

Elementi di calcolabilità e complessità

 `matteogiorgi.github.io`

a.a. 2020

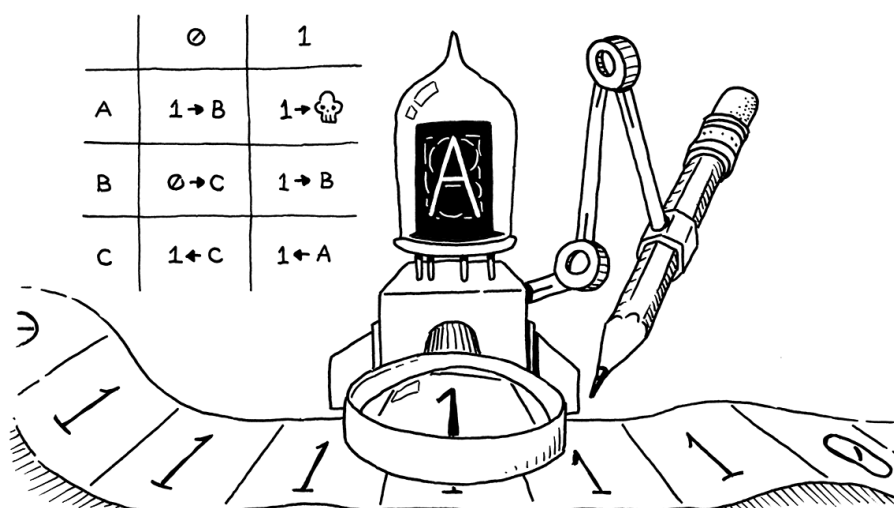
Beep-boop



Queste note sono state redatte dal sottoscritto durante le lezioni del corso di *Elementi di calcolabilità e complessità* tenuto dal prof. Pierpaolo Degano con l'ausilio del dott. Giulio Masetti per l'anno accademico 2019-2020.

Il materiale usato per la stesura, oltre alle note distribuite dal professore, comprende, in maniera più o meno estensiva, i seguenti testi:

- M. Sipser - *Introduction to the theory of computation*
- R.G. Taylor - *Models of computation and formal languages*
- N.J. Cutland - *Computability, introduction to recursive function theory*
- S.B. Cooper - *Computability theory*
- A. Bernasconi, B. Codenotti - *Introduzione alla complessità computazionale*
- G. Ausiello, F. D'Amore, G. Gambosi - *Linguaggi, modelli, complessità*



Algoritmi e macchine



Idea intuitiva di algoritmo

Il punto di partenza della teoria della calcolabilità è l'esigenza di formalizzare l'idea intuitiva di *funzione calcolabile* da un algoritmo, ovvero di *funzione algoritmica*¹.

Si può dire che un algoritmo sia un procedimento di calcolo che consente di pervenire alla soluzione di un problema, numerico o simbolico, mediante una sequenza finita di operazioni, completamente e univocamente determinate: una serie di istruzioni la cui esecuzione consente di trasformare l'insieme finito di dati simbolici che descrivono il problema, nella soluzione del problema stesso.

Caratteristiche distintive²

1. l'insieme delle istruzioni che definisce l'algoritmo è finito
2. l'insieme delle informazioni che rappresentano il problema
 - ha cardinalità finita
 - ha un effetto limitato su dati discreti
 - è descritta da dati finiti
3. il procedimento di calcolo (o *computazione*) è suddiviso in passi discreti e non fa uso di dispositivi analogici
4. ogni passo di computazione dipende solo dai precedenti e da una porzione finita dei dati in modo deterministico (è determinato senza ambiguità - non è soggetto ad alcuna distribuzione probabilistica non banale)
5. non c'è limite al numero di passi necessari all'esecuzione di un algoritmo, nè alla memoria richiesta per contenere i dati iniziali, intermedi e finali

In conclusione, una procedura algoritmica riceve in ingresso una descrizione finita dei dati del problema e restituisce, dopo un tempo finito, una descrizione finita del

¹La nozione di funzione algoritmica sarà poi formalizzata dal concetto di *funzione ricorsiva*

²Può essere utile aggiungere una ulteriore caratteristica a quelle elencate dal prof: *esiste un agente di calcolo in grado di eseguire le istruzioni (un calcolatore)*

risultato. La sua natura deterministica fa sì che l'algoritmo fornisca sempre lo stesso risultato ogni volta che riceve in ingresso gli stessi dati: così facendo l'algoritmo stabilisce una relazione funzionale tra l'insieme dei dati e quello dei risultati.

Macchina di Turing

Esattamente come *funzioni ricorsive* e λ -calcolo, le Macchine di Turing sono un modello di calcolo. Nella sua versione più tradizionale una *MdT* si presenta come un dispositivo che accede ad un nastro potenzialmente illimitato diviso in celle, ciascuna contenente un simbolo appartenente ad un dato alfabeto Σ (alfabeto della macchina), comprendente i simboli $\#$ e \triangleright che denotano rispettivamente l'assenza di informazione nella cella e la marca di inizio stringa.

- la MdT opera tramite un *cursore*, che può scorrere sul nastro in entrambe le direzioni e scrivere i caratteri σ_i appartenenti all'alfabeto Σ
- gli *stati* q_i della macchina appartengono all'insieme finito degli stati Q e identificano istante per istante le informazioni contenute nella macchina

$\triangleright a b \dots a \underline{a} b \# \#$

- il meccanismo che fa evolvere la computazione della macchina è detta *funzione di transizione*³ δ e consente, partendo dallo stato q_x e dal carattere σ_x presente sulla cella puntata dalla testina, di portare la macchina in un altro stato q_y , scrivere un carattere σ_y su tale cella precedentemente occupata da σ_x ed eventualmente spostare la testina ($\Leftarrow, \Rightarrow, \equiv$)

Def. Una Macchina di Turing è definita formalmente come la quadrupla

$$M = (Q, \Sigma, \delta, q_0)$$

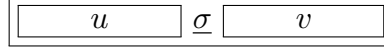
- Q è l'insieme finito degli stati q_i che non contiene lo stato di accettazione h
- Σ è l'insieme finito dei simboli (alfabeto della macchina) al quale non appartengono i simboli di spostamento $\Leftarrow, \Rightarrow, \equiv$
- $\delta \subseteq (Q \times \Sigma) \times (Q \cup h) \times \Sigma \times \{\Leftarrow, \Rightarrow, \equiv\}$ è la relazione di transizione, tale che il carattere puntato dal cursore non possa mai trovarsi a sinistra di \triangleright
- $q_0 \in Q$ è lo stato iniziale

³Nel trattare MdT deterministiche (quelle definite in questo capitolo) non è errato considerare δ come una funzione. La definizione formale fa riferimento a MdT nastro singolo, comprese quelle non-deterministiche dove δ restituisce un insieme di possibili configurazioni successive: ecco perchè sarà qui introdotta come relazione

Configurazione, transizione e computazione

Def. Una configurazione (istantanea) C di una MdT è definita dalla quadrupla

$$(q, u, \sigma, v) \in (Q \cup \{h\}) \times \Sigma^* \times \Sigma \times \Sigma^F$$



- q è lo stato corrente
- σ è il simbolo corrente
- u è la stringa di caratteri a sinistra del simbolo corrente
- v è la stringa di caratteri a destra del simbolo corrente

Ne viene intuitivo dedurre che Σ^* rappresenti l'insieme di cardinalità infinita delle stringhe generabili dalla *giustapposizione* (\circ) dei caratteri dell'alfabeto della macchina Σ , mentre Σ^F è più facile a scriversi che a dirsi: $\Sigma^* \circ (\Sigma \setminus \{\#\}) \cup \{\epsilon\}$ ⁴.

In generale una configurazione di una MdT non è altro che la coppia formata dallo stato corrente della macchina più la stringa⁵ rappresentante la situazione sul nastro.

δ come funzione

Alla luce delle definizioni di MdT e configurazione, è importante analizzare meglio la relazione di transizione δ , definita precedentemente come la quadrupla

$$((q_x, \sigma_x), q_y, \sigma_y, D)$$

- (q_x, σ_x) è la coppia stato di partenza, carattere puntato dal cursore
- q_y è lo stato di arrivo
- σ_y è il carattere scritto nella cella precedentemente occupata da σ_x
- D è lo spostamento del cursore ($\Leftarrow, \Rightarrow, \equiv$)

Adesso è facilmete intuibile che, una macchina nella medesima configurazione di partenza che compie il medesimo spostamento del cursore, si troverà nella medesima configurazione di arrivo.

Questa constatazione permette di restringere la relazione δ in modo che sia una funzione rispetto al suo primo argomento (coppia stato corrente, carattere letto):

$$\delta(q_x, \sigma_x) = (q_y, \sigma_y, D)$$

⁴Quando definiremo meglio cos'è un linguaggio accettato da una MdT (o da un automa a stati finiti) sarà più chiaro come costruire un insieme di stringhe

⁵Quando verranno trattate macchine a k nastri, si parlerà di una k -upla di stringhe, ciascuna delle quali riferita ad un nastro della macchina

Nuova definizione di MdT

Prima di procedere, è necessario utilizzare le considerazioni fatte fin'ora e ritoccare la nostra definizione di MdT estendendo la quadrupla ad una quintupla con l'introduzione di $\{q_A, q_R\}$; questo faciliterà il nostro percorso nell'utilizzo di macchine e linguaggi regolari come strumento per trattare la classe dei *problemi decisionali*.

Def. Una Macchina di Turing deterministica è definita come la quintupla

$$M = (Q, \Sigma, \delta, q_0, \{q_A, q_R\})$$

- Q è l'insieme finito degli stati q_i che non contiene gli stati terminali q_A e q_R
- $\Sigma \not\supseteq \{\Leftarrow, \Rightarrow, \equiv\}$ è sempre l'insieme finito dei simboli (alfabeto di macchina)
- $\delta: (Q \times \Sigma) \rightarrow (Q \times \Sigma \times \{\Leftarrow, \Rightarrow, \equiv\})$ è la funzione di transizione
- $q_0 \in Q$ è lo stato iniziale
- $\{q_A, q_R\} \not\subseteq Q$ è l'insieme formato dagli stati terminali di accettazione e rifiuto

Computazione e passo di computazione

Def. Una computazione di una MdT è costituita da una sequenza di configurazioni, tale che C_0 rappresenti la configurazione iniziale e C_{i+1} il risultato dell'applicazione della funzione δ alla configurazione C_i (ovvero il passo di computazione $C_i \rightarrow C_{i+1}$). Si dirà inoltre che la computazione converge \downarrow se, per $n \geq 1$ tale che

$$C_0 \rightarrow C_1 \rightarrow \dots \rightarrow C_n$$

C_n è una configurazione finale, in caso contrario si dirà che diverge \uparrow .

Per completezza, dato che un passo di computazione di una macchina M può essere visto come una relazione \rightarrow_M tra C_i e C_{i+1} , una computazione di M è definibile come la *chiusura riflessiva e transitiva*⁶ di \rightarrow_M che, in accordo con la notazione usata precedentemente, può essere scritta come

$$C_0 \rightarrow_M^* C_n$$

⁶La chiusura riflessiva e transitiva \bar{R} di una relazione R è la più piccola relazione definita per induzione con le proposizioni: $\boxed{\forall a \in A, \exists \bar{R}(a, a)}$, $\boxed{R(a, b) \Rightarrow \bar{R}(a, b)}$, $\boxed{\bar{R}(a, b), \bar{R}(b, c) \Rightarrow \bar{R}(a, c)}$. Alternativamente ed in modo del tutto equivalente, può essere definita come $\bar{R} = \cap_{R \subseteq S} S$, dove S è anch'essa una relazione riflessiva e transitiva (dimostrare l'equivalenza per esercizio).

Esempio di MdT

Consideriamo una macchina M che calcoli la somma di due numeri naturali rappresentati in notazione unaria con il simbolo $|$ e separati dal simbolo $+$. La successione

$$\begin{aligned} (q_0, \underline{\triangleright}| + ||\#) &\rightarrow (q_0, \underline{\triangleright}| + ||) \rightarrow (q_0, \underline{\triangleright}| \pm ||) \rightarrow (q_1, \underline{\triangleright}|||) \rightarrow \\ &\rightarrow (q_1, \underline{\triangleright}|||) \rightarrow (q_1, \underline{\triangleright}|||\underline{\#}) \rightarrow (q_2, \underline{\triangleright}|||) \rightarrow (h, \underline{\triangleright}|||\underline{\#}) \end{aligned}$$

rappresenterà la computazione $(q_0, \underline{\triangleright}| + ||\#) \rightarrow_M^* (h, \underline{\triangleright}|||\underline{\#})$, mentre la funzione δ può essere tabellata come segue

q	σ	δ
q_0	\triangleright	$q_0, \triangleright, \Rightarrow$
q_0	$ $	$q_0, , \Rightarrow$
q_0	$+$	$q_1, , \Rightarrow$
q_1	$ $	$q_1, , \Rightarrow$
q_1	$\#$	$q_2, \#, \Leftarrow$
q_2	$ $	$h, \#, \equiv$

Automi e linguaggi



In questo capitolo verranno richiamate alcune nozioni utili per studiare *decidibilità*, *riducibilità* ed eventualmente l'insolubilità di problemi. Sarà utile avere ben chiaro cosa siano automi, linguaggi regolari e la loro relazione con le MdT definite.

Def. Un automa finito deterministico (DFA) è la quintupla

$$(Q, \Sigma, \delta, q_0, F)$$

- Q è l'insieme finito degli stati
- Σ è l'insieme finito dei simboli (alfabeto)
- $\delta: Q \times \Sigma \rightarrow Q$ è la funzione di transizione
- $q_0 \in Q$ è lo stato iniziale
- $F \subseteq Q$ è l'insieme degli stati di accettazione

La funzione di transizione δ definisce le regole per il cambiamento di stato: specifica esattamente uno stato successivo per ogni possibile combinazione di stato e simbolo in input. Se ne deduce che, *da ogni stato esce esattamente un arco di transizione per ogni possibile simbolo di input* (ecco perchè automa deterministico o DFA).

Def. Un automa finito non deterministico (NFA) è la quintupla

$$(Q, \Sigma, \Delta, q_0, F)$$

- Q è l'insieme finito degli stati
- Σ è l'insieme finito dei simboli (alfabeto)
- $\Delta: Q \times \Sigma_\epsilon \rightarrow \mathcal{P}(Q)$ è la funzione di transizione
- $q_0 \in Q$ è lo stato iniziale
- $F \subseteq Q$ è l'insieme degli stati di accettazione

Le due definizioni di automa differiscono nel tipo⁷ della funzione di transizione: Δ prende uno stato, un simbolo (compreso il simbolo nullo ϵ) e produce l'insieme dei

⁷inteso come *arrow type*: il tipo dei parametri in input-output per i quali una funzione può essere assegnata

possibili stati successivi (sottoinsieme di $\mathcal{P}(Q)$, insieme delle parti di Q); contrariamente, δ produce un singolo stato successivo dalla coppia in input stato attuale, simbolo letto.