

# Elementi di Calcolabilità e Complessità

Appunti del corso di ECC del Professor Pierpaolo Degano, A.A. 2021/2022

Luca De Paulis

27 novembre 2021

## Introduzione

Questo file contiene i miei appunti (rielaborati) del corso di Elementi di Calcolabilità e Complessità tenuto dal Professor Pierpaolo Degano nell'anno 2021/2022. Dato che questi appunti sono stati scritti per me stesso, potrebbero essere pieni di errori o ragionamenti incomprensibili a tutti tranne che a me: in ogni caso ogni segnalazione è ben accetta!

Luca De Paulis

# Indice

---

<b>1</b>	<b>Introduzione alla Calcolabilità</b>	<b>1</b>
1.1	Macchine di Turing	1
1.2	Linguaggi FOR e WHILE	4
1.3	Calcolabilità di funzioni	8
1.4	Funzioni ricorsive	10
1.4.1	Enumerazione di Gödel	13
1.4.2	Funzione di Ackermann	15
1.4.3	Non esiste un formalismo capace di esprimere tutte e sole le funzioni calcolabili totali	15
1.5	Funzioni generali ricorsive	16
1.5.1	Tesi di Church-Turing	17
1.6	Primi teoremi sulle funzioni calcolabili	17
1.6.1	Enumerazioni effettive	18
1.6.2	Equivalenza tra MdT e funzioni generali ricorsive	19
<b>2</b>	<b>Calcolabilità di problemi</b>	<b>23</b>
2.1	Problemi di decisione	23
2.2	Separazione di $\mathcal{R}$ e $\mathcal{RE}$	25
2.3	Riduzioni di classi di problemi	27
2.4	Studio di $\mathcal{R}$ e $\mathcal{RE}$ tramite riduzioni	29
2.4.1	Altri problemi completi per $\mathcal{RE}$	31
2.5	Il Teorema di Rice	32
<b>3</b>	<b>Teoria della Complessità</b>	<b>36</b>
3.1	Complessità deterministica	37
3.2	Complessità in spazio	40
3.3	Non-Determinismo e Complessità non-deterministica	43
3.4	Funzioni di misura appropriata	45
<b>A</b>	<b>Esercizi</b>	<b>49</b>
A.1	Esercizi di calcolabilità	49

# 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  $(Q, \Sigma, \delta, q_0)$  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**.
- $\Sigma$  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**.
- $\delta$  è una funzione

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

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

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

- $q_0$  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  $\Sigma$ ). 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  $\sigma$ ;
- la macchina usa la funzione di transizione  $\delta$  per effettuare la mossa: in particolare calcola  $\delta(q, \sigma)$ , dove  $q$  è lo stato corrente, e ne ottiene una tripla  $(q', \sigma', M)$ ;
- la macchina cambia stato da  $q$  a  $q'$ ;
- la macchina scrive al posto di  $\sigma$  il simbolo  $\sigma'$ ;
- 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  $\Sigma$ , il **monoide libero** su  $\Sigma$ , anche chiamato **insieme delle parole su  $\Sigma$** , è l'insieme  $\Sigma^*$  così definito:

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

dove

- $\Sigma^0 := \{\varepsilon\}$ , dove  $\varepsilon$  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  $\varepsilon$  è l'identità destra e sinistra di tale operazione.

**Osservazione 1.1.1** (-NoValue-). Un elemento di  $\Sigma^*$  è una stringa di caratteri di  $\Sigma$  di lunghezza arbitraria, ma sempre finita, in quanto ogni elemento di  $\Sigma^*$  deve essere contenuto in un qualche  $\Sigma^n$ .

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

- gli elementi di  $\Sigma^*$  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  $\Sigma$ ;
- la porzione a destra del simbolo corrente, che è una stringa e quindi un elemento di  $\Sigma^*$ .

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

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

ovvero l'insieme delle stringhe in  $\Sigma$  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  $\triangleright$ ,
- $\sigma$  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  $(q, u, \sigma, v)$  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** (-NoValue-). 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 Linguaggi FOR e WHILE

Introduciamo ora un secondo paradigma per il calcolo di algoritmi, ovvero quello dato dai linguaggi FOR e WHILE. In effetti anche se le MdT rispondono ai nostri requisiti formali per un algoritmo e sono il modello teorico delle **macchine di Von Neumann**, al giorno d'oggi non costruiamo una nuova macchina per ogni algoritmo che dobbiamo risolvere: usiamo dei **linguaggi di programmazione** che verranno interpretati o compilati e restituiranno il risultato del calcolo.

I linguaggi FOR e WHILE sono quindi la base teorica dei moderni linguaggi imperativi, e anche se sembrano mancare di espressività rispetto ad essi, vedremo che in realtà il linguaggio WHILE riesce a risolvere tutti e soli i problemi risolvibili da un linguaggio moderno.

## Sintassi astratta

### Definizione 1.2.1 – Sintassi astratta di FOR e WHILE

$\text{EXPR} ::= n \mid x \mid E_1 + E_2 \mid E_1 \cdot E_2 \mid E_1 - E_2$	Espr. aritmetiche
$\text{BEXPR} ::= b \mid E_1 < E_2 \mid \neg b \mid B_1 \vee B_2$	Espr. booleane
$\text{CMD} ::= \text{skip} \mid x := E \mid C_1; C_2 \mid \text{if } B \text{ then } C_1 \text{ else } C_2$	Comandi
$\mid \text{for } x = E_1 \text{ to } E_2 \text{ do } C \mid \text{while } B \text{ do } C$	

dove  $n \in \mathbb{N}$ ,  $x \in \text{Var}$  (che è un insieme *numerabile* di variabili),  $b \in \mathbb{B} := \{\mathcal{T}, \mathcal{F}\}$ .

Il linguaggio FOR contiene solo il comando `for`, il linguaggio WHILE contiene solo il comando `while`.

## Semantica

Per definire la **semantica** dei linguaggi FOR e WHILE abbiamo bisogno di alcuni costrutti ausiliari. In particolare ogni nostro programma conterrà delle variabili che possono essere valutate oppure aggiornate (tramite il comando di assegnamento): dobbiamo *memorizzare* il loro valore.

### Definizione 1.2.2 – Funzione memoria e funzione di aggiornamento

La funzione **memoria** è una funzione

$$\sigma : \text{Var} \rightarrow \mathbb{N}$$

definita solo per un sottoinsieme finito di  $\text{Var}$ .

La funzione di **aggiornamento** è una funzione

$$-[-/-] : (\text{Var} \times \mathbb{N}) \times \mathbb{N} \times \text{Var} \rightarrow (\text{Var} \times \mathbb{N})$$

definita da

$$\sigma[n/x](y) := \begin{cases} n & \text{se } y = x, \\ \sigma(y) & \text{altrimenti.} \end{cases}$$

**Osservazione 1.2.1** (-NoValue-). La funzione di aggiornamento prende una memoria ( $\sigma : \text{Var} \rightarrow \mathbb{N}$ ), un valore intero ( $n \in \mathbb{N}$ ) e una variabile ( $x \in \text{Var}$ ) e produce una nuova memoria  $\sigma[n/x] : \text{Var} \rightarrow \mathbb{N}$  che si comporta come  $\sigma$  su tutte le variabili diverse da  $x$ , ma restituisce  $n$  quando l'input è  $x$ .

Tramite la memoria possiamo definire la funzione di valutazione delle espressioni aritmetiche, ovvero la loro **semantica**.

### Definizione 1.2.3 – Funzione di valutazione semantica (aritmetica)

La **funzione di valutazione semantica (aritmetica)** è una funzione

$$\mathcal{E}[-] : \text{EXPR} \times (\text{Var} \rightarrow \mathbb{N}) \rightarrow \mathbb{N}$$



definita per induzione strutturale a partire da

$\mathcal{E}[\![n]\!]\sigma$	$:= n$	(val. dei naturali)
$\mathcal{E}[\![x]\!]\sigma$	$:= \sigma(x)$	(val. delle variabili)
$\mathcal{E}[\![E_1 + E_2]\!]\sigma$	$:= \mathcal{E}[\![E_1]\!]\sigma + \mathcal{E}[\![E_2]\!]\sigma$	(val. della somma)
$\mathcal{E}[\![E_1 \cdot E_2]\!]\sigma$	$:= \mathcal{E}[\![E_1]\!]\sigma \cdot \mathcal{E}[\![E_2]\!]\sigma$	(val. del prodotto)
$\mathcal{E}[\![E_1 - E_2]\!]\sigma$	$:= \mathcal{E}[\![E_1]\!]\sigma - \mathcal{E}[\![E_2]\!]\sigma$	(val. della sottrazione)

Dato che il nostro linguaggio modella solo numeri naturali (quindi positivi), l'operazione di sottrazione sarà quella data dal **meno limitato**:

$$a - b := \begin{cases} a - b, & \text{se } a > b \\ 0, & \text{altrimenti.} \end{cases}$$

Analogamente possiamo definire la semantica delle espressioni booleane.

**Definizione 1.2.4** – Funzione di valutazione semantica (booleana)

La **funzione di valutazione semantica (booleana)** è una funzione

$$\mathcal{B}[\![-]\!] : \text{BEXPR} \times (\text{Var} \rightarrow \mathbb{N}) \rightarrow \mathbb{N}$$

definita per induzione strutturale a partire da

$\mathcal{B}[\![t]\!]\sigma$	$:= \mathcal{T}$	(val. del true)
$\mathcal{B}[\![f]\!]\sigma$	$:= \mathcal{F}$	(val. del false)
$\mathcal{B}[\![E_1 < E_2]\!]\sigma$	$:= \mathcal{E}[\![E_1]\!]\sigma < \mathcal{E}[\![E_2]\!]\sigma$	(val. del minore)
$\mathcal{B}[\![\neg B]\!]\sigma$	$:= \neg \mathcal{B}[\![B]\!]\sigma$	(val. del not)
$\mathcal{B}[\![B_1 \vee B_2]\!]\sigma$	$:= \mathcal{B}[\![B_1]\!]\sigma \vee \mathcal{B}[\![B_2]\!]\sigma$	(val. della sottrazione)

Osserviamo che i simboli usati nel linguaggio (come  $+$ ,  $<$ ,  $\neg$ , ed altri) sono solo **simboli formali**: per essere più precisi dovremmo differenziarli dalle funzioni effettive (ovvero quelle che compaiono a destra del  $:=$ ).

**Osservazione 1.2.2** (-NoValue-). Le funzioni  $\mathcal{E}$  e  $\mathcal{B}$  si comportano come un **interprete**: ad esempio  $\mathcal{E}$  prende un'espressione aritmetica, una memoria e restituisce la valutazione dell'espressione nella memoria data.

Tuttavia tramite il **currying** possiamo esprimere  $\mathcal{E}$  come una funzione

$$\mathcal{E}[\![-]\!] : \text{EXPR} \rightarrow ((\text{Var} \rightarrow \mathbb{N}) \rightarrow \mathbb{N})$$

ovvero come una funzione che prende un'espressione aritmetica e restituisce una *funzione* che a sua volta prenderà una memoria per restituire finalmente la valutazione dell'espressione nella memoria.

Anche se le due modalità in pratica ci portano allo stesso risultato, la seconda modella più l'azione di un **compilatore**: infatti nella seconda versione  $\mathcal{E}$  prende un'espressione,

cioè del codice, e restituisce un *eseguibile* che avrà bisogno dei dati (cioè della memoria) per dare il suo risultato.

Lo stile usato per definire la semantica delle espressioni viene chiamato **semantica denotazionale**: in questo stile cerchiamo di associare ad ogni costrutto del linguaggio una funzione che ne dà la semantica (ad esempio abbiamo associato al + del linguaggio la funzione che somma due naturali).

Per quanto riguarda i comandi adopereremo un altro stile, detto **semantica operativa**. Come si evince dal nome, cercheremo di definire una *macchina astratta* che modifica il proprio *stato interno* valutando a piccoli passi il comando da eseguire.

#### Definizione 1.2.5 – Sistema di transizioni

Si dice **sistema di transizioni** una coppia  $(\Gamma, \rightarrow)$  dove

- $\Gamma$  è l'insieme delle **configurazioni** oppure stati;
- $\rightarrow: \Gamma \rightarrow \Gamma$  è una funzione, detta **funzione di transizione**.

Nel caso della nostra macchina astratta, le configurazioni saranno delle coppie

$$\langle c, \sigma \rangle \in \text{CMD} \times (\text{Var} \rightarrow \mathbb{N})$$

ovvero delle coppie "comando da valutare", "memoria".

Per definire la semantica operativa dei comandi useremo un approccio **small-step**, in cui ogni transizione

$$\langle c, \sigma \rangle \rightarrow \langle c', \sigma' \rangle$$

rappresenta un singolo passo dell'esecuzione del programma. Una **computazione** diventa allora una sequenza di passi, ovvero un elemento della chiusura transitiva e riflessiva di  $\rightarrow$ , che indicheremo come al solito come  $\rightarrow^*$ .

Analogamente alle MdT, una computazione **termina con successo** se

$$\langle c, \sigma \rangle \rightarrow^* \sigma',$$

ovvero se esauriamo la valutazione del comando  $c$  in un numero finito (anche se arbitrario) di passi.

La semantica operativa dei comandi è dunque data attraverso una serie di assiomi e regole di inferenza, che insieme ci permettono di valutare ogni comando per induzione strutturale.

$$\frac{-}{\langle \text{skip}, \sigma \rangle \rightarrow \sigma} \quad \text{Assioma dello skip}$$

$$\frac{-}{\langle x := E, \sigma \rangle \rightarrow \sigma[n/x]} \quad \text{se } \mathcal{E}[E]\sigma = n \quad \text{Assioma dell'assegnamento}$$

$$\frac{\langle C_1, \sigma \rangle \rightarrow \langle C'_1, \sigma' \rangle}{\langle C_1; C_2, \sigma \rangle \rightarrow \langle C'_1; C_2, \sigma' \rangle} \quad \text{Regola della sequenza 1}$$

$$\frac{\langle C_1, \sigma \rangle \rightarrow \langle C_2, \sigma' \rangle}{\langle C_1; C_2, \sigma \rangle \rightarrow \sigma'} \quad \text{Regola della sequenza 2}$$

$$\frac{-}{\langle \text{if } B \text{ then } C_1 \text{ else } C_2, \sigma \rangle \rightarrow \langle C_1, \sigma \rangle} \quad \text{se } \mathcal{B}[B]\sigma = \mathcal{T} \quad \text{Assioma cond. 1}$$

$$\frac{-}{\langle \text{if } B \text{ then } C_1 \text{ else } C_2, \sigma \rangle \rightarrow \langle C_2, \sigma \rangle} \quad \text{se } \mathcal{B}[B]\sigma = \mathcal{F} \quad \text{Assioma cond. 2}$$

$$\frac{-}{\langle \text{for } i = E_1 \text{ to } E_2 \text{ do } C, \sigma \rangle \rightarrow \langle i := n; C; \text{for } i = n_1 + 1 \text{ to } n_2 \text{ do } C, \sigma \rangle} \quad \begin{array}{l} \text{se } \mathcal{B}[E_2 < E_1]\sigma = \mathcal{F}, \mathcal{E}[E_1]\sigma = n_1, \mathcal{E}[E_2]\sigma = n_2 \end{array} \quad \text{Assioma del for 1}$$

$$\frac{-}{\langle \text{for } i = E_1 \text{ to } E_2 \text{ do } C, \sigma \rangle \rightarrow \sigma} \quad \text{se } \mathcal{B}[E_2 < E_1]\sigma = \mathcal{T} \quad \text{Assioma del for 2}$$

$$\frac{-}{\langle \text{while } B \text{ do } C, \sigma \rangle \rightarrow \langle \text{if } B \text{ then } (C; \text{while } B \text{ do } C) \text{ else skip}, \sigma \rangle} \quad \text{Assioma del while}$$

Dalla regola di transizione del for segue una proprietà fondamentale del linguaggio FOR: ogni suo programma termina in tempo finito. Infatti prima della prima iterazione la semantica ci impone di valutare le espressioni  $E_1$  ed  $E_2$ , che verranno valutate a dei naturali  $n_1, n_2$ . A questo punto il ciclo for verrà eseguito esattamente  $n_2 - n_1$  volte (dove il  $-$  è sempre limitato, per cui se  $n_1 > n_2$  non eseguiamo mai il ciclo) in quanto gli estremi di iterazione non possono essere modificati dai comandi del corpo del for.

Questo ci dimostra immediatamente che il linguaggio FOR **non è equivalente** alle macchine di Turing, ovvero esistono macchine di Turing che codificano algoritmi non risolvibili dal linguaggio FOR. (Studieremo in seguito cosa significa *codificare algoritmi*.)

Il linguaggio WHILE invece può codificare algoritmi che non terminano. Ad esempio si vede subito che la configurazione

$$\langle \text{while } \mathcal{T} \text{ do skip}, \sigma \rangle$$

diverge a prescindere da  $\sigma$ .

### 1.3 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 1.3.1 – 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

- $f : A \rightarrow B$  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 1.3.2 – Funzioni totali e parziali**

Sia  $f : A \rightarrow B$ .

- $f$  **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  $f(a) \uparrow$ , o con  $f(a) = \perp$ ) 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 1.3.3 – Dominio ed immagine**

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

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

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

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

**Definizione 1.3.4 – Iniettività/surgettività/bigettività**

Sia  $f : A \rightarrow B$  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  $\text{Im } f = B$ .
- $f$  è **bigettiva** se è iniettiva e surgettiva.

**Calcolare funzioni**

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

**Definizione 1.3.5 – Turing-calcolabilità**

Siano  $\Sigma, \Sigma_0, \Sigma_1$  alfabeti,  $\triangleright, \# \notin \Sigma_0 \cup \Sigma_1 \subseteq \Sigma$ .

Sia inoltre  $f : \Sigma_0 \rightarrow \Sigma_1$ ,  $M = (Q, \Sigma, \delta, q_0)$  una MdT.

Si dice allora che  $M$  **calcola**  $f$  (e che  $f$  è **Turing-calcolabile**) se per ogni  $v \in \Sigma_0$

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

Indicando con  $M(v)$  il risultato della computazione della macchina  $M$  sulla configurazione iniziale  $(q_0, \triangleright v)$ , 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 1.3.6 – WHILE-calcolabilità**

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

$$n = g(x) \text{ se e solo se } (C, \sigma) \rightarrow^* \sigma^* \text{ e } \sigma^*(x) = n.$$

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  $\Sigma_0^* \rightarrow \Sigma_1^*$  nel caso delle MdT,  $\text{Var} \rightarrow \mathbb{N}$  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  $f : A \rightarrow B$ : se gli insiemi  $A, B$  sono numerabili possiamo scegliere delle **codifiche**  $A \rightarrow \mathbb{N}, \mathbb{N} \rightarrow B$ . A questo punto possiamo

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

In questo modo possiamo limitarci a solo funzioni  $\mathbb{N} \rightarrow \mathbb{N}$ , a patto che la codifica sia **effettiva**, cioè sia calcolabile anch'essa. Vedremo in seguito che esistono codifiche per rappresentare macchine di Turing come numeri.

## 1.4 Funzioni ricorsive

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

Per semplificare la notazione useremo la  $\lambda$ -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 1.4.1** – Funzioni primitive ricorsive

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

I. **Zero:**  $\lambda x_1, \dots, x_n. 0$  per ogni  $n \in \mathbb{N}$

II. **Successore:**  $\lambda x. x + 1$

III. **Proiezione:**  $\lambda x_1, \dots, x_n. x_i$  per ogni  $n \in \mathbb{N}, i = 1, \dots, n$

e che sia chiusa per gli schemi

IV. **Composizione:** se  $g_1, \dots, g_k : \mathbb{N}^n \rightarrow \mathbb{N}, h : \mathbb{N}^k \rightarrow \mathbb{N}$  appartengono a  $\mathcal{PR}$ , allora

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

appartiene ancora a  $\mathcal{PR}$ ;

V. **Ricorsione Primitiva:** se  $h : \mathbb{N}^{n+1} \rightarrow \mathbb{N}, g : \mathbb{N}^{n-1} \rightarrow \mathbb{N}$  appartengono a  $\mathcal{PR}$ , allora

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

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

appartiene ancora a  $\mathcal{PR}$ .

Una funzione è quindi primitiva ricorsiva se può essere costruita dagli schemi della definizione, ovvero se esiste una successione di funzioni  $f_1, \dots, f_n$  tale che

- $f_n = f$ ,
- per ogni  $i = 1, \dots, n$ ,  $f_i$  è definita come uno dei casi base (ovvero è la funzione zero, successore o proiezione) oppure è ottenuta dagli schemi induttivi (composizione e ricorsione primitiva) e *solamente* dalle funzioni  $f_1, \dots, f_{i-1}$ .

Osserviamo che il calcolo di ogni funzione ricorsiva primitiva *termina sempre*: infatti i casi base (I, II e III) terminano in un singolo passo e per induzione strutturale si vede che anche i casi IV e V terminano in tempo finito, poiché la ricorsione si fa sempre diminuendo il valore di  $x_1$  nello schema V.

Facciamo degli esempi di funzioni ricorsive primitive.

**Esempio 1.4.2** (-NoValue-). Consideriamo la seguente sequenza di funzioni:

$$\begin{aligned} f_1 &= \lambda x. x, & f_2 &= \lambda x. x + 1, & f_3 &= \lambda x_1, x_2, x_3. x_2, \\ f_4 &= f_2(f_3(x_1, x_2, x_3)), & f_5 &= \begin{cases} f_5(0, x_2) = f_1(x_2) \\ f_5(n+1, x_2) = f_4(n, f_5(n, x_2), x_2) \end{cases} \end{aligned}$$

Ognuna delle funzioni è primitiva ricorsiva: infatti

1. la prima corrisponde alla proiezione per  $i = n = 1$ ;

2. la seconda corrisponde al successore;
3. la terza corrisponde alla proiezione con  $n = 3, i = 2$ ;
4. la quarta è la composizione di  $f_2$  ed  $f_3$ ;
5. l'ultima è ottenuta per ricorsione primitiva dalle prime quattro funzioni.

Possiamo porci il problema di come si effettui il calcolo di una funzione primitiva ricorsiva quando ci vengono forniti degli argomenti.

Consideriamo due **regole di valutazione**.

► **Call by value**

Nel **call by value** si valutano prima gli operandi di una funzione e poi la funzione esterna: la **redex** (ovvero la prossima espressione da valutare) è la funzione più interna più a sinistra.

$$\begin{aligned}
 \underline{f_5(2, 3)} &= f_4(1, \underline{f_5(1, 3)}, 3) \\
 &= f_4(1, f_4(0, \underline{f_5(0, 3)}), 3) \\
 &= f_4(1, f_4(0, \underline{f_1(3)}), 3) \\
 &= f_4(1, \underline{f_4(0, 3, 3)}, 3) \\
 &= f_4(1, f_2(\underline{f_3(0, 3, 3)}), 3) \\
 &= f_4(1, \underline{f_2(3)}, 3) \\
 &= \underline{f_4(1, 4, 3)} \\
 &= f_2(\underline{f_3(1, 4, 3)}) \\
 &= \underline{f_2(4)} \\
 &= 5.
 \end{aligned}$$

► **Call by need**

Nel **call by need** valutiamo un'espressione *solo quando è necessario*: questa regola ci impone di valutare sempre l'espressione più esterna per prima. Per far ciò eviteremo di essere eccessivamente pignoli nella sintassi delle funzioni primitive ricorsive.

$$\begin{aligned}
f_5(2, 3) &= f_4(1, f_5(1, 3), 3) \\
&= f_2(f_3(1, f_5(1, 3), 3)) \\
&= f_3(1, f_5(1, 3), 3) + 1 \\
&= f_5(1, 3) + 1 \\
&= f_4(0, f_5(0, 3), 3) + 1 \\
&= f_2(f_3(0, f_5(0, 3), 3)) + 1 \\
&= f_3(0, f_5(0, 3), 3) + 1 + 1 \\
&= f_5(0, 3) + 1 + 1 \\
&= f_1(3) + 1 + 1 \\
&= 3 + 1 + 1 = 5.
\end{aligned}$$

In entrambi i casi è chiaro che la funzione  $f_5$  così definita è la somma.

#### 1.4.1 Enumerazione di Gödel

Vogliamo ora mostrare che le macchine di Turing sono numerabili e esiste una loro enumerazione fatta da funzioni ricorsive primitive.

##### **Definizione 1.4.3** – Relazione primitiva ricorsiva

Una relazione  $P \subseteq \mathbb{N}^k$  è detta **primitiva ricorsiva** se lo è la sua funzione caratteristica  $\chi_P : \mathbb{N}^k \rightarrow \{0, 1\}$ , definita da

$$\chi_P(x_1, \dots, x_k) := \begin{cases} 1 & \text{se } (x_1, \dots, x_k) \in P \\ 0 & \text{altrimenti.} \end{cases}$$

La funzione caratteristica di un sottoinsieme di  $\mathbb{N}^k$  è quindi una funzione a valori booleani (ovvero è un predicato) che restituisce 1 sugli elementi che appartengono al sottoinsieme e 0 altrimenti. In futuro confonderemo senza porci troppi problemi le relazioni e le loro funzioni caratteristiche.

Per costruire l'enumerazione delle MdT ci serve un predicato molto importante, che è il predicato  $P : \mathbb{N} \rightarrow \{0, 1\}$  definito da

$$P(p) = 1 \text{ se e solo se } p \text{ è un numero primo.}$$

È possibile dimostrare che tale predicato è primitivo ricorsivo: i numeri primi saranno quindi una parte fondamentale dell'enumerazione.

Gli altri due ingredienti della ricetta sono i seguenti.

- Il **Teorema di Esistenza e Unicità della Fattorizzazione in Primi**, che dice che se  $P = p_0, p_1, \dots$  è l'insieme dei numeri primi (considerato questa volta come relazione unaria!) allora per ogni  $n \in \mathbb{N}$  esiste un numero finito di esponenti  $e_i \neq 0$  tali che

$$n = \prod_{i \in \mathbb{N}} p_i^{e_i}.$$



- La funzione che prende un  $n = \prod_{i \in \mathbb{N}} p_i^{e_i}$  e restituisce l'esponente  $e_k$  del  $k$ -esimo fattore della fattorizzazione è primitiva ricorsiva.

In particolare se considerando una sequenza finita di naturali  $(n_0, \dots, n_k)$  essa può essere codificata in modo *unico* come il numero

$$N := p_0^{n_0+1} \cdot p_k^{n_k+1}$$

e dalla codifica possiamo ricavare la sequenza originale grazie alle funzioni che danno gli esponenti della fattorizzazione.

Possiamo vedere finalmente una *quasi*-codifica delle macchine di Turing: in particolare delineeremo una funzione iniettiva che mappa le macchine di Turing ai naturali. La codifica vera e propria, chiamata **enumerazione di Gödel**, è in realtà una funzione bigettiva e primitiva ricorsiva.

Data una macchina  $M := (Q, \Sigma, \delta, q_0)$ , siccome  $Q$  e  $\Sigma$  sono finiti possiamo numerare i loro elementi:

$$Q = \{q_0, \dots, q_n\}, \quad \Sigma = \{\sigma_0, \dots, \sigma_m\}.$$

Ogni transizione specificata da  $\delta$  può essere rappresentata come una quintupla

$$(q_i, \sigma_j, q_k, \sigma_l, D) \in Q \times \Sigma \times Q \times \Sigma \times \{L, R, -\}$$

e pertanto possiamo codificarla come il naturale

$$p_0^{i+1} \cdot p_1^{j+1} \cdot p_2^{k+1} \cdot p_3^{l+1} \cdot p_4^{m_D}.$$

Dobbiamo risolvere alcune piccole inesattezze:

- $q_k$  potrebbe essere lo stato terminatore  $h$ , dunque numereremo  $h$  come lo stato  $q_{k+1}$ ;
- non abbiamo definito come numerare i simboli  $L, R, -$ , ma possiamo semplicemente considerarli come ulteriori simboli rispetto a quelli di  $\Sigma$ , dunque numereremo

$$L \mapsto \sigma_{m+2}, \quad R \mapsto \sigma_{m+3}, \quad - \mapsto \sigma_{m+4}.$$

Abbiamo quindi associato un numero ad ogni quintupla. Ma una macchina di Turing è semplicemente un insieme di quintuple: ordiniamole lessicograficamente (ovvero prima le ordiniamo per  $i$ , poi per  $j$ , ecc) e quindi abbiamo una sequenza finita di numeri naturali  $g_0, \dots, g_r$ , ognuno dei quali codifica una quintupla.

Definiremo quindi **numero di Gödel** della macchina  $M$  il numero  $N_M := p_0^{g_0+1} \cdots p_r^{g_r+1}$ . Questa pseudo-codifica è sicuramente iniettiva grazie al Teorema di Fattorizzazione Unica, ma non è detto che sia surgettiva: l'idea della vera enumerazione di Gödel è simile ma la realizzazione è molto più complessa.

Osserviamo che una volta numerate le quintuple possiamo anche enumerare intere computazioni con un singolo numero: infatti una computazione (terminante) è una successione finita di configurazioni  $\gamma = (q_i, w_j) \in Q \times \Sigma^*$  e le configurazioni possono certamente essere enumerate.

Infine ogni passaggio fatto finora è primitivo ricorsivo, dunque il procedimento di enumerazione delle MdT e delle computazioni è primitivo ricorsivo.

### 1.4.2 Funzione di Ackermann

La maggior parte delle funzioni che usiamo comunemente è primitiva ricorsiva: i logici di inizio '900 si chiesero perciò se le funzioni primitive ricorsive potessero modellare *tutti* gli algoritmi che *terminano sempre*, ovvero tutte le funzioni totali.

La risposta purtroppo è **no** e ci è data dalla **funzione di Ackermann**, definita da

$$A(z, x, y) := \begin{cases} A(0, 0, y) & = y \\ A(0, x + 1, y) & = A(0, x, y) + 1 \\ A(1, 0, y) & = 0 \\ A(z + 2, 0, y) & = 1 \\ A(z + 1, x + 1, y) & = A(z, A(z + 1, x, y), y). \end{cases}$$

Questa funzione è totale: basta mostrarlo per induzione sui casi ricorsivi, che sono il secondo e il quinto. Il primo termina in tempo finito poiché il secondo parametro decresce ad ogni applicazione; il quinto termina poiché l'applicazione interna avviene col secondo parametro diminuito di uno, mentre nell'applicazione esterna il primo parametro decresce.

Tuttavia l'ultimo caso non può essere espresso in termini di funzioni ricorsive primitive: la doppia ricorsione innestata non rientra nei cinque schemi e non è neanche ricavabile dagli schemi. Inoltre questa funzione è *intuitivamente calcolabile*: ad ogni passo restituiamo un risultato oppure calcoliamo ricorsivamente la funzione diminuendo il valore degli argomenti, quindi è certamente scrivere un programma che la calcola.

Segue che le funzioni primitive ricorsive **non sono tutte le funzioni calcolabili totali**.

### 1.4.3 Non esiste un formalismo capace di esprimere tutte e sole le funzioni calcolabili totali

La speranza è quindi che esista un formalismo, diverso dalle funzioni primitive ricorsive, capace di esprimere *tutte e sole* le funzioni calcolabili totali.

#### Teorema 1.4.4 –

Non esiste un formalismo capace di esprimere tutte e soli le funzioni calcolabili totali.

**Dimostrazione.** Supponiamo per assurdo che esista un formalismo  $\mathcal{F}$  capace di esprimere tutte e sole le funzioni calcolabili totali. Sicuramente  $|\mathcal{F}| = |\mathbb{N}|$ : infatti sono al più numerabili poiché ogni funzione calcolabile è un algoritmo, e quindi è una stringa su un alfabeto finito; d'altro canto sono almeno  $|\mathbb{N}|$  poiché le funzioni costanti sono certamente calcolabili totali.

Consideriamo allora una numerazione  $\mathbb{N} \rightarrow \mathcal{F}$ ,  $n \mapsto f_n$  che sia *bigettiva e calcolabile*.<sup>a</sup>

Costruiamo la funzione  $g : \mathbb{N} \rightarrow \mathbb{N}$ ,  $g(n) = f_n(n) + 1$ . Tale funzione è

- calcolabile, in quanto è la composizione della numerazione di  $\mathcal{F}$  che è calcolabile, del calcolo di  $f_n(n)$  (che si può fare in quanto  $f_n$  è calcolabile) e del successore;
- totale, in quanto composizione di funzioni totali.

Segue che  $g$  è una funzione calcolabile totale, e quindi  $g \in \mathcal{F}$ .

Tuttavia per ogni  $n \in \mathbb{N}$  vale che  $g(n) = f_n(n) + 1 \neq f_n(n)$ , e dunque in particolare  $g \neq f_n$  per ogni  $n \in \mathbb{N}$ . Ma le funzioni di  $\mathcal{F}$  sono tutte e sole della forma  $f_n$  per qualche  $n \in \mathbb{N}$ , da cui segue che  $g \notin \mathcal{F}$ , che è assurdo.  $\square$

<sup>a</sup>Dovremmo dimostrare che ne esiste una, ma faremo finta di niente.

La tecnica usata nella dimostrazione di questo teorema viene chiamata **diagonalizzazione** ed è una tecnica usata molto frequentemente nella logica e nella teoria della calcolabilità.

## 1.5 Funzioni generali ricorsive

Il problema messo in luce dal **Teorema 1.4.4** ci impedisce di creare un formalismo che esprima solo funzioni totali: per risolverlo dobbiamo estendere la classe di funzioni di nostro interesse alle *funzioni parziali*. Questo non è assurdo: molte funzioni di nostro interesse (anche aritmetiche) sono non definite su alcuni input, e abbiamo anche visto che esistono MdT e funzioni WHILE che non convergono.

Per farlo, introduciamo un ultimo formalismo.

### Definizione 1.5.1 – Operatore di minimizzazione

Dato un predicato  $P$ , ovvero una funzione  $P : \mathbb{N} \rightarrow \{0, 1\}$ , possiamo costruire l'**operatore di minimizzazione**  $\mu$  tale che

$$\mu y. P(y) := \min\{y : P(y) = 1\}.$$

Osserviamo che  $\mu y. P(y)$  potrebbe non essere definito: se  $P$  è il predicato sempre falso, non esiste un minimo  $y$  che lo renda vero.

### Definizione 1.5.2 – Funzioni generali ricorsive

L'insieme delle funzioni **generali ricorsive**  $\mathcal{GR}$  è il minimo insieme di funzioni contenenti gli schemi I, II, III delle funzioni primitive ricorsive, chiuso per gli schemi IV e V e per lo schema

VI. **Minimizzazione:** se  $\varphi : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \in \mathcal{GR}$ , allora la funzione  $\psi : \mathbb{N}^n \rightarrow \mathbb{N}$  definita da

$$\psi(x_1, \dots, x_n) := \mu y. \left( \varphi(\bar{x}, y) = 0 \text{ e } (\forall z \leq y. \varphi(\bar{x}, z) \downarrow) \right)$$

appartiene ancora a  $\mathcal{GR}$ .

Una funzione ottenuta per minimizzazione è intuitivamente calcolabile: si calcola  $\varphi(\bar{x}, y)$  per  $y = 0, 1, 2, \dots$  e ci si ferma al primo valore che soddisfi entrambe le proprietà. Osserviamo che una  $\psi$  ottenuta in tale modo *può essere parziale* in due casi:

- se  $\varphi(\bar{x}, y) \neq 0$  per ogni  $y$  allora non c'è minimo, e quindi la computazione non termina;
- se  $\varphi(\bar{x}, z) \uparrow$  per qualche valore  $z$  precedente al primo zero, nel calcolare  $\varphi(\bar{x}, z)$  non ci fermeremo mai, e quindi il calcolo di  $\psi$  non termina.

**Esempio 1.5.3 (-NoValue-).** Sia  $\varphi := \lambda x, y. 3$ .  $\varphi$  è primitiva ricorsiva, e quindi è anche totale, ma  $\psi$  ottenuta per minimizzazione su  $\varphi$  è **sempre indefinita**.

Infatti  $\psi(x)$  è il minimo  $y$  per cui  $\varphi(x, y) = 0$  (e l'altra condizione) ma questo non accade mai.

### 1.5.1 Tesi di Church-Turing

Abbiamo quindi visto diversi formalismi capaci di esprimere funzioni intuitivamente calcolabili, ovvero algoritmi. In che relazione sono?

Negli anni '20 e '30 i principali ideatori di questi formalismi (come Church, Turing, Gödel) dimostrarono l'equivalenza di tutti i formalisti che abbiamo visto: in particolare Turing e Church congetturarono che tutti i modelli capaci di esprimere funzioni calcolabili fossero **Turing-equivalenti**.

#### Teorema 1.5.4 – Tesi di Church-Turing

Le funzioni (intuitivamente) calcolabili sono tutte e sole le funzioni Turing-calcolabili.

Dato che le funzioni Turing-calcolabili sono tutte e sole quelle WHILE-calcolabili oppure tutte e sole le funzioni generali ricorsive, da questo momento in poi non specificheremo più il formalismo usato (tanto sono tutti equivalenti!) e parleremo semplicemente di **funzioni calcolabili**.

## 1.6 Primi teoremi sulle funzioni calcolabili

Avendo stabilito il *framework* in cui lavoreremo, possiamo finalmente iniziare a dimostrare alcune proprietà delle funzioni calcolabili.

#### Teorema 1.6.1 – Esistenza di funzioni non calcolabili

Le funzioni calcolabili sono in quantità numerabile. In particolare esistono funzioni non calcolabili.

Per dimostrare questo teorema useremo il fatto che le funzioni  $\mathbb{N} \rightarrow \mathbb{N}$  sono in quantità più che numerabile, quindi dimostriamolo.

#### Teorema 1.6.2 – Diagonalizzazione di Cantor

Siano  $A, B$  insiemi con  $|A| \geq |\mathbb{N}|$ ,  $|B| \geq 2$ . Allora

$$|\{f : A \rightarrow B\}| > |\mathbb{N}|.$$

**Dimostrazione.** È sufficiente dimostrare il Teorema nel caso in cui  $A$  sia numerabile e  $B$  abbia esattamente due elementi. Allora senza perdita di generalità sia  $A = \mathbb{N}$ ,  $B = \{0, 1\}$ .

Sia  $\mathcal{F} := |\{f : \mathbb{N} \rightarrow \{0, 1\}\}|$  e supponiamo per assurdo  $|\mathcal{F}| = |\mathbb{N}|$ . Allora esiste una numerazione bigettiva degli elementi di  $\mathcal{F}$ , ovvero una funzione  $n \mapsto f_n \in \mathcal{F}$ .

Consideriamo allora  $g : \mathbb{N} \rightarrow \{0, 1\}$  (e quindi  $g \in \mathcal{F}$ ) definita da

$$g(n) := \begin{cases} 0 & \text{se } f_n(n) = 1, \\ 1 & \text{altrimenti.} \end{cases}$$

Ma allora  $g(n) \neq f_n(n)$  per ogni  $n$ , dunque  $g \neq f_n$  per ogni  $n$ . Ma gli elementi di  $\mathcal{F}$  sono tutti e soli della forma  $f_n$  al variare di  $n \in \mathbb{N}$ , dunque  $g \notin \mathcal{F}$ , che è assurdo.  $\square$

Possiamo dimostrare il **Teorema 1.6.1**.

**Dimostrazione del Teorema 1.6.1.** Sia  $\mathcal{C}$  l'insieme delle funzioni calcolabili. Mostriamo che  $|\mathcal{C}| \geq |\mathbb{N}|$  e  $|\mathcal{C}| \leq |\mathbb{N}|$ .

- ▶  $|\mathcal{C}| \geq |\mathbb{N}|$  Le funzioni  $\lambda x. n$  al variare di  $n \in \mathbb{N}$  sono in quantità numerabile e sono tutte calcolabili.
- ▶  $|\mathcal{C}| \leq |\mathbb{N}|$  Ogni funzione calcolabile è calcolata da una macchina di Turing, dunque  $|\mathcal{C}| \leq |\mathcal{M}|$  dove  $\mathcal{M}$  è l'insieme delle MdT; inoltre  $|\mathcal{M}| \leq |\mathbb{N}|$  poiché possiamo numerarle tramite l'enumerazione di Gödel, dunque  $|\mathcal{C}| \leq |\mathbb{N}|$ .

Segue che  $|\mathcal{C}| = |\mathbb{N}|$ .

Per dimostrare che esistono funzioni non calcolabili osserviamo che  $\mathcal{C}$  è un sottoinsieme di tutte le funzioni  $\mathbb{N} \rightarrow \mathbb{N}$ . Tuttavia per il Teorema 1.6.2 le funzioni  $\mathbb{N} \rightarrow \mathbb{N}$  sono in quantità più che numerabile, dunque  $\mathcal{C}$  deve essere un sottoinsieme proprio delle funzioni  $\mathbb{N} \rightarrow \mathbb{N}$ : in particolare devono esistere funzioni che non sono in  $\mathcal{C}$ .  $\square$

### 1.6.1 Enumerazioni effettive

Dato che abbiamo dimostrato che le funzioni calcolabili sono numerabili possiamo porci il problema di come *enumerarle*. Per far ciò non enumereremo direttamente le funzioni, ma solo le macchine di Turing.

In particolare considereremo sono **enumerazioni effettive**, ovvero enumerazioni che dipendono solo dalla **sintassi** della macchina di Turing, cioè soltanto dai simboli che compaiono al suo interno, e non dal comportamento.<sup>1</sup>

Si può dimostrare che tutti i teoremi che vedremo sono indipendenti dal formalismo e dall'enumerazione scelta, purché quest'ultima sia effettiva: fissiamo quindi una enumerazione effettiva  $n \mapsto M_n$ . Tale enumerazione induce un'enumerazione sulle funzioni calcolabili: indicheremo con  $\varphi_i$  la funzione calcolata dalla macchina  $M_i$ .

Osserviamo però che dati due indici  $i, j$  diversi sicuramente vale che  $M_i \neq M_j$  ma è possibile che  $\varphi_i = \varphi_j$ , ovvero è possibile che due macchine diverse calcolino la stessa funzione.

In realtà vale un teorema molto più forte, solitamente conosciuto come **Padding Lemma**.

#### Teorema 1.6.3 – Padding Lemma

Per ogni indice  $i$  esiste un insieme numerabile  $A_i$  di indici tale che per ogni  $j \in A_i$

$$\varphi_j = \varphi_i,$$

ovvero ogni funzione calcolabile è calcolata da infinite MdT.

**Dimostrazione.** Consideriamo l'algoritmo che calcola  $\varphi_i$ : aggiungendo uno skip alla fine si ottiene un algoritmo diverso (e quindi una macchina di Turing diversa) che calcola la stessa funzione. Aggiungendo altri skip otteniamo una quantità numerabile di algoritmi che calcolano  $\varphi_i$ .  $\square$

<sup>1</sup>In realtà una enumerazione si dice effettiva se è ottenuta post-componendo l'enumerazione di Gödel con una bigezione  $\mathbb{N} \leftrightarrow \mathbb{N}$ .

### 1.6.2 Equivalenza tra MdT e funzioni generali ricorsive

Ora mostriamo che ogni funzione calcolabile può essere scritta in una forma standard, detta **Forma Normale di Kleene**.

#### Teorema 1.6.4 – Forma Normale di Kleene

Esistono un predicato  $T : \mathbb{N}^3 \rightarrow \{0, 1\}$  (detto **predicato di Kleene**) e una funzione  $U : \mathbb{N} \rightarrow \mathbb{N}$  entrambi calcolabili totali tali che

$$\forall i, x : \varphi_i(x) = U(\mu y. T(i, x, y)).$$

Inoltre  $T$  e  $U$  sono primitivi ricorsivi.

**Dimostrazione.** Definiamo  $T(i, x, y) = 1$  se e solo se la *computazione*  $M_i(x)$  converge ad una configurazione  $(h, \triangleright z)$  e  $y$  è la codifica di tale computazione.

$T$  è calcolabile: in effetti basta recuperare la macchina  $M_i$  dalla lista (che è un'operazione calcolabile), decodificare  $y$  come una computazione  $c_1 \dots c_n$  (dove tutte queste sono configurazioni) e verificare che  $M_i(x)$  converga effettivamente ad una configurazione  $c_n = (h, \triangleright z)$  tramite la computazione codificata da  $y$ .<sup>a</sup>

Allora possiamo definire  $U$  in modo che  $U(y) = \text{"la codifica di } z\text{"}$ . La computazione del membro destro procede quindi in questo modo: si scorrono i valori di  $y$  e si trova il primo valore di  $y$  che corrisponde alla computazione di  $M_i(x)$ . Se esiste, ritorniamo la codifica di  $z$ , altrimenti il procedimento non termina.

È facile vedere che ciò è uguale a  $\varphi_i(x)$  per ogni  $x$ : distinguiamo due casi.

- Se  $\varphi_i(x) = n$  la computazione di  $M_i(x)$  termina e dà come configurazione finale  $(h, \triangleright z)$ , dove  $n$  codifica  $z$ . Ma allora esiste un  $y \in \mathbb{N}$  che codifica la computazione terminante di  $M_i(x)$  (e tale  $y$  è anche unico, poiché la computazione è unica) e dunque  $y$  è il minimo valore del terzo parametro per cui vale che  $T(i, x, y) = 1$ . Per definizione di  $U$ ,  $U(y)$  è la codifica di  $z$  e dunque è  $n$ .
- Se  $\varphi_i(x)$  diverge, allora non esiste una codifica della computazione di  $M_i(x)$  (poiché la computazione diverge) e pertanto non esiste un  $y$  per cui  $T(i, x, y) = 1$ . In particolare  $U(y)$  diverge.

Infine  $T$  ed  $U$  sono primitivi ricorsivi in quanto lo sono le codifiche e i controlli effettuati, e composizione di funzioni primitive ricorsive è ancora primitiva ricorsiva.  $\square$

<sup>a</sup>Osserviamo che questo procedimento termina sempre poiché le computazioni sono di lunghezza finita, dunque possiamo verificare in tempo finito se il calcolo di  $M_i(x)$  corrisponde alla computazione cercata oppure no.

**Osservazione 1.6.1 (-NoValue-).** Il teorema ci dice che ogni funzione calcolabile  $\varphi_i$  è esprimibile come composizione di due funzioni primitive ricorsive ( $T, U$ ) e una funzione generale ricorsiva (data dalla minimizzazione), o equivalentemente da due comandi FOR e un comando WHILE.

Il Teorema di Forma Normale è uno strumento molto potente e lo useremo per dimostrare uno dei risultati fondamentali della Teoria della Calcolabilità.

**Teorema 1.6.5 – Teorema di Enumerazione**

Esiste un indice  $z$  tale che per ogni indice  $i$ , input  $x$  si ha

$$\varphi_z(i, x) = \varphi_i(x).$$

Il Teorema di Enumerazione ci garantisce l'esistenza di una MdT particolare, chiamata **Macchina Universale**, capace di simulare tutte le altre macchine di Turing. Osserviamo che per il **Padding Lemma** in realtà esistono infinite macchine universali.

**Dimostrazione.** Siano  $U, T$  i predicati dati dal **Teorema 1.6.4** e definiamo

$$\varphi_z := \lambda i, x. U(\mu y T(i, x, y)).$$

Tale funzione è ben definita e calcolabile (poiché composizione di funzioni calcolabili), inoltre per il **Teorema 1.6.4** si ha che  $\varphi_i(x) = \varphi_z(i, x)$ , come voluto.  $\square$

Per quanto il Teorema di Enumerazione possa sembrare eccessivamente potente (abbiamo costruito un algoritmo che può simulare tutti gli algoritmi!) in realtà la macchina Universale svolge esattamente il ruolo di un interprete: prende in input un altro programma e dei dati ed esegue il programma su quei dati.

Osserviamo inoltre che ciò funziona solo perché possiamo trasformare una funzione, cioè un programma, in dati, e ciò è possibile solo perché le funzioni calcolabili sono numerabili.

Abbiamo quindi un metodo per trasformare un indice in un argomento. È possibile fare il contrario?

**Teorema 1.6.6 – Teorema del Parametro**

Esiste una funzione calcolabile totale ed iniettiva  $s : \mathbb{N}^2 \rightarrow \mathbb{N}$  tale che per ogni  $i, x$

$$\varphi_{s(i, x)} = \lambda z. \varphi_i(x, z).$$

Il senso intuitivo del Teorema del Parametro (anche chiamato Teorema s-1-1 per un motivo che vedremo definendo la sua forma generale) è che se un algoritmo dipende da due input e uno dei due è costante/conosciuto, allora possiamo riscrivere l'algoritmo in modo da *eliminare* il parametro.

**Dimostrazione "intuitiva".** Dato l'indice  $i$  e fissato  $x$ , la funzione  $\lambda z. \varphi_i(x, z)$  è certamente calcolabile (si prende la macchina  $i$ -esima e le si danno in input  $x$  e  $z$ ). Per la Tesi di Church-Turing esiste allora un indice  $s(i, x)$  tale che

$$\varphi_{s(i, x)} = \lambda z. \varphi_i(x, z).$$

Consideriamo allora la funzione  $s : \mathbb{N}^2 \rightarrow \mathbb{N}$  definita da  $(i, x) \mapsto s(i, x)$ : tale funzione è calcolabile totale poiché la procedura delineata è un algoritmo per ottenere  $s(i, x)$  a partire dagli input e tale algoritmo termina sempre.

Per rendere  $s$  iniettiva, scegliamo un ordinamento degli input (ad esempio l'ordinamento lessicografico) e per ogni input  $(i, x)$  controlliamo che  $s(i, x) > s(i', x')$  per ogni  $(i', x') < (i, x)$ , ovvero che  $s$  sia strettamente crescente almeno fino a  $(i, x)$ .

Se così non fosse, sostituiamo il valore di  $s(i, x)$  con uno degli altri indici che calcola la stessa funzione e che sia maggiore di tutti gli  $s(i', x')$ : tale indice esiste sempre per il [Padding Lemma](#).<sup>a</sup>

Segue che la  $s$  costruita in questo modo è strettamente crescente e dunque iniettiva.  $\square$

<sup>a</sup>Infatti esistono solo un numero finito di coppie  $(i', x')$  che siano *lessicograficamente minori* di  $(i, x)$ , mentre esistono un numero infinito di indici che calcolano la stessa macchina dell'indice  $s(i, x)$ , dunque tra tutti questi infiniti indici ce ne sarà almeno uno più grande di tutti gli  $s(i', x')$ .

**Osservazione 1.6.2.** Il [Teorema del Parametro](#) ci dice che esiste una funzione calcolabile totale iniettiva a due variabili  $s$  tale che  $\varphi_{s(i, x)} = \lambda y. \varphi_i(x, y)$  per ogni  $i, x$ . Allora fissato un indice  $i$  possiamo considerare direttamente la funzione ad una variabile

$$f := \lambda x. s(i, x),$$

che è ancora calcolabile totale, iniettiva, e tale che

$$\varphi_{f(x)}(y) = \varphi_i(x, y).$$

Il [Teorema del Parametro](#) ci permette di dimostrare il seguente teorema.

**Teorema 1.6.7 – Teorema di Ricorsione di Kleene**

Per ogni  $f$  calcolabile totale esiste un indice  $n$  tale che

$$\varphi_n = \varphi_{f(n)}.$$

**Dimostrazione.** Sia  $f$  una funzione calcolabile totale e costruiamo  $n$  tale che  $\varphi_n = \varphi_{f(n)}$ . Consideriamo la funzione  $\psi : \mathbb{N}^2 \rightarrow \mathbb{N}$  definita da

$$\psi(u, z) := \begin{cases} \varphi_{\varphi_u(u)}(z), & \text{se } \varphi_u(u) \downarrow, \\ \perp, & \text{altrimenti.} \end{cases} \quad (1.1)$$

Tale funzione è intuitivamente calcolabile: si prova a calcolare  $\varphi_u(u)$ ; se non converge allora anche  $\psi(u, z)$  non converge, mentre se converge possiamo recuperare la macchina di indice  $\varphi_u(u)$  e calcolarla su  $z$ .

Segue quindi che esiste un indice  $i$  tale che  $\varphi_i = \psi$ . Per il [Teorema del Parametro](#) insieme all'[OSSERVAZIONE 1.6.2](#) possiamo considerare la funzione  $d := \lambda u. s(i, u)$  calcolabile totale, iniettiva e tale che

$$\varphi_{d(u)}(z) = \varphi_i(u, z) = \psi(u, z). \quad (1.2)$$

Dato che  $f$  e  $d$  sono entrambe calcolabili totali, lo sarà anche la loro composizione  $f \circ d$ . In particolare  $f \circ d$  sarà ancora iniettiva, ed esisterà un indice  $v$  tale che

$$\varphi_v = f \circ d. \quad (1.3)$$

Per totalità di  $\varphi_v$ ,  $\varphi_v(v)$  converge: segue che

$$\varphi_{d(v)} \stackrel{(1.2)}{=} \lambda z. \psi(v, z) \stackrel{(1.1)^2}{=} \lambda z. \varphi_{\varphi_v(v)}(z) = \varphi_{\varphi_v(v)}. \quad (1.4)$$



Sia allora  $n := d(v)$  e mostriamo che vale la tesi. In effetti

$$\varphi_n = \varphi_{d(v)} \stackrel{(1.4)}{=} \varphi_{\varphi_v(v)} \stackrel{(1.3)}{=} \varphi_{f(d(v))} = \varphi_{f(n)},$$

come volevamo. □

---

Qui usiamo la definizione di  $\psi$  insieme al fatto che  $\varphi_v(v)$  converge.

# 2

## Calcolabilità di problemi

---

### 2.1 Problemi di decisione

Finora abbiamo studiato i vari formalismi per esprimere algoritmi e le loro caratteristiche principali, insieme ai diversi teoremi che ne seguono. Vogliamo ora studiare i *problemi* che possono essere risolti da una determinata classe di funzioni.

I nostri problemi sono **problemi di decisione**: dato un insieme  $I \subseteq \mathbb{N}^k$  vogliamo stabilire se un dato elemento  $x \in \mathbb{N}^k$  appartenga o no a  $I$ . In particolare ogni problema è identificato da un insieme.

Per parlare di *appartenenza* ad un insieme conviene definire due funzioni che saranno di grande rilevanza in seguito.

#### Definizione 2.1.1 – Funzione caratteristica e semicaratteristica di un insieme

Sia  $I \subseteq \mathbb{N}^k$ . Si dice **funzione caratteristica** di  $I$  la funzione  $\chi_I : \mathbb{N}^k \rightarrow \{0, 1\}$  definita da

$$\chi_I(x) := \begin{cases} 1, & \text{se } x \in I, \\ 0, & \text{se } x \notin I. \end{cases}$$

Si dice inoltre **funzione semicaratteristica** di  $I$  la funzione parziale  $\tilde{\chi}_I : \mathbb{N}^k \rightarrow \{0, 1\}$  definita da

$$\tilde{\chi}_I(x) := \begin{cases} 1, & \text{se } x \in I, \\ \perp, & \text{se } x \notin I. \end{cases}$$

Possiamo ora definire le due principali classi di problemi che analizzeremo.

#### Definizione 2.1.2 – Insiemi ricorsivi e ricorsivamente enumerabili

Sia  $I \subseteq \mathbb{N}^k$ .

- $I$  si dice **ricorsivo** oppure **decidibile** se  $\chi_I$  è calcolabile totale.
- $I$  si dice **ricorsivamente enumerabile** (in breve r.e.) oppure **semidecidibile** se esiste un indice  $i$  tale che  $I = \text{dom}(\varphi_i)$ .

Chiameremo  $\mathcal{R}$  la classe degli insiemi ricorsivi,  $\mathcal{RE}$  la classe degli insiemi ricorsivamente enumerabili.

Intuitivamente  $I$  è decidibile se è possibile *decidere* in tempo finito se un elemento appartiene o meno all'insieme. Per quanto riguarda gli insiemi semidecidibili, facciamo un'osservazione iniziale.

**Osservazione 2.1.1** (-NoValue-).  $I$  è r.e. se e solo se  $\tilde{\chi}_I$  è calcolabile (parziale).

**Dimostrazione.** Se  $\tilde{\chi}_I$  è calcolabile, allora esiste un indice  $i$  con  $\varphi_i = \tilde{\chi}_I$ . In particolare  $\text{dom}(\varphi_i) = \text{dom}(\tilde{\chi}_I) = I$ , dunque  $I$  è r.e.

Viceversa, se  $I$  è r.e. esiste un indice  $i$  tale che  $\text{dom}(\varphi_i) = I$ . Allora la funzione  $\tilde{\chi}_I$  è calcolabile: dato  $x$  iniziamo a calcolare  $\varphi_i(x)$ ; se il procedimento termina poniamo  $\tilde{\chi}_I(x) = 1$ , altrimenti continueremo all'infinito e quindi la computazione di  $\tilde{\chi}_I$  non terminerà.  $\square$

Quindi un insieme  $I$  è semidecidibile se per ogni elemento  $x \in I$  possiamo controllare in tempo finito l'appartenenza, mentre per gli elementi  $x \notin I$  il procedimento non termina mai.

Il fatto che gli insiemi r.e. si chiamano proprio in questo modo deriva da un'altra particolare caratterizzazione.

**Proposizione 2.1.3**

$I$  è r.e. se e solo se  $I$  è vuoto oppure esiste una funzione  $f$  calcolabile totale tale che  $I = \text{Im}(f)$ .

**Dimostrazione.**  $\square$

Quali sono le relazioni tra insiemi ricorsivi e insiemi r.e.? Vediamone alcune che seguono immediatamente dalle definizioni.

**Proposizione 2.1.4** –  $\mathcal{R} \subseteq \mathcal{RE}$

Se  $I$  è ricorsivo, allora  $I$  è ricorsivamente enumerabile.

**Dimostrazione.** Infatti se  $I$  è ricorsivo la funzione  $\tilde{\chi}_I$  è calcolabile: in effetti dato  $x$ , se  $\chi_I(x) = 1$  allora  $\tilde{\chi}_I(x) = 1$ , altrimenti  $\tilde{\chi}_I(x)$  è indefinito. Segue che  $I$  è r.e. poiché  $I = \text{dom}(\tilde{\chi}_I)$ .  $\square$

Per la prossima proposizione abbiamo bisogno di definire il **complementare** di un problema.

**Definizione 2.1.5** – Complementare di un problema

Dato un insieme  $I$ , il suo complementare  $\bar{I}$  è definito da

$$\bar{I} := \{x : x \notin I\}.$$

**Proposizione 2.1.6 –**

Se  $I$  e  $\bar{I}$  sono entrambi r.e., allora sono entrambi ricorsivi.

**Dimostrazione.** Osserviamo che basta mostrare che  $I$  sia ricorsivo: a questo punto replicando il ragionamento su  $\bar{I}$  e  $\bar{\bar{I}} = I$  si ottiene che anche  $\bar{I}$  è ricorsivo.

Per definizione di insieme r.e., esistono due indici  $i, j$  tali che

$$I = \text{dom}(\varphi_i), \quad \bar{I} = \text{dom}(\varphi_j).$$

Per calcolare  $\chi_I$ , dato  $x$  eseguiamo questa sequenza di passi:

- eseguiamo un passo di computazione di  $\varphi_i(x)$ : se converge (cioè  $x \in \text{dom}(\varphi_i) = I$ ) allora  $\chi_I(x) = 1$ , altrimenti continuiamo;
- eseguiamo un passo di computazione di  $\varphi_j(x)$ : se converge (cioè  $x \in \text{dom}(\varphi_j) = \bar{I}$ ) allora  $\chi_I(x) = 0$ , altrimenti continuiamo;
- eseguiamo due passi di computazione di  $\varphi_i(x)$ ...

e così via. Ma  $x$  deve appartenere ad uno tra  $I$  e  $\bar{I}$ , dunque questo procedimento ad un certo punto termina. Segue che  $\chi_I$  è calcolabile.  $\square$

## 2.2 Separazione di $\mathcal{R}$ e $\mathcal{RE}$

Dai risultati ottenuti nella sezione precedente potremmo essere indotti a sperare che tutti i problemi semidecidibili siano anche decidibili. Purtroppo ciò non è vero, e lo dimostriamo attraverso un particolare insieme, chiamato tradizionalmente  $K$ :

$$K := \{ n : \varphi_n(n) \downarrow \} \quad (2.1)$$

**Teorema 2.2.1**

$K$  è r.e. ma non è ricorsivo.

Per chiarezza dividiamo in due parti la dimostrazione.

**Dimostrazione che  $K$  è r.e.** Per quanto detto precedentemente, per mostrare che  $K$  è r.e. basta far vedere che la sua funzione semicaratteristica

$$\tilde{\chi}_K := n \mapsto \begin{cases} 1, & \text{se } \varphi_n(n) \downarrow \\ \perp, & \text{altrimenti} \end{cases}$$

è calcolabile. Ma questa funzione è intuitivamente calcolabile:

- si esegue un passo del calcolo di  $\varphi_0(0)$ : se converge allora  $\tilde{\chi}_K(0)$  vale 1, altrimenti si continua;

- si esegue un passo del calcolo di  $\varphi_1(1)$ : se converge allora  $\tilde{\chi}_K(0)$  vale 1, altrimenti si continua;
- si eseguono due passi del calcolo di  $\varphi_0(0)$ ...

e così via. Questo procedimento ad un certo punto termina per tutti i valori di  $n$  che sono in  $K$ , e per gli altri invece non termina mai.  $\square$

**Dimostrazione che  $K$  non è ricorsivo.** Supponiamo per assurdo che  $K$  sia ricorsivo: per definizione allora  $\chi_K$  è calcolabile totale. Definiamo allora  $f : \mathbb{N} \rightarrow \mathbb{N}$  data da

$$f(n) := \begin{cases} \varphi_n(n) + 1, & \text{se } \chi_K(n) = 1 \\ 0, & \text{altrimenti.} \end{cases}$$

Dato che  $\chi_K$  è calcolabile totale possiamo calcolare  $\chi_K(n)$ ; inoltre se  $\chi_K(n) = 1$  (ovvero  $n \in K$ ) per definizione di  $K$  si ha che  $\varphi_n(n)$  converge.

Per la Tesi di Church-Turing allora esiste un indice  $i$  tale che  $\varphi_i = f$ , e quindi in particolare  $\varphi_i(i) = f(i)$ . Ma ciò è assurdo:

- se  $\varphi_i(i)$  converge allora  $f(i) = \varphi_i(i) + 1 \neq \varphi_i(i)$ ;
- se  $\varphi_i(i)$  diverge allora  $f(i)$  converge (a 0).

Segue in particolare che  $K$  non può essere ricorsivo.  $\square$

#### ► Piccola parentesi sul *bootstrapping*

L'insieme  $K$  può risultare abbastanza contorto e quindi è facile farsi venire l'idea che la dimostrazione funzioni solo perché abbiamo scelto un insieme "innaturale". In realtà l'auto-applicazione non è strana, e compare anche nel mondo reale, ad esempio quando si parla di compilatori.

Infatti dato un compilatore  $C_L^{L \rightarrow A}$  scritto nel linguaggio  $L$  e che compila codice  $L$  (alto livello) in codice scritto nel linguaggio  $A$  (più a basso livello), potrebbe essere necessario dover usare il compilatore in una macchina che nativamente non sa far girare il codice  $L$ , ma sa far girare solo codice nel linguaggio  $A$ . Vogliamo perciò un modo efficiente per ottenere un compilatore  $L \rightarrow A$  scritto in  $A$ .

Il metodo più semplice è detto **bootstrapping**: in pratica si dà in pasto al compilatore  $C_L^{L \rightarrow A}$  il suo stesso codice, ovvero si dà il comando  $C_L^{L \rightarrow A} \left( C_L^{L \rightarrow A} \right)$ . Il risultato è un codice scritto in  $A$  che mantiene la semantica originale, ovvero è un compilatore  $C_A^{L \rightarrow A}$ .

Tuttavia il bootstrapping non è l'unico motivo per cui il problema  $K$  è importante anche da un punto di vista applicativo:  $K$  è strettamente legato al **problema della fermata**, che ora definiremo formalmente.

#### **Definizione 2.2.2** – Problema della fermata

Dato un indice  $i$  e un input  $x$ , dire se  $\varphi_i(x)$  converge.

Come ogni problema decisionale, il problema della fermata può essere rappresentato tramite un insieme. In questo caso l'insieme è indicato con

$$K_0 := \left\{ (i, x) : \varphi_i(x) \downarrow \right\}.$$

Questo problema è intuitivamente molto importante: se fosse decidibile, potremmo decidere in tempo finito se una funzione  $\varphi_i$  si arresta sull'input  $x$  oppure continua in eterno.

**Teorema 2.2.3** –  $K_0$  non è ricorsivo

L'insieme  $K_0$  non è ricorsivo.

**Dimostrazione.** Osserviamo che  $(x, x) \in K_0$  se e solo se  $x \in K$ : se  $K_0$  fosse decidibile lo sarebbe anche  $K$ , ma ciò è assurdo.  $\square$

## 2.3 Riduzioni di classi di problemi

Nella dimostrazione del [Teorema 2.2.3](#) abbiamo sfruttato una tecnica comune in matematica: abbiamo *ridotto* il problema  $K_0$  al problema  $K$  e in questo modo abbiamo dimostrato che  $K_0$  non può essere decidibile.

Vogliamo ora generalizzare questo concetto.

**Definizione 2.3.1** – Riduzione secondo una funzione

Dati due problemi  $A, B$ , si dice che  $A$  **si riduce secondo**  $f$  a  $B$  (e si scrive  $A \leq_f B$ ) se

$$x \in A \iff f(x) \in B.$$

**Osservazione 2.3.1** (-NoValue-).  $K \leq_f K_0$  secondo la funzione  $f : \mathbb{N} \rightarrow \mathbb{N}^2$  definita da  $f(x) := (x, x)$ .

**Osservazione 2.3.2** (-NoValue-).  $A \leq_f B$  se e solo se  $\overline{A} \leq_f \overline{B}$ .

Spesso non ci interessa quale sia la funzione che permette la riduzione di  $A$  a  $B$ , ma solo a quale classe di funzioni appartiene.

**Definizione 2.3.2** – Riduzione secondo una classe di funzioni

Siano  $A, B$  problemi,  $\mathcal{F}$  insieme di funzioni. Allora si dice che  $A$  **si riduce secondo**  $\mathcal{F}$  a  $B$  (e si scrive  $A \leq_{\mathcal{F}} B$ , o anche  $A \leq B$  se l'insieme  $\mathcal{F}$  è deducibile dal contesto) se esiste una  $f \in \mathcal{F}$  tale che  $A \leq_f B$ .

Come scegliamo l'insieme  $\mathcal{F}$ ? In generale dipende dalle classi di problemi che vogliamo confrontare: infatti per poter studiare queste classi è importante che la riduzione rispetti alcune proprietà.

**Definizione 2.3.3** – Riduzione che classifica due classi

Date  $\mathcal{D}, \mathcal{E}$  classi di problemi con  $\mathcal{D} \subseteq \mathcal{E}$ ,  $\mathcal{F}$  insieme di funzioni, si dice che la relazione  $\leq_{\mathcal{F}}$  **classifica** le classi  $\mathcal{D}, \mathcal{E}$  se

1.  $A \leq_{\mathcal{F}} A$ ,
2. se  $A \leq_{\mathcal{F}} B$  e  $B \leq_{\mathcal{F}} C$ , allora  $A \leq_{\mathcal{F}} C$ ,
3. se  $A \leq_{\mathcal{F}} B$  e  $B \in \mathcal{D}$ , allora  $A \in \mathcal{D}$ ,
4. se  $A \leq_{\mathcal{F}} B$  e  $B \in \mathcal{E}$ , allora  $A \in \mathcal{E}$ .

**Osservazione 2.3.3** (-NoValue-). Sfruttando la definizione di riduzione, possiamo riscrivere le proprietà in forma *algebraica*:

1.  $\text{id}_A \in \mathcal{F}$ ,
2. se  $f$  e  $g$  appartengono a  $\mathcal{F}$ , allora anche la composizione  $gf$  appartiene ad  $\mathcal{F}$ ,
3. se  $f \in \mathcal{F}$  e  $B \in \mathcal{D}$ , allora  $f^{-1}[B] \in \mathcal{D}$ ,
4. se  $f \in \mathcal{F}$  e  $B \in \mathcal{E}$ , allora  $f^{-1}[B] \in \mathcal{E}$ .

Questo in particolare mi dice che se  $\leq_{\mathcal{F}}$  classifica  $\mathcal{D}, \mathcal{E}$ , allora  $\leq_{\mathcal{F}}$  è un **preordine** su  $\mathcal{D}$  e su  $\mathcal{E}$ .

► **Intuizione** Qual è il significato intuitivo di una relazione che classifica due classi? Possiamo leggere  $\leq_{\mathcal{F}}$  come "è al più difficile quanto":

- $A$  è al più difficile quanto se stesso,
- se  $A$  è al più difficile quanto  $B$  e  $B$  è al più difficile quanto  $C$ , allora  $A$  è al più difficile quanto  $C$ ,
- i problemi difficili al più quanto  $B$  si trovano tutti nel più piccolo insieme contenente  $B$ : se  $A$  è al più difficile quanto  $B$  e  $B$  appartiene a  $\mathcal{D}$  (risp.  $\mathcal{E}$ ), allora anche  $A$  appartiene a  $\mathcal{D}$  (risp.  $\mathcal{E}$ ), cioè  $A$  **non sta fuori**  $\mathcal{D}$  (**risp.**  $\mathcal{E}$ ).

Fissiamo ora due classi  $\mathcal{D}, \mathcal{E}$  con  $\mathcal{D} \subseteq \mathcal{E}$  e una classe di funzioni  $\mathcal{F}$ .

**Definizione 2.3.4** – Grado di un problema

Definiamo il **grado** di un problema  $A$  è

$$\text{deg } A := \{ B : A \leq_{\mathcal{F}} B \text{ e } B \leq_{\mathcal{F}} A \},$$

ovvero è l'insieme di tutti i problemi con la stessa difficoltà di  $A$ .

**Definizione 2.3.5** – Problemi ardui e completi

Sia  $H$  un problema.

- H si dice  **$\leq_{\mathcal{F}}$ -arduo per  $\mathcal{E}$**  se per ogni  $A \in \mathcal{E}$  si ha  $A \leq_{\mathcal{F}} H$ , ovvero se H è almeno difficile quanto tutti i problemi di  $\mathcal{E}$ .
- H si dice  **$\leq_{\mathcal{F}}$ -completo per  $\mathcal{E}$**  se è  $\leq_{\mathcal{F}}$ -arduo per  $\mathcal{E}$  e  $H \in \mathcal{E}$ .

In particolare possiamo studiare la relazioni tra  $\mathcal{D}$  e  $\mathcal{E}$  tramite i problemi  $\leq_{\mathcal{F}}$ -ardui/completi per  $\mathcal{E}$ .

### Proposizione 2.3.6

Se  $C$  è  $\leq_{\mathcal{F}}$ -completo per  $\mathcal{E}$  e  $C \in \mathcal{D}$ , allora  $\mathcal{E} = \mathcal{D}$ .

**Dimostrazione.** Dato che  $\mathcal{D} \subseteq \mathcal{E}$ , basta mostrare che  $\mathcal{E} \subseteq \mathcal{D}$ . Sia allora  $B \in \mathcal{E}$ : dato che  $C$  è  $\leq_{\mathcal{F}}$ -completo per  $\mathcal{E}$  segue che  $B \leq_{\mathcal{F}} C$ . Ma  $C \in \mathcal{D}$ , dunque anche  $B \in \mathcal{D}$ .  $\square$

### Proposizione 2.3.7 –

Se  $A$  è  $\leq_{\mathcal{F}}$ -arduo per  $\mathcal{E}$  e  $A \leq_{\mathcal{F}} B$ , allora  $B$  è  $\leq_{\mathcal{F}}$ -arduo per  $\mathcal{E}$ . In particolare se  $B \in \mathcal{E}$  allora  $A, B$  sono  $\leq_{\mathcal{F}}$ -completi per  $\mathcal{E}$ .

**Dimostrazione.** Se  $H \in \mathcal{E}$ . Dato che  $A$  è  $\leq_{\mathcal{F}}$ -arduo per  $\mathcal{E}$  si ha  $H \leq_{\mathcal{F}} A$ ; inoltre  $A \leq_{\mathcal{F}} B$  dunque per transitività  $H \leq_{\mathcal{F}} B$ , ovvero  $B$  è  $\leq_{\mathcal{F}}$ -arduo.

Inoltre se  $B \in \mathcal{E}$  segue anche che  $A$  lo è, poiché  $A \leq_{\mathcal{F}} B$ . Allora per definizione  $A, B$  sono  $\leq_{\mathcal{F}}$ -completi per  $\mathcal{E}$ .  $\square$

## 2.4 Studio di $\mathcal{R}$ e $\mathcal{RE}$ tramite riduzioni

Vogliamo studiare ora le classi di problemi  $\mathcal{R}$  e  $\mathcal{RE}$  tramite riduzioni: come prima cosa dobbiamo identificare una classe di funzioni.

### Definizione 2.4.1 – Classe rec

Indicheremo con

$$\text{rec} := \{ \varphi_i : \text{dom}(\varphi_i) = \mathbb{N} \}$$

la classe di tutte le funzioni calcolabili totali, che quindi chiameremo (per motivi storici) **ricorsive**.

### Proposizione 2.4.2

$\leq_{\text{rec}}$  classifica  $\mathcal{R} \subseteq \mathcal{RE}$ .

**Dimostrazione.** Basta mostrare le quattro condizioni date dalla definizione. In particolare lo faremo attraverso le condizioni algebriche equivalenti.

1. L'identità è ricorsiva.



2. Se  $f, g$  sono ricorsive, allora anche la loro composizione  $gf$  lo è.
3. Supponiamo  $A \leq_{\text{rec}} B$  con  $B \in \mathcal{R}$  (cioè  $\chi_B$  è ricorsiva). Vogliamo dimostrare che  $A \in \mathcal{R}$ , cioè che  $\chi_A$  è ricorsiva.

Per definizione di  $\leq_{\text{rec}}$  esiste una funzione  $f \in \text{rec}$  con  $A \leq_f B$ , cioè  $x \in A$  se e solo se  $f(x) \in B$ , ovvero  $\chi_A(x) = 1$  se e solo se  $\chi_B(f(x)) = \chi_B \circ f(x) = 1$ . Ma allora  $\chi_A = \chi_B f$  e dunque  $\chi_A$  è ricorsiva poiché composizione di funzioni ricorsive.

4. Supponiamo  $A \leq_{\text{rec}} B$  con  $B \in \mathcal{RE}$ , ovvero con  $\tilde{\chi}_B$  calcolabile. Vogliamo dimostrare che  $A$  è r.e., cioè che  $\tilde{\chi}_A$  è calcolabile.

Per definizione di  $\leq_{\text{rec}}$  esiste una funzione  $f \in \text{rec}$  con  $A \leq_f B$ , ovvero  $x \in A$  se e solo se  $f(x) \in B$ . Mostriamo che  $\tilde{\chi}_A = \tilde{\chi}_B f$ :

- se  $x \in A$  (e quindi  $\tilde{\chi}_A(x) = 1$ ) allora  $f(x) \in B$  e quindi  $\tilde{\chi}_B(f(x)) = \tilde{\chi}_B f(x) = 1$ ;
- se  $x \notin A$  (cioè  $\tilde{\chi}_A(x)$  diverge) allora  $f(x) \notin B$ , e quindi  $\tilde{\chi}_B(f(x)) = \tilde{\chi}_B \circ f(x)$  diverge.

Segue che  $\tilde{\chi}_A = \tilde{\chi}_B f$ . In particolare  $\tilde{\chi}_A$  è calcolabile, poiché composizione di funzioni calcolabili.  $\square$

Dunque in questa sezione diremo che un problema è arduo/completo per  $\mathcal{RE}$  sottointendendo la relazione  $\leq_{\text{rec}}$ .

**Osservazione 2.4.1** (-NoValue-). Osserviamo che  $\bar{K} \not\leq_{\text{rec}} K$  e  $K \not\leq_{\text{rec}} \bar{K}$ :

- se per assurdo  $\bar{K} \leq_{\text{rec}} K$ , allora  $\bar{K}$  sarebbe r.e. (perché  $K$  lo è), ma questo implicherebbe (per la [Proposizione 2.1.6](#)) che sia  $K$  che  $\bar{K}$  sono ricorsivi, il che è assurdo (poiché  $K$  non è ricorsivo);
- come osservato in precedenza,  $A \leq_{\mathcal{F}} B$  se e solo se  $\bar{A} \leq_{\mathcal{F}} \bar{B}$ , dunque  $K \leq_{\text{rec}} \bar{K}$  se e solo se  $\bar{K} \leq_{\text{rec}} K$ , che abbiamo dimostrato essere falso.

- **Problemi co- $\mathcal{RE}$**  I problemi tali che i loro complementari sono in  $\mathcal{RE}$  formano una classe chiamata co- $\mathcal{RE}$ . Dato che ogni problema ricorsivo ha anche un complementare ricorsivo,  $\mathcal{R} \subseteq \text{co-}\mathcal{RE}$ ; tuttavia esistono anche problemi al di fuori di co- $\mathcal{RE}$ .

Per studiare le relazioni tra gli insiemi  $\mathcal{R}$  e  $\mathcal{RE}$  vorremo trovare un problema completo per  $\mathcal{RE}$ .

### Teorema 2.4.3

$K$  è completo per  $\mathcal{RE}$ .

**Dimostrazione.** Dato che  $K$  è r.e., basta dimostrare che  $K$  è arduo per  $\mathcal{RE}$ . Sia allora  $A \in \mathcal{RE}$ , ovvero tale che esista un indice  $i$  tale che  $\text{dom}(\varphi_i) = A$ , ovvero  $A = \{x : \varphi_i(x) \downarrow\}$ .

Definiamo allora la funzione  $\psi : \mathbb{N}^2 \rightarrow \mathbb{N}$  data da  $\psi(x, y) := \varphi_i(x)$ . (Il parametro  $y$  non fa niente.) Dato che  $\psi$  è calcolabile dovrà esistere un indice  $j$  con  $\psi = \varphi_j$ . In particolare  $A = \{x : \varphi_j(x, y) \downarrow\}$ .

Per il [Teorema del Parametro](#) e l'[OSSERVAZIONE 1.6.2](#), possiamo considerare la funzione  $f := \lambda x. s(j, x)$ : il Teorema ci garantisce che  $\varphi_j(x, y) = \varphi_{f(x)}(y)$  per ogni  $x, y$ . Osserviamo in particolare che  $f$  è calcolabile totale.

Ma  $y$  non ha un effetto sulla computazione ( $\varphi_j(x, y) = \varphi_j(x, y')$  per ogni  $y, y'$ ), ovvero  $\varphi_{f(x)}$  è **costante**. Segue che

$$A = \{x : \varphi_{f(x)}(y) \downarrow\} = \{x : \varphi_{f(x)}(f(x)) \downarrow\} = \{x : f(x) \in K\},$$

ovvero  $A \leq_f K$ . Dato che  $f \in \text{rec}$ , segue la tesi.  $\square$

#### 2.4.1 Altri problemi completi per $\mathcal{RE}$

Il fatto che  $K \leq_{\text{rec}} K_0$  mostra (per il [Proposizione 2.3.7](#)) che anche  $K_0$  è completo per  $\mathcal{RE}$ . Cerchiamo altri problemi completi per  $\mathcal{RE}$ .

► **TOT è completo per  $\mathcal{RE}$**

Consideriamo il problema

$$\text{TOT} := \{i : \text{dom}(\varphi_i) = \mathbb{N}\} = \{i : \varphi_i \in \text{rec}\}.$$

#### Proposizione 2.4.4 –

Vale la riduzione

$$K \leq_{\text{rec}} \text{TOT}.$$

In particolare TOT è completo per  $\mathcal{RE}$ .

**Dimostrazione.** Consideriamo la funzione  $\psi : \mathbb{N}^2 \rightarrow \mathbb{N}$  definita da

$$\psi(x, y) := \begin{cases} 1, & \text{se } x \in K \\ \perp, & \text{se } x \notin K. \end{cases}$$

Dato che  $K$  è semidecidibile  $\psi$  è calcolabile: basta calcolare  $\tilde{\chi}_K(x)$  (che è calcolabile); se la computazione termina (resitutando 1) poniamo  $\psi(x, y) = 1$ , altrimenti la computazione di  $\tilde{\chi}_K(x)$  non termina e quindi anche  $\psi(x, y)$  diverge.

Siccome  $\psi$  è calcolabile esisterà un indice  $i$  tale che  $\varphi_i = \psi$ . Per il [Teorema del Parametro](#) (insieme all'[OSSERVAZIONE 1.6.2](#)) esisterà  $f$  calcolabile totale,  $f := \lambda x. s(i, x)$  tale che

$$\varphi_i(x, y) = \varphi_{f(x)}(y).$$

Ora abbiamo due casi:

- se  $x \in K$  allora per ogni  $y$  si ha

$$\varphi_{f(x)}(y) = \psi(x, y) = 1,$$

dunque  $f(x)$  è indice di una funzione calcolabile totale, ovvero  $f(x) \in \text{TOT}$ ;

- se  $x \notin K$  allora per ogni  $y$  si ha

$$\varphi_{f(x)}(y) = \psi(x, y) = \perp,$$

dunque  $f(x)$  non è indice di una funzione calcolabile totale (è sempre indefinita!) e quindi  $f(x) \notin \text{TOT}$ .

Segue che  $x \in K$  se e solo se  $f(x) \in \text{TOT}$ , ovvero (dato che  $f$  è calcolabile totale)  $K \leq_{\text{rec}} \text{TOT}$ .  $\square$

## 2.5 Il Teorema di Rice

Alla fine dell'ultima sezione abbiamo mostrato come  $\text{TOT}$  sia un altro esempio di insieme non ricorsivo. Per costruire  $\text{TOT}$  abbiamo sfruttato un'idea particolarmente semplice: abbiamo preso tutti e soli gli *indici* di tutte le funzioni calcolabili totali. Questo approccio ci consente di definire diversi altri insiemi interessanti:

$$\begin{aligned} \text{FIN} &:= \{ i : \text{dom}(\varphi_i) \text{ è finito} \} \\ \text{INF} &:= \{ i : \text{dom}(\varphi_i) \text{ è infinito} \} = \overline{\text{FIN}} \\ \text{REC} &:= \{ i : \text{dom}(\varphi_i) \text{ è ricorsivo} \} \\ \text{CONST} &:= \{ i : \varphi_i \text{ è costante e totale} \} \\ \text{EXT} &:= \{ i : \varphi_i \text{ è estendibile ad una funzione calc. tot.} \} \end{aligned} \quad (2.2)$$

Possiamo studiare più velocemente tali insiemi?

### Definizione 2.5.1 – Insiemi di indici che rappresentano funzioni

Sia  $I \subseteq \mathbb{N}$  un insieme di indici. I si dice **insieme di indici che rappresentano funzioni** (**iirf** per gli amici) se per ogni  $x, y$  vale che

$$x \in I \text{ e } \varphi_y = \varphi_x \implies y \in I.$$

In pratica un insieme di indici è un iirf se quando contiene un indice  $i$  allora contiene tutti gli indici che rappresentano  $\varphi_i$  (che sappiamo essere infiniti per il [Padding Lemma](#)).

L'importanza di questo tipo di insiemi di indici è che ci consentono di collegare sintassi e semantica: se riusciamo a dimostrare che un iirf gode di una determinata proprietà, allora le *funzioni rappresentate dall'insieme* godono di tale proprietà.

### Proposizione 2.5.2 –

Se  $I$  è un iirf, allora  $\bar{I}$  è un iirf.

**Dimostrazione.** Supponiamo per assurdo che  $\bar{I}$  non sia un iirf: dovranno esistere  $x, y$  tali che  $x \in \bar{I}$ ,  $\varphi_x = \varphi_y$  ma  $y \notin \bar{I}$ , ovvero  $y \in I$ . Ma  $I$  è un iirf, dunque anche  $x$  deve appartenere ad  $I$ : questo è assurdo poiché abbiamo supposto appartenesse al suo complementare. Segue la tesi.  $\square$

**Teorema 2.5.3 – Index Set Theorem**

Sia  $I$  un iirf,  $I \neq \emptyset$ ,  $I \neq \mathbb{N}$ . Allora  $K \leq_{\text{rec}} I$  oppure  $K \leq_{\text{rec}} \bar{I}$ .

**Dimostrazione.** Sia  $i_0$  tale che  $\varphi_{i_0}$  sia la funzione sempre indefinita e supponiamo senza perdita di generalità  $i_0 \in \bar{I}$ .<sup>a</sup> Siccome  $I$  è non vuoto dovrà esistere un  $i_1 \in I$ ; inoltre dato che  $I$  è un iirf certamente  $\varphi_{i_1} \neq \varphi_{i_0}$  (altrimenti  $i_0 \in I$ ), dunque  $\varphi_{i_1}$  non è ovunque indefinita. Definiamo allora la seguente funzione:

$$\psi(x, y) := \begin{cases} \varphi_{i_1}(y), & \text{se } x \in K \\ \perp, & \text{altrimenti.} \end{cases}$$

Questa funzione è intuitivamente calcolabile: se  $x \in K$  (possiamo verificarlo in tempo finito siccome  $K$  è semidecidibile) allora basta prendere la funzione  $i_1$ -esima della numerazione e calcolarla su  $y$ ; altrimenti non riusciremo mai a verificare che  $x \notin K$  e dunque  $\psi$  sarà indefinita.

Per la Tesi di Church-Turing, insieme al [Teorema del Parametro](#) e l'[OSSERVAZIONE 1.6.2](#) possiamo allora considerare la funzione  $f$  calcolabile totale tale che

$$\varphi_{f(x)}(y) = \psi(x, y).$$

Mostriamo che  $K \leq_f I$ :

- se  $x \in K$  allora  $\varphi_{f(x)} = \varphi_{i_1}$ , ma dato che  $i_1 \in I$  e quest'ultimo è un iirf segue che  $f(x) \in I$ ;
- se  $x \notin K$  allora  $\varphi_{f(x)}$  è sempre indefinita, ovvero  $\varphi_{f(x)} = \varphi_{i_0}$ . Ma dato che per la [Proposizione 2.5.2](#) anche  $\bar{I}$  è un iirf segue che  $f(x) \in \bar{I}$ , ovvero  $f(x)$  non appartiene ad  $I$ .

Segue la tesi. □

<sup>a</sup>Se  $i_0$  appartenesse a  $I$  potremmo scambiare  $I$  e  $\bar{I}$  e alla fine dimostreremmo che  $K \leq_{\text{rec}} \bar{I}$ .

L'[Index Set Theorem](#) ci permette di dimostrare uno dei risultati più importanti della Teoria della Calcolabilità, che è il [Teorema di Rice](#).

**Teorema 2.5.4 – Teorema di Rice**

Sia  $\mathcal{F}$  un insieme di funzioni calcolabili,  $I_{\mathcal{F}} := \{i : \varphi_i \in \mathcal{F}\}$  l'insieme degli indici delle funzioni di  $\mathcal{F}$ .

Allora  $I_{\mathcal{F}}$  è ricorsivo se e solo se  $\mathcal{F}$  è vuoto oppure contiene tutte le funzioni calcolabili.

**Dimostrazione.** Mostriamo entrambi i versi dell'implicazione.

← Ovvio: se  $\mathcal{F}$  è vuoto allora  $I_{\mathcal{F}}$  è vuoto, se contiene tutte le funzioni calcolabili allora  $I_{\mathcal{F}} = \mathbb{N}$  e entrambi questi insiemi sono ricorsivi.<sup>a</sup>

→ Se  $\mathcal{F}$  è non vuoto e non contiene tutte le funzioni calcolabili, allora  $I_{\mathcal{F}}$  è un insiemi

di indici strettamente compreso tra  $\emptyset$  e  $\mathbb{N}$ . Per l'[Index Set Theorem](#) segue che  $K \leq_{\text{rec}} I_{\mathcal{F}}$  o al suo complemento, e dunque  $I_{\mathcal{F}}$  non è ricorsivo.<sup>b</sup>  $\square$

<sup>a</sup>Le loro funzioni caratteristiche sono rispettivamente la funzione costante 0 e la funzione costante 1, che sono ovviamente calcolabili.

<sup>b</sup>Se  $K \leq_{\text{rec}} \overline{I_{\mathcal{F}}}$  allora  $\overline{I_{\mathcal{F}}}$  è non ricorsivo, ma un insieme è ricorsivo se e solo se lo è il suo complemento, dunque neanche  $I_{\mathcal{F}}$  lo è.

Il Teorema di Rice ci dice in breve che, data una **qualsiasi proprietà semantica** non banale di un programma, il problema di decidere se una funzione soddisfa o no quella proprietà **non è decidibile**. In particolare tutti gli insiemi definiti in (2.2) non sono ricorsivi.

In realtà **nessuno** di quegli insiemi è ricorsivamente enumerabile: possiamo mostrare che  $\overline{K}$  si riduce ad ognuno di essi, e sappiamo già che  $\overline{K}$  non è r.e. Vediamolo per esercizio su FIN e INF.

► [FIN non è ricorsivamente enumerabile](#)

Mostriamo che  $\overline{K} \leq_{\text{rec}} \text{FIN}$ .

**Dimostrazione.** Consideriamo la funzione

$$\psi(x, y) := \begin{cases} 1, & \text{se } x \in K \\ \perp, & \text{altrimenti.} \end{cases}$$

Questa funzione è intuitivamente calcolabile: siccome  $K$  è semidecidibile possiamo decidere in tempo finito che  $x$  appartiene a  $K$ , e in tal caso poniamo  $\psi(x, y) = 1$ ; altrimenti non sapremo mai se  $x$  appartiene a  $K$  e la funzione  $\psi$  divergerà.

Per la Tesi di Church-Turing, il [Teorema del Parametro](#) e l'[OSSERVAZIONE 1.6.2](#) esiste una funzione  $f$  calcolabile totale tale che

$$\varphi_{f(x)}(y) = \psi(x, y).$$

Mostriamo che  $\overline{K} \leq_f \text{FIN}$ :

- se  $x \in \overline{K}$ , ovvero  $x$  non appartiene a  $K$ , allora  $\varphi_{f(x)}$  è sempre indefinita. In particolare il suo dominio è vuoto e quindi è finito, dunque  $f(x) \in \text{FIN}$ ;
- se  $x \notin \overline{K}$  si ha che  $x \in K$ , dunque  $\varphi_{f(x)}$  è costantemente 1, dunque il suo dominio è tutto  $\mathbb{N}$  e quindi  $f(x)$  non appartiene a FIN.

Segue la tesi.  $\square$

► [INF non è ricorsivamente enumerabile](#)

Mostriamo che  $\overline{K} \leq_{\text{rec}} \text{INF}$ .

**Dimostrazione.** Consideriamo la funzione

$$\psi(x, y) := \begin{cases} 1, & \text{se } \varphi_x(x) \text{ non converge in meno di } y \text{ passi} \\ \perp, & \text{altrimenti.} \end{cases}$$

Questa funzione è intuitivamente calcolabile: proviamo a calcolare  $\varphi_x(x)$ ; se in  $y$  passi ancora non ha terminato la sua computazione poniamo  $\psi(x, y) = 1$ , altrimenti la poniamo indefinita.

Per la Tesi di Church-Turing, il [Teorema del Parametro](#) e l'[OSSERVAZIONE 1.6.2](#) esiste una funzione  $f$  calcolabile totale tale che

$$\varphi_{f(x)}(y) = \psi(x, y).$$

Mostriamo che  $\bar{K} \leq_f \text{INF}$ :

- se  $x \in \bar{K}$ , ovvero  $x$  non appartiene a  $K$ , allora  $\varphi_x(x)$  non convergerà mai e dunque  $\psi(x, y)$  sarà 1 per ogni  $y$ . In particolare  $\varphi_{f(x)}$  è costantemente 1, dunque il suo dominio è tutto  $\mathbb{N}$ , dunque  $f(x) \in \text{INF}$ ;
- se  $x \notin \bar{K}$  si ha che  $x \in K$ , dunque dovrà esistere un  $\bar{y} \in \mathbb{N}$  tale che  $\varphi_x(x)$  converge in  $\bar{y}$  passi. Ma allora

$$\psi(x, y) = \varphi_{f(x)}(y) \text{ diverge per ogni } y \geq \bar{y}$$

dunque il dominio di  $\psi(x, y)$  è al più l'insieme  $\{0, \dots, \bar{y}\}$ , dunque è finito. Segue che  $f(x)$  non appartiene a  $\text{INF}$ .

Segue la tesi. □

**Osservazione 2.5.1** (-NoValue-). Siccome  $\text{FIN}$  e  $\text{INF}$  sono l'uno il complementare dell'altro e sono entrambi non r.e., sono anche **non co-RE**.

# 3

## Teoria della Complessità

---

Nella prima parte del corso abbiamo studiato la risolubilità di problemi: in particolare abbiamo studiato come, sotto determinate ipotesi, esistono problemi decidibili, problemi semidecidibili e problemi ancora più difficili. Abbiamo visto che esiste una gerarchia rispetto alla *difficoltà* e abbiamo studiato una parte di questa gerarchia, ovvero le classi  $\mathcal{R}$  e  $\mathcal{RE}$ .

Vogliamo ora chiederci *come* si calcola e *quante risorse* siano necessarie: nella realtà non abbiamo a disposizione memoria infinita o tempo illimitato, e perciò vogliamo sapere quali problemi possono essere risolti data la quantità di risorse che abbiamo a disposizione.

Iniziamo a introdurre dei vincoli sulla nostra teoria. Innanzitutto considereremo come risorse solamente il *tempo* e lo *spazio*, anche se queste non sono le uniche risorse esistenti. Potremmo infatti studiare anche il numero di messaggi scambiati, la banda di rete utilizzata, l'energia consumata, eccetera.

Nel far ciò ci scontriamo immediatamente con una difficoltà: per i problemi non decidibili è possibile che la valutazione di un'istanza del problema (ovvero, decidere se un elemento appartiene o no all'insieme che codifica il problema) diverga, e quindi nessuna quantità finita di risorse è sufficiente. Per questo motivo ci limiteremo da ora in poi a studiare *problemi decidibili*.

A questo punto siamo interessati a calcolare quante risorse sono necessarie in termini della *grandezza dell'input*. Per far ciò insieme ad ogni problema  $P$  e al suo insieme di input  $I \supseteq P^1$  consideriamo una funzione

$$|\cdot| : I \rightarrow \mathbb{N}$$

detta **taglia**, che associa ad ogni  $x \in I$  la sua "grandezza", indicata con  $|x|$ .

Tipici esempi di taglie sono il numero di bit nei problemi che hanno come input numeri, oppure il numero di elementi del vettore in input se il problema ha come input vettori, o il numero di nodi se l'input è un grafo, eccetera. Non ci occuperemo di studiare le taglie associate a problemi classici, anche perché spesso sono molto intuitive.

Dato un problema  $P$  vogliamo quindi misurare la complessità di ogni singola *istanza* del problema, ed in particolare vogliamo misurare la complessità del **caso pessimo**. Per far ciò possiamo cercare una funzione

$$f : \mathbb{N} \rightarrow \mathbb{N}$$

che, data la taglia di un input  $x \in I$ , maggiora il numero di risorse necessarie alla macchina scelta per risolvere l'istanza. Siccome siamo interessati principalmente a stime asintotiche e ai casi

---

<sup>1</sup>Un problema  $P$  può essere considerato come un insieme, e la domanda è stabilire se un dato elemento di input  $x \in I$  appartenga o no a  $P$ : in particolare ogni elemento di  $P$  può essere scelto come input, e quindi  $P \subseteq I$ .

pessimi, vogliamo inoltre che se  $|x| < |y|$  allora  $f(|x|) \leq f(|y|)$ . In casi particolarmente fortunati riusciremo a trovare la *minima* funzione che maggiore la quantità di risorse necessarie.

Osserviamo ora che se un problema richiede al più  $k$  risorse, allora qualsiasi sistema con  $k' \geq k$  risorse può risolvere il problema dato: possiamo quindi creare una gerarchia di classi di problemi, e per studiare queste classi useremo gli stessi strumenti visti nella prima parte, ovvero le riduzioni e i problemi completi.

Tuttavia la gerarchia tra classi dipende a priori dal contesto, ovvero da come misuriamo il consumo di risorse e anche dal modello di computazione scelto. Per questo richiediamo infine che la nostra teoria sia *invariante* rispetto sia ai modelli di calcolo, sia rispetto alla rappresentazione dei dati.

Sotto tutte queste ipotesi in questa parte del corso riusciremo a descrivere un piccolo frammento della gerarchia delle classi di complessità:

$$\text{LOGSPACE} \subseteq \mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{PSPACE} = \mathcal{NPSPACE} \subseteq \mathcal{R} \subseteq \mathcal{RE}.$$

L'interesse moderno per questa gerarchia è che abbiamo dimostrato che  $\text{LOGSPACE} \subsetneq \mathcal{PSPACE}$ , ovvero abbiamo trovato un problema in  $\mathcal{PSPACE}$  che non è in  $\text{LOGSPACE}$ . Questo significa che almeno una delle inclusioni

$$\text{LOGSPACE} \subseteq \mathcal{P}, \quad \mathcal{P} \subseteq \mathcal{NP}, \quad \mathcal{NP} \subseteq \mathcal{PSPACE}$$

deve essere stretta, tuttavia ancora non sappiamo quale.

### 3.1 Complessità deterministica

Vogliamo studiare la complessità in tempo e spazio usando come modello base di *calcolatore* le Macchine di Turing. Come prima cosa, facciamo una piccola estensione delle MdT normali.

#### Definizione 3.1.1 – Macchina di Turing a $k$ nastri

Una **Macchina di Turing a  $k$  nastri** è una quintupla  $M = (Q, \Sigma, \delta, q_0)$  tale che

- (1)  $\#, \triangleright \in \Sigma$ , mentre  $L, R, - \notin \Sigma$ ,
- (2)  $S\hat{I}, N\hat{O}$  sono due stati speciali che non appartengono a  $Q$ ,
- (3) la funzione di transizione ha la forma

$$\delta : Q \times \Sigma^k \rightarrow (Q \cup \{S\hat{I}, N\hat{O}\}) \times (\Sigma \times \{L, R, -\})^k$$

e inoltre valgono le altre condizioni delle MdT, opportunamente riscritte.

Una MdT a  $k$  nastri quindi è una normale MdT che può leggere contemporaneamente  $k$  simboli diversi e la cui funzione di transizione lavora considerando lo stato corrente e tutti i  $k$  simboli letti.

In particolare una configurazione ha la forma

$$(q, u_1 \underline{\sigma}_1 v_1, u_2 \underline{\sigma}_2 v_2, \dots, u_k \underline{\sigma}_k v_k).$$

Una macchina a  $k$  nastri può essere quindi pensata come una macchina a  $k$  *processori*: ogni nastro contiene dell'informazione, e i vari nastri possono eseguire calcoli aiutandosi l'un l'altro oppure ognuno per i fatti suoi.



Perché non abbiamo diviso lo stato in  $k$ -uple? Perché in generale non cambia niente: possiamo immaginare l'insieme  $Q$  composto da  $k$ -uple e ogni coordinata della  $k$ -upla rappresenta lo stato del singolo nastro.

Introduciamo le macchine a  $k$  nastri formalmente solo ora perché da un punto di vista della calcolabilità non apportano nessun miglioramento: un problema è decidibile/semidecidibile da una macchina a  $k$  nastri se e solo se è decidibile/semidecidibile da una macchina standard ad 1 nastro.

### Definizione 3.1.2 – Tempo deterministico richiesto

Sia  $M$  una MdT a  $k$  nastri che risolve il problema  $I$ . Diremo che  $t \in \mathbb{N}$  è **tempo deterministico richiesto** per decidere l'istanza  $x \in I$  se

$$(q_0, \sqsupseteq x, \sqsupseteq, \dots, \sqsupseteq) \rightarrow^t (h, u_1, u_2, \dots, u_t)$$

con  $h \in \{S, I, NO\}$ .

Il *deterministico* nella definizione precedente evidenzia il fatto che la MdT considerata è deterministica, ovvero che la sua  $\delta$  è una funzione di transizione e non semplicemente una relazione. Questa differenza, finora immateriale, sarà fondamentale nello studio della Teoria della Complessità.

Questo ci dà un modo per misurare il tempo richiesto per la decisione di ogni istanza, ma noi vorremmo una funzione che varia in base alla taglia  $|x|$  del caso  $x \in I$ .

### Definizione 3.1.3 – Tempo per la decisione

Sia  $M$  una MdT a  $k$  nastri che risolve il problema  $I$ . Sia inoltre  $f : \mathbb{N} \rightarrow \mathbb{N}$  una funzione crescente.

Diremo che  $M$  **decide  $I$  in tempo deterministico  $f$**  se per ogni  $x \in I$  il tempo deterministico  $t_x$  richiesto da  $M$  per decidere l'istanza  $x \in I$  è tale che

$$t \leq f(|x|).$$

### Definizione 3.1.4 – Classe delle funzioni decidibili in tempo det. $f$

Sia  $f : \mathbb{N} \rightarrow \mathbb{N}$  monotona crescente. La **classe di complessità di tempo deterministico  $f$**  è la classe

$$\text{TIME}(f) := \{ I : \exists M \text{ che decide } I \text{ in tempo det. } f \}.$$

Spesso ci converrà ragionare in termini di ordini di grandezza: ricordiamo che date due funzioni  $f, g : A \rightarrow \mathbb{R}$  diremo che  $f$  è  **$\mathcal{O}$ -grande** di  $g$  (e lo indichiamo impropriamente con  $f = \mathcal{O}(g)$ ) se esiste  $c \in [0, +\infty]$  tale che

$$f(x) \leq c \cdot g(x) \quad \text{definitivamente,}$$

o equivalentemente se

$$\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} \leq c.$$

Scriveremo quindi spesso  $\text{TIME}(f)$  per indicare in realtà  $\text{TIME}(\mathcal{O}(f))$ , ovvero la classe di tutti gli algoritmi decidibili in tempo deterministico *ordine di*  $f$ .

Vogliamo ora dimostrare che l'aggiunta di nastri è un procedimento *effettivo*, ovvero che non altera in modo non-algoritmico la capacità di computazione delle macchine di Turing.

**Teorema 3.1.5 – Riduzione del numero di nastri**

Sia  $M$  a  $k$  nastri che decide  $I$  in tempo deterministico  $f$ . Allora esiste  $M'$  ad un nastro che decide  $I$  in tempo deterministico  $\mathcal{O}(f^2)$ .

**Dimostrazione.** Consideriamo una configurazione della macchina a  $k$  nastri

$$(q, \sqsupseteq w_1, \dots, \text{resp } w_k)_M.$$

Per farla diventare ad un nastro la rappresentiamo come

$$(q', \triangleright \triangleright' w_1 \triangleleft' \triangleright' w_2 \triangleleft' \dots \triangleright' w_k \triangleleft')_{M'}.$$

Per memorizzare il simbolo corrente, aggiungiamo a  $\Sigma$  un simbolo  $\bar{\sigma}$  per ogni  $\sigma \in \Sigma$ .

Il primo passo da fare è prendere l'input della macchina  $M$  e trasformarlo nel relativo input della macchina  $M'$ . L'input di  $M$  sarà della forma

$$(q, \triangleright x, \triangleright, \dots, \triangleright);$$

per scriverlo in  $M'$  eseguiamo i seguenti passi:

$$\begin{aligned} (q, \triangleright x) &\rightarrow^{|x|+1} (q, \triangleright \triangleright' x) \\ &\rightarrow^{\mathcal{O}(|x|)} (q, \sqsupseteq \triangleright' x \triangleleft' \triangleright' \triangleleft' \dots \triangleright' \triangleleft'). \end{aligned}$$

Dunque per scrivere l'input su  $M'$  abbiamo bisogno (al caso pessimo) di  $\mathcal{O}(|x|)$  passi.

Vogliamo studiare ora il tempo (massimo) necessario per l'esecuzione di un passo di computazione: data una configurazione di  $M'$

$$(q, \sqsupseteq \triangleright' u_1 \bar{\sigma}_1 v_1 \triangleleft' \dots \triangleright' u_k \bar{\sigma}_k v_k \triangleleft')$$

con il cursore nel respingente "vero", per eseguire tutti i passi ci basta

- (1) scorrere il nastro verso destra per leggere tutti i caratteri correnti,
- (2) tornare al respingente a sinistra,
- (3) scorrere il nastro ed eseguire le computazioni,
- (4) tornare al respingente.

Dunque sono sufficienti 4 letture complete del nastro di  $M'$ .

Osserviamo che ogni *sottonastro* di  $M'$ , ovvero ogni stringa  $u_i \bar{\sigma}_i v_i$ , è lunga al più  $f(|x|)$ : in effetti la macchina  $M$  esegue al più  $f(|x|)$  passi, e in un passo può scrivere al più una casella del nastro.

Segue che il nastro di  $M'$  in totale è lungo al più

$$\ell := k(f(|x|) + 2) + 1.^2$$

Segue che per ogni passo di computazione eseguiamo  $\mathcal{O}(\ell) = \mathcal{O}(f)$  operazioni; dato che eseguiamo al più  $f(|x|)$  passi di computazione segue che  $M'$  decide  $I$  in al più

$$f \cdot \mathcal{O}(f) = \mathcal{O}(f^2)$$

passi. □

Il +2 è dovuto ai due respingenti finti  $\triangleright'$  e  $\triangleleft'$ , mentre il +1 è dovuto al respingente vero  $\triangleright$  di  $M'$ .

### Teorema 3.1.6 – Teorema di Accelerazione Lineare

Se  $I \in \text{TIME}(f)$ , allora per ogni  $\varepsilon > 0$  si ha che

$$I \in \text{TIME}(\varepsilon \cdot f(n) + n + 2).$$

Possiamo finalmente definire una delle più importanti classi di complessità studiate.

### Definizione 3.1.7 – Classe $\mathcal{P}$

La **classe di complessità  $\mathcal{P}$**  è definita come

$$\mathcal{P} := \bigcup_{k \in \mathbb{N}} \text{TIME}(n^k),$$

considerando gli ordini di grandezza.

## 3.2 Complessità in spazio

Vogliamo ora definire le misure di complessità in spazio per i problemi decidibili. Iniziamo discutendo una nuova estensione delle Macchine di Turing.

### Definizione 3.2.1 – Macchina di Turing I/O

Una **Macchina di Turing I/O** è una macchina di Turing a  $k$  nastri ( $k \geq 3$ )  $M = (Q, \Sigma, \delta, q_0)$  con i seguenti vincoli aggiuntivi:

(1) Se

$$\delta(q, \sigma_1, \dots, \sigma_k) = (q', (\sigma'_1, D_1), \dots, (\sigma'_k, D_k))$$

allora  $\sigma'_1 = \sigma_1$  e  $D_k \in \{R, -\}$ . Inoltre se  $D_k = -$  allora  $\sigma'_k = \sigma_k$ .

(2) Se  $\sigma_1 = \#$  allora  $D_1 \in \{-, L\}$ .

L'idea delle macchine I/O è che il primo e l'ultimo nastro hanno i ruoli privilegiati di *lettore* e *scrittore*. Infatti il primo nastro non può essere modificato grazie alla prima condizione, e inoltre arrivati alla fine (cioè alla porzione vuota) non possiamo proseguire verso destra. Analogamente l'ultimo nastro può essere solo scritto: infatti non si può riscrivere un carattere già scritto e ci si può solo muovere verso destra.

Anche questa estensione delle MdT è effettiva, come mostrato dal seguente Teorema.

**Teorema 3.2.2**

Per ogni MdT a  $k$  nastri che decide  $I$  in tempo deterministico  $f$ , esiste una MdT I/O a  $(k + 2)$ -nastri che decide  $I$  in tempo deterministico  $c \cdot f$  per qualche  $c \in [0, +\infty]$ .

**Dimostrazione.** Basta copiare il contenuto del nastro di input nei nastri  $2, \dots, k + 1$ , eseguire gli stessi passi della macchina di partenza sui nastri *di lavoro* e infine copiare l'output sul nastro  $k + 2$ .  $\square$

Il nostro scopo è misurare lo spazio necessario ad una macchina I/O per risolvere un'istanza di un problema. Per farlo potremmo eseguire la macchina e infine contare il numero di caselle non bianche, ma questo non funzionerebbe poiché la macchina può cancellare pezzi scritti durante la computazione.

Introduciamo quindi un'altra banale estensione, ovvero il simbolo di fine stringa  $\triangleleft$ : ogni volta che abbiamo necessità di più spazio ci basterà spostare tale simbolo a destra, ma avremo cura di non spostarlo mai verso sinistra o cancellarlo in modo da memorizzare la quantità *massima* di memoria usata.

**Definizione 3.2.3 – Spazio richiesto per la decisione e classe SPACE**

Sia  $M$  una MdT a  $k$  nastri I/O che decide il problema  $I$ .

Data un'istanza  $x \in I$  e la computazione di decisione

$$(q_0, \triangleright x \triangleleft, \triangleright \triangleleft, \dots, \triangleright \triangleleft) \rightarrow^* (S\dot{I}, w_1, \dots, w_k)$$

diremo che lo **spazio richiesto** per la decisione dell'istanza  $x$  è

$$\sum_{i=2}^{k-1} |w_i|.^\alpha$$

Diremo inoltre che  $M$  **decide  $I$  in spazio deterministico  $f$**  se per ogni  $x \in I$  lo spazio richiesto per la decisione di  $x$  è minore o uguale a  $f(|x|)$ .

Infine la **classe SPACE( $f$ )** è la classe

$$\text{SPACE}(f) := \{ I : \exists M \text{ a } k \text{ nastri I/O che decide } I \text{ in spazio det. } f \}.$$

<sup>a</sup>Qui  $|w_i|$  indica la lunghezza della stringa  $w_i$ .

**Osservazione 3.2.1** (Alcune osservazioni sulle definizioni date).

- Lo "spazio richiesto" è dato dalla somma delle lunghezze di tutti i nastri di lavoro, ma non del nastro di lettura né di quello di scrittura.

In effetti il nastro di scrittura non ha molto peso, in quanto contiene solamente la risposta  $S\dot{I}$  oppure  $N\dot{O}$ . Invece se includessimo il nastro di lettura otterremo che lo spazio è sempre almeno lineare nella dimensione dell'input, e questo *appiattirebbe* la gerarchia che cercheremo di delineare.

- Talvolta lo spazio richiesto viene definito come

$$\max\{|w_i| : i = 2, \dots, k-1\}.$$

Siccome

$$\sum_{i=2}^{k-1} |w_i| \leq (k-2) \cdot \max_{i=2, \dots, k-2} |w_i|$$

e noi siamo interessati solamente all'ordine di grandezza, queste definizioni sono equivalenti.

Enunciamo un analogo del [Teorema 3.1.6](#).

**Teorema 3.2.4 – Compressione lineare dello spazio**

Sia  $I \in \text{SPACE}(f)$ : allora per ogni  $\varepsilon \in [0, +\infty]$  si ha che

$$I \in \text{SPACE}(2 + \varepsilon \cdot f).$$

Definiamo ora le classi di complessità in spazio che studieremo in questo corso.

**Definizione 3.2.5**

Le classi  $\mathcal{PSPACE}$  e  $\text{LOGSPACE}$  sono definite come segue:

$$\mathcal{PSPACE} := \bigcup_{k \in \mathbb{N}} \text{SPACE}(n^k) \quad \text{LOGSPACE} := \bigcup_{k \in \mathbb{N}} \text{SPACE}(k \log(n)).$$

Uno dei risultati fondamentali della Teoria della Complessità (che noi non dimostreremo) è il seguente:

**Teorema 3.2.6**

$$\text{LOGSPACE} \subsetneq \mathcal{PSPACE}$$

ovvero esiste un problema risolvibile in spazio lineare che non può essere risolto in spazio logaritmico.

Per costruire la gerarchia vogliamo scoprire in che relazione è  $\mathcal{P}$  con le classi  $\text{LOGSPACE}$  e  $\mathcal{PSPACE}$ .

**Teorema 3.2.7**

$$\text{LOGSPACE} \subseteq \mathcal{P} \subseteq \mathcal{PSPACE}.$$

**Dimostrazione.** Il fatto che  $\mathcal{P}$  sia un sottoinsieme di  $\mathcal{PSPACE}$  è una conseguenza del principio generale che in  $t$  unità di tempo una MdT può scrivere al più  $t$  caselle del suo nastro, dunque in tempo polinomiale una MdT può scrivere al più un numero polinomiale di caselle.

Dimostriamo che  $\text{LOGSPACE} \subseteq \mathcal{P}$ : sia allora  $M$  una MdT a 3 nastri <sup>a</sup> che risolve un

problema  $I$  in spazio logaritmico, ovvero la lunghezza massima del singolo nastro di lavoro è al più  $k \log n$ , dove  $n$  è la taglia dell'input.

Segue che il numero massimo di configurazioni attraversabili da  $M$  è al più

$$N := |\Sigma|^{k \log n} \cdot k \log n \cdot |Q| \cdot n;$$

infatti  $\Sigma^{k \log n}$  è il numero massimo di possibili stringhe scritte sul nastro,  $k \log n$  è il numero massimo di posizioni del cursore,  $|Q|$  è il numero massimo di stati e  $n$  è il numero massimo di posizioni del cursore nel nastro di input.

Vogliamo dimostrare che esiste  $t$  tale che  $N \leq n^t$ , ovvero tale che  $\log N \leq t \log n$ . Per definizione di  $N$  però

$$\begin{aligned} \log N &= \log(|\Sigma|^{k \log n} \cdot k \log n \cdot |Q| \cdot n) \\ &= k \log n \log |\Sigma| + \log(k \log n) + \log |Q| + \log n, \end{aligned}$$

dunque dividendo per  $\log n$  otteniamo un possibile valore di  $t$ . □

<sup>a</sup>Se fossero più nastri basterebbe dividere ad un certo punto per un'opportuna costante.

### 3.3 Non-Determinismo e Complessità non-deterministica

Studiamo infine un'ultima estensione delle macchine di Turing.

#### **Definizione 3.3.1** – Macchine di Turing non deterministiche

Una **macchina di Turing non deterministica** è una quadrupla  $N = (Q, \Sigma, \Delta, q_0)$  definita allo stesso modo di una macchina di Turing solita tranne per il fatto che

$$\Delta \subseteq (Q \times \Sigma) \times ((Q \cup \{h\}) \times \Sigma \times \{L, R, -\})$$

è una relazione, detta **relazione di transizione**.

La differenza è quindi che a partire da una configurazione vi sono più configurazioni raggiungibili in output, e la macchina ogni volta ne sceglie una in modo arbitrario e quindi *non deterministico*.

Questa definizione può sembrare fuori dal mondo, ma è collegata strettamente a due tipi di strategie di risoluzione dei problemi molto usate.

- **Forza bruta** Dato un problema, un possibile modo di risolverlo è sempre quello di generare tutte le possibili soluzioni e controllarle una ad una: tale metodo viene detto *brute force* o metodo del *forza bruta*, in quanto brutalmente tentiamo ogni possibilità. Generando lo spazio delle soluzioni esplicitamente, ogni volta che ne tentiamo una stiamo in realtà percorrendo un cammino su tale albero: la scelta della prossima soluzione da tentare corrisponde alla *scelta non deterministica* da compiere.

**Definizione 3.3.2** – Decisione non deterministica e tempo richiesto

Una macchina di Turing non deterministica  $N$  **decide** un problema  $I$  se per ogni  $x$  vale che  $x \in I$  se e solo se esiste una computazione terminante

$$N(x) \rightarrow_N^* (S\hat{I}, w).$$

$N$  **decide  $I$  in tempo non deterministico  $f$**  se decide  $I$  e per ogni  $x \in I$  esiste una computazione terminante

$$N(x) \rightarrow_N^t (S\hat{I}, w)$$

con  $t \leq f(|x|)$ . Infine denotiamo con  $\text{NTIME}(f)$  la classe di problemi

$$\text{NTIME}(f) := \{ I : \exists N \text{ non det. che decide } I \text{ in tempo non det. } f \}.$$

Avendo definito  $\text{NTIME}$ , vorremmo sapere in che relazione è con la classe  $\text{TIME}$  definita in precedenza.

**Teorema 3.3.3** – Relazione tra  $\text{NTIME}$  e  $\text{TIME}$ 

$\text{NTIME}(f) \subseteq \text{TIME}(c^f)$  per qualche costante  $c$ .

**Dimostrazione.** Sia  $I$  un problema in  $\text{NTIME}(f)$  e sia  $M$  una macchina che lo risolve in tempo non det.  $f$ : vogliamo trovare una macchina  $M'$  che lo risolve in tempo  $c^f$  per qualche costante  $c$ .

Data la relazione di transizione  $\Delta$ , consideriamo una coppia  $(q, \sigma) \in Q \times \Sigma$  e definiamo

$$\begin{aligned} \deg(q, \sigma) &:= |\{ (q', \sigma', D') : (q, \sigma, q', \sigma', D') \in \Delta \}| \\ \deg \Delta &:= \max \{ \deg(q, \sigma) : (q, \sigma) \in Q \times \Sigma \}. \end{aligned}$$

Intuitivamente,  $\deg(q, \sigma)$  è il numero di possibili scelte che la macchina non deterministica può fare quando legge  $\sigma$  nello stato  $q$ , cioè è il fattore di ramificazione dell'albero delle computazioni quando ci troviamo in  $(q, \sigma)$ , mentre  $\deg \Delta$  è il massimo tra tutti i fattori di ramificazione.

Per semplicità, chiamiamo  $d := \deg \Delta$ . Ordiniamo lessicograficamente le quintuple di  $\Delta$ : a questo punto ogni computazione consiste in una sequenza di scelte  $(c_1, \dots, c_t)$  dove ognuna delle scelte è necessariamente compresa tra 0 e  $d - 1$ .

Per simulare la computazione di  $M$  attraverso una macchina deterministica, adottiamo una strategia di visita dell'albero delle computazioni a *profondità limitata*: fissiamo inizialmente  $t = 1$ ,  $c_1 = 0$  e controlliamo se la computazione codificata da  $(c_1)$  termina. Se sì bene, altrimenti incrementiamo  $c_1$  di 1 e eseguiamo il controllo. Arrivati al punto in cui  $c_1 = d - 1$  (e quindi non possiamo incrementarlo ulteriormente) aumentiamo  $t$  e controlliamo tutte le computazioni lunghe 2.

Dato che  $M$  decide  $I$  in tempo non deterministico  $f$ , per ogni input  $x$  avremo che il tempo  $t$  richiesto per decidere il caso  $x \in I$  è al più  $f(|x|)$ . In particolare ogni sequenza che rappresenta una computazione è al più lunga  $f(|x|)$ . Segue che la macchina  $M'$  deve fare al più  $d^{f(|x|)}$  scelte, da cui  $I \in \text{TIME}(d^f)$ .  $\square$

Introduciamo finalmente la classe dei problemi  $\mathcal{NP}$  e la sua analoga versione per lo spazio,

$\mathcal{NPSPACE}$ .

### Definizione 3.3.4 – Classe $\mathcal{NP}$

Definiamo la classe  $\mathcal{NP}$  come

$$\mathcal{NP} := \bigcup_{k \in \mathbb{N}} \mathcal{NTIME}(n^k).$$

Osserviamo che ovviamente

$$\mathcal{P} \subseteq \mathcal{NP}$$

in quanto ogni problema risolvibile in tempo polinomiale deterministico può anche essere risolto non deterministicamente. La domanda da *un miliardo di dollari*<sup>3</sup> è se il contenimento è stretto, ovvero esiste un problema in  $\mathcal{NP}$  che non appartiene a  $\mathcal{P}$ , o se le due classi sono in realtà le stesse.

### Definizione 3.3.5 – Classe $\mathcal{NPSPACE}$

Un problema  $I$  si dice **decidibile in spazio non deterministico**  $f$  se esiste una macchina di Turing I/O non deterministica  $N$  tale che per ogni  $x$  *esista* una computazione

$$N(x, \triangleright, \dots, \triangleright) \rightarrow_N^* (S\hat{I}, w_1, \dots, w_k)$$

tale che

$$\sum_{i=2}^{n-1} |w_i| \leq f(|x|).$$

Chiamiamo  $\mathcal{NSPACE}(f)$  la classe

$$\mathcal{NSPACE}(f) := \{ I : \exists N \text{ non det. che decide } I \text{ in spazio non det. } f \}.$$

Infine, definiamo la classe  $\mathcal{NPSPACE}$  come

$$\mathcal{NPSPACE} := \bigcup_{k \in \mathbb{N}} \mathcal{NSPACE}(n^k).$$

Analogamente al caso temporale,  $\mathcal{PSPACE} \subseteq \mathcal{NPSPACE}$ : potremmo dunque porci lo stesso problema riguardo al contenimento dei due insiemi. Tuttavia, al contrario del problema  $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$ , il problema  $\mathcal{PSPACE} \stackrel{?}{=} \mathcal{NPSPACE}$  è stato risolto.

### Teorema 3.3.6 – Teorema di Savitch

$$\mathcal{PSPACE} = \mathcal{NPSPACE}.$$

## 3.4 Funzioni di misura appropriata

Finora abbiamo studiato le classi  $\mathcal{TIME}$  e  $\mathcal{SPACE}$  (e le corrispettive non deterministiche  $\mathcal{NTIME}$ ,  $\mathcal{NSPACE}$ ) con funzioni di misura  $f$  qualsiasi. In realtà per ottenere risultati significativi abbiamo bisogno di alcuni vincoli in più sulla funzione di misura.

<sup>3</sup>Letteralmente.



**Definizione 3.4.1** – Funzione di misura appropriata

Una funzione  $f : \mathbb{N} \rightarrow \mathbb{N}$  si dice **di misura appropriata** se

- (1) è (debolmente) monotona crescente,
- (2) è calcolabile ed esiste una macchina  $M$  che calcola  $f$  sull'input  $x$  in
  - tempo  $\mathcal{O}(f(|x|) + |x|)$ ,
  - spazio  $\mathcal{O}(f(|x|))$ .

Fortunatamente i polinomi e le funzioni esponenziali/logaritmiche rispettano queste condizioni; inoltre si può dimostrare che somma/prodotto/composizione di funzioni appropriate è ancora appropriata, dunque la teoria delle funzioni di misura appropriate include i casi a cui siamo davvero interessati.

**Teorema 3.4.2** – Teorema di Gerarchia

Se  $f$  è appropriata allora

- (1)  $\text{TIME}(f(n)) \subsetneq \text{TIME}(f(2n+1)^3)$ ,<sup>4</sup>
- (2)  $\text{SPACE}(f(n)) \subsetneq \text{SPACE}(f(x) \cdot \log(f(x)))$ .

Come conseguenza otteniamo i seguenti due teoremi.

**Teorema 3.4.3**

$$\mathcal{P} \subsetneq \text{EXP} := \bigcup_{k \in \mathbb{N}} \text{TIME}(2^{n^k}).$$

**Dimostrazione.** Innanzitutto  $\mathcal{P} \subseteq \text{TIME}(2^n)$  poiché i polinomi sono sempre limitati superiormente dalle funzioni esponenziali (definitivamente). Per il [Teorema di Gerarchia](#) segue che  $\text{TIME}(2^n) \subsetneq \text{TIME}(2^{(2n+1)^3})$ , che è a sua volta un sottoinsieme di EXP. Segue dunque la tesi.  $\square$

**Teorema 3.4.4**

$$\mathcal{P} \subseteq \mathcal{NP} \subseteq \text{EXP}.$$

**Dimostrazione.** Il fatto che  $\mathcal{P} \subseteq \mathcal{NP}$  è già stato dimostrato; l'inclusione di  $\mathcal{NP}$  in EXP deriva dal [Teorema 3.3.3](#).  $\square$

Le funzioni di misura appropriate ci consentono finalmente di descrivere la gerarchia di cui parliamo dall'inizio del capitolo.

<sup>4</sup>Sorprendentemente, questo fatto si dimostra facendo vedere che il sottoinsieme  $\{x : \varphi_x(x) \downarrow \text{ in al più } f(|x|) \text{ passi} \}$  di  $K$  appartiene a  $\text{TIME}(f(2n+3)^3)$  ma non a  $\text{TIME}(f(n))$ .

**Teorema 3.4.5**

Sia  $f$  appropriata,  $k$  costante. Allora

- (1)  $\text{TIME}(f) \subseteq \text{NTIME}(f)$ ,
- (2)  $\text{SPACE}(f) \subseteq \text{NSPACE}(f)$ ,
- (3)  $\text{NTIME}(f) \subseteq \text{TIME}\left(k^{\log n + f(n)}\right)$ ,
- (4) vale la gerarchia

$$\text{LOGSPACE} \subseteq \mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{PSPACE} = \mathcal{NPSPACE}.$$

Inoltre  $\mathcal{NP} \subseteq \text{EXP}$ .

La gerarchia definita sopra tuttavia non è superiormente limitata, ovvero non esiste una classe che include tutti i problemi. In effetti una tale classe non può esistere, come garantito dal seguente teorema.

**Teorema 3.4.6 – Illimitatezza della gerarchia di complessità**

Per ogni funzione  $g : \mathbb{N} \rightarrow \mathbb{N}$  calcolabile totale<sup>a</sup> esiste una funzione  $f : \mathbb{N} \rightarrow \mathbb{N}$  calc. tot. tale che

- (1) esiste un problema  $I$  tale che  $I \in \text{TIME}(f)$  ma  $I \notin \text{TIME}(g)$ ,
- (2)  $f \geq g$  definitivamente, ovvero  $f(n) \geq g(n)$  per tutti gli  $n \in \mathbb{N}$  eccetto un numero finito.

<sup>a</sup>non necessariamente appropriata

Concludiamo la discussione delle funzioni di misura appropriate mostrando quale è il prezzo da pagare se volessimo considerare tutte le funzioni calcolabili totali, e non solo quelle appropriate. Lo facciamo enunciando due teoremi, ma senza dimostrarli.

**Teorema 3.4.7 – Teorema di Accelerazione, Blum**

Per ogni funzione  $h : \mathbb{N} \rightarrow \mathbb{N}$  calcolabile totale, ma non appropriata, esiste un problema  $I$  tale che, per ogni macchina  $M$  che decide  $I$  in tempo  $f$ , esiste una macchina  $M'$  che decide  $I$  in tempo  $f'$  con

$$f \geq h \circ f'$$

quasi ovunque.

Il Teorema di Accelerazione di Blum ci dice che data una funzione non appropriata  $h$  possiamo costruire un problema  $I$  che *non ammette algoritmo ottimo*: il suo tempo di esecuzione può essere ridotto all'infinito seguendo la successione di macchine  $M, M', M'', \dots$  descritto nell'enunciato.

**Teorema 3.4.8 – Teorema della Lacuna, Borodin**

Esiste una funzione calcolabile totale  $f$  (non appropriata) tale che

$$\text{TIME}(f) = \text{TIME}(2^f).$$

Se il Teorema della Lacuna fosse ammissibile la gerarchia delineata verrebbe distrutta: le classi  $\mathcal{P}$  ed  $\text{EXP}$  collasserebbero e studiare la complessità sarebbe inutile.

Un ultimo tentativo è quello di condensare le definizioni di complessità in spazio e tempo usando il cosiddetto **approccio assiomatico alla complessità**, dovuto ancora una volta a Blum.

**Definizione 3.4.9** – Funzioni che misurano la complessità

Una funzione  $\varphi$  **misura la complessità** se è della forma

$$\varphi : ((\mathbb{N} \rightarrow \mathbb{N}) \times \mathbb{N}) \rightarrow \mathbb{N}^a$$

e soddisfa le seguenti due condizioni:

- (1) per ogni  $\psi : \mathbb{N} \rightarrow \mathbb{N}$ ,  $x \in \mathbb{N}$  si ha che  $\varphi(\psi, x)$  converge se e solo se  $\psi(x)$  converge,
- (2) per ogni  $\psi : \mathbb{N} \rightarrow \mathbb{N}$ ,  $x, k \in \mathbb{N}$  è possibile decidere se  $\varphi(\psi, x) = k$ .

<sup>a</sup>Ovvero prende in input una funzione  $\mathbb{N} \rightarrow \mathbb{N}$  e un numero naturale e restituisce in output un altro numero naturale.

Il primo assioma ci dice che  $\varphi$  misura la complessità del calcolo di  $\psi$ , il secondo ci assicura che è possibile calcolare la complessità usando  $\varphi$ . Se  $\varphi$  contasse il numero di passi per calcolare  $\psi(x)$  otterremmo la misura di complessità in tempo; se contasse lo spazio otterremmo la complessità in spazio.

Le funzioni di misura appropriata soddisfano gli assiomi, tuttavia esistono anche funzioni non appropriate che misurano la complessità e ancora una volta ci portano a situazioni controintuitive (come il [Teorema 3.4.8](#)).



## Esercizi

---

### A.1 Esercizi di calcolabilità

In questa sezione raccogliamo alcuni esercizi sulla parte di Calcolabilità.

#### Nessun limite al tempo

Esiste una  $t$  calcolabile totale tale che  $t(i, n)$  maggiore il tempo di calcolo di  $\varphi_i(n)$ ?

**Soluzione.** Supponiamo per assurdo esista una tale  $t$  calcolabile totale. Essa dovrà essere necessariamente della forma

$$t(i, n) := \begin{cases} k_{i,n}, & \text{se } \varphi_i(n) \text{ converge} \\ 0, & \text{se } \varphi_i(n) \text{ diverge.} \end{cases}$$

dove  $k_{i,n}$  è maggiore o uguale del numero di passi di computazione effettuati nel calcolo di  $\varphi_i(n)$ . Indicheremo il numero di passi esatti con  $T_i(n)$ .<sup>a</sup>

Dato che  $t$  è calcolabile possiamo definire

$$f(x) := \begin{cases} \varphi_x(x) + 1, & \text{se } T_x(x) \leq t(x, x) \\ 0, & \text{altrimenti.} \end{cases}$$

Osserviamo che questa definizione ci dice che  $f(x)$  è  $\varphi_x(x) + 1$  se  $\varphi_x(x)$  converge, 0 altrimenti.

Per la Tesi di Church-Turing esiste  $i$  tale che  $\varphi_i = f$ . Mostriamo che ciò è assurdo: in effetti  $\varphi_i(i) \neq f(i)$  in quanto

- se  $\varphi_i(i)$  converge, allora  $f(i) = \varphi_i(i) + 1 \neq \varphi_i(i)$ ;
- se  $\varphi_i(i)$  diverge, allora  $f(i) = 0$ .

Segue che  $t$  non può essere calcolabile. □

---

<sup>a</sup>Questa funzione non è necessariamente calcolabile!

Osserviamo che la seconda parte della dimostrazione è identica alla dimostrazione della non-ricorsività di  $K$ : in alternativa possiamo quindi mostrare che se  $t$  fosse calcolabile allora  $K$  sarebbe ricorsivo.

**Soluzione alternativa.** Supponiamo come sopra che esista una  $t$  calcolabile e della forma vista. Allora definiamo

$$f(x) := \begin{cases} 1, & \text{se } t(x, x) > 0 \\ 0, & \text{se } t(x, x) = 0. \end{cases}$$

Tale  $f$  è certamente calcolabile, in quanto  $t$  lo è.

Ma  $f$  è esattamente la funzione caratteristica di  $K$ : se  $t(i, i)$  è diverso da 0 allora la macchina  $\varphi_i$  calcolata su  $i$  termina la sua computazione, e quindi  $i \in K$ ; viceversa se  $t(i, i)$  è 0 allora  $\varphi_i(i)$  diverge, e quindi  $i$  non appartiene a  $K$ .

Tuttavia  $K$  non è ricorsivo, dunque segue l'assurdo.  $\square$

### Calcolatori con memoria finita in ciclo

Esiste una funzione calcolabile totale che determina se  $\varphi_i(x)$  se uno specifico calcolatore  $C$  con memoria finita è in ciclo?

**Soluzione.** La risposta è sì: siano  $Q_C, \Sigma_C, \delta_C, q_0$  le caratteristiche della MdT che modella  $C$ .

Siano inoltre  $m - 1 := |Q_C|$ ,  $n := |\Sigma_C|$ ,  $k$  la lunghezza del nastro di  $C$ . Allora il numero totale di configurazioni è

$$l := k^n \cdot m \cdot k.^a$$

Costruiamo allora una macchina universale  $U$  che calcola la macchina  $M_i$  su  $x$  a partire dallo stato  $q_0$  e con un campo aggiuntivo inizialmente inizializzato a  $l$ : ad ogni passo di  $M_i$  diminuiamo di 1 il valore di  $l$ .

Alla fine del calcolo possiamo controllare il valore finale di  $l$ : se è maggiore di 0 allora ci sono ancora degli stati non visitati, dunque  $M_i$  non è in ciclo; altrimenti lo è.  $\square$

<sup>a</sup>  $k^n$  è il numero di possibili nastri,  $m$  è il numero di possibilità per lo stato (incluso il terminatore  $h$ ),  $k$  è il numero di possibilità per la testina.

### Esercizio su insiemi non ricorsivi

L'insieme  $I := \{ i : \text{dom}(\varphi_i) = \{ 3 \} \}$  è ricorsivo?

**Soluzione 1.** Dimostriamo che  $I$  non è ricorsivo applicando l'[Index Set Theorem](#): abbiamo bisogno di mostrare che  $\emptyset \neq I \neq \mathbb{N}$  e che  $I$  è un iirf.

(1)  $I$  non è vuoto perché la funzione

$$\lambda x. \begin{cases} 1, & \text{se } x = 3 \\ \perp, & \text{altrimenti} \end{cases}$$

è calcolabile (ad esempio è facile scrivere un programma WHILE che la calcola) ed ha come dominio esattamente  $\{ 3 \}$ .

(2)  $I$  non è tutto  $\mathbb{N}$  in quanto ad esempio la funzione costantemente uguale a 1 è calcolabile ma non ha dominio  $\{3\}$ .

(3)  $I$  è un iirf: supponiamo che  $x \in I$  e  $y$  sia un altro indice tale che  $\varphi_x = \varphi_y$ . Ma allora

$$\text{dom}(\varphi_y) = \text{dom}(\varphi_x) = \{3\}$$

e dunque  $y \in I$ .

Per l'[Index Set Theorem](#) segue la tesi.  $\square$

**Soluzione 2.** Mostriamo che  $K \leq_{\text{rec}} I$ : definiamo

$$\psi(x, y) := \begin{cases} 1, & \text{se } x \in K \text{ e } y = 3 \\ \perp, & \text{altrimenti.} \end{cases}$$

Per la Tesi di Church-Turing insieme al [Teorema del Parametro](#) e all'[OSSERVAZIONE 1.6.2](#) esiste una funzione  $f$  calcolabile totale tale che  $\varphi_{f(x)}(y) = \psi(x, y)$ .

Allora  $K \leq_f I$ : in effetti

- se  $x \in K$  allora  $\varphi_{f(x)}$  vale 1 quando l'input è 3 ed è indefinita altrimenti, dunque  $\text{dom}(\varphi_{f(x)}) = \{3\}$ , ovvero  $f(x)$  appartiene ad  $I$ ;
- se  $x \notin K$  allora  $\varphi_{f(x)}$  è sempre indefinita e dunque ha dominio vuoto, ovvero  $f(x)$  non appartiene a  $I$ .

Segue quindi che  $I$  non è ricorsivo.  $\square$