DECIDIBILITÀ E INDECIDIBILITÀ

Indecidibilità - Il metodo della diagonalizzazione
(Capitolo IV, sezione 4.2, prima parte)

- Il metodo della diagonalizzazione di Cantor
- Esistenza di linguaggi non Turing riconoscibili

La dimostrazione dell'esistenza di un linguaggio non Turing riconoscibile (e di un linguaggio indecidibile) utilizza una tecnica chiamata *diagonalizzazione*, scoperta 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?

Il metodo della diagonalizzazione

- Cantor propose una soluzione interessante al problema di confrontare gli insiemi infiniti, in particolare a come stabilire se, dati due insiemi infiniti, uno sia "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.
- Introdusse il metodo della diagonalizzazione per provare che esistono insiemi infiniti di differente cardinalità.
- In particolare mostrò che l'insieme $\mathbb{N}$ dei numeri interi positivi ha cardinalità "inferiore" a quella dell'insieme $\mathbb{R}$ dei numeri reali.

- **OBIETTIVI:**
  - Il metodo della diagonalizzazione fu successivamente usato per dimostrare che esistono linguaggi non Turing riconoscibili.
  - Il metodo della diagonalizzazione e l'autoreferenzialità sono usati per dimostrare il teorema seguente

Teorema

Il linguaggio

$$A_{TM} = \{\langle M, w\rangle \mid M \text{ è una macchina di Turing che accetta la parola } w\}$$

non è decidibile.

Definizione

Dati due insiemi non vuoti X e Y,
una funzione $f : X \to Y$ da X in Y è una relazione che associa a ogni elemento x in X uno e un solo $y = f(x)$ in Y.
X è il **dominio** *della funzione,*
Y è il **codominio** *della funzione.*

Definizione

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

Definizione

Una funzione $f : X \to Y$ *è suriettiva* $\Leftrightarrow \forall y \in Y \; \exists x \in X : y = f(x)$

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.*

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

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 biettiva

Sia $\mathbb{N}$ l'insieme dei numeri interi positivi e sia $\mathbb{N}_p = \{2n \mid n \in \mathbb{N}\}$ l'insieme dei numeri interi positivi pari.

Utilizzando la definizione di cardinalità possiamo vedere che $\mathbb{N}$ ed $\mathbb{N}_p$ hanno la stessa cardinalità.

Infatti,

$$f : \mathbb{N} \to \{2n \mid n \in \mathbb{N}\}$$

dove $f(n) = 2n$, per ogni $n \in \mathbb{N}$, è biettiva.

Possiamo visualizzare f più facilmente attraverso la tabella seguente.

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

Figura tratta da M. Sipser, Introduzione alla teoria della computazione.

Consideriamo l'insieme $\mathbb{Q}^+ = \{\frac{x}{y} \mid x, y \in \mathbb{N}, x > 0, y > 0\}$ dei numeri razionali positivi.

Utilizzando la definizione di cardinalità possiamo vedere che $\mathbb{N}$ e $\mathbb{Q}^+$ hanno la stessa cardinalità.

Dobbiamo definire una funzione biettiva tra i due insiemi.

Creiamo una matrice infinita contenente tutti i numeri razionali positivi.

La riga i-esima contiene tutti i numeri con numeratore i e la colonna j-esima ha tutti i numeri con denominatore j.

Quindi il numero $\frac{i}{j}$ occupa la i-esima riga e la j-esima colonna.

Per definire una biezione tra $\mathbb{N}$ e $\mathbb{Q}^+$ dobbiamo definire una corrispondenza biunivoca tra gli elementi della matrice e quelli di $\mathbb{N}$.

Un modo per farlo è descritto nella figura seguente.

Esempio

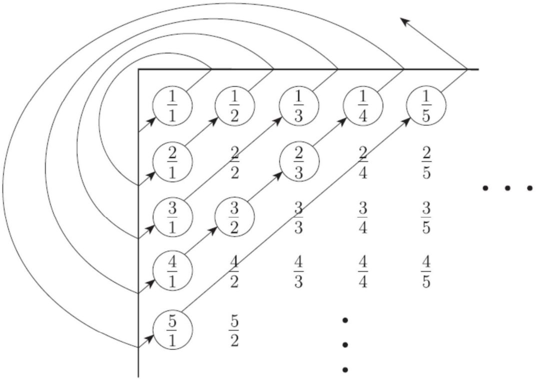

Figura tratta da M. Sipser, Introduzione alla teoria della computazione.

Esempio

Lo stesso ragionamento porta a definire una biezione tra $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ ed $\mathbb{N}$ e quindi a concludere che $\mathbb{N}^2$ ed $\mathbb{N}$ hanno la stessa cardinalità.

Sia $\mathbb{N}^2 = \{(x, y) \mid x, y \in \mathbb{N}, x, y > 0\}$, la funzione $f : \mathbb{N}^2 \to \mathbb{N}$ definita come segue è biettiva

$$\begin{aligned} \forall (x, y) \in \mathbb{N}^2 \quad f((x, y)) &= \frac{(x + y)(x + y + 1)}{2} + x \\ &= \frac{1}{2}((x + y)^2 + 3x + y) \in \mathbb{N} \end{aligned}$$

La funzione f è nota come la **funzione coppia di Cantor**. È graficamente rappresentata dalla seguente matrice.

In questa matrice infinita il valore di f sulla coppia $(i,j) \in \mathbb{N} \times \mathbb{N}$ occupa la i-esima riga e la j-esima colonna. Cioè le entrate della matrice sono i valori della funzione e $f(i,j)$ si trova all'incrocio tra la riga i e la colonna j.

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

Definizione

Un insieme X è numerabile se esiste una funzione biettiva $f : \mathbb{N} \to X$ di $\mathbb{N}$ su X.
Un insieme X è enumerabile se esiste una funzione biettiva **calcolabile** *$f : \mathbb{N} \to X$ di $\mathbb{N}$ su X.*
Un insieme X è contabile se è finito o numerabile.

Esempio L'insieme dei numeri pari è numerabile.

Esempio $\mathbb{Q}^+ = \{\frac{x}{y} \mid x, y \in \mathbb{N}, x > 0, y > 0\}$, $\mathbb{N}^2$ sono numerabili.

Teorema

$\mathbb{R}$ *non è numerabile.*

$\mathbb{R}$ non è numerabile

Mostriamo che non esiste nessuna funzione biettiva di $\mathbb{N}$ sull'insieme $\mathbb{R}$ dei numeri reali.

La dimostrazione è per contraddizione.

Supponiamo quindi che esista una funzione biettiva f di $\mathbb{N}$ su $\mathbb{R}$.

Mostriamo che esiste un numero reale x che non è immagine di nessun elemento di $\mathbb{N}$.

Il numero x sarà un numero compreso tra 0 e 1.

Illustriamo prima l'idea della prova su un esempio.

La tabella seguente mostra alcuni valori di un'ipotetica biezione f tra $\mathbb{N}$ e $\mathbb{R}$.

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

Figura tratta da M. Sipser, Introduzione alla teoria della computazione.

$\mathbb{R}$ non è numerabile

Scegliamo x in modo che sia diverso dagli elementi della tabella procedendo “per diagonale”.

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

$$x = 0.4641\ldots$$

Figura tratta da M. Sipser, Introduzione alla teoria della computazione.

- Idea della prova (metodo della diagonalizzazione).
  - Supponiamo per assurdo che esista una funzione biettiva f di $\mathbb{N}$ su $\mathbb{R}$.
  - Allora possiamo costruire la tabella:

n	$f(n)$				
1	$d_{1,1}$	$d_{1,2}$	$\dots$	$\dots$	$\dots$
2	$d_{2,1}$	$d_{2,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
i	$d_{i,1}$	$d_{i,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

dove $d_{1,1}d_{1,2}\dots$ è la parte decimale del numero reale $f(1)$, $d_{2,1}d_{2,2}\dots$ è la parte decimale del numero reale $f(2)$ e in generale $d_{i,1}d_{i,2}\dots$ è la parte decimale del numero reale $f(i)$.

n	$f(n)$				
1	$d_{1,1}$	$d_{1,2}$	$\dots$	$\dots$	$\dots$
2	$d_{2,1}$	$d_{2,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
i	$d_{i,1}$	$d_{i,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

quindi $f(1) = r_1, d_{1,1}d_{1,2}\dots$, $f(2) = r_2, d_{2,1}d_{2,2}\dots$ e in generale $f(i) = r_i, d_{i,1}d_{i,2}\dots$.

n	$f(n)$				
1	$d_{1,1}$	$d_{1,2}$	$\dots$	$\dots$	$\dots$
2	$d_{2,1}$	$d_{2,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
i	$d_{i,1}$	$d_{i,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

- Le cifre sulla diagonale di questa matrice $d_{1,1}d_{2,2}\dots$ definiscono un numero reale $r = 0, d_{1,1}d_{2,2}\dots$.
- Il numero reale $0, d'_{1,1}d'_{2,2}\dots$ che si ottiene scegliendo in ogni posizione (della parte decimale) una cifra diversa dalla corrispondente cifra in r non è immagine di nessun intero positivo (non può essere $f(1)$ perché $d'_{1,1} \neq d_{1,1}$, non può essere $f(2)$ perché $d'_{2,2} \neq d_{2,2}$,.....)

Nella dimostrazione precedente avremmo potuto anche limitarci a considerare i numeri reali nell'intervallo $]0, 1[$ perché questo insieme ha cardinalità non superiore a $\mathbb{R}$.

- $|X| \leq |Y| \Leftrightarrow$ esiste una funzione iniettiva $f : X \to Y$
- $|X| \leq |Y|$, $|X| \neq |Y| \Rightarrow |X| < |Y|$
- $|X| \leq |Y|$, $|Y| \leq |X| \Rightarrow |X| = |Y|$

$|\mathbb{N}| < |\mathbb{R}|$

- $n \in \mathbb{N} \to n \in \mathbb{R}$ è una funzione iniettiva di $\mathbb{N}$ in $\mathbb{R}$. Quindi $|\mathbb{N}| \leq |\mathbb{R}|$.
- Non esiste nessuna funzione biettiva di $\mathbb{N}$ sull'insieme $\mathbb{R}$ dei numeri reali. Quindi $|\mathbb{N}| \neq |\mathbb{R}|$, $\mathbb{N}$ e $\mathbb{R}$ non hanno la stessa cardinalità.
- Quindi da $|\mathbb{N}| \leq |\mathbb{R}|$ e $|\mathbb{N}| \neq |\mathbb{R}|$ deduciamo $|\mathbb{N}| < |\mathbb{R}|$.

Corollario

Esistono linguaggi che non sono Turing riconoscibili.

Il Metodo della diagonalizzazione per provare che esistono linguaggi non Turing riconoscibili

E' possibile usare il metodo della diagonalizzazione per provare che esistono linguaggi che non sono Turing riconoscibili.

La prova consiste nel provare le affermazioni seguenti:

- Dato un alfabeto Σ, l'insieme Σ^* è numerabile.
- L'insieme delle codifiche delle macchine di Turing, e quindi l'insieme delle macchine di Turing è numerabile.
  Nota: la codifica di una macchina di Turing è una stringa.
- L'insieme dei linguaggi Turing riconoscibili **è numerabile**.
  Nota: a ogni linguaggio Turing riconoscibile è associata (la codifica di) una macchina di Turing.
- L'insieme dei linguaggi sull'alfabeto Σ **ha cardinalità maggiore del numerabile**.

Sia $\Sigma = \{a_1, a_2, \ldots a_k\}$ un alfabeto. Possiamo definire una corrispondenza biunivoca tra $\mathbb{N}$ e Σ^* che permette di enumerare le stringhe in ordine radix: $w_1 = \epsilon, w_2 = a_1, w_3 = a_2, \ldots,$ (vedremo come).

Ad esempio, se $\Sigma = \{a, b\}$, la sequenza è

$$\epsilon, a, b, aa, ab, ba, bb, \ldots,$$

e $w_2 = a$, $w_6 = ba$, $w_8 = ?$

Non numerabilità dell'insieme dei linguaggi

Sia $\Sigma^* = \{w_1, w_2, \ldots\}$.

Sia $\mathcal{B}$ l'insieme delle sequenze binarie infinite
cioè delle sequenze infinite di 0 e 1.

È possibile associare a ogni linguaggio L una sequenza binaria infinita s_L (la sequenza caratteristica di L) così definita:

il bit i-esimo di s_L è 1 se l'i-esima stringa w_i è in L, il bit i-esimo di s_L è 0 se $w_i \notin L$.

Esempio

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

La sequenza binaria del linguaggio delle stringhe binarie che iniziano con 0

Figura tratta da M. Sipser, Introduzione alla teoria della computazione.

Non numerabilità dei linguaggi

Un linguaggio può essere messo in corrispondenza biunivoca con una sequenza binaria di lunghezza infinita.

Esempio1: $\Sigma = \{a,b\}$, $L = \{ a^n b^n \mid n \geq 0 \}$

Σ^* =	ε	a	b	aa	ab	ba	bb	aaa	aab	aba	abb	baa	...	bbb	aabb	...
f(L) =	1	0	0	0	1	0	0	0	0	0	0	0	...	0	1	....

Esempio

Esempio2: $\Sigma = \{a,b\}$, $L = \{ ab^n \mid n \geq 0 \}$

Σ^* =	ε	a	b	aa	ab	ba	bb	aaa	aab	aba	abb	baa	...	bbb	...	abbb	...
f(L) =	0	1	0	0	1	0	0	0	0	0	1	0	...	0	...	1	...

Non numerabilità dell'insieme dei linguaggi

Sia $\mathcal{B}$ l'insieme delle sequenze binarie infinite.
È possibile associare a ogni linguaggio L una sequenza binaria infinita s_L, la sequenza caratteristica di L.

Questa relazione è una corrispondenza biunivoca tra l'insieme $\mathcal{B}$ delle sequenze binarie infinite e l'insieme $\mathcal{P}(\Sigma^*)$ dei linguaggi su Σ, cioè

- A ogni linguaggio L è associata una sola sequenza binaria infinita s tale che $s = s_L$
- A ogni sequenza binaria infinita s è associato un solo linguaggio L tale che $s = s_L$

In altri termini, l'applicazione $f : \mathcal{P}(\Sigma^*) \to \mathcal{B}$ definita da $f(L) = s_L$ è biettiva.

Non numerabilità dell'insieme delle sequenze binarie

L'insieme $\mathcal{B}$ non è numerabile.

- Idea della prova (metodo della diagonalizzazione).
  - Mostriamo che non esiste nessuna funzione biettiva di $\mathbb{N}$ sull'insieme $\mathcal{B}$ delle sequenze binarie infinite. Supponiamo per assurdo che esista una funzione biettiva f di $\mathbb{N}$ su $\mathcal{B}$.
  - Allora possiamo costruire la tabella:

n			$f(n)$		
1	$d_{1,1}$	$d_{1,2}$	$\dots$	$\dots$	$\dots$
2	$d_{2,1}$	$d_{2,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
i	$d_{i,1}$	$d_{i,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

dove $d_{1,1}d_{1,2}\dots$ è la sequenza binaria infinita associata a $f(1)$, $d_{2,1}d_{2,2}\dots$ è la sequenza binaria infinita associata a $f(2)$ e in generale $d_{i,1}d_{i,2}\dots$ è la sequenza binaria infinita associata a $f(i)$.

Non numerabilità dell'insieme delle sequenze binarie

n	$f(n)$				
1	$d_{1,1}$	$d_{1,2}$	$\dots$	$\dots$	$\dots$
2	$d_{2,1}$	$d_{2,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
i	$d_{i,1}$	$d_{i,2}$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

- Le cifre sulla diagonale di questa matrice $d_{1,1}d_{2,2}\dots$ definiscono una sequenza binaria infinita s.
- La sequenza binaria infinita $\bar{d}_{1,1}\bar{d}_{2,2}\dots$ che si ottiene scegliendo in ogni posizione il complemento della corrispondente cifra in s non è immagine di nessun intero positivo (non può essere $f(1)$ perché $\bar{d}_{1,1} \neq d_{1,1}$, non può essere $f(2)$ perché $\bar{d}_{2,2} \neq d_{2,2}$,.....)

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

Dimostrazione

Esiste un'applicazione biettiva f di $\mathcal{P}(\Sigma^*)$ in $\mathcal{B}$, quindi $|\mathcal{B}| = |\mathcal{P}(\Sigma^*)|$.

Poiché, come abbiamo provato, $\mathcal{B}$ non è numerabile, concludiamo che $\mathcal{P}(\Sigma^*)$ non è numerabile.

Esistono linguaggi non Turing riconoscibili

Corollario

Esistono linguaggi che non sono Turing riconoscibili.

La funzione $h : \Sigma^* \to \mathcal{P}(\Sigma^*)$, dove $h(w) = \{w\}$, è iniettiva.
Ne consegue

$$|\mathbb{N}| = |\Sigma^*| < |\mathcal{P}(\Sigma^*)|$$

Proveremo che

$$|\{L \subseteq \Sigma^* \mid L \text{ è Turing riconoscibile}\}| = |\Sigma^*|$$

Quindi

$$|\{L \subseteq \Sigma^* \mid L \text{ è Turing riconoscibile}\}| = |\mathbb{N}| < |\mathcal{P}(\Sigma^*)|.$$

L'insieme dei linguaggi Turing riconoscibili è numerabile ma l'insieme di tutti i linguaggi ha cardinalità maggiore del numerabile. Quindi esistono linguaggi che non sono Turing riconoscibili.

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

(Seconda) Dimostrazione

Supponiamo per assurdo che $\mathcal{P}(\Sigma^*)$ sia numerabile.

Quindi esiste un'applicazione biettiva h di $\mathbb{N}$ in $\mathcal{P}(\Sigma^*)$.

Sia $L_1, L_2, \ldots$ la lista dei linguaggi, cioè degli elementi di $\mathcal{P}(\Sigma^*)$, dove $L_1 = h(1)$, $L_2 = h(2)$ e in generale $L_i = h(i)$.

Σ^* è enumerabile, sia g una biezione di $\mathbb{N}$ in Σ^* e siano $w_1, w_2, \ldots$ gli elementi di Σ^*, con $w_i = g(i)$.

Definiamo una matrice (infinita) avente come indici di riga i linguaggi $L_1, L_2, \ldots$ e indici di colonna le stringhe $w_1, w_2, \ldots$.

Non numerabilità dell'insieme dei linguaggi

	w_1	w_2	$\dots$	w_j	
L_1	0	1	$\dots$	0	$\dots$
L_2	1	1	$\dots$	1	$\dots$
L_3	0	0	$\dots$	1	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
L_i	1	0	$\dots$	0	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
.	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Nella matrice scriviamo 1 all'incrocio tra la riga L_i e la colonna w_j se $w_j \in L_i$, altrimenti scriviamo 0. Quindi la riga corrispondente ad L_i è la sequenza caratteristica di L_i.

Non numerabilità dell'insieme dei linguaggi

Definiamo un linguaggio L come segue:

$$\forall i > 0 \quad w_i \in L \Leftrightarrow w_i \notin L_i$$

$L \in \mathcal{P}(\Sigma^*)$ ma per ogni $i > 0$, $L \neq L_i$.

Infatti, sia h tale che $L = L_h$. La domanda "$w_h \in L$?" conduce a una contraddizione.

Assumiamo $w_h \in L$. Per la definizione di L deve essere $w_h \notin L_h$. Ma per ipotesi $L = L_h$, assurdo.

Assumiamo $w_h \notin L$. Per la definizione di L deve essere $w_h \in L_h$. Ma per ipotesi $L = L_h$, assurdo.

Numerabilità dell'insieme delle parole

Σ^* è numerabile

Idea della dimostrazione:

Provare che $|\mathbb{N}| \leq |\Sigma^*|$ e poi che $|\Sigma^*| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

Per provare che $|\mathbb{N}| \leq |\Sigma^*|$ bisogna definire una funzione iniettiva da $\mathbb{N}$ in Σ^*.

Vediamo prima su un esempio come potremmo definire una tale funzione.

Sia $\Sigma = \{a, b\}$.
Consideriamo l'applicazione f tale che $f(n) = a^n$.

Quindi ad esempio $f(1) = a$, $f(5) = a^5 = aaaaa$.

L'applicazione f è iniettiva.

Per provare che $|\Sigma^*| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ bisogna definire una funzione iniettiva da Σ^* in $\mathbb{N} \times \mathbb{N}$.

Ad ogni parola associamo una coppia di numeri di cui il primo è la lunghezza della parola aumentata di uno.

Vediamo prima su un esempio come potremmo definire una tale funzione.

Numerabilità dell'insieme delle parole

Per ogni $n \in \mathbb{N}$ sia $f_n : \Sigma^n \to \mathbb{N}$ un'applicazione iniettiva.
Inoltre poniamo $f_0(\epsilon) = 1$.

Esempio. Sia $\Sigma = \{a, b\}$.
$f_1(a) = 1$, $f_1(b) = 2$.

$f_2(aa) = 1$, $f_2(ab) = 2$, $f_2(ba) = 3$, $f_2(bb) = 4$.

Definiamo una funzione g tale che $g(w) = (|w| + 1, f_{|w|}(w))$.

Ad esempio, $g(b) = (2, 2)$, $g(ab) = (3, 2)$ e $g(bb) = (3, 4)$.

L'applicazione $g : w \in \Sigma^* \to (|w| + 1, f_{|w|}(w)) \in \mathbb{N} \times \mathbb{N}$ è iniettiva.

Σ^* è numerabile

Dimostrazione

Sia $\sigma \in \Sigma$, l'applicazione $f : n \in \mathbb{N} \to \sigma^n \in \Sigma^*$ è iniettiva, quindi

$$|\mathbb{N}| \leq |\Sigma^*|$$

Per ogni $n \in \mathbb{N}$ sia $f_n : \Sigma^n \to \mathbb{N}$ un'applicazione iniettiva. Inoltre poniamo $f_0(\epsilon) = 1$.

Definiamo una funzione g tale che $g(w) = (|w| + 1, f_{|w|}(w))$.

L'applicazione $g : w \in \Sigma^* \to (|w| + 1, f_{|w|}(w)) \in \mathbb{N} \times \mathbb{N}$ è iniettiva.

Siano $x, y \in \Sigma^*$ tali che $x \neq y$.

Se $|x| \neq |y|$ allora
$g(x) = (|x| + 1, f_{|x|}(x)) \neq (|y| + 1, f_{|y|}(y)) = g(y)$ perché la prima coordinata è diversa.

Se $|x| = |y|$ allora $f_{|x|}(x) \neq f_{|y|}(y)$ e
$g(x) = (|x| + 1, f_{|x|}(x)) \neq (|y| + 1, f_{|y|}(y)) = g(y)$ perché la seconda coordinata è diversa.

Ne consegue

$$|\Sigma^*| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

Quindi

$$|\Sigma^*| = |\mathbb{N}|$$

$\square$

Numerabilità dell'insieme delle codifiche delle macchine di Turing

L'insieme $\{\langle M\rangle \mid M$ è una TM sull'alfabeto $\Sigma\}$ è numerabile.

Dimostrazione

È possibile codificare una MT M con una stringa su un alfabeto Σ e l'applicazione $f : \langle M\rangle \to \langle M\rangle \in \Sigma^*$ è iniettiva. Quindi

$$|\{\langle M\rangle \mid M \text{ è una TM sull'alfabeto } \Sigma\}| \leq |\Sigma^*| = |\mathbb{N}|$$

Sia $n \in \mathbb{N}$, sia $\sigma \in \Sigma$. Il linguaggio $\{\sigma^n\}$ è decidibile, sia M_n una macchina di Turing che decide $\{\sigma^n\}$.

L'applicazione $g : n \in \mathbb{N} \to \langle M_n\rangle$ è iniettiva. Quindi

$$|\mathbb{N}| \leq |\{\langle M\rangle \mid M \text{ è una TM sull'alfabeto } \Sigma\}$$

Da cui

$$|\{\langle M\rangle \mid M \text{ è una TM sull'alfabeto } \Sigma\} = |\mathbb{N}|$$

$\square$

Numerabilità dell'insieme dei linguaggi Turing riconoscibili

L'insieme $\{L \subseteq \Sigma^* \mid L$ è Turing riconoscibile$\}$ è numerabile.

Dimostrazione

Possiamo associare a ogni linguaggio Turing riconoscibile una TM che lo riconosce e questa corrispondenza è iniettiva.

Quindi: $|\{L \subseteq \Sigma^* \mid L$ è Turing riconoscibile$\}|$
$\leq |\{\langle M \rangle \mid M$ è una TM sull'alfabeto $\Sigma\}| \leq |\mathbb{N}|$

Sia $n \in \mathbb{N}$ e sia $\sigma \in \Sigma$. Il linguaggio $\{\sigma^n\}$ è Turing-riconoscibile.

L'applicazione $g : n \in \mathbb{N} \to \{\sigma^n\}$ è iniettiva.

Quindi $|\mathbb{N}| \leq |\{L \subseteq \Sigma^* \mid L$ è Turing riconoscibile$\}|$

Da cui: $|\mathbb{N}| = |\{L \subseteq \Sigma^* \mid L$ è Turing riconoscibile$\}|$.

$\square$