Elementi di Calcolabilità e Complessità

Luca De Paulis

22 settembre 2021

Indice

INDICE i

1 INTRODUZIONE ALLA CALCOLABILITÀ 1
1.1 Macchine di Turing 1
1.2 Calcolabilità di funzioni 4
1.3 Funzioni ricorsive 6

1

Introduzione alla Calcolabilità

Nella prima parte del corso, dedicata alla **Teoria della Calcolabilità**, cercheremo di studiare cosa significhi *calcolare* qualcosa e quali siano i limiti delle *procedure* a disposizione degli esseri umani per calcolare.

Per far ciò bisogna innanzitutto definire il concetto di **algoritmo** oppure procedura: lo faremo definendo dei vincoli che ogni algoritmo deve soddisfare per esser ritenuto tale.

1. Dato che gli uomini possono calcolare solo seguendo procedure finite, un algoritmo deve essere **finito**, ovvero deve essere costituito da un numero finito di istruzioni.
2. Inoltre devono esserci un numero **finito** di istruzioni distinte, e ognuna deve avere un **effetto limitato** su **dati discreti** (nel senso di non continui).
3. Una **computazione** è quindi una sequenza finita di passi discreti con durata finita, né analogici né continui.
4. Ogni passo dipende solo dai **passi precedenti** e viene scelto in modo **deterministico**: se ripetiamo due volte la stessa esatta computazione nelle stesse condizioni dobbiamo ottenere lo stesso risultato e la stessa sequenza di passi.
5. Non imponiamo un limite al numero di passi e alla memoria a disposizione.

Questi vincoli non definiscono precisamente cosa sia un algoritmo, anzi, vedremo che vi sono diversi modelli di computazione che soddisfano questi 5 requisiti. Le domande a cui vogliamo rispondere sono:

- Modelli diversi che rispettano questi vincoli risolvono gli stessi problemi?
- Un tale modello risolve necessariamente tutti i problemi?

1.1 MACCHINE DI TURING

Il primo modello di computazione che vedremo è stato proposto da Alan Turing nel 1936, ed è pertanto chiamato in suo nome.

Definizione 1.1.1 – Macchina di Turing

Una **Macchina di Turing** (MdT per gli amici) è una quadrupla (Q, Σ, δ, q_0) dove

- Q è un insieme finito, detto **insieme degli stati**. In particolare assumiamo che esista uno stato $h \notin Q$, detto stato terminatore o **halting state**.
- Σ è un insieme finito, detto **insieme dei simboli**. In particolare

  - esiste $\# \in \Sigma$ e lo chiameremo **simbolo vuoto**;
  - esiste $\triangleright \in \Sigma$ e lo chiameremo **respingente**.
- δ è una funzione

$$\delta : Q \times \Sigma \to (Q \cup \{ h \}) \times \Sigma \times \{ L, R, - \}$$

  detta **funzione di transizione**. È soggetta al vincolo

$$\forall q \in Q : \exists q' \in Q : \quad \delta(q, \triangleright) = (q', \triangleright, R).$$

- q_0 è un elemento di Q detto **stato iniziale**.

La definizione formale di Macchina di Turing può sembrare complicata, ma l'idea alla base è molto semplice: abbiamo una macchina che opera su un **nastro illimitato** (a destra) su cui sono scritti simboli (ovvero elementi di Σ). In ogni istante di tempo, la *testa* della macchina legge una casella del nastro, contenente il **simbolo corrente**. La macchina mantiene inoltre al suo interno uno stato (ovvero un elemento di Q), inizialmente settato allo stato iniziale q_0.

Un singolo passo di computazione è il seguente:

- la macchina legge il simbolo corrente σ;
- la macchina usa la funzione di transizione δ per effettuare la mossa: in particolare calcola $\delta(q, \sigma)$, dove q è lo stato corrente, e ne ottiene una tripla (q', σ', M);
- la macchina cambia stato da q a q';
- la macchina scrive al posto di σ il simbolo σ';
- la macchina si sposta nella direzione indicata da M: se $M = L$ si sposta di un posto a sinistra, se $M = R$ si sposta di un posto a destra, se $M = -$ rimane ferma.

Per formalizzare questi concetti abbiamo bisogno di altre definizioni.

Definizione 1.1.2 – Monoide libero, o Parole su un Alfabeto

Dato un insieme finito Σ, il **monoide libero** su Σ, anche chiamato **insieme delle parole su** Σ, è l'insieme Σ^* così definito:

$$\Sigma^* := \bigcup_{n \in \mathbb{N}} \Sigma^n$$

dove

- $\Sigma^0 := \{ \varepsilon \}$, dove ε è la parola vuota;
- $\Sigma^{n+1} := \{ \sigma \cdot w : \sigma \in \Sigma, w \in \Sigma^n \}$ è l'insieme delle parole di lunghezza $n + 1$, ottenute preponendo ad una parola di lunghezza n (ovvero $w \in \Sigma^n$) un simbolo $\sigma \in \Sigma$.

Tale insieme ammette un'operazione, ovvero la **concatenazione** di parole, e la parola vuota ε è l'identità destra e sinistra di tale operazione.

Osservazione 1.1.1. Un elemento di Σ^* è una stringa di caratteri di Σ di lunghezza arbitraria, ma sempre finita, in quanto ogni elemento di Σ^* deve essere contenuto in un qualche Σ^n.

Il nastro di una MdT può quindi essere formalizzato come un elemento di Σ^*. Questo tuttavia ancora non ci soddisfa per alcuni motivi:

- gli elementi di Σ^* sono illimitati a destra, ma non a sinistra, dunque la MdT potrebbe muoversi a sinistra ripetutamente fino a "cadere fuori dal nastro";
- non stiamo memorizzando da alcuna parte la posizione del cursore della MdT.

Per risolvere il primo problema possiamo assumere che ogni nastro inizi con il simbolo speciale $\triangleright$: per il vincolo sulla funzione di transizione ogni volta che la MdT si troverà nella casella più a sinistra (contenente $\triangleright$) sarà costretta a muoversi verso destra lasciando scritto il respingente.

Per quanto riguarda il secondo invece possiamo dividere il nastro infinito in tre parti:

- la porzione a sinistra del simbolo corrente, che è una stringa di lunghezza arbitraria che inizia per $\triangleright$ e quindi un elemento di $\triangleright\Sigma^*$;
- il simbolo corrente, che è un elemento di Σ;
- la porzione a destra del simbolo corrente, che è una stringa e quindi un elemento di Σ^*.

Quest'ultima porzione è una stringa che potrebbe terminare con un numero infinito di caratteri vuoti (#): dato che non siamo interessati (per il momento) a tenere tutti i simboli vuoti a destra dell'ultimo simbolo non-vuoto del nastro, considereremo la porzione a destra "eliminando" tutti i *blank* superflui.

In particolare indicando sempre con $\varepsilon \in \Sigma^*$ la stringa vuota e convenendo che

- $\#\varepsilon = \varepsilon\# = \varepsilon$ (la concatenazione della stringa vuota con il *blank* dà ancora la stringa vuota);
- $\sigma\varepsilon = \varepsilon\sigma = \sigma$ per ogni $\sigma \neq \#$ (la concatenazione della stringa vuota con un simbolo non-*blank* dà il simbolo)

possiamo considerare l'insieme

$$\Sigma^F := \Big(\Sigma^* \cdot (\Sigma \setminus \{\#\})\Big) \cup \{\varepsilon\},$$

ovvero l'insieme delle stringhe in Σ che finiscono con un carattere non-*blank*, più la stringa vuota.

Usando queste convenzioni, la stringa che definisce il nastro è finita: siamo pronti a definire la *configurazione* di una MdT in un dato istante.

Definizione 1.1.3 – Configurazione di una MdT

Sia $M = (Q, \Sigma, \delta, q_0)$ una MdT. Una **configurazione** è una quadrupla

$$(q, u, \sigma, v) \in Q \times \triangleright\Sigma^* \times \Sigma \times \Sigma^F.$$

Più nel dettaglio:

- q è lo stato corrente,
- u è la porzione del nastro che precede il simbolo corrente, ed inizia per $\triangleright$,
- σ è il simbolo corrente,
- v è la porzione del nastro che segue il simbolo corrente, ed è vuota oppure termina per un simbolo diverso da #.

Osserviamo che:

- il simbolo corrente può essere #;

- è possibile che il simbolo corrente sia # e $v = \varepsilon$ (cioè vuota),
- è possibile che u sia vuota solo nel caso in cui il simbolo corrente è $\triangleright$, poiché significherebbe trovarsi all'inizio del nastro.

Spesso indicheremo la quadrupla (q, u, σ, v) con $(q, u\underline{\sigma}v)$: la sottolineatura ci indicherà il simbolo corrente. In contesti in cui non sia necessario sapere la posizione del cursore scriveremo semplicemente (q, w) per risparmiare tempo.

Esempio 1.1.4. Ad esempio la configurazione

$$(q_0, \triangleright ab\#\#b\#a\underline{\#}b\#a)$$

indica che la MdT è nello stato q_0, sta leggendo il carattere #, a sinistra del simbolo letto ha la stringa $\triangleright ab\#\#b\#a$ e a destra $b\#a$.

1.2 CALCOLABILITÀ DI FUNZIONI

Dopo aver definito le computazioni per le MdT e per i linguaggi `FOR` e `WHILE`, vogliamo spiegare cosa significa che una MdT o un comando *calcola* una funzione.

Funzioni

Prima di tutto, ricordiamo le definizioni di base sulle funzioni.

Definizione 1.2.1 – Funzione

Dati A, B insiemi, una **funzione** f da A in B è un sottoinsieme di $A \times B$ tale che

$$(a, b), (a, b') \in f \implies b = b'.$$

Scriveremo

- $f : A \to B$ per indicare una funzione da A in B
- $b = f(a)$ per dire $(a, b) \in f$.

Notiamo inoltre che non abbiamo fatto assunzioni sulla **totalità** di f: per qualche valore di $a \in A$ potrebbe non esistere un valore $b \in B$ tale che $f(a)$, cioè f potrebbe *non essere definita* in a.

Definizione 1.2.2 – Funzioni totali e parziali

Sia $f : A \to B$.

- f **converge su** $a \in A$ (e lo si indica con $f(a)\downarrow$) se esiste $b \in B$ tale che $f(a) = b$;
- f **diverge su** $a \in A$ (e lo si indica con $f(a)\uparrow$) se f non converge su a;
- f è **totale** se $f(a)\downarrow$ per ogni $a \in A$;
- f è **parziale** se non è totale.

In generale le nostre funzioni saranno parziali.

Definizione 1.2.3 – Dominio ed immagine

Sia $f : A \to B$. Si dice **dominio** di f l'insieme

$$\operatorname{dom} f := \{ a \in A \ : \ f(a)\downarrow \}.$$

Si dice **immagine** di f l'insieme

$$\operatorname{Im} f := \{ b \in B \ : \ b = f(a) \text{ per qualche } a \in A \}.$$

Definizione 1.2.4 – Iniettività/surgettività/bigettività

Sia $f : A \to B$ una funzione.

- f è **iniettiva** se per ogni $a, a' \in A$, $a \neq a'$, allora $f(a) \neq f(a')$.
- f è **surgettiva** se $\operatorname{Im} f = B$.
- f è **bigettiva** se è iniettiva e surgettiva.

Calcolare funzioni

Definiamo ora quando una macchina/un comando *implementa* una funzione.

Definizione 1.2.5 – Turing-calcolabilità

Siano $\Sigma, \Sigma_0, \Sigma_1$ alfabeti, $\triangleright, \# \notin \Sigma_0 \cup \Sigma_1 \subsetneq \Sigma$.
Sia inoltre $f : \Sigma_0 \to \Sigma_1$, $M = (Q, \Sigma, \delta, q_0)$ una MdT.
Si dice allora che M **calcola** f (e che f è **Turing-calcolabile**) se per ogni $v \in \Sigma_0$

$$w = f(v) \text{ se e solo se } (q_0, \underline{\triangleright} v) \to^* (h, \triangleright w \underline{\#}).$$

Indicando con $M(v)$ il risultato della computazione della macchina M sulla configurazione iniziale $(q_0, \underline{\triangleright} v)$, questa definizione ci dice che gli output della funzione e della MdT sono esattamente gli stessi. In particolare, dato che le funzioni possono essere *parziali* e le macchine di Turing possono *divergere*, $M(v)\downarrow$ se e solo se f è definita su v, cioè se esiste w tale che $f(v) = w$.

Definizione 1.2.6 – `WHILE`-calcolabilità

Sia C un comando `WHILE`, g : `Var` $\to \mathbb{N}$. Si dice allora che C **calcola** g (e che g è **`WHILE`-calcolabile**) se per ogni $\sigma \in$ `Var`

$$y = f(x) \text{ se e solo se } (C, \sigma) \to^* \sigma^* \text{ e } \sigma^*(x) = n.$$

Analogamente possiamo definire il concetto di funzione `FOR`-calcolabile.
È vero che le funzioni `WHILE`-calcolabili sono tutte e sole le funzioni `FOR`-calcolabili? **No**: infatti dato che non abbiamo fatto assunzioni sulla totalità di g, essa può essere `WHILE`-calcolabile ma non `FOR`-calcolabile.
Un possibile problema nella definizione di calcolabilità data è che abbiamo supposto che le funzioni abbiano una specifica forma: sono funzioni $\Sigma_0^* \to \Sigma_1^*$ nel caso delle MdT, `Var` $\to \mathbb{N}$ nel caso dei comandi. Scegliendo altri insiemi con le stesse caratteristiche (quindi di cardinalità numerabile) cambiano le funzioni calcolabili?
Fortunatamente la risposta è **no**. Consideriamo una funzione $f : A \to B$: se gli insiemi A, B sono numerabili possiamo scegliere delle **codifiche** $A \to \mathbb{N}$, $\mathbb{N} \to B$. A questo punto possiamo

- trasformare l'input $a \in A$ in un naturale tramite la prima codifica;
- fare il calcolo tramite una funzione $\mathbb{N} \to \mathbb{N}$,
- trasformare l'output in un elemento di B tramite la seconda codifica.

In questo modo possiamo limitarci a solo funzioni $\mathbb{N} \to \mathbb{N}$, a patto che la codifica sia **effettiva**, cioè sia calcolabile anch'essa.

1.3 FUNZIONI RICORSIVE

Introduciamo ora un ultimo formalismo per rappresentare un modello di calcolo, ovvero quello delle funzioni ricorsive.

Per semplificare la notazione useremo la λ-notazione per le funzioni anonime: la funzione $\lambda x.\ f(x)$ è la funzione che prende un unico parametro di ingresso x e restituisce $f(x)$.

Definizione 1.3.1 – Funzioni primitive ricorsive

La classe delle **funzioni primitive ricorsive** $\mathcal{PR}$ è la minima classe di funzioni che contenga

- ZERO $\quad \lambda x_1, \dots, x_n.\ 0 \quad$ per ogni $n \in \mathbb{N}$
- SUCCESSORE $\quad \lambda x.\ x + 1$
- PROIEZIONE $\quad \lambda x_1, \dots, x_n.\ x_i \quad$ per ogni $n \in \mathbb{N}, i = 1, \dots, n$

e che sia chiusa per le seguenti operazioni:

- COMPOSIZIONE se $g_1, \dots, g_k : \mathbb{N}^n \to \mathbb{N}$, $h : \mathbb{N}^k \to \mathbb{N}$ appartengono a $\mathcal{PR}$, allora

$$\lambda x_1, \dots, x_n.\ h\Big(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)\Big)$$

appartiene ancora a $\mathcal{PR}$;

- RICORSIONE PRIMITIVA se $h : \mathbb{N}^{n+1} \to \mathbb{N}$, $g : \mathbb{N}^{n-1} \to \mathbb{N}$ appartengono a $\mathcal{PR}$, allora

$$f : \mathbb{N}^n \to \mathbb{N}$$

$$f(x_1, \dots, x_n) := \begin{cases} f(0, x_2, \dots, x_n) = g(x_2, \dots, x_n) \\ f(n+1, x_2, \dots, x_n) = h(n, f(n, x_2, \dots, x_n), x_2, \dots, x_n) \end{cases}$$

appartiene ancora a $\mathcal{PR}$.