

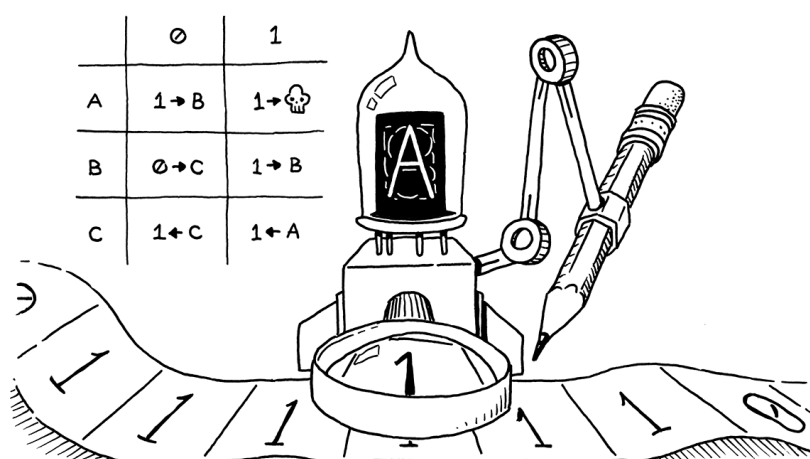
UNIVERSITÀ DEGLI STUDI DI TRIESTE

---

*Marco Sgobino*

Dispense del corso di

# COMPLESSITÀ E CRITTOGRAFIA



---

*Anno Accademico 2021-2022*



# Indice

<b>1</b>	<b>La macchina di Turing</b>	<b>5</b>
1.1	Descrizione . . . . .	5
1.2	Uso di una macchina di Turing . . . . .	7
1.3	Equivalenza fra macchina di Turing e $\mathcal{R}$ . . . . .	8
1.4	Potenziamento apparente della macchina di Turing . . . . .	9
1.5	Macchina RAM per <i>accettare</i> stringhe . . . . .	13
<b>2</b>	<b>Le macchine non deterministiche</b>	<b>17</b>
2.1	Alcune definizioni sulle stringhe . . . . .	18
2.2	Gerarchie delle potenze di calcolo . . . . .	18
2.3	La macchina di Turing non deterministica . . . . .	18
2.3.1	Equivalenza fra macchine non deterministiche e macchine multinastro . . . . .	20
<b>3</b>	<b>Le reti neurali di Hopfield</b>	<b>23</b>
3.1	Il neurone reale ed il neurone simulato . . . . .	25



# Capitolo 1

## La macchina di Turing

### 1.1 Descrizione

TODO rifai tutti i disegni presi dall'insegnante.

Una *macchina di Turing* è una macchina che è descritta da un insieme di *simboli*  $\Gamma = \{\alpha, \beta, \gamma, \delta, \dots\}$  *finito* e da un insieme di *stati*  $Q = \{q_1, q_2, \dots, q_n\}$  anch'esso *finito*. La macchina di Turing dispone di un nastro di memoria *potenzialmente illimitato* a destra e a sinistra; essa è in grado di identificare il simbolo nella posizione dove la *testina* della macchina è collocata sul nastro. Ad ogni iterazione della macchina di Turing, viene letto il simbolo ove sia collocata la sua testina; a seconda dello stato  $q_i$ , viene intrapresa un'azione, che può essere una fra le 3 seguenti:

- spostamento della testina a destra;
- spostamento della testina a sinistra;
- riscrittura del simbolo sotto la testina con uno qualsiasi appartenente all'alfabeto di simboli.

Una macchina di Turing può anche essere accompagnato da un alfabeto *ausiliario*, ovvero sia un alfabeto  $\mathcal{V}$  comprendente simboli simili a quelli di  $\Gamma$ , ma che vengono utilizzati qualora la macchina di Turing avesse *già processato* la cella in questione. Tipicamente, l'utilizzo dell'alfabeto ausiliario è importante nel caso specifico in cui si adoperino algoritmi e procedure per le quali è

d'interesse ricordare se una cella sia già stata in precedenza processata dalla macchina di Turing, oppure no.

Nello specifico, una macchina di Turing è univocamente identificata dalla sua *matrice di transizione*  $\delta : Q \times \Gamma \rightarrow Q \times (\Gamma \cup \{L, R\})^1$ , dove i simboli  $L$  ed  $R$  sono rappresentativi dell'azione di spostarsi, rispettivamente, a sinistra e a destra del nastro di memoria. La matrice di transizione lega, dunque, ciascuno stato al simbolo collocato immediatamente sotto alla testina nel nastro di memoria, stabilendo in maniera univoca l'azione da intraprendere. L'insieme delle azioni che la macchina di Turing compie è quindi la realizzazione del programma stesso.

	$q_1$	$q_2$	$\cdots$	$q_n$
$\alpha$	$\beta/q_2$	$\gamma/q_2$	$\cdots$	
$\beta$	$L/q_1$	$\gamma/q_3$	$\cdots$	
$\gamma$	$\gamma/q_3$	$R/q_2$	$\cdots$	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	

Tabella 1.1: Possibile matrice di transizione per una macchina di Turing. Le righe corrispondono ai simboli dell'alfabeto  $\Gamma$ , mentre le colonne sono corrispondenti ai singoli stati dell'insieme  $Q$ .

Diversamente dal modello RAM, la quantità di memoria destinata ad ogni cella è *limitata*, poiché vi può essere collocato soltanto un numero finito di simboli, quelli appunto dell'insieme  $\Gamma$ . Ciononostante, la macchina di Turing si presta meglio alla trattazione di stringhe, poiché i simboli possono rappresentare qualsivoglia tipologia di entità astratta, mentre per il modello RAM si avrebbe necessità di una codifica fra numeri reali e simboli da trattare: non vi è più dunque la limitazione imposta dal fatto che all'interno di una cella possa risiedere esclusivamente un numero naturale, non importa quanto grande sia; nella macchina di Turing le celle possono contenere simboli di qualsiasi natura essi siano.

<sup>1</sup>In talune circostanze, è possibile trovare una definizione differente, cioè

$$\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\};$$

in altre parole, è una macchina che *si muove sempre sul nastro*, poiché per ogni stato è sempre definito un movimento. Per questo tipo di macchina, sono necessarie diverse regole d'ingaggio, e i programmi in essa costruiti saranno radicalmente differenti. La differenza fra i due modelli rappresenta un'evidenza della versatilità della macchina di Turing.

Tipicamente, all'alfabeto che definisce una macchina di Turing viene definito un sottoinsieme sigma di simboli di input,  $\Sigma \subset \Gamma$ , in concomitanza al quale viene definito un simbolo vuoto, *blank*,  $b \in \Gamma - \Sigma$ . Il simbolo  $b$  rappresenta dunque l'idea di *cella vuota*. Ricapitolando, ogni macchina di Turing viene univocamente definita da:

- un insieme finito di simboli  $\Gamma$  – essi comprendono sia i simboli di input  $\Sigma$  che il simbolo *blank*  $b$ ;
- un insieme finito di stati  $Q$ ;
- una funzione (matrice) di transizione  $\delta : Q \times \Gamma \rightarrow Q \times (\Gamma \cup \{L, R\})$ .

Una diversa maniera per definire una macchina di Turing è tramite la *quaterna* o *quadrupla*  $q_i, s_j, \alpha, q_k$ , dove  $q_i$  è lo stato in cui si trova la macchina,  $s_j$  è il simbolo letto dalla testina,  $\alpha$  è il simbolo scritto nella matrice di transizione,  $q_k$  è lo stato successivo in cui la macchina di Turing si troverà al termine dell'esecuzione di  $\alpha$ . In particolare, l'operazione che la macchina di Turing effettua dipende dal simbolo  $\alpha$  scritto nella matrice di transizione:

- se  $\alpha = s_i$ , sostituisci il simbolo  $s_j$  con  $s_i$ ;
- se  $\alpha = R$ , muovi la testina a destra;
- se  $\alpha = L$ , muovi la testina a sinistra;

Lo stop della computazione di una macchina di Turing avviene qualora la coppia  $q_i, s_j$  **non** sia presente nella matrice di transizione. Questa tecnica è analoga a quanto osservato per il modello RAM, nel quale la macchina ha termine se si è giunti al termine della procedura e sono state esaurite le istruzioni nella sequenza. Nel caso di una coppia simbolo—stato non presente nella matrice di transizione, la macchina di Turing si fermerà, e vi sarà il riconoscimento del valore finale di computazione, espresso come nel caso del modello RAM con una convenzione che permetta di identificare il valore finale del risultato della computazione.

## 1.2 Uso di una macchina di Turing

Una macchina di Turing, come verrà illustrato in seguito, può essere espressa anche mediante *grafo* oltre che mediante matrice di sostituzione. In ogni caso, ogni possibile definizione di macchina di Turing è del tutto equiva-

lente, e varia esclusivamente nella forma nella quale è proposta. Una macchina di Turing, non importa come sia stata definita, può essere adoperata sostanzialmente per compiere 3 diversi operazioni:

1. per il *calcolo* di una funzione – la macchina di Turing è intesa come *calcolatore*, e lo scopo è quello di calcolare una funzione  $f : \mathbb{N}^n \rightarrow \mathbb{N}$ . In questo caso, la macchina di Turing risulta essere meno efficiente del modello RAM, per via dell'assenza del comodo sistema di istruzioni presente in quest ultimo;
2. per il *riconoscimento* di una stringa – la macchina di Turing è intesa come *accettore*. In questo contesto la MdT è molto più efficiente del modello RAM, poiché non è richiesta la codifica da numeri naturali a simboli;
3. per la *decisione* di un predicato – la macchina di Turing è intesa come *decisore*.

Convenzionalmente, l'esito di una macchina di Turing è una particolare configurazione di memoria dello stato finale. In particolare, si è scelto che il risultato  $f(x)$  sia da leggersi come il numero totale di occorrenze di 1 (meno una) sul nastro nella configurazione iniziale, se la computazione è andata a convergenza - indefinito altrimenti. La sequenza di occorrenze del simbolo 1 è delimitata dal carattere *blank*. Per quanto invece riguarda i risultati di tipo *vettoriale*, cioè del tipo  $f(x_1, x_2, \dots, x_n)$ , ebbene sarà sufficiente costruire  $n$  “quadrati” in cui racchiudere gli  $x + 1$  simboli 1, ciascuno delimitato dal simbolo  $b$ . In altre parole, la situazione è quella descritta dalla Figura ??.

TODO figura mdtRisultato

Solitamente, è particolarmente difficile programmare sulla macchina di Turing - questo è principalmente dovuto al fatto che la macchina di Turing è una macchina a stati, dove non vi è un insieme di istruzioni da applicare direttamente, ma bisogna determinare la matrice di transizione relativa a ciò che bisogna calcolare, stato per stato e simbolo per simbolo.

### 1.3 Equivalenza fra macchina di Turing e $\mathcal{R}$

Un importante teorema definisce l'equivalenza della macchina di Turing (avente insieme delle funzioni computabili  $\mathcal{TC}$  all'insieme delle funzioni



parziali ricorsive  $\mathcal{R}$ , e lo lega indissolubilmente all'insieme delle funzioni computabili dal modello RAM  $C$ .

**Teorema 1** *dell'equivalenza della macchina di Turing all'insieme  $\mathcal{R}$*

$$\mathcal{R} \equiv \mathcal{TC} \equiv C$$

Un possibile spunto di dimostrazione di  $\mathcal{TC} \subseteq \mathcal{R}$  si ha per il fatto che la configurazione e lo stato della MdT durante la computazione possono essere codificati da un numero naturale; le operazioni sulla macchina sono rappresentate da funzioni ricorsive su questi numeri. Il viceversa è invece mostrabile tenendo conto che si può verificare che  $\mathcal{TC}$  contiene le funzioni di base ed è chiusa rispetto a sostituzione, ricorsione e minimazione illimitata.

## 1.4 Potenziamento apparente della macchina di Turing

Una macchina di Turing può essere potenziata mediante l'estensione di essa tramite l'uso di *nastri multitraccia*. In altre parole, anziché adoperare un singolo nastro, si adoperano più nastri contemporaneamente. La macchina di Turing viene espansa tramite l'aggiunta di uno *stato della memoria supplementiva*, che sostanzialmente ci indica il numero del nastro dove la macchina di Turing sta agendo. Dunque, ci possiamo immaginare una macchina di Turing con tanti nastri e tante testine che lavorano contemporaneamente, come elencato in Figura 1.1.

Dal punto di vista della capacità computazione, una macchina di Turing multinastro non aumenta né diminuisce le capacità - tuttavia, tale rappresentazione può avere il vantaggio di presentare una maggiore somiglianza con il tipo di computazione svolto all'interno di un computer moderno. Si pensi infatti alla memoria RAM, alla memoria cache, al disco rigido e così via; una macchina di Turing può dunque “simulare” qualsiasi computer moderno<sup>2</sup>.

Una macchina di Turing multinastro deve essere implementata con un *sistema multitraccia* - in altre parole, vengono adoperate *tante testine quante sono*

<sup>2</sup>Un computer può a sua volta simulare da una macchina di Turing, dal momento che possono essere applicati potenzialmente infiniti banchi di memoria al computer - nella pratica, tuttavia, sappiamo che ciò non è possibile, e i banchi di memoria non saranno mai del tutto *illimitati*

*i nastri*. Ci si può facilmente ricondurre alla macchina di Turing convenzionale semplicemente eliminando il sistema multitraccia, o per meglio dire, una macchina di Turing multitraccia può essere *simulata* da una macchina di Turing convenzionale: essa dunque, non produce alcun tipo di miglioramento dal punto di vista computazione, cioè le due macchine hanno la *stessa* potenza computazionale (Figura 1.2).

Il medesimo discorso si applica anche al tentativo di *menomare* la macchina di Turing, nel senso che potremmo pensare di rendere il nastro semi-infinito, cioè illimitato solo a destra o solo a sinistra (Figura 1.3). In tal caso, tuttavia, benché questa apparente limitazione venga messa in atto, di fatto la macchina di Turing menomata avrà la medesima capacità computazionale di quella “standard”, perché possiamo sempre avere a disposizione una quantità illimitata di memoria, o far uso di trucchi come quello dell’alfabeto ausiliario  $\mathcal{V}$ .

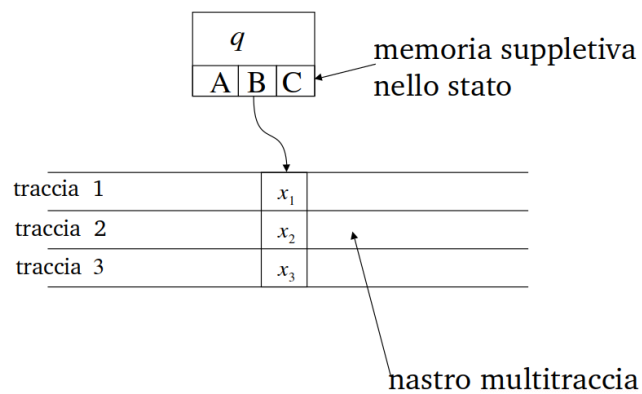


Figura 1.1: Macchina con memoria con nastro multitraccia.

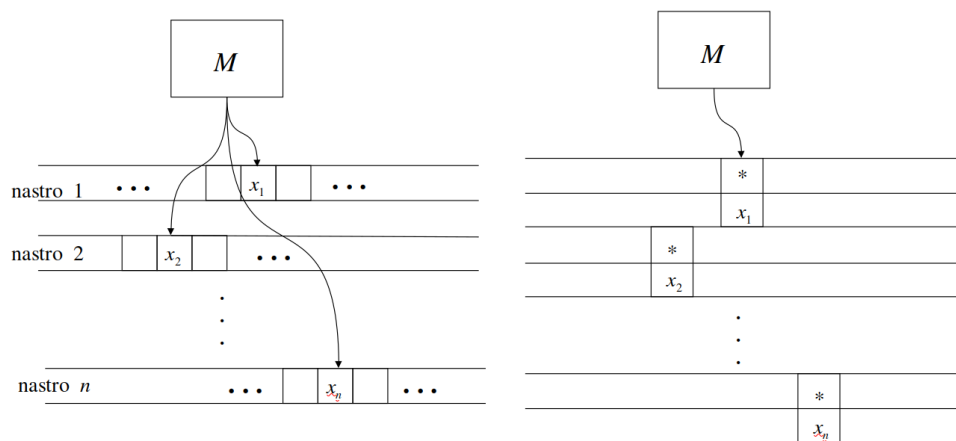


Figura 1.2: Equivalenza fra una macchina di Turing a multitraccia e una macchina di Turing a singola testina.

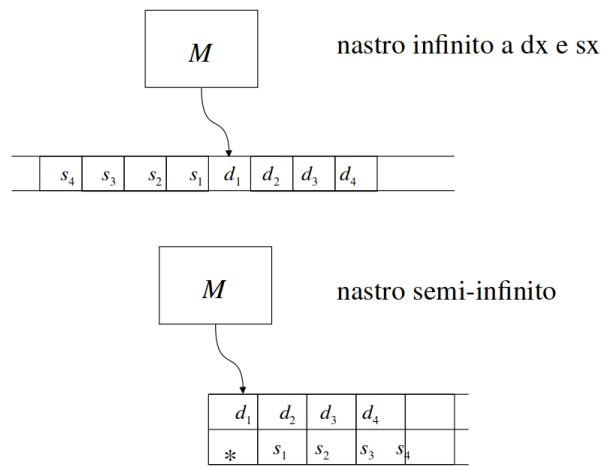


Figura 1.3: Equivalenza fra macchina di Turing a nastro illimitato solo a destra e a nastro illimitato da ambedue le parti.

## 1.5 Macchina RAM per *accettare* stringhe

Nel modello RAM, per accettare una stringa è necessario operare una codifica. In particolare, la stringa viene codificata in un numero naturale e la macchina risponde con “1” o “0” a seconda che la stringa venga o meno accettata. Con la macchina di Turing, invece, si può far intervenire direttamente uno *stato di accettazione* ACCETTAZIONE  $q_Y$  o uno *stato di rifiuto* RIFIUTO  $q_N$ . Un'altra possibilità è quella di semi-decidere riguardo l'accettazione di una stringa, cioè una macchina in grado di riconoscere la stringa in questione, ma di non poter rifiutare la stringa, poiché ci sarebbe un'infinita computazione, e dunque divergenza. Tipicamente, lo stato iniziale viene denotato con  $q_0$ , e potrebbero esserci degli stati ulteriori “intermedi”. Un esempio di accettazione è dato dalla macchina illustrata in Figura 1.4. La macchina riconosce il linguaggio dato dalle stringhe con due “zeri” nelle ultime due posizioni a destra, in particolare tutte le stringhe che terminano con “00”.

TODO aggiungi mdt definita a grafo

Una macchina di Turing può anche essere “definita a grafo”. In questo modello di definizione, la macchina di Turing,

- ha un *nastro semi-illimitato* a destra, diviso in celle;
- ha un alfabeto *ausiliario*  $\mathcal{V}$ ;
- ha un simbolo di spaziatura  $\Delta$ , equivalente al simbolo *blank*  $b$ ;
- un puntatore, del tutto equivalente alla testina;
- un *programma*, definito come **grafo finito orientato**, con i vertici definiti come *stato*. Vi è uno stato di inizio, indicato con INIZIO, e un sottoinsieme eventualmente vuoto di stati di arresto, indicati con ACCETTAZIONE. I nodi del grafo sono collegati da *archi*.

Ciascun arco è della forma

TODO rifai

(i) ---( $\alpha$ ,  $\beta$ ,  $\gamma$ ) ---> (j)

dove

$$\alpha \in \Sigma \cup \mathcal{V} \cup \{\Delta\}, \beta \in \Sigma \cup \mathcal{V} \cup \{\Delta\} \text{ e } \gamma \in \{L, R\}.$$

Dunque, siamo nello stato  $i$ ; la macchina legge  $\alpha$ , scrive  $\beta$  al posto di  $\alpha$ , e infine va a destra oppure a sinistra a seconda che il simbolo  $\gamma$  sia pari ad  $R$  o ad  $L$ .

TODO aggiungi esempio lettura stringa speciale

Tale problema espresso qui sopra (add figure) è molto noto nella teoria della computabilità, poiché è un tipico esempio di problema che è risolubile da una macchina di Turing, ma **non risolubile** mediante una macchina *a stati finiti*. Le macchine a stati finiti, infatti, non presentano alcun tipo di *memoria*, e dunque per questa particolare mancanza non sono in grado di risolvere il problema. La macchina di Turing, invece, è in grado di risolverlo in virtù della sua superiore potenza di computazione.

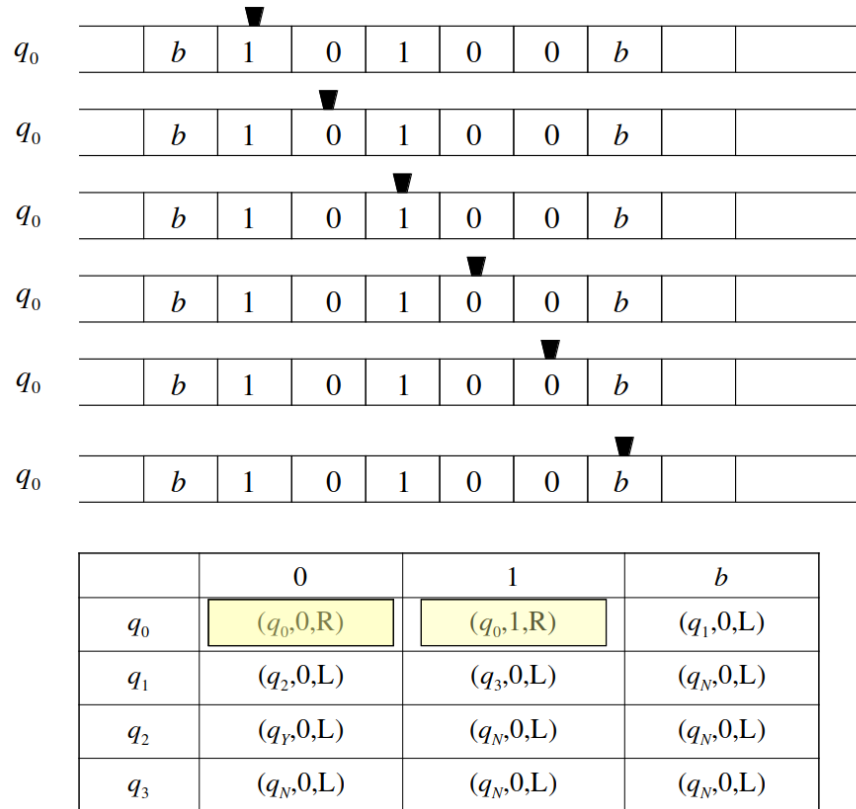


Figura 1.4: Macchina che riconosce il linguaggio dato dalle stringhe con due 0 nelle ultime due posizioni a destra, e suo funzionamento.





## Capitolo 2

# Le macchine non deterministiche

Oltre alla macchina di Turing, sono possibili altre tipologie di macchine, con vari livelli di gerarchia fra potenze di calcolo. Il seguente elenco ne illustra alcune,

- macchine a *stati finiti*: in questo caso, hanno 0 *memorie push-down* - le macchine a stati finiti sono le meno potenti in assoluto dal punto di vista computazionale, e non sono in grado di risolvere il problema *TODO* add figure del riconoscimento di stringhe  $a^n b^n$ ;
- macchine a 1 *memoria push-down*: dotata di una memoria push-down, ha una maggiore potenza di calcolo rispetto alla macchina a stati finiti;
- macchine a 2 *memorie push-down*: dotata di 2 memorie push-down, essa è equivalente alla macchina di Turing.
- una macchina con 3 o più pile push-down non fornisce vantaggi dal livello della potenza computazionale, e sono tutte Turing-equivalenti - il vantaggio è semmai nella semplificazione di calcoli fornita dall'introduzione della pila aggiuntiva.

## 2.1 Alcune definizioni sulle stringhe

Sia dato l'alfabeto  $\Sigma^*$ . Faremo uso di tre fondamentali funzioni definite su  $\Sigma^*$ :

- l'operazione  $\text{testa}(x)$ , che fornisce la “testa” di una stringa, ovverosia la lettera di estrema sinistra della parola  $x$ ;
- l'operazione  $\text{coda}(x)$ , la quale invece fornisce la “coda” di una stringa, o la stringa privata della sua testa  $x$ ;
- l'operazione  $\sigma \cdot x$ , che *concatena* la lettera  $\sigma$  e la parola  $x$ , per formare un'unica parola nuova.

## 2.2 Gerarchie delle potenze di calcolo

La gerarchia delle potenze di calcolo è la seguente, dall'alto verso il basso:

1. Macchine non deterministiche di Turing, con due memorie push-down — Macchine di Turing, Modello RAM, Macchine di Post, macchine finite con due memorie push-down (sono in grado di accettare  $\{a^n b^n a^n | n \geq 0\}$ ). Si potrebbe dimostrare che le macchine di Turing deterministiche e non deterministiche hanno la medesima potenza di calcolo;
2. Macchine finite non deterministiche con una memoria push-down, sono in grado di riconoscere  $\{ww^R | w \in \{a, b\}^*\}$ <sup>1</sup>;
3. macchine finite con una memoria push-down, riconoscono  $\{a^n b^n | n \geq 0\}$ ;
4. Macchine finite non deterministiche senza memorie push-down — macchine finite senza memorie push-down — automi finiti.

## 2.3 La macchina di Turing non deterministica

La macchina di Turing effettiva è di tipo *deterministico*. Il *non determinismo* viene introdotto per due ragioni:

---

<sup>1</sup>Il *nodo di decisione* che introduce il non determinismo serve per gestire la situazione data dall'incapacità di riconoscere il punto di rottura  $ww^R$ , cioè il punto in cui finisce  $w$  ed inizia  $w^R$ . Con il non determinismo, ogniqualvolta si arriva al nodo di decisione si tengono valide entrambe le possibilità - dunque, è più potente.

- si desidera osservare se una macchina di Turing non deterministica sia o meno più *potente* di una macchina di Turing deterministica;
- si cerca di valutare se possano esistere differenti paradigmi di computazione (ad esempio, computazione parallela).

Una *macchina di Turing non deterministica* può avere nel suo diagramma di flusso dei *nodi di decisione* del tipo seguente, TODO add figure

ovverosia dei nodi dove a fronte di un medesimo simbolo vi sono *più archi possibili* - il non determinismo viene dunque introdotto da questo fenomeno: una macchina di Turing non deterministica può scegliere il suo percorso con una legge non deterministica, ma semmai dettata dal caso o da una *scelta arbitraria*. Una macchina non deterministica accetta l'idea che vi siano più possibilità di sviluppo di una computazione a fronte di un medesimo simbolo identificato sul nastro e stato; sono dunque possibili diversi percorsi di computazione. Questo tipo di macchina, ad esempio, potrebbe concepire il *parallelismo* nella computazione, nel senso che più possibilità e percorsi nel calcolo sono possibili. Questa potenzialità, apparentemente migliorativa, **non aumenta** la potenza di calcolo della macchina di Turing. Una macchina di Turing deterministica può, infatti, simulare una macchina non deterministica, è sufficiente compiere una ricerca per ogni diramazione dell'albero dei nodi - con un aumento esponenziale del numero di operazioni da effettuare, ma pur sempre realizzabile e computabile da una macchina di Turing. Una macchina non deterministica ha dunque il potenziale vantaggio di poter risolvere problemi in *tempo lineare* che dalla macchina deterministica sarebbero risolti in tempo esponenziale.

In questo caso, il parallelismo è insito nella macchina non deterministica, e la stringa si considera *accettata* qualora uno qualunque fra i percorsi possibili incappa nello stato di ACCETTAZIONE. Una parola  $w \in \Sigma^*$  si dice *accettata* da una macchina di Turing non deterministica se esiste una computazione della macchina  $M$  che cominci con entrata  $x = w$ , e che termini ad un arresto con lo stato di ACCETTAZIONE. Se  $w$  non viene accettata e lo stato di arresto è quello del RIFIUTO, allora si dice che  $w$  è *rifiutata*. In alternativa, siamo di fronte ad un ciclo  $w \in \text{ciclo}(M)$ .

In altre parole, possiamo pensare ad una macchina di Turing non deterministica come ad una macchina avente per ogni cella, nella matrice di transizione, un *insieme*  $\delta(q, s)$  di triple  $q_i, s_i, \alpha_i$ , dove  $\alpha_i \in \{L, R\}$  e ad ogni elemento

dell'insieme corrisponde una possibile scelta da compiere arbitrariamente o casualmente, e dunque da lì è ottenuto il non determinismo della macchina. Ogni possibile scelta genererà un diverso ramo nell'albero della computazione - per l'accettazione di un simbolo è sufficiente che uno *qualsiasi* fra i rami di computazione termini nello stato di ACCETTAZIONE. Dunque, benché una macchina di Turing non deterministica non **aumenti** la potenza di calcolo intrinseca della macchina, essa consente la **parallelizzazione** dei possibili percorsi della computazione, rendendo di fatto possibile risolvere in tempo lineare problemi che sarebbero risolubili (comunque), ma in tempo esponenziale per una macchina deterministica.

### 2.3.1 Equivalenza fra macchine non deterministiche e macchine multinastro

**Teorema 2** *Ogni macchina di Turing non deterministica ha un equivalente macchina di Turing deterministica multinastro.*

DIMOSTRAZIONE — Una traccia della dimostrazione è una ricerca nell'albero di computazione. Con almeno due nastri, si simula con uno la macchina non deterministica mentre con l'altro si collezionano tutti i possibili  $k$  “prossimi passi” della tabella di transizione. La macchina di Turing deterministica allora controllerà tutte le configurazioni stato—simbolo, livello per livello, dell'albero di computazione. Lo stato finale di ACCETTAZIONE terminerà la computazione complessiva.

L'idea è quella, dunque, di *simulare* il non determinismo compiendo un numero crescente in modo esponenziale di passi, uno per ogni ramo dell'albero non deterministico di computazione.

**Teorema 3** *Ogni macchina di Turing non deterministica  $T_M(n)$  ha un equivalente macchina di Turing deterministica con ordine  $2^{O(T_M(n))}$ .*

DIMOSTRAZIONE — Una traccia può essere che il numero massimo di foglie è  $O(b^{T_M(n)})$ , dove  $b$  è il numero di figli. Il tempo per viaggiare dalla radice lungo ogni ramo è, per una macchina multinastro,

$$O(T_M(n)b^{T_M(n)}) = 2^{O(T_M(n))},$$

mentre per una macchina a nastro singolo

$$(2^{O(T_M(n))})^2 = 2^{O(2T_M(n))} = 2^{O(T_M(n))},$$

dunque l'ordine è lo stesso.

In altre parole, una macchina non deterministica è in grado di “evocare” un numero esponenziale ed arbitrariamente elevato di macchine di Turing deterministiche - tale funzionalità però è irrealizzabile, poiché corrisponderebbe a dotare la propria macchina di un numero arbitrario di unità di calcolo, ciascuna per ogni possibile passo della computazione, per farle lavorare in parallelo.



## Capitolo 3

# Le reti neurali di Hopfield

Le *reti neurali* incarnano un diverso paradigma rispetto a quello della computazione procedurale. Storicamente, esse prendono spunto dalla natura, in particolare dal concetto di *neurone*, inteso come singola unità di calcolo, dotata di input, di output e di una *funzione caratteristica*. Diversamente dall'idea della computazione procedurale, dove la *complessità* è definita tramite la complessità di tipo computazionale (o temporale), le reti neurali esprimono la loro complessità attraverso la **complessità strutturale**, o **complessità circuitale**. La computazione è di tipo *collettivo*, ed emerge come proprietà dell'*evoluzione dinamica* della rete. Ogni decisore locale, detto *neurone*, non ha visibilità della computazione globale, e svolge il proprio compito localmente — ogni decisore locale concorre alla soluzione globale in modo sfumato: la rete è **robusta** rispetto a malfunzionamenti locali.

Dal punto di vista strettamente logico, il paradigma di computazione a reti neurali è l'unico paradigma radicalmente differente da quello procedurale, mentre il paradigma *a DNA*<sup>1</sup> è una tipologia di calcolo che, nella realtà, non differisce sostanzialmente dal metodo procedurale.

Esistono due filoni di reti neurali; il primo associato ai **perceptron**, macchine a strati che fungono da riconoscitori di pattern e configurazioni. Le variabili di ingresso rappresentano un ente, una configurazione del sistema

---

<sup>1</sup>Trattasi di un paradigma di calcolo dove si va a cercare lo spazio delle soluzioni, e si eleggono quelle più “performanti” — talune soluzioni saranno la base dalla quale saranno definite le successive soluzioni, convergendo dunque alla soluzione. La potenza di questo metodo è quello di potersi permettere una ricerca esauriente della soluzione, poiché ciascun DNA è infinitesimamente piccolo, e dunque può essere esaminato in parallelo.

esterno, e il perceptron è in grado di fornire in output una risposta che consente di riconoscere tale configurazione o pattern in base a come essa sia stata configurata e ai suoi parametri. Il secondo filone, invece, è quello della *rete di Hopfield*; tale filone sarebbe in grado, in linea di principio, di **risolvere problemi**. Mediante una rete di Hopfield è possibile risolvere il *travelling salesman problem*, un problema presumibilmente intrattabile<sup>2</sup>.

Le reti neurali hanno avuto grande successo in 3 periodi storici:

- all'inizio degli anni 40 - nel 1948 fu fornito il primo modello di neurone e rete neurale. L'idea fu quella di avvalersi di una macchina fisica per simulare il comportamento dei neuroni naturali, presenti nel nostro cervello. All'epoca uscirono anche articoli su memorie a breve e lungo termine adoperando reti neurali;
- durante gli anni 80 - nei primi anni 80, Hopfield individuò un modello di reti neurali che associava le reti neurali ad un particolare modello matematico; qualità che prima era assente. Si tratta di una caratteristica fondamentale: quando si cerca di risolvere problemi con le reti neurali, l'assenza di teoremi (ad esempio, quelli asintotici) non ci permette di stabilire la *qualità* di una soluzione, oppure se la computazione andrà in qualche maniera a buon fine. Dunque, l'assenza di un buon apparato matematico che faccia da base alle reti neurali è il principale svantaggio di tale paradigma. Hopfield riuscì a fornire la soluzione di alcuni fra questi problemi matematici, suggerendo la possibilità di risolvere problemi, come ad esempio quello sopra citato del *travelling salesman problem*. Ci fu allora una corsa dal punto di vista scientifico riguardo la possibilità di risolvere in maniera efficiente i problemi presumibilmente intrattabili. Si può dimostrare, tuttavia, che la potenza di computazione di una macchina di Hopfield **non è superiore** alla capacità di computazione della macchina di Turing. Con una macchina di Hopfield non è dunque possibile risolvere in tempo polinomiale problemi che non sono risolubili in tale maniera già dalla macchina di Turing - vi è dunque l'*equivalenza* fra le due macchine. Le reti di Hopfield caddero pertanto ben presto in disuso;

---

<sup>2</sup>“Presumibilmente” si riferisce al fatto che, fino ad ora, nessuno è riuscito a dimostrare né che tale problema può essere risolto in tempo polinomiale, né che non può esserlo



- il terzo ed ultimo periodo d'oro delle reti neuronali è al giorno d'oggi, dove la potenza di calcolo superiore delle macchine moderne apre la strada ad un uso maggiormente ampio delle reti neuronali, che si avvalgono della pura potenza computazionale di gran lunga maggiore rispetto al passato per produrre risultati in tempo apprezzabile.

### 3.1 Il neurone reale ed il neurone simulato

Una macchina di Hopfield simula un neurone reale. Vi sono all'incirca  $10^{11}$  neuroni (dieci miliardi) nel cervello, i quali formano una rete neuronale di una complessità disarmante. Il cervello è in grado di svolgere una quantità di compiti enorme, in modo efficiente - il cervello dunque è la struttura più complessa che esista nell'universo noto. I segnali elettrici nel cervello si sviluppano nell'ambito dei *segnali continui* (benché vi siano degli *spike*), tuttavia il suo funzionamento si svolge nell'ambito dei *segnali discreti*; un neurone si "eccita" o si "rilassa", manifestando dunque un comportamento del tutto discreto da questo punto di vista.

TODO aggiungi figure neuroni, hopfield, e tutto il resto