
2	(2,1)	(2,2)	(2,3)	(2,4)	...
3	(3,1)	(3,2)	(3,3)	(3,4)	...
4	(4,1)	(4,2)	(4,3)	(4,4)	...
...	...	...	...	...	...

Se cominciamo ad enumerare gli elementi della prima riga ... non arriveremo mai alla seconda!
Un modo per farlo é procedere per diagonali dall'angolo in alto a sinistra. La numerazione sará la seguente.

Insiemi numerabili: $\mathbb{N}^2$

Un modo per farlo é procedere per diagonali dall'angolo in alto a sinistra. La numerazione sará la seguente.

	1	2	3	4	
1	1	2	4	7	...
2	3	5	8	...	...
3	6	9	...	...	...
.	...	...	...	...	...
i	...	...	...	...	...
.	...	...	...	...	...
.	...	...	...	...	...

Figura: Come elencare le coppie di $\mathbb{N}^2$

$(1,1)$, $(1,2)$, $(2,1)$, $(1,3)$, $(2,2)$, ...

Insiemi numerabili: Q_+

Esempio. L'insieme Q_+ dei numeri razionali positivi è numerabile

Creiamo una matrice infinita contenente tutti i numeri razionali positivi. Il numero i/j occupa la i-esima riga e la j-esima colonna.

Insiemi numerabili: Q_+

Esempio. L'insieme Q_+ dei numeri razionali positivi è numerabile

Creiamo una matrice infinita contenente tutti i numeri razionali positivi. Il numero i/j occupa la i-esima riga e la j-esima colonna.
In questo modo, gli elementi di Q_+ sono ripetuti:
$1/1 = 2/2 = 3/3 = \ldots$, $1/2 = 2/4$, ...
Per definire una biezione tra $\mathbb{N}$ e Q_+ dobbiamo elencare gli elementi della matrice non ripetuti. Come fare?

Insiemi numerabili: Q_+

Esempio. L'insieme Q_+ dei numeri razionali positivi è numerabile

Creiamo una matrice infinita contenente tutti i numeri razionali positivi. Il numero i/j occupa la i-esima riga e la j-esima colonna. In questo modo, gli elementi di Q_+ sono ripetuti:
$1/1 = 2/2 = 3/3 = ..., 1/2 = 2/4, ...$
Per definire una biezione tra $\mathbb{N}$ e Q_+ dobbiamo elencare gli elementi della matrice non ripetuti. Come fare? Se cominciamo ad enumerare gli elementi della prima riga ... non arriveremo mai alla seconda! Un modo per farlo é descritto nella
figura seguente.

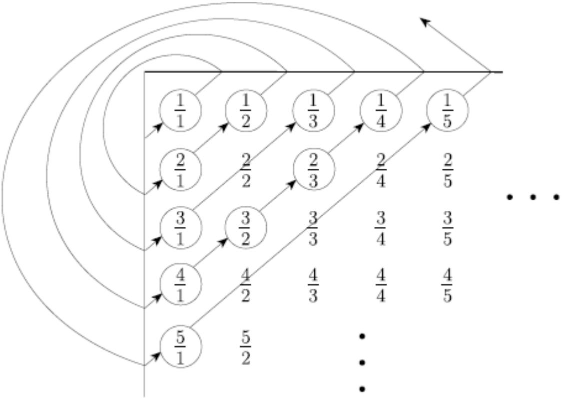


Figura: Q_+ é numerabile

Insiemi numerabili: Σ^*

Esempio. L'insieme Σ^* di tutte le stringhe sull'alfabeto Σ è numerabile.

Insiemi numerabili: Σ^*

Esempio. L'insieme Σ^* di tutte le stringhe sull'alfabeto Σ è numerabile.

Possiamo elencare le stringhe secondo l'ordine radix, cioè per lunghezza e, a parità di lunghezza, in ordine lessicografico.

Esempio: $\Sigma = \{0, 1\}$, $w_0 = \epsilon$, $w_1 = 0$, $w_2 = 1$, $w_3 = 00$, ...

Insiemi numerabili: MdT

Esempio. L'insieme

$$\{\langle M \rangle \mid M \text{ è una MdT sull'alfabeto } \Sigma\}$$

è numerabile.

Insiemi numerabili: MdT

Esempio. L'insieme

$$\{\langle M \rangle \mid M \text{ è una MdT sull'alfabeto } \Sigma\}$$

è numerabile.

Abbiamo visto che è possibile codificare le MdT tramite stringhe su un alfabeto (anche binario).
E l'insieme di tutte le stringhe su un alfabeto è numerabile.

Insiemi numerabili: MdT

Esempio. L'insieme

$$\{\langle M \rangle \mid M \text{ è una MdT sull'alfabeto } \Sigma\}$$

è numerabile.

Abbiamo visto che è possibile codificare le MdT tramite stringhe su un alfabeto (anche binario).
E l'insieme di tutte le stringhe su un alfabeto è numerabile.

E' quindi numerabile anche l'insieme *RE* dei linguaggi riconosciuti da MdT (o Ricorsivamente Enumerabili): il primo sarà il linguaggio riconosciuto dalla prima MdT, il secondo dalla seconda, e così via.

L'insieme dei numeri reali non è numerabile

Esempio. L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.
Lo dimostreremo col metodo della diagonalizzazione di Cantor.

L'insieme dei numeri reali non è numerabile

Esempio. L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.
Lo dimostreremo col metodo della diagonalizzazione di Cantor.
Se per assurdo $\mathbb{R}$ fosse numerabile, allora potremmo elencare tutti i numeri reali:

$$f(1),\ f(2),\ f(3),\dots$$

L'insieme dei numeri reali non è numerabile

Esempio. L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.
Lo dimostreremo col metodo della diagonalizzazione di Cantor.
Se per assurdo $\mathbb{R}$ fosse numerabile, allora potremmo elencare tutti i numeri reali:

$$f(1),\ f(2),\ f(3), \ldots$$

Per esempio:

n	$f(n)$
1	3.14159...
2	55.55555...
3	0.12345...
4	0.50000...
$\vdots$	$\vdots$

L'insieme dei numeri reali non è numerabile (cont.)

Concentriamoci sulle parti decimali e organizziamole in una matrice:

$i \backslash f(i)$	f_1	f_2	f_3	$\dots$	$\dots$	$\dots$
1	$f_1(1)$	$f_2(1)$	$f_3(1)$	$\dots$	$f_i(1)$	$\dots$
2	$f_1(2)$	$f_2(2)$	$f_3(2)$	$\dots$	$f_i(2)$	$\dots$
3	$f_1(3)$	$f_2(3)$	$f_3(3)$	$\dots$	$f_i(3)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$f_1(i)$	$f_2(i)$	$f_3(i)$	$\dots$	$f_i(i)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Vedremo come costruire un numero $x \in \mathbb{R}$ che non è presente nell'elenco, col metodo della diagonale.

L'insieme dei numeri reali non è numerabile (cont.)

Per esempio:

n	$f(n)$
1	3.14159...
2	55.55555...
3	0.12345...
4	0.50000...
$\vdots$	$\vdots$

$i \backslash f(i)$	f_1	f_2	f_3	f_4	f_5	...
1	1	4	1	5	9	...
2	5	5	5	5	5	...
3	1	2	3	4	5	...
4	5	0	0	0	0	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$f_1(i)$	$f_2(i)$	$f_3(i)$	...	$f_i(i)$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

L'insieme dei numeri reali non è numerabile (cont.)

$i \backslash f(i)$	f_1	f_2	f_3	$\dots$	$\dots$	$\dots$
1	$f_1(1)$	$f_2(1)$	$f_3(1)$	$\dots$	$f_i(1)$	$\dots$
2	$f_1(2)$	$f_2(2)$	$f_3(2)$	$\dots$	$f_i(2)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$f_1(i)$	$f_2(i)$	$f_3(i)$	$\dots$	$f_i(i)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Sia $x \in (0,1)$ il numero $x = 0, x_1 x_2 \dots x_i \dots$
ottenuto scegliendo $x_i \neq f_i(i)$ per ogni $i \geq 1$. Chiaramente $x \in \mathbb{R}$.

L'insieme dei numeri reali non è numerabile (cont.)

$i \backslash f(i)$	f_1	f_2	f_3	$\dots$	$\dots$	$\dots$
1	$f_1(1)$	$f_2(1)$	$f_3(1)$	$\dots$	$f_i(1)$	$\dots$
2	$f_1(2)$	$f_2(2)$	$f_3(2)$	$\dots$	$f_i(2)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$f_1(i)$	$f_2(i)$	$f_3(i)$	$\dots$	$f_i(i)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Sia $x \in (0,1)$ il numero $x = 0, x_1 x_2 \dots x_i \dots$
ottenuto scegliendo $x_i \neq f_i(i)$ per ogni $i \geq 1$. Chiaramente $x \in \mathbb{R}$.

Il numero x compare nella lista?

L'insieme dei numeri reali non è numerabile (cont.)

$i \backslash f(i)$	f_1	f_2	f_3	$\dots$	$\dots$	$\dots$
1	$f_1(1)$	$f_2(1)$	$f_3(1)$	$\dots$	$f_i(1)$	$\dots$
2	$f_1(2)$	$f_2(2)$	$f_3(2)$	$\dots$	$f_i(2)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
i	$f_1(i)$	$f_2(i)$	$f_3(i)$	$\dots$	$f_i(i)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Sia $x \in (0,1)$ il numero $x = 0, x_1 x_2 \dots x_i \dots$
ottenuto scegliendo $x_i \neq f_i(i)$ per ogni $i \geq 1$. Chiaramente $x \in \mathbb{R}$.

Il numero x compare nella lista?
Se $x = f(j)$ allora la sua j-esima cifra decimale soddisferebbe $x_j = f_j(j)$. Ma $x_j \neq f_j(j)$ (per def. di x): contraddizione!

Quindi $x \in \mathbb{R}$ non può comparire nella lista e $\mathbb{R}$ non è numerabile.

Per esempio

n	$f(n)$
1	$3.\underline{1}4159\ldots$
2	$55.5\underline{5}555\ldots$
3	$0.12\underline{3}45\ldots$
4	$0.500\underline{0}0\ldots$
$\vdots$	$\vdots$

$$x = 0.4641\ \ldots$$

Buoni e cattivi

Numerabili	Non numerabili
$\mathbb{N}$	$\mathbb{R}$
$\mathbb{N}^2$	$\mathcal{B}$
$\mathbb{Q}_+$	$\mathcal{P}(\Sigma^*)$
Σ^*	
MdT	
RE	

$\mathcal{B}$ è l'insieme di tutte le sequenze binarie infinite.

Buoni e cattivi

Numerabili	Non numerabili
$\mathbb{N}$	$\mathbb{R}$
$\mathbb{N}^2$	$\mathcal{B}$
$\mathbb{Q}_+$	$\mathcal{P}(\Sigma^*)$
Σ^*	
MdT	
RE	

$\mathcal{B}$ è l'insieme di tutte le sequenze binarie infinite.
E' possibile dimostrare che $\mathcal{B}$ non è numerabile col metodo di diagonalizzazione, in modo simile alla dimostrazione che $\mathbb{R}$ non è numerabile (esercizio).

$\mathcal{P}(\Sigma^*)$ non è numerabile

Teorema

L'insieme $\mathcal{P}(\Sigma^*)$ dei linguaggi su Σ non è numerabile.

$\mathcal{P}(\Sigma^*)$ non è numerabile

Teorema

L'insieme $\mathcal{P}(\Sigma^*)$ dei linguaggi su Σ non è numerabile.

E' possibile dimostrarlo in 2 modi.

- Dimostrazione 1 (come sul libro)
- Dimostrazione 2 (diagonalizzazione diretta)

Dimostrazione 1

L'insieme $\mathcal{B}$ di tutte le sequenze binarie infinite non è numerabile.
Esiste una biezione $f: \mathcal{P}(\Sigma^*) \to \mathcal{B}$ quindi anche $\mathcal{P}(\Sigma^*)$ non è numerabile (avendo la stessa cardinalità).

Dimostrazione 1

L'insieme $\mathcal{B}$ di tutte le sequenze binarie infinite non è numerabile. Esiste una biezione $f: \mathcal{P}(\Sigma^*) \to \mathcal{B}$ quindi anche $\mathcal{P}(\Sigma^*)$ non è numerabile (avendo la stessa cardinalità).

$\Sigma = \{0, 1\}$ alfabeto binario
$\Sigma^* = \{w_1, w_2, w_3, \ldots\}$, $L \subseteq \Sigma^*$.
χ_L sequenza caratteristica di L: l'i-esimo bit di χ_L è 1 se $w_i \in L$, 0, altrimenti.

Dimostrazione 1

L'insieme $\mathcal{B}$ di tutte le sequenze binarie infinite non è numerabile. Esiste una biezione $f: \mathcal{P}(\Sigma^*) \to \mathcal{B}$ quindi anche $\mathcal{P}(\Sigma^*)$ non è numerabile (avendo la stessa cardinalità).

$\Sigma = \{0, 1\}$ alfabeto binario
$\Sigma^* = \{w_1, w_2, w_3, \ldots\}$, $L \subseteq \Sigma^*$.
χ_L sequenza caratteristica di L: l'i-esimo bit di χ_L è 1 se $w_i \in L$, 0, altrimenti.

Esempio

A, linguaggio di tutte le stringhe in Σ^* che cominciano per 0

$$\begin{array}{lcccccccccc}
\Sigma^* = \{ & \varepsilon, & 0, & 1, & 00, & 01, & 10, & 11, & 000, & 001, & \cdots \;\} \\
A = \{ & & 0, & & 00, & 01, & & & 000, & 001, & \cdots \;\} \\
\chi_A = & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \cdots
\end{array}$$

Dimostrazione 2

Supponiamo per assurdo che $\mathcal{P}(\Sigma^*)$ sia numerabile.
Sia $L_1, L_2, \ldots$ la lista degli elementi di $\mathcal{P}(\Sigma^*)$
e siano $w_1, w_2, \ldots$ gli elementi di Σ^*.

Dimostrazione 2

Supponiamo per assurdo che $\mathcal{P}(\Sigma^*)$ sia numerabile.
Sia $L_1, L_2, \ldots$ la lista degli elementi di $\mathcal{P}(\Sigma^*)$
e siano $w_1, w_2, \ldots$ gli elementi di Σ^*.

	w_1	w_2	w_3	$\ldots$	w_i	w_j
L_1	$x_{1,1}$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
L_2	$\cdot$	$x_{2,2}$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$x_{3,3}$	$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$x_{4,4}$	$\cdot$	$\cdot$
L_i	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$x_{i,i}$	$x_{i,j}$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$

con $x_{i,j} = 1$ se $w_j \in L_i$, $x_{i,j} = 0$, altrimenti.
Quindi la riga i-esima è la sequenza caratteristica di L_i.

Dimostrazione 2

	w_1	w_2	w_3	$\dots$	w_i	w_j
L_1	$x_{1,1}$	.	.	.	.	.
L_2	.	$x_{2,2}$	.	.	.	.
.	.	.	$x_{3,3}$	.	.	.
.	.	.	.	$x_{4,4}$	.	.
L_i	.	.	.	.	$x_{i,i}$	$x_{i,j}$
.	.	.	.	.	.	.
.	.	.	.	.	.	.

con $x_{i,j} = 1$ se $w_j \in L_i$, $x_{i,j} = 0$, altrimenti.

Sia $L = \{w_i \in \Sigma^* \mid w_i \notin L_i\}$

Può L comparire nella lista?

Dimostrazione 2

$$
\begin{array}{c|cccccc}
 & w_1 & w_2 & w_3 & \dots & w_i & w_j \\
\hline
L_1 & x_{1,1} & \cdot & \cdot & \cdot & \cdot & \cdot \\
L_2 & \cdot & x_{2,2} & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & x_{3,3} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & x_{4,4} & \cdot & \cdot \\
L_i & \cdot & \cdot & \cdot & \cdot & x_{i,i} & x_{i,j} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{array}
$$

con $x_{i,j} = 1$ se $w_j \in L_i$, $x_{i,j} = 0$, altrimenti.

Sia $L = \{w_i \in \Sigma^* \mid w_i \notin L_i\}$
Può L comparire nella lista?
Supponiamo $L = L_h$

- $w_h \in L \Rightarrow x_{h,h} = 0 \Rightarrow w_h \notin L_h = L$ contraddizione
- $w_h \notin L \Rightarrow x_{h,h} = 1 \Rightarrow w_h \in L_h = L$ contraddizione

Concludendo

Numerabili	Non numerabili
$\mathbb{N}$	$\mathbb{R}$
$\mathbb{N}^2$	$\mathcal{B}$
$\mathbb{Q}_+$	$\mathcal{P}(\Sigma^*)$
Σ^*	
MdT	
RE	

Esistono più linguaggi/problemi che macchine di Turing/algoritmi.

Concludendo

Numerabili	Non numerabili
$\mathbb{N}$	$\mathbb{R}$
$\mathbb{N}^2$	$\mathcal{B}$
$\mathbb{Q}_+$	$\mathcal{P}(\Sigma^*)$
Σ^*	
MdT	
RE	

Esistono più linguaggi/problemi che macchine di Turing/algoritmi.
Esistono più linguaggi che linguaggi Turing riconoscibili.

Concludendo

Numerabili	Non numerabili
$\mathbb{N}$	$\mathbb{R}$
$\mathbb{N}^2$	$\mathcal{B}$
$\mathbb{Q}_+$	$\mathcal{P}(\Sigma^*)$
Σ^*	
MdT	
RE	

Esistono più linguaggi/problemi che macchine di Turing/algoritmi.
Esistono più linguaggi che linguaggi Turing riconoscibili.

Teorema

Esistono linguaggi che non sono Turing riconoscibili.

Linguaggi non riconoscibili

Teorema

Esistono linguaggi che non sono Turing riconoscibili.

Esistono.... ma abbiamo un esempio?

Linguaggi non riconoscibili

Teorema
Esistono linguaggi che non sono Turing riconoscibili.

Esistono.... ma abbiamo un esempio?

Sia $A_{TM} = \{\langle M, w\rangle \mid M$ è una MdT che accetta la parola $w\}$

Nel seguito dimostreremo che:

- A_{TM} è riconoscibile
- A_{TM} non è decidibile
- $\overline{A_{TM}}$ non è riconoscibile.

Per le prove useremo il metodo della diagonalizzazione e l'autoreferenzialità.

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$?

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$?
$B \in B$?

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$?
$B \in B$?
$A \in C$?

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$?
$B \in B$?
$A \in C$?
$B \in C$?
$C \in C$?

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$? NO

Autoreferenzialità

Consideriamo i seguenti insiemi:

A = l'insieme di tutti gli insiemi finiti
B = l'insieme di tutti gli insiemi infiniti
C = l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$? NO
$B \in B$? SI

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$? NO
$B \in B$? SI
$A \in C$? SI (perchè $A \notin A$)

Autoreferenzialità

Consideriamo i seguenti insiemi:

$A =$ l'insieme di tutti gli insiemi finiti
$B =$ l'insieme di tutti gli insiemi infiniti
$C =$ l'insieme di tutti gli insiemi che non sono elementi di sé stessi

$A \in A$? NO
$B \in B$? SI
$A \in C$? SI (perchè $A \notin A$)
$B \in C$? NO (perchè $B \in B$)
$C \in C$? ??

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

- se il barbiere rade se stesso,

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

- se il barbiere rade se stesso,
  allora per definizione il barbiere non rade se stesso;

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

- se il barbiere rade se stesso,
  allora per definizione il barbiere non rade se stesso;
- se il barbiere non rade se stesso

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

- se il barbiere rade se stesso,
  allora per definizione il barbiere non rade se stesso;
- se il barbiere non rade se stesso
  allora, dato che il barbiere rade tutti quelli che non si radono da soli, il barbiere rade se stesso.

Paradosso di Bertrand Russel

In un paese vive un solo barbiere, un uomo ben sbarbato, che rade tutti e soli gli uomini del villaggio che non si radono da soli.

Chi sbarba il barbiere?

- se il barbiere rade se stesso,
  allora per definizione il barbiere non rade se stesso;
- se il barbiere non rade se stesso
  allora, dato che il barbiere rade tutti quelli che non si radono da soli, il barbiere rade se stesso.

Si tratta di un'antinomia: compresenza di due affermazioni contraddittorie che possono essere entrambe dimostrate o giustificate.
In generale Russel pose il problema dell'insieme di tutti gli insiemi che non contengono se stessi.
Autoreferenza può causare problemi!

Un problema indecidibile

$$A_{TM} = \{\langle M, w\rangle \mid M \text{ è una MdT e } M \text{ accetta } w\}$$

A_{TM} è il linguaggio associato al problema decisionale dell'accettazione di una macchina di Turing.

Un problema indecidibile

$$A_{TM} = \{\langle M, w \rangle \mid M \text{ è una MdT e } M \text{ accetta } w\}$$

A_{TM} è il linguaggio associato al problema decisionale dell'accettazione di una macchina di Turing.

Teorema

Il linguaggio A_{TM} non è decidibile.

Un problema indecidibile

Supponiamo per assurdo che esiste una macchina di Turing H con due possibili risultati di una computazione (accettazione, rifiuto), che decida il linguaggio A_{TM}. Il decisore H su input $\langle M, w\rangle$:

$$H = \begin{cases} \mathit{accetta} & \text{se } \langle M, w\rangle \in A_{TM}, \text{ cioè se } M \text{ accetta } w \\ \mathit{rifiuta} & \text{se } \langle M, w\rangle \notin A_{TM}, \text{ cioè se } M \text{ non accetta } w \end{cases}$$

Un problema indecidibile

Supponiamo per assurdo che esiste una macchina di Turing H con due possibili risultati di una computazione (accettazione, rifiuto), che decida il linguaggio A_{TM}. Il decisore H su input $\langle M, w \rangle$:

$$H = \begin{cases} \textit{accetta} & \text{se } \langle M, w \rangle \in A_{TM}, \text{ cioè se } M \text{ accetta } w \\ \textit{rifiuta} & \text{se } \langle M, w \rangle \notin A_{TM}, \text{ cioè se } M \text{ non accetta } w \end{cases}$$

$$\langle M, w \rangle \to \boxed{H} \to \begin{cases} \textit{accetta} & \text{se } M \text{ accetta } w \\ \textit{rifiuta} & \text{se } M \text{ non accetta } w \end{cases}$$

Un problema indecidibile

Costruiamo una nuova MdT D che usa H come sottoprogramma.
La MdT D sull'input $\langle M \rangle$, dove M è una MdT:

1. Simula H sull'input $\langle M, \langle M \rangle \rangle$
2. Fornisce come output l'opposto di H, cioè se H accetta, *rifiuta* e se H rifiuta, *accetta*

Un problema indecidibile

Costruiamo una nuova MdT D che usa H come sottoprogramma.
La MdT D sull'input $\langle M \rangle$, dove M è una MdT:

1. Simula H sull'input $\langle M, \langle M \rangle \rangle$
2. Fornisce come output l'opposto di H, cioè se H accetta, *rifiuta* e se H rifiuta, *accetta*

$$\langle M \rangle \to \boxed{\boxed{C} \to \langle M, \langle M \rangle \rangle \to \boxed{H} \to \begin{cases} \mathit{accetta} \\ \mathit{rifiuta} \end{cases} \to \boxed{I}} \to \begin{cases} \mathit{rifiuta} \\ \mathit{accetta} \end{cases}$$

Un problema indecidibile

Costruiamo una nuova MdT D che usa H come sottoprogramma.
La MdT D sull'input $\langle M \rangle$, dove M è una MdT:

1. Simula H sull'input $\langle M, \langle M \rangle \rangle$
2. Fornisce come output l'opposto di H, cioè se H accetta, *rifiuta* e se H rifiuta, *accetta*

$$\langle M \rangle \rightarrow \boxed{\boxed{C} \rightarrow \langle M, \langle M \rangle \rangle \rightarrow \boxed{H} \rightarrow \begin{cases} \textit{accetta} \\ \textit{rifiuta} \end{cases} \rightarrow \boxed{I}} \rightarrow \begin{cases} \textit{rifiuta} \\ \textit{accetta} \end{cases}$$

Quindi

$$D(\langle M \rangle) = \begin{cases} \textit{rifiuta} & \text{se } M \text{ accetta } \langle M \rangle, \\ \textit{accetta} & \text{se } M \text{ non accetta } \langle M \rangle \end{cases}$$

Un problema indecidibile

Se ora diamo in input a D la sua stessa codifica $\langle D \rangle$ abbiamo

Un problema indecidibile

Se ora diamo in input a D la sua stessa codifica $\langle D \rangle$ abbiamo

$$D(\langle D \rangle) = \begin{cases} \textit{rifiuta} & \text{se } D \text{ accetta } \langle D \rangle \\ \textit{accetta} & \text{se } D \text{ non accetta } \langle D \rangle \end{cases}$$

Un problema indecidibile

Se ora diamo in input a D la sua stessa codifica $\langle D\rangle$ abbiamo

$$D(\langle D\rangle) = \begin{cases} \textit{rifiuta} & \text{se } D \text{ accetta } \langle D\rangle \\ \textit{accetta} & \text{se } D \text{ non accetta } \langle D\rangle \end{cases}$$

$$\langle D\rangle \to \boxed{\boxed{C} \to \langle D, \langle D\rangle\rangle \to \boxed{H} \to \begin{cases} \textit{accetta} \\ \textit{rifiuta} \end{cases} \to \boxed{I}} \to \begin{cases} \textit{rifiuta} \\ \textit{accetta} \end{cases}$$

Un problema indecidibile

Se ora diamo in input a D la sua stessa codifica $\langle D \rangle$ abbiamo

$$D(\langle D \rangle) = \begin{cases} \textit{rifiuta} & \text{se } D \text{ accetta } \langle D \rangle \\ \textit{accetta} & \text{se } D \text{ non accetta } \langle D \rangle \end{cases}$$

$$\langle D \rangle \rightarrow \boxed{\boxed{C} \rightarrow \langle D, \langle D \rangle \rangle \rightarrow \boxed{H} \rightarrow \begin{cases} \textit{accetta} \\ \textit{rifiuta} \end{cases} \rightarrow \boxed{I}} \rightarrow \begin{cases} \textit{rifiuta} \\ \textit{accetta} \end{cases}$$

Cioè D accetta $\langle D \rangle$ se e solo se D non accetta $\langle D \rangle$.
Assurdo!
Tutto causato dall'assunzione che esiste H!
Quindi H non esiste!

$\square$

Un problema indecidibile

1. **Nota:** MdT M deve essere in grado di accettare/rifiutare ogni stringa.

2. **Nota:** La codifica $\langle M \rangle$ di M è una stringa.

Un problema indecidibile

1. **Nota:** MdT M deve essere in grado di accettare/rifiutare ogni stringa.
2. **Nota:** La codifica $\langle M \rangle$ di M è una stringa.
3. **Nota:** Far operare una macchina sulla sua codifica ... a volte si fa nella pratica: è analogo ad usare un compilatore Pascal per compilarlo (il compilatore Phyton è scritto in Phyton).

A_{TM} è indecidibile: riepilogo della dimostrazione

1. Definiamo $A_{TM} = \{\langle M, w\rangle \mid M$ è MdT che accetta $w\}$
2. Assumiamo A_{TM} decidibile; sia H MdT che lo decide
3. Usiamo H per costruire MdT D che inverte le decisioni; $D(\langle M\rangle)$: accetta se M non accetta $\langle M\rangle$; rifiuta se M accetta $\langle M\rangle$.
4. Diamo in input a D la sua codifica $\langle D\rangle$: $D(\langle D\rangle)$ accetta sse D rifiuta.

   Contraddizione