Una goedelizzazione effettiva delle macchine di turing.

Dispensa a cura della Prof.ssa Sportelli.[1]

Dato un insieme A di oggetti, il termine "aritmetizzazione" significa semplicemente "attribuzione ad ogni oggetto dell'insieme A di un numero naturale distintivo di quell'oggetto stesso".

In parole povere, l'idea è quella di associare ad ogni oggetto dell'insieme A un numero naturale e, viceversa, partendo da tale numero naturale ricavare univocamente ed algoritmicamente l'oggetto ad esso associato.

Si ricordi che l'aritmetizzazione di un insieme A è possibile se e solo se l'insieme A è enumerabile.

Il primo utilizzo dell'arimetizzazione è dovuto a Goedel nel 1931 con la dimostrazione del risultato fondamentale di incompletezza dell'aritmetica; da qui anche il termine equivalente di goedelizzazione.

In questa sede si intende dimostrare che l'insieme delle macchine di Turing è un insieme goedelizzabile e, pertanto, enumerabile in modo effettivo. Per far ciò è sufficiente esibire una funzione iniettiva ed invertibile π del tipo $\pi : I_{MT} \rightarrow \mathbb{N}$ dove I_{MT} è l'insieme di tutte le macchine di Turing.

Notazione sulle macchine di Turing.

Si è visto che una macchina di Turing MT è una macchina ideale che opera su un nastro bi-infinito suddiviso in celle; tali celle possono contenere al più un simbolo alla volta. L'insieme finito di simboli sui quali opera una macchina di Turing MT costituisce l'alfabeto $\Sigma = \{s_o, s_{1,} s_{2,} \ldots, s_k\}$ della MT. Fra questi simboli uno, convenzionalmente s_0, rappresenta la mancanza di simboli in una cella, cioè la cella vuota.

Una macchina di Turing, inoltre, è dotata di una testina di lettura/scrittura che è collocata, in ogni fase del calcolo, su di una singola cella. Sia Q un insieme finito, $Q = \{q_{0,} q_{1,} q_{2,} \ldots, q_n\}$, l'insieme degli stati interni della macchina; una volta fissato l'alfabeto, ciò che caratterizza una macchina di Turing rispetto a tutte le altre è la tavola delle sue quintuple, generate dalla funzione di transizione δ. La funzione è del tipo $\delta : Q \times \Sigma \rightarrow \Sigma \times M \times Q$, dove $M = \{m_0 = D, m_1 = S, m_2 = C\}$ è l'insieme degli spostamenti della testina di lettura/scrittura della macchina. La coppia < qi, s_r > rappresenta la configurazione che genera l'operazione atomica < s_t, m_h, q_j >, dove $0 \leqslant r, t \leqslant k, 0 \leqslant i, j \leqslant n$ e $0 \leqslant h \leqslant 2$:

< qi, s_r > → < s_t, m_h, q_j >

Tutto ciò può essere espresso sinteticamente mediante la quintupla ordinata $(q_i, s_r, s_t, m_h, q_j)$. In altre parole una quintupla esprime il fatto che la macchina, trovandosi in uno stato $q_i \in Q$ e leggendo un simbolo $s_r \in \Sigma$, mediante la funzione di transizione sostituisce il simbolo s_r con il simbolo s_t, sposta la testina di lettura/scrittura di una cella a destra (D) sul nastro, di una cella a sinistra (S), o la lascia ferma sulla cella su cui già si trova (C), e assume lo stato interno q_j.

L'insieme delle quintuple ordinate mediante la δ, omettendo il simbolo →, costituisce l'insieme delle istruzioni della macchina di Turing MT, ovvero la sua tavola di computazione.

Poichè ogni macchina di Turing è il modello di un calcolo deterministico, è necessario

1 Dispensa digitalizzata da Fabio D'Asaro. Si prega di perdonare eventuali errori di ricopiatura.

individuare in Q uno stato iniziale, convenzionalmente q_1, ed inoltre occorre che ogni singola configurazione possa dar luogo ad una sola operazione atomica (ciò si traduce nel fatto che le coppie iniziali delle quintuple della tabella di MT siano tutte distinte fra di loro).

Infine, le istruzioni di una tabella, applicate ad un certo input, possono sia dar luogo ad un calcolo che ad uno che si ferma. Affinchè il calcolo possa terminare è necessario che ad alcune delle configurazioni possibili non corrisponda alcuna istruzione, altrimenti, qualunque fosse il risultato di un'operazione, esisterebbe sempre un altro passo computazionale generato da essa. Le configurazioni che non danno luogo a nessuna operazione atomica sono dette configurazioni finali. Non a tutte le configurazioni finali, tuttavia, corrisponde un risultato. Il risultato, ovvero l'output del calcolo eseguito dalla macchina MT, è leggibile sul nastro se e solo se la macchina termina il suo calcolo e si trova nello stato finale accettante, che convenzionalmente è indicato con lo stato q_0.

L'aritmetizzazione delle k-ple.

Consideriamo la seguente funzione $\gamma : \cup_{(k>0)} \mathbb{N}^k \rightarrow \mathbb{N}$; tale funzione associa ad una qualsiasi k-pla $(n_1, n_2, \ldots, n_k)$ di numeri naturali un numero naturale nel seguente modo: $\gamma(n_1, n_2, \ldots, n_k) = 2_1^n + 2^{(n_1+n_2+1)} + 2^{(n_1+n_2+n_3+2)} + \ldots + 2^{(n_1+n_2+\ldots+n_k+k-1)} - 1$; è possibile dimostrare che la funzione è biettiva.

Si tratta, quindi, di una codifica effettiva delle k-ple mediante un numero naturale e poichÈ γ oltre ad essere biettiva è anche invertibile (cioè la γ^{-1} è calcolabile), è possibile, mediante un numero naturale n, risalire mediante la γ^{-1} alla k-pla ad esso associata.

Esempi:

Sia $k=2, \gamma(0,3) = 2^0 + 2^{(0+3+1)} - 1 = 1 + 16 - 1 = 16$.

Viceversa per calcolare $\gamma^{-1}(16)$ si somma a 16 il numero 1 (16+1=17) e si calcola l'esponente di 2 nella scomposizione in fattori primi del numero così ottenuto; in questo caso l'esponente di 2 nella scomposizione in fattori primi di 17 è 0. Allora $n_1 = 0$.

Successivamente si sottrae al numero scomposto in fattori primi $2^{(n_1)}(17 - 2^0 = 17 - 1 = 16)$ e si torna a calcolare l'esponente di 2 nella scomposizione in fattori primi del numero così ottenuto; in questo caso l'esponente di 2 nella scomposizione in fattori primi di 16 è 4. Allora dal fatto che $4 = n_1 + n_2 + 1$ si ottiene $n_2 = 3$.

Poichè 16 è una potenza di 2, il calcolo ha termine ed al numero 16 corrisponde la coppia $(n_1, n_2) = (0,3)$.

Come ulteriore esempio, calcoliamo $\gamma^{-1}(349)$.

$349 + 1 = 350$; scomponendo 350 si trova che $350 = 2 \times 175$; allora l'esponente di 2 è 1 e pertanto n_1=1.

$350 - 2^1 = 350 - 2 = 348$; scomponendo 348 si trova che $348 = 2^2 \times 87$; allora il secondo esponente è 2.

$348 - 2^2 = 348 - 4 = 344$; scomponendo 344 si trova che $344 = 2^3 \times 43$; allora il terzo esponente è 3.

$344 - 2^3 = 344 - 8 = 336$; scomponendo 336 si trova che $336 = 2^4 \times 21$; allora il quarto esponente è 4.

$336-2^4=336-16=320$; scomponendo 320 si trova che $320=2^6\times 5$; allora il quinto esponente è 6.

$320-2^6=320-64=256=2^8$; allora il sesto esponente è 8.

In pratica $349=2^1+2^2+2^3+2^4+2^6+2^8-1$ e

		$n_1=1$
$2 = n_1 + n_2 + 1$	da cui:	$n_2=0$
$3 = n_1 + n_2 + n_3 + 2$	da cui:	$n_3=0$
$4 = n_1 + n_2 + n_3 + n_4 + 3$	da cui:	n4=0
$6 = n_1 + n_2 + n_3 + n_4 + n_5 + 4$	da cui:	$n_5=1$
$8 = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + 5$	da cui:	$n_6=1$

In definitiva $\gamma^{-1}(349)=(1,0,0,0,1,1)$.

Aritmetizzazione delle istruzioni di una macchina di Turing.

Poichè le istruzioni di una macchina di Turing sono le quintuple della corrispondente tavola computazionale, possiamo pensare di utilizzare la funzione γ precedentemente definita per codificare le quintuple che la compongono.

Una generica quintupla di una macchina di Turing ha la forma $(q_i, s_r, s_t, m_h, q_j)$.

Da questa possiamo passare in modo naturale alla quintupla ordinata degli indici (i, r, t, h, j) , con $0\leqslant r,t\leqslant k, 0\leqslant i,j\leqslant n$ e $0\leqslant h\leqslant 2$.

Allora ad ogni quintupla di una generica macchina di Turing corrisponderà un numero natuale $\gamma(i,r,t,h,j)$.

In questo caso, tuttavia, la γ è semplicemente iniettiva e non surgettiva sull'insieme N dei numeri naturali; γ^{-1} è ancora calcolabile, ma soltanto ad un sottoinsieme proprio dei numeri naturali corrispondono quintuple appartenenti ad una possibile tavola computazionale di una macchina di una MT. Se calcolando la $\gamma^{-1}(n)$ si ottiene una quintupla e se in tale quintupla il quarto elemento $h\in\{0,1,2\}$, allora il numero n rappresenta un'istruzione di una possibile macchina di Turing.

Esempio: (4.1 – pag. 132 del libro di testo)

Consideriamo la seguente tabella composta da 2 istruzioni:

I_1	q_1	s_1	s_1	m_o	q_1
I_2	q_1	s_0	s_1	m_2	q_0

della macchina di Turing che ha come alfabeto $\Sigma=\{s_{0,}s_1\}$ (nell'esempio del libro s_1 è la barra verticale |) e come insieme degli stati l'insieme $Q=\{q_{0,}q_1\}$; come si è visto questa macchina di Turing computa la funzione f(x) = x + 1.

$\gamma(I_1) = \gamma(1,1,1,0,1) = 2^1 + 2^{(1+1+1)} + 2^{(1+1+1+2)} + 2^{(1+1+1+3)} + 2^{(1+1+1+1+4)}$ -1= $2+2^3+2^5+2^6+2^8-1=2+8+32+64+256-1$ = 361

$\gamma(I_2) = \gamma(1,0,1,2,0) = 2^1 + 2^{(1+1)} + 2^{(1+1+2)} + 2^{(1+1+2+3)} + 2^{(1+1+2+4)}$ -1= $2+2^2+2^4+2^4+2^7+2^8-1=2+4+16+128+256-1=405$

Goedelizzazione dell'insieme delle macchine di Turing.

Dalla codifica delle quintuple si può adesso passare alla codifica di un'intera tabella di computazione. Baster‡ definire ancora una volta una funzione iniettiva ed invertibile che, presi come argomento i numeri naturali che rappresentano la codifica delle quintuple, restituisca come valore un numero n che rappresenta l'intera macchina di Turing MT.

Sia <MT> = < $I_{1,} I_{2,} \ldots, I_u$ > la tabella, costituita dalle istruzioni I_i (per $1 \leqslant i \leqslant u$), della macchina di Turing MT.

Considerata la successione þ dei numeri primi, sia p_i l'i-esimo numero primo. Definiamo la funzione $\pi(MT)$ come segue:

$$\pi(\gamma(I_1), \gamma(I_2), \ldots, \gamma(I_n)) \quad = \quad \prod_{1=1}^{u} (p_i)^{(\gamma(I_i))} = 2^{(\gamma(I_1))} \times 3^{(\gamma(I_2))} \times 5^{(\gamma(I_3))} \times \ldots \times (p_u)^{(\gamma(I_n))}$$

Per l'unicità della decomposizione di un numero in fattori primi, la funzione π appena definita è una funzione iniettiva ed invertibile; tuttavia, non è una funzione surgettiva (in quanto i numeri naturali nella cui decomposizione in fattori primi non compaiono tutti i primi u numeri primi non appartengono al rango di %pi). Pertanto comunque preso un numero naturale n, non è detto che esso sia la codifica di una macchina di Turing, ma se n in $\pi(MT)$, allora conoscendo n ed invertendo le funzioni π e γ si può risalire in modo effettivo alla tavola computazionale della macchina di Turing MT.

Esempio (continuazione):

Siamo ora in grado di codificare la macchina di Turing dell'esempio precedente con un numero naturale n, in particolare $n = 2^{361} \times 3^{405}$.

Enumerabilità dell'insieme delle macchine di Turing e della classe di funzioni Turing-Calcolabili

Per concludere si può quindi affermare che l'insieme delle macchine di Turing è un insieme effettivamente enumerabile, in quanto è il campo di esistenza di una funzione calcolabile $\pi : I_{MT} \rightarrow \mathbb{N}$, ovvero, equivalentemente, è il rango della funzione calcolabile $\pi^{-1} : \mathbb{N} \rightarrow I_{MT}$.

Il poter disporre di una enumerazione effettiva di tutte le macchine di Turing consente di dimostrare l'esistenza di una Macchina di Turing Universale (teorema 6.2 – pag 233 del libro di testo).

Si noti che non è importante il modo con cui si ottiene un'effettiva enumerazione dell'insieme I_{MT} , anzi esistono in teoria infinite codifiche delle macchine di Turing mediante numeri naturali.

Inoltre, la codifica qui adottata (e in generale la maggior parte delle codifiche) è tale che a numeri naturali differenti possono corrispondere macchine di Turing che, pur presentando tabelle computazionali fondamentalmente diverse, sono equivalenti ovvero eseguono esattamente lo stesso calcolo; infatti, presa comunque una macchina di Turing MT_h, una qualsiasi permutazione delle istruzione della sua tabella computazionale dà luogo ad un'altra macchina di Turing Mt_k fondamentalmente distinta da MT_h, ma del tutto equivalente.

Consideriamo, infine, il fatto che le macchine di Turing distinte, anche non equivalenti, possono computare la stessa funzione (infatti, esiste in generale più di un algoritmo per calcolare una funzione e ad algoritmi distinti corrispondono macchine di Turing distinte).

In definitiva, disponendo di un'enumerazione degli elementi dell'insieme I_{MT}, cioè di un'enumerazione effettiva dell'insieme delle funzioni Turing-calcolabili (associando ad ogni macchina di Turing che ammette risultato, la funzione da essa calcolata); per le considerazioni espresse sopra tale enumerazione sar‡ certamente con ripetizioni.

Non è difficile tuttavia, da un'enumerazione con ripetizioni ottenerne una senza ripetizioni: nella costruzione della nuova enumerazione basta tralasciare gli elementi, cioè le funzioni, già inclusi nell'enumerazione stessa.

Per la tesi di Church, che asserisce che l'insieme delle funzioni Turing-calcolabili coincide con la classe delle funzion i calcolabili (algoritmicamente), possiamo dunque concludere che l'insieme delle funzioni calcolabili è un insieme enumerabile (e quindi, poichè è anche infinito, sarà di un infinito numerabile).