

# Università di Trieste

## Laurea in ingegneria elettronica e informatica

Enrico Piccin - Corso di Algoritmi e Strutture dati - Prof. Andrea Sgarro  
Anno Accademico 2021/2022 - 2 Marzo 2022

### Indice

<b>1</b>	<b>Introduzione</b>	<b>2</b>
1.1	Architettura dei calcolatori . . . . .	6
1.2	Diagramma di flusso . . . . .	6
<b>2</b>	<b>Ordinamento (sorting)</b>	<b>7</b>
2.1	Bubble-Sort . . . . .	7
2.2	Insertion-sort . . . . .	8
2.3	Pseudocodice . . . . .	8
2.3.1	Assegnazione . . . . .	8
2.3.2	Condizione . . . . .	9
2.3.3	Ciclo for . . . . .	9
2.3.4	Ciclo while . . . . .	9
<b>3</b>	<b>Grafi</b>	<b>11</b>
<b>4</b>	<b>Algoritmi aritmetici</b>	<b>16</b>
4.1	Algoritmo di Euclide . . . . .	17
4.2	Notazione $O$ grande . . . . .	20
4.3	Funzioni di complessità . . . . .	22
4.4	Classi di complessità . . . . .	23

## 1 Introduzione

**Algoritmo** è una parola molto antica, non connessa all'utilizzo e all'invenzione del calcolatore. Alla base della teoria della computazione si pone il **Liber abaci** (tradotto "Libro della computazione"), scritto nel 1200 da Leonardo Bonacci, in contatto con la popolazione araba, in quanto mercante; egli è venuto a conoscenza della **numerazione araba**, introducendola in Occidente e spiegandola dettagliatamente all'interno del **Liber abaci**.

La numerazione araba è uno straordinario passo in avanti nella scienza, in quanto con essa viene introdotto il concetto di **notazione posizionale**, così come l'importanza del numero 0: i numeri non servono solamente per contare, come si pensava in precedenza, e per questo rinnegando il numero 0.

A Firenze, sempre negli stessi anni, ci fu una **protesta sindacale** contro l'innovazione tecnologica, contro questa nuova scoperta, facendo pressione affinché il governo abolisse il nuovo sistema di numerazione, in quanto avrebbe fatto perdere il posto di lavoro a tutti coloro che prima eseguivano difficili calcoli con la numerazione romana: tuttavia, tale proteste, com'è noto, possono rallentare il progresso, ma mai arrestarlo.

Leonardo Bonacci, nei suoi viaggi in Oriente, venne a conoscenza del **Liber abaci** di Al-Gorasmy, proveniente dalla Coresmia, ma che parlava persiano, da cui poi sarebbe stato tratto il nome **Algoritmo**, che letteralmente significa **procedimento di calcolo**.

### ALGORITMO

Algoritmo significa letteralmente **procedimento di calcolo**. Tuttavia, bisogna chiarire che un algoritmo è un procedimento di calcolo non necessariamente numerico, ma molto più generale, che va ben al di là dei numeri.

Un altro importante elemento che contraddistingue l'algoritmo è la **meccanicità**, ovvero la sua esecuzione può essere affidata ad una macchina: ciò significa che un algoritmo non deve necessariamente essere meccanizzato, ma deve essere **meccanizzabile**; in altre parole, l'esecuzione (bada bene, l'esecuzione e non la sua ideazione) dell'algoritmo è completamente **stupida**.

**Esempio 1:** L'algoritmo della moltiplicazione è molto chiaro e semplice: basta solamente accedere ad una **base di dati** in cui sono memorizzati i prodotti elementari fra numeri molto piccoli, e quindi molto più semplici da trattare.

Una volta eseguite le operazioni di moltiplicazione tramite quanto esposto in precedenza, è necessario eseguire delle operazioni di addizione, che era necessario aver precedentemente memorizzato. Ecco che quello che si è appena eseguito è un **procedimento di calcolo**.

**Esempio 2:** L'algoritmo della divisione fa sempre uso di una base di dati, nella quale devono essere memorizzati i risultati del prodotto del divisore con tutti i numeri decimali da 0 a 9 e confrontare ciascun prodotto con il termine da dividere per ottenere il quoziente.

Alternativamente, si sarebbe potuto creare un ciclo da 0 a 9 in cui per ogni indice si sarebbe dovuto verificare se questo fosse il fattore moltiplicativo corretto per ottenere la quantità giusta da sottrarre.

**Osservazione:** In ciascuno di tali esempi è essenziale la meccanicità del processo esecutivo, che appare evidente.

Quando si rappresentano delle quantità e, a maggior ragione, quando si effettuano dei calcoli, è fondamentale fissare una base di rappresentazione, da cui poi dipendono le cifre che si possono impiegare per la rappresentazione stessa.

La notazione posizionale permette anche di comprendere la rappresentazione di qualsiasi quantità con qualsiasi base, effettuando anche delle conversioni di base a seconda della maggiore o minore convenienza di rappresentazione.

Per esempio, volendo convertire una quantità rappresentata in base  $B = 7$  in una base  $C = 10$  si deve procedere come segue

$$(5203)_7 = 5 \cdot 7^3 + 2 \cdot 7^2 + 0 \cdot 7^1 + 3 \cdot 7^0 = 1715 + 98 + 0 + 3 = (1816)_{10}$$

Ovviamente le basi di rappresentazione sono almeno binarie, in quanto la **base unaria** non può, per ovvie ragioni, rappresentare alcuna quantità se non quella unica che viene permessa dalla base scelta, ossia lo 0.

Tuttavia, il processo inverso, atto a passare dalla rappresentazione di una quantità in base 10 ad una in base 3, non risulta essere così immediato.

Per cercare un algoritmo che permette di effettuare tale conversione, si effettua un primo **passaggio contointuitivo** (che suggerisce, tuttavia, il corretto processo esecutivo), che prevede di rappresentare una quantità in base 10 in una quantità ancora in base 10, tramite un processo di divisioni successive. Si consideri, a tal proposito

$$(3412)_{10}$$

e si divida progressivamente tale numero per 10, come segue

3412	10
341	2
34	1
3	4
0	3

Leggendo, ora, i resti, al contrario si ottiene il numero cercato all'inizio. Se ora si prova a considerare un'altra base, come 3, l'operazione porta ad un risultato analogo

3412	3
1137	1
379	0
126	1
42	0
14	0
4	2
1	1
0	1

Per cui si è ottenuto

$$(3412)_{10} = (11200101)_3$$

Scegliendo la base 2 si ottiene, per esempio

241	2
120	1
60	0
30	0
15	0
7	1
3	1
1	1
0	1

Per cui si è ottenuto

$$(241)_{10} = (11110001)_2$$

Ovviamente la lunghezza di rappresentazione in base 2 prevede un numero di cifre pari a circa il triplo di quelle impiegate per rappresentare la medesima quantità in base 10, proprio perché

$$\log_2(10) \cong 3.3$$

Per passare da base 10 a base 100, le operazioni sono molto semplici

$$(375712)_{10} = [(37)(57)(12)]_{100}$$

usando come simboli

$$(00), (01), \dots, (75), \dots, (99)$$

Si consideri, ora la base 8 e si scriva un numero binario in base ottale:

$$(010101010)_2 = [(010)(101)(010)]_8 = (252)_8$$

Ancora una volta, le cifre impiegate per la rappresentazione sono state ridotte ad un terzo, sempre perché

$$\log_2(8) = 3$$

E se ora si volesse impiegare la base 16 si otterrebbe:

$$(010101010)_2 = [(1010)(1010)]_{16} = (\text{AA})_{16}$$

**Osservazione:** Si consideri una lunghezza  $l = 5$ . Allora usando 5 cifre, non tutte nulle, in base 10, i numeri  $n$  che si possono rappresentare sono

$$10000 \leq n \leq 99999 \quad \equiv \quad 10^4 \leq n < 10^5 \quad \equiv \quad 10^{l-1} \leq n < 10^l$$

Da ciò si può estrapolare un risultato importante

$$\log_{10}(10^{l-1}) \leq \log_{10}(n) < \log_{10}(10^l) \quad \equiv \quad l - 1 \leq \log_{10}(n) < l$$

che è una relazione esatta. Tuttavia, approssimativamente, si può scrivere che

$$l_{10}(n) \cong \log_{10}(n)$$

3 Marzo 2022

Com'è noto, il matematico indiano **Ramanujan** ha affermato che la matematica esatta non rappresenta una base solida per la realtà, mentre la matematica vera è fatta di approssimazioni.

**Hardy** scoprì quanto fosse importante lo studio di **Ramanujan** e insieme a lui portò avanti la teoria dei numeri, una teoria **asintotica** che, come lui stesso affermava, non può essere esatta, ma fatta di approssimazioni.

Se, per esempio, si considera una quantità scritta in base 5, quale  $n = (412)_5$

$$(412)_5 = 4 \cdot 5^2 + 1 \cdot 5^1 + 2 \cdot 5^0 = (107)_{10}$$

Se, ora, si fissa una lunghezza  $l = 4$ , una lunghezza rigida, senza considerare zeri in testa, si può capire che con 4 cifre si possono rappresentare, in base 5 numeri  $n$  nell'intervallo

$$1000 \leq n < 10000$$

ovvero tale per cui

$$5^{l-1} \leq n < 5^l$$

e ciò funziona con qualsiasi base, per cui, in generale, fissata una lunghezza  $l$  e una base  $\mathcal{B}$  si ha che le quantità che possono essere rappresentate con  $l$  cifre, non tutte uguali a 0 è

$$\mathcal{B}^{l-1} \leq n < \mathcal{B}^l$$

Traducendo tale risultato tramite il logaritmo in base  $\mathcal{B}$ , sfruttando la crescenza in senso stretto della funzione logaritmica, si ottiene, equivalentemente

$$l - 1 \leq \log_{\mathcal{B}}(n) < l$$

in cui, ovviamente,

$$\log_{\mathcal{B}}(n) < l \leq \log_{\mathcal{B}}(n) + 1$$

che si può scrivere che

$$l_{\mathcal{B}}(n) \cong \log_{\mathcal{B}}(n)$$

Per cui l'**errore massimo** che si può commettere è di 1 cifra in base  $\mathcal{B}$ , nel caso peggiore, ma sarà sempre un po' maggiore del  $\log_{\mathcal{B}}(n)$ , per cui il logaritmo è una **sottostima della lunghezza**. Tuttavia, nello spirito di Hardy, sarà utile anche scrivere che la lunghezza binaria di  $n$  è circa uguale al logaritmo binario di  $n$ , ovvero

$$\log_{\mathcal{B}}(n) \cong \log_2(n)$$

in cui si può interpretare il  $\log_{\mathcal{B}}(n)$  come una **lunghezza analogica**, mentre  $l_{\mathcal{B}}(n)$  è una **lunghezza digitale**, in quanto **intera**, con precisione alla cifra (senza nulla in mezzo): in molti casi sarà più utile la lunghezza analogica di quella digitale, in quanto molto più precisa.

Grazie a questa formula è possibile capire facilmente come si alterano le lunghezze quando si effettua un cambiamento di base. Per esempio, si può osservare che

$$\log_2(10) \cong 3.38$$

per cui la lunghezza in base 2 è circa tre volte la lunghezza in base 10.

**Esempio:** Per trasformare un numero da base 10 in base 5 si deve procedere per divisioni successive per 5, considerando i resti (per questo si parla di *divisione intera*). Per esempio si ha che

$$10 \div 3 = 3 \text{ con resto di } 1$$

in cui, ovviamente, il resto  $r$  può essere

$$0 \leq r < D$$

con  $D$  divisore. Convertendo 32 da base 10 a base 5 ci si aspetta di ottenere un resto  $0 \leq r \leq 4$ .

## 1.1 Architettura dei calcolatori

Il calcolatore, naturalmente, si basa sulla logica binaria, ovvero opera impiegando la rappresentazione in base 2.

Il metodo più utilizzato per rappresentare caratteri diversi da quelli binari, tramite una codifica binaria, è il metodo ASCII (dall'inglese, American Standard Code For Information Interchange). Naturalmente, siccome la codifica tramite ASCII fa uso di soli 7 bit (sarebbero 8, ma un bit è riservato alla parità, per la rilevazione degli errori), il numero di  $n$ -uple binarie che si possono ottenere è  $2^7$ , un numero certamente irrisorio per la rappresentazione di tutti i caratteri alfanumerici necessari per la comunicazione multilingua.

In generale, fissata una lunghezza  $n$ , il numero di  $n$ -uple binarie distinte è, ovviamente,  $2^n$ , che rappresenta una crescita esponenziale, praticamente infinita, anche se, ovviamente, in teoria sono un numero ben limitato.

**Esempio:** Si consideri una macchina calcolatrice che considera delle istruzioni di 9 bit come di seguito esposto:

NOME ISTRUZIONE	ISTRUZIONE
ADD	010 $\times \times \times \times \times$
PUNCH	100 $\times \times \times \times \times$

Tabella 1: Tabella di istruzioni operative per un calcolatore

Naturalmente, tale linguaggio è **Assembly**, ovvero un linguaggio molto simile al linguaggio macchina, che risulta particolarmente complesso da impiegare per lo sviluppo di software.

## 1.2 Diagramma di flusso

Si consideri il seguente **flowchart**, o **diagramma di flusso**:

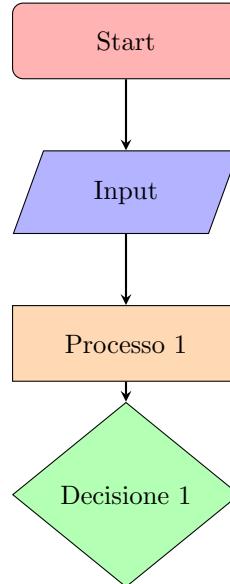


Figura 1: Diagramma di flusso

Tuttavia, tale tecnica di progettazione algoritmica è oramai superata, lasciando il posto allo **pseudocodice**, ossia un linguaggio di definizione delle istruzioni slegato da qualsiasi specifico linguaggio di programmazione di riferimento, che permette di esporre una serie di istruzioni esecutive molto simili a quelle di un programma vero e proprio.

## 2 Ordinamento (sorting)

Si espongono, di seguito, i principi di algoritmica dei più importanti algoritmi di ordinamento. Ciascuno di tali algoritmi prevede di effettuare l'ordinamento di  $n$  numeri forniti come input, in modo debolmente crescente, in caso di uguaglianza.

### 2.1 Bubble-Sort

Si espone di seguito l'algoritmo di ordinamento **bubble-sort** impiegando lo *pseudocodice*:

---

#### Algorithm 1 Bubble-sort

---

- 1: **do** the following  $n - 1$  times
  - 2:     *point* to the 1<sup>st</sup> element
  - 3:     **do** the following  $n - 1$  times
  - 4:         *compare* with next
  - 5:         **if** wrong order *exchange*
  - 6:         *point* to the next
- 

Naturalmente tale algoritmo è corretto e lo si può verificare immediatamente, considerando, per esempio, i seguenti 5 elementi, così ordinati:

2	3	1	4	5
---	---	---	---	---

Ovviamente il procedimento ci porta ad eseguire l'algoritmo 4 volte. Nella prima iterazione si ottiene

2	1	3	4	5
---	---	---	---	---

la seconda iterazione, invece, porta ad ottenere

1	2	3	4	5
---	---	---	---	---

mentre le ultime due iterazioni sono superflue. Si capisce facilmente che tale algoritmo non risulta essere pienamente efficiente, in quanto alcune iterazioni potrebbero essere evitate, tramite un **flag**, per esempio. Allo stato attuale, il numero delle iterazioni da eseguire è

$$\#\text{iterazioni} = (n - 1) \cdot (n - 1)$$

Se, invece, si facesse in modo di evitare alcune iterazioni si avrebbe un numero di iterazioni

$$(n - 1) \leq \#\text{iterazioni} \leq (n - 1)^2$$

considerando  $n - 1 \cong n$ , e quindi  $(n - 1)^2 \cong n^2$  si può dire che la complessità del bubble-sort è **quadratica**, in quanto il numero delle iterazioni è  $n^2$ .

4 Marzo 2022

L'algoritmo bubble-sort non viene utilizzato, ad oggi, così come non si impiega lo pseudocodice in *pseudo-english* (da leggere psude-english). Esso è funzionale, ma non efficiente, in quanto la sua complessità è  $n^2$ .

Ecco che per definire un algoritmo di ordinamento non è necessaria solamente la sua funzionalità, ma anche l'efficienza.

## 2.2 Insertion-sort

L'insertion-sort è un algoritmo di ordinamento che prevede di considerare ciascuna quantità da ordinare ad una ad una e di effettuare un confronto solo quando ci sono dei cambiamenti.

La prima quantità è ovviamente già in ordine con se stessa. Se la seconda è più piccola della prima, si effettua uno scambio, per cui ora i primi due numeri sono ordinati. Si considera, ora, il terzo numero e se questo è più piccolo del secondo si effettua uno scambio e un nuovo confronto tra la seconda e la prima e così via.

Pertanto si effettuano tutti i confronti solamente quando si ha uno scambio delle quantità: questo comporta che il minimo numero di iterazioni è  $n - 1$ , se  $n$  è il numero delle quantità da ordinare. Se, invece, tutte le quantità sono in disordine si effettua un numero di iterazioni pari

$$1 + 2 + \dots + (n - 2) + (n - 1) = \frac{n \cdot (n + 1)}{2}$$

una formula molto semplice che Gauss determinò come segue, ovverosia scrivendo la somma dei numeri da 1 a  $k$  in ordine crescente e poi decrescente, come mostrato di seguito:

$$\begin{array}{cccccccccc} 1 & + & 2 & + & 3 & + & \dots & + & k - 1 & + & k \\ k & + & k - 1 & + & k - 2 & + & \dots & + & 2 & + & 1 \end{array}$$

essendo  $k$  numeri in ambedue le righe, sommando i due termini corrispondenti, uno sotto l'altro, si ottiene sempre  $k + 1$  che, sommato per  $k$  volte produce  $k \cdot (k + 1)$ . Tuttavia, dal momento che tale quantità è il doppio di quella richiesta si ottiene

$$\frac{k \cdot (k + 1)}{2}$$

Pertanto si ha che il numero di iterazioni dell'algoritmo *insertion-sort* è

$$n \cong n - 1 \leq \#\text{iterazioni} \leq \frac{n \cdot (n - 1)}{2} \cong n^2$$

che, in maniera approssimata è

$$n \leq \#\text{iterazioni} \leq n^2$$

pertanto, nel caso migliore, la **complessità è lineare**, mentre nel caso peggiore, la **complessità è quadratica**.

## 2.3 Pseudocodice

Per la scrittura dello pseudocodice si devono impiegare delle notazioni e dei simboli ben specifici, che di seguito vengono riportati.

### 2.3.1 Assegnazione

L'**assegnazione** viene indicata con il simbolo  $=$  (oppure  $:=$  o  $\leftarrow$ ), anche se l'assegnazione non è un'uguaglianza. Per esempio, la notazione

$$A = 3$$

significa che nella cella di memoria  $A$  viene inserito il valore 3. Analogamente, se si scrive

$$A = A + 1$$

significa che il valore presente nella cella di memoria  $A$  viene incrementato di 1 unità.

### 2.3.2 Condizione

La specifica della **condizione** avviene tramite l'istruzione **if**, secondo la notazione seguente:

```
if  $C$  then
    istruzioni
else
    istruzioni
```

### 2.3.3 Ciclo for

Il **ciclo for** è un'istruzione di ciclo in cui vengono indicate specificatamente le iterazioni che devono essere eseguite, secondo la notazione seguente

```
for  $i = 0$  to  $n$  do
```

### 2.3.4 Ciclo while

Il **ciclo while** è un'istruzione di ciclo in cui si effettuano le istruzioni fintantoché la condizione specificata è vera

```
while  $C$  do
```

Si consideri lo pseudocodice dell'algoritmo **INSERTION-SORT(A)**, esposto di seguito, dove  $A$  sta ad indicare **array**, ovvero un record di  $\text{length}[A] = n$  valori da ordinare, già forniti in input. Di seguito si espone lo pseudocodice, in cui si parte da 1 come posizione iniziale dell'array:

---

#### Algorithm 2 Insertion-sort

---

```
1: for  $j = 2$  to  $\text{length}[A] = n$ 
2:   do  $key = A[j]$ 
3:   ...
4:    $i = j - 1$ 
5:   while  $i > 0 \wedge A[i] > key$ 
6:     do  $A[i + 1] = A[i]$ 
7:        $i = i - 1$ 
8:        $A[i + 1] = key$ 
```

---

Tale codice è concluso e il suo funzionamento può essere facilmente verificato come segue, considerando l'array  $A$  di lunghezza  $\text{length}[A] = 6$ :

5	2	4	6	1	3
---	---	---	---	---	---

Partendo con  $j = 2$  si fissa  $key = A[j] = 2$  e imponendo  $i = 1$ , si entra all'interno del ciclo *while*, in quanto  $i > 0$  e  $A[i] > key$  e si effettua l'istruzione  $A[i + 1] = A[i]$  e  $A[i + 1] = key$ , trovandosi nella configurazione seguente

2	5	4	6	1	3
---	---	---	---	---	---

Terminato il ciclo while e il ciclo for si procede con  $j = 3$  si fissa  $key = A[j] = 4$  e imponendo  $i = 2$ , si entra all'interno del ciclo *while*, in quanto  $i > 0$  e  $A[i] > key$  e si effettua l'istruzione  $A[i + 1] = A[i]$  e  $A[i + 1] = key$ , trovandosi nella configurazione seguente

2	4	5	6	1	3
---	---	---	---	---	---

Adesso, terminato il ciclo while e for, si considera  $j = 4$ , specificando  $key = A[j] = 6$  e  $i = 3$ . In questo caso, tuttavia, non si entra nel ciclo while, in quanto  $i > 0$ , ma  $A[i] < key$ . Si procede direttamente con  $j = 5$ ,  $key = A[j] = 1$  e  $i = 4$  e si entra nel ciclo while, compiendo tutte le iterazioni

2	4	5	1	6	3
2	4	1	5	6	3
2	1	4	5	6	3
1	2	4	5	6	3

e così via fino ad arrivare all'ordinamento finale

1	2	3	4	5	6
---	---	---	---	---	---

Ecco che, come si può vedere, tale algoritmo ha una complessità che, nel caso migliore, è **lineare** ( $n$ ) e nel caso peggiore è **quadratica** ( $n^2$ ).

Mentre si chiama **complessità tipica** la **complessità media**, ovvero la complessità dell'algoritmo nel caso intermedio. In questo caso la complessità tipica è  $n^2$ , che può essere calcolata, in maniera non propriamente corretta, come segue

$$\frac{n + n^2}{2} = n^2$$

Esiste, infine, anche una **complessità empirica**, basata sull'uso pratico dell'algoritmo: in particolare, l'algoritmo insertion-sort funziona particolarmente bene quando il **numero degli elementi da ordinare è ridicolmente basso**, il che potrebbe essere un controsenso; tuttavia, potrebbe essere particolarmente utile ricorrere all'ordinamento di pochi numeri all'interno di una procedura particolarmente complessa: ecco, allora, che l'utilizzo di insertion-sort diviene conveniente (cosa che non accade per bubble-sort).

**Osservazione:** È importante osservare che l'algoritmo di insertion-sort è un **algoritmo di ordinamento in loco**, ovvero tale per cui non si impiega un altro array per l'ordinamento, ma tutte le operazioni si effettuano sullo stesso array di partenza.

**Osservazione:** Quando si parla di algoritmica, non è possibile parlare di **completezza** senza parlare di **complessità**.

### 3 Grafi

Il **grafo** è una **struttura finita**. Gli elementi costituitivi di un grafo sono i **vertici** (o **nodi**) e gli **archi** (o **lati**) (dall'inglese *arcs* o *edges*). Per indicare i vertici si impiega la lettera  $v$ , mentre per indicare gli archi si usa la lettera  $\xi$ .

Un arco collega due vertici distinti che, per il momento, non è orientato, non rappresenta una freccia, in quanto si parla di **grafi semplici**, come illustrato di seguito:



Figura 2: Esempio di grafo semplice

Il calcolo della copertura dei vertici prende il nome di **vertex cover** e prevede di definire il numero minimo di vertici essenziali per coprire tutti gli archi. L'ottimizzazione del grafo, in questo caso, prevede di determinare la copertura minima.

Si supponga di avere a disposizione  $k$  vertici (che si indica come  $|v| = k$ , in cui  $|v|$  rappresenta la **cardinalità** dell'insieme dei vertici). Naturalmente, la copertura minima pari a 0 si ha quando i vertici del grafo sono tutti scollegati, ovvero non ci sono archi.

Il numero di archi in un grafo completo è pari a

$$\frac{|v| \cdot (|v| - 1)}{2}$$

per cui si potrebbe, in questo caso limite, affermare che la copertura minima sia  $k$ , ma se si elimina un nodo ancora la copertura sussiste, in quanto su ogni arco vi sarà sempre almeno un nodo coperto. Quindi si può affermare che la *vertex cover*, nel caso generale è compresa tra 0 e  $k - 1$ , con  $k$  numero dei vertici.

9 Marzo 2022

Il problema del **vertex cover**, ovvero di “ricoprimento dei vertici”, è un problema che riguarda la teoria dei grafi.

Gli elementi costitutivi di un grafo sono i **vertici** (o **nodi**, molto più raramente chiamati *punti*) e gli **archi** (dall’inglese *edges*, traducibili in **spigoli** o, più impropriamente, in *lati*), per il momento non orientati, che collegano due vertici, per il momento necessariamente distinti.

La notazione per indicare vertici e archi è la seguente

- L’insieme dei vertici si denota con  $v$
- L’insieme degli archi si denota con  $\xi$

Naturalmente, sussiste la possibilità che in un grafo tutti i vertici siano sconnessi ed **isolati**, ovvero il numero degli archi sia nullo, per cui si ottiene che  $|\xi| = 0$ .

Analogamente, volendo collegare tutti i nodi con un arco (ottenendo un **grafo completo**), si procede come segue: partendo da un primo vertice se ne collega un secondo, necessariamente distinto; ma non volendo considerare ogni arco due volte, si divide per due, ottenendo

$$\frac{|v| \cdot (|v| - 1)}{2} \cong |v|^2$$

da cui si evince che il numero degli archi, in un grafo, è compreso tra

$$0 \leq |\xi| \leq \frac{|v| \cdot (|v| - 1)}{2}$$

considerando  $|v|$  la cardinalità, ossia il numero dei vertici considerati che costituiscono il grafo.

Il problema di **vertex cover** è un problema di ottimizzazione: ridurre il numero minimo di vertici tale per cui nel grafo ad ogni arco deve essere collegato almeno un vertice coperto. Per esempio, in un grafo dove ogni nodo è isolato, il numero minimo dei vertici da coprire è 0, in quanto non ci sono archi. Nel caso di un **grafo completo**, come quello esposto di seguito

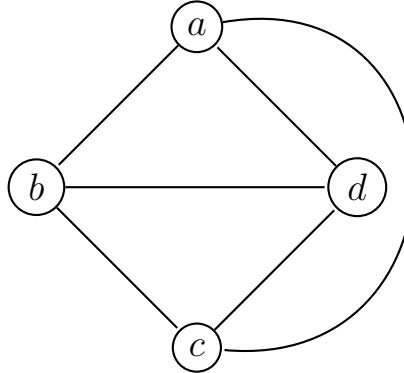


Figura 3: Esempio di grafo semplice completo

la copertura minima non è, come contrariamente si potrebbe pensare all’inizio, pari a  $|v|$ , in quanto eliminando uno qualsiasi dei nodi, ancora ad ogni arco sarà collegato almeno un nodo comperto. Pertanto si ha che il numero  $\#nodi$  dei nodi che si dovranno coprire al fine di risolvere il problema del vertex cover in un grafo avente  $|v|$  vertici sarà sempre compreso tra

$$0 \leq \#nodi \leq |v| - 1$$

Per la risoluzione meccanica del **vertex cover** vi sono due algoritmi, di cui solo il secondo realmente efficace. Si consideri, a titolo esemplificativo, il grafo seguente

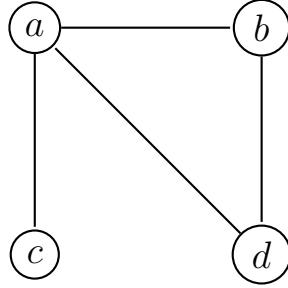


Figura 4: Esempio di grafo semplice

in cui, naturalmente, per coprire tutti gli archi sarà sufficiente considerare il vertice  $a$  e il vertice  $d$  (oppure il nodo  $b$ ), ottenendo, come possibile copertura

$a$	$b$	$c$	$d$
-----	-----	-----	-----

1	0	0	1
---	---	---	---

in cui con  $\boxed{1}$  si rappresenta la copertura del rispettivo vertice. Ecco che questa è una  $k$ -upla binaria di **peso**  $w = 1 + 1 = 2$ , in cui  $k = 4$ : usando tale notazione, quindi, un procedimento meccanico, atto a verificare la corretta copertura prevede di considerare tutti gli archi e verificare per ciascuno di essi che almeno ad un vertice collegato dall'arco in questione corrisponda un 1; se un arco è collegato a due vertici cui corrisponde 0, la copertura è scorretta, ovviamente.

Tuttavia, la  $k$ -upla 1001 è anche una codifica binaria su 4 bit del numero  $(9)_{10}$ , che suggerisce la procedura di controllo seguente, definita a partire da  $k$  numero di vertici

---

**Algorithm 3** Vertex-cover

---

```

1: for  $i = 0$  to  $2^k$ 
2:    $i \rightarrow$  binario
3:    $check(i)$ 

```

---

ove  $check(i)$  è una procedura che svolge il compito precedentemente esposto: presa in ingresso una  $k$ -upla binaria, cui si fa corrispondere la copertura di rispettivi vertici, verifica per ciascun arco che ad esso sia collegato un vertice effettivamente coperto, ovvero cui corrisponde un 1 nella  $k$ -upla binaria considerata; alla fine della procedura si ottiene la copertura di peso minore, ovvero quella con meno 1 e quindi che prevede meno vertici coperti.

Tale algoritmo non risulta propriamente efficiente; pertanto, al fine di eliminare alcune iterazioni, si potrebbe pensare di partire con il peso  $w$  ed effettuare il medesimo  $check$  per tutte  $n$ -uple di peso  $w$ , come mostrato di seguito:

---

**Algorithm 4** Vertex-cover

---

```

1: for  $w = 0$  to  $k - 1$ 
2:   for all

```

---

che è un procedimento più razionale, in quanto si controlla progressivamente se sono sufficienti un numero sempre maggiore di vertici da coprire (basta 1 vertice? Bastano 2 e così via...) e si esce dal ciclo quando si trova il primo, in quanto quella copertura sarà certamente la minima.

Da notare che si cicla fino a  $k - 1$  e non fino a  $k$ , in quanto è noto dalla teoria che il numero di vertici che si andranno a coprire per risolvere un qualsiasi problema di vertex-cover è sempre compreso tra 0 e  $k - 1$ , con  $k$  numero di vertici: ma l'unica  $n$ -upla con peso massimo è quella con tutti 1, la quale costituisce una sola configurazione tra le  $2^k$  possibili. Pertanto, nel caso peggiore, si potrebbe procedere ad effettuare un numero di iterazioni pari a  $2^k - 1$ , che non è molto dissimile dal caso precedente, in cui si facevano inevitabilmente  $2^k$  iterazioni.

Questo algoritmo, pertanto, pur essendo corretto, è ispirato al meccanismo dell'**exhaustive search** (dall'inglese, ricerca esauriente), che prevede di controllare tutti gli archi al fine di verificarne la

corretta copertura.

Il motivo per cui tale algoritmo è inutilizzabile è che presenta un numero di **iterazioni esponenziale** e, conseguentemente, una **complessità esponenziale**, la quale è intollerabile, dal momento che il numero delle iterazioni cresce esponenzialmente al variare dell'input.

Di seguito si espone, invece, un nuovo algoritmo che risolve il problema del **vertex cover**; alla base di tale algoritmo si pone la seguente idea: si considerino dapprima due nodi connessi da un arco e si eliminino tutti gli archi che incidono sul primo e sul secondo vertice e si proceda a considerare un nuovo arco che insiste su due nodi ancora non considerati e si eliminino tutti gli altri archi che incidono sui nodi stessi e così via, fino ad esaurire tutti gli archi a disposizione, tale che alla fine della procedura si ottiene un ricoprimento vero e proprio.

Come di consueto, nello pseudocodice esposto di seguito, l'input non viene specificato a priori, ma il numero delle iterazioni per specificare l'input è noto, ossia è pari a  $\cong |v| + |\xi|$ .

Lo pseudocodice è il seguente:

---

**Algorithm 5** Vertex-cover

---

```

1:  $C \leftarrow \emptyset$ 
2:  $E' \leftarrow \xi(\mathcal{G})$ 
3: while  $E' \neq \emptyset$ 
4:   do ...  $(u, v)$  in  $E'$ 
5:      $C \leftarrow C \cup \{u, v\}$ 
6:     delete incidenti
7: return  $C$ 
```

---

In cui  $C$  è un contenitore, inizialmente vuoto, all'interno del quale successivamente andranno inseriti i vertici necessari per la vertex cover. Invece,  $E'$  è un contenitore, inizialmente pieno, in quanto contiene tutti gli archi che dovranno essere esaminati/scartati. Dopodiché, fintantoché non ci sono più archi da analizzare, si considera un primo arco, designato con la notazione  $(u, v)$ , i cui due estremi, appunto  $u$  e  $v$  andranno ad essere inseriti all'interno di  $C$ , mentre verranno eliminati da  $E'$  tutti gli archi incidenti in  $u$  o in  $v$ , finché non si avranno più archi a disposizione.

Il numero di iterazioni in cui tale algoritmo si impegna è, approssimativamente, pari a  $|v| + |\xi|$ , ovvero si ha una **complessità lineare**: questa è un'ottima notizia, in quanto significa che tale algoritmo è velocissimo; l'unico problema è che esso è scorretto.

Si consideri, a titolo di esempio, il seguente grafo semplice:

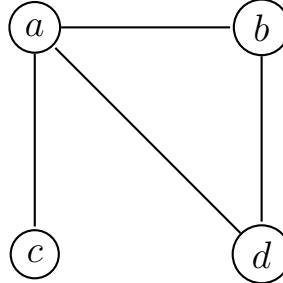


Figura 5: Esempio di scorrettezza dell'algoritmo considerato

In questo caso, l'algoritmo, considerando per primo l'arco  $a - b$ , elimina tutti gli altri archi e produce un risultato corretto.

Tuttavia, se il primo arco considerato dall'algoritmo fosse  $a - c$ , l'algoritmo è costretto a considerare anche l'arco  $b - d$ , non producendo un risultato corretto.

Tale algoritmo prende il nome di **algoritmo approssimato**, in quanto non sempre produce un risultato corretto, ma mai disastroso.

Tuttavia, non esiste un algoritmo che sia corretto e anche accettabile dal punto di vista del numero delle iterazioni e quindi della complessità: pertanto ci si deve accontentare dell'algoritmo approssimato appena esposto.

Per capire il range di risposta di tal algoritmo, si assuma che il numero di nodi ottimali necessari alla copertura sia  $|\mathcal{O}|$  e il numero dei nodi effettivamente ottenuti dalla procedura algoritmica sia

$|\mathcal{P}|$ , legati dalla seguente relazione, dimostrata con l'esempio precedente:

$$|\mathcal{O}| \leq |\mathcal{P}|$$

Naturalmente, per quanto visto con l'esempio precedente, tale disuguaglianza può anche essere stretta. Ovviamente, se ora si considerano gli archi privilegiati dall'algoritmo esposto, denotati con  $|\mathcal{A}|$ , ovverosia l'insieme degli archi che l'algoritmo ha via via considerato, esso, naturalmente, presenta la seguente cardinalità

$$|\mathcal{A}| = \frac{|\mathcal{P}|}{2}$$

in quanto su ogni arco vi sono due nodi ( $u$  e  $v$  nello pseudocodice), per cui basta considerarne la metà. Ora, il numero di nodi ottimale  $|\mathcal{O}|$  deve essere necessariamente almeno uguale al numero di archi privilegiati  $|\mathcal{A}|$ , dal momento che ciascuno di tali archi deve insistere almeno su un vertice coperto. Pertanto  $|\mathcal{O}|$  e  $|\mathcal{A}|$  sono legati dalla seguente relazione

$$|\mathcal{O}| \geq |\mathcal{A}|$$

per cui si ottiene che

$$\frac{|\mathcal{P}|}{2} \leq |\mathcal{O}| \leq |\mathcal{P}|$$

## 4 Algoritmi aritmetici

L'**algoritmo di Euclide** permette di calcolare il **Massimo Comune Divisore (M.C.D.)** tra due numeri, ma non procedendo alla fattorizzazione in fattori primi tra le due quantità considerate. Infatti, normalmente, per determinare l'M.C.D. tra due quantità è necessario procedere alla scomposizione delle due in fattori primi, come mostrato di seguito per i numeri 12 e 9:

$$12 = 3 \cdot 2 \cdot 2$$

$$9 = 3 \cdot 3$$

da cui si evince che

$$\text{MCD}(12, 9) = (12, 9) = 3$$

Tuttavia, non è possibile procedere attraverso la fattorizzazione per la risoluzione di tale problema, in quanto gli algoritmi per la fattorizzazione sono estremamente lenti. L'algoritmo di Euclide, invece, risolve tale problematica in maniera corretta, veloce ed efficiente, basandosi sul meccanismo della **ricorsività** e delle divisioni intere. Infatti, com'è noto, la divisione può essere di due tipologie

1. Divisione esatta:  $10 \div 3 = 3, \bar{3}$
2. Divisione intera:  $10 \div 3 = 3$  con resto 1

10 Marzo 2022

Naturalmente, un algoritmo non può essere applicato concretamente se ha una crescita esponenziale: esso è inutilizzabile, in quanto il tempo di risposta è troppo elevato per avere un impiego pratico.

L'esposto seguente, tratto da un lavoro di Gary & Johnson, ne dà una fondamentale prova pratica, considerando un calcolatore le cui istruzioni durano 0,000001 s per essere processate; naturalmente l'algoritmo considera input variabili, di lunghezza 10, 20, 30, 40, 50 e 60 e si suppone, per semplicità, che la lunghezza dell'input determini in modo quanto più preciso e linearmente dipendente il numero delle operazioni che devono essere eseguite: pertanto, se l'input ha lunghezza 60 significa che sono necessarie 60 operazioni per terminare l'algoritmo e quindi 0,00006 s sarà il tempo impiegato per l'esecuzione.

Se, invece, la complessità dell'algoritmo è quadratica, allora ciò significa che se l'input è di lunghezza 60, il numero di operazioni diviene  $60 \cdot 60 = 3600$  e quindi il numero di secondi diviene 0,0036 s.

Se la complessità è cubica, allora con lunghezza dell'input di 60 il numero di operazioni diviene  $60 \cdot 60 \cdot 60$  e quindi il tempo impiegato è di 0,216 s.

Con una complessità quintica, a 60 di lunghezza corrispondono  $60^5$  istruzioni e quindi 13 minuti di esecuzione.

Passando ad una complessità esponenziale, come  $2^n$ , con lunghezza dell'input pari a 60 si hanno  $2^{60}$  istruzioni e quindi un tempo esecutivo di 360 secoli. Passando appena a  $3^n$ , con lunghezza dell'input pari a 60 si hanno  $3^{60}$  istruzioni e quindi un tempo esecutivo di  $1,3 \cdot 10^{13}$  secoli.

**Osservazione:** Si osservi che considerare un calcolatore 1000 volte più veloce può essere significativo se la complessità dell'algoritmo è polinomiale, ma è totalmente ininfluente se la complessità è esponenziale.

## 4.1 Algoritmo di Euclide

Si consideri il seguente algoritmo, noto come **algoritmo di euclide**, estremamente fulmineo:

---

### Algorithm 6 Euclide

---

```
1: begin
2:    $a, b = m, n$ 
3:   while  $b \neq 0$  do  $a, b = b, a \text{ mod } b$ 
4:   mcd = a
5: end
```

---

In questo caso l'algoritmo considera come input **due numeri interi**  $m$  e  $n$  di cui ha senso determinare l'**m.c.d.**: pertanto essi devono essere necessariamente interi per ipotesi, in quanto nell'algoritmo non è previsto un controllo sintattico a monte. Generalmente si considerano  $m > n$ , ma ciò è ininfluente, in quanto il programma provvede ad effettuare un cambiamento del loro ordine in automatico.

Nell'algoritmo vi sono delle assegnazioni composte, in cui

$$a, b = m, n$$

ovvero ad  $a$  si assegna il valore  $m$ , mentre a  $b$  si assegna il valore  $n$ . Così come in seguito si ha

$$a, b = b, a \text{ mod } b$$

ovvero ad  $a$  si assegna il vecchio valore  $b$ , mentre a  $b$  si assegna il resto della divisione intera tra  $a$  e  $b$ . Alla fine del ciclo si ottiene che l'**m.c.d.** cercato è proprio  $a$ .

Si consideri, a tal proposito, il seguente esempio:

$$\begin{array}{|c|c|} \hline 12 & 9 \\ \hline a & b \\ \hline \end{array}$$

Dopo il primo passo si ottiene

$$\begin{array}{|c|c|} \hline 9 & 3 \\ \hline a & b \\ \hline \end{array}$$

ed infine

$$\begin{array}{|c|} \hline 3 \\ \hline a & b \\ \hline \end{array}$$

ecco che nella prima cella si ha proprio l'm.c.d. cercato. Ora, tuttavia, bisogna verificare se tale algoritmo sia effettivamente corretto e che quella considerata non sia solo una combinazione; inoltre, per determinare la complessità dell'algoritmo è necessario considerare, essenzialmente, il numero di **iterazioni libere** del ciclo while, in quanto la complessità dell'algoritmo dipende unicamente da tale fattore.

**Osservazione:** Si osservi, innanzitutto, che il ciclo while si chiude visto che in posizione  $b$  sarà presente un resto, ovvero una quantità intera che progressivamente diminuisce fino a diventare 0. L'ultimo passaggio, naturalmente, è il più semplice, in quanto l'algoritmo, prima dell'ultima iterazione, si ritroverà sempre nella situazione desiderata:

$$\boxed{\alpha \cdot \text{m.c.d.}} \quad \boxed{\text{m.c.d.}}$$

per cui nell'ultima iterazione, effettuando la divisione intera tra una quantità e un suo multiplo non si può che ottenere resto 0 e, quindi, nella cella  $a$  si ha proprio l'm.c.d. che si sta cercando, come mostrato di seguito:

$$\boxed{\text{m.c.d.}} \quad \boxed{0}$$

Per la dimostrazione della correttezza dell'algoritmo, anche nelle fasi intermedie, si deve dimostrare essenzialmente che, a qualunque fase del processo esecutivo

$$\text{M.C.D.}(a, b) = \text{M.C.D.}(b, a \bmod b)$$

ovvero che quello che si trova nelle celle  $a - b$  nell'istante  $t$  e ciò che si trova in  $a - b$  all'istante successivo hanno entrambi lo stesso massimo comune divisore: bisogna, di fatto, dimostrare quella che in matematica prende il nome di **invariante**; in questo caso l'invariante è proprio l'm.c.d. Infatti, le quantità che si trovano progressivamente nelle due celle hanno sempre lo stesso massimo comune divisore, a qualunque istante, fino ad arrivare alla configurazione finale in cui nella prima cella è presente un multiplo del valore della seconda cella.

Per dimostrare, quindi, l'invarianza seguente:

$$\text{M.C.D.}(a, b) = \text{M.C.D.}(b, a \bmod b)$$

si deve dimostrare che un diviore di  $(a, b)$  è anche divisore di  $(b, a \bmod b)$  e viceversa, per cui hanno lo stesso massimo comune divisore. Si supponga, allora, che  $\alpha$  divida sia  $a$  che  $b$ , per cui si ha che  $a = \alpha a'$  e  $b = \alpha b'$ ; inoltre, considerando  $r = a \bmod b$  quale il resto della divisione tra  $a$  e  $b$ , si può scrivere, per il teorema del quoziente e resto

$$a = qb + r$$

Pertanto, sapendo che  $\alpha$  divide sia  $a$  che  $b$ , bisogna verificare che  $\alpha$  divida anche  $r = a \bmod b$  per concludere la dimostrazione dell'invarianza. Tuttavia, il teorema del quoziente e resto permette di ricavare  $r$  come segue in cui, ovviamente, si ha che

$$r = a - qb = \alpha \cdot (a' - qb')$$

in cui è evidente come  $\alpha$  sia, effettivamente, un divisore anche di  $r = a \bmod b$ . Procedendo, ora, al contrario, supponendo che  $b = \alpha b'$  e  $r = \alpha r'$ , sempre per il teorema del quoziente e resto si può scrivere  $a = qb + r = \alpha \cdot (qb' + r')$ , per cui, ancora una volta,  $\alpha$  divide anche  $a$ , come volevasi dimostrare.

**Osservazione:** Avendo dimostrato la correttezza dell'algoritmo di Euclide, bisogna ora procedere alla verifica della sua straordinaria rapidità. Il problema della complessità dell'algoritmo di Euclide, il quale era un alessandrino, venne risolto brillantemente da un matematico francese di nome **Lamé**, nel 1844, il quale, a tutti gli effetti, è da reputarsi il padre della **teoria della complessità**, quando **Reynaud**, nel 1811 lo aveva già preceduto, ma si parla sempre della prima metà dell'800.

Per comprendere il meccanismo alla base dello studio della complessità, si consideri un numero rappresentato in base 10, quale il seguente  $n = (37855)_{10}$ , il quale viene progressivamente ridotto

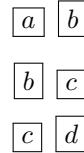
di **almeno** 10 volte ad ogni iterazione, portandolo progressivamente a 3785, 378, 37, 3 ed infine 0. Pertanto, al più, il numero di iterazioni necessarie per annientare questo valore e portarlo a 0 è pari alla **lunghezza decimale** del numero  $n$  (in questo caso pari a 5) che, con una buona dose di approssimazione può essere considerata

$$l_{10}(n) \cong \log_{10}(n)$$

Se, ora, il numero  $n$  considerato viene scritto in binario e ad ogni iterazione viene annientato della metà, al più serviranno un numero di iterazioni pari alla lunghezza binaria del numero  $n$  considerato per annientarlo, ovvero

$$\#\text{iterazioni} \leq l_2(n) \cong \log_2(n)$$

Con questa premessa, considerando l'algoritmo di Euclide e procedendo con i calcoli di **Lamé**, si prendano ad esempio tre iterazioni successive del ciclo while, che producono i seguenti tre stati corrispondenti a tre istanti consecutivi dell'esecuzione:



in cui, ovviamente, si ha che  $a \geq b \geq c \geq d$ ; inoltre, per come sono stati ottenuti  $a, b, c$  e  $d$  appare evidente che

$$a = bq + c \text{ e } b = qc + d$$

A parte il caso iniziale in cui i due numeri  $a \leq b$ , cui l'algoritmo provvede cambiandoli d'ordine, in generale si ha sempre che  $a > b$  e, quindi, il **quoziente** della divisione tra i due numeri è sempre **almeno 1**, quindi, siccome  $q \geq 1$  deve essere che

$$b = qc + d \geq c + d$$

ma non solo: è anche noto che il valore della prima posizione è sempre maggiore o uguale del valore nella seconda posizione, ovvero  $c \geq d$ , per cui si ha che

$$b = qc + d \geq c + d \geq 2d$$

Questo significa che in ogni passo doppio, ovvero ogni due iterazioni, il contenuto della seconda cella di memoria è dimezzato, o peggio, in quanto si ha che  $b \geq 2d$ . Volendo far sì che l'elemento nella seconda cella divenga zero, poiché ad ogni doppia iterazione il suo valore viene almeno dimezzato, il numero di passi doppi necessari è al più uguale al logaritmo in base 2 di  $n$ , quindi

$$\#\text{passi doppi} \cong \log_2(n) \longrightarrow \#\text{passi singoli} < 2 \log_2(n)$$

pertanto, il numero di passi di cui si necessita per terminare il ciclo while è estremamente piccolo, anche nel caso in cui il numero  $n$  considerato è estremamente grande.

**Osservazione:** Un altro modo per descrivere l'algoritmo di Euclide è quello che riguarda la **ricorsività**, come mostrato di seguito

---

#### Algorithm 7 Euclide

---

```

1: Procedura Euclid(a,b)
2: if  $b = 0$  then
3:   return  $a$ 
4: else
5:   return Euclid( $b, a \bmod b$ )

```

---

**Esempio:** Per esempio, si considerino le iterazioni seguenti

$$\text{Euclid}(30, 21) \longrightarrow \text{Euclid}(21, 9) \longrightarrow \text{Euclid}(9, 3) \longrightarrow \text{Euclid}(3, 0) = 3$$

## 4.2 Notazione $O$ grande

Si considerino due funzione  $f(x)$  e  $g(x)$  infinite a  $+\infty$ , ovvero

$$\lim_{x \rightarrow +\infty} f(x) = +\infty \quad \text{e} \quad \lim_{x \rightarrow +\infty} g(x) = +\infty$$

Allora le due funzioni si rassomiglieranno per  $x \rightarrow +\infty$  quando hanno lo stesso ordine di infinito, ovvero

$$\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = \alpha \in \mathbb{R}^+ - \{0\}$$

Tuttavia, taluna è una generalizzazione molto spartana, ma la notazione  $O$  grande lo è ancora di più. Si considerino, nuovamente, due funzioni  $f(x)$  e  $g(x)$ , le quali non debbono più essere infinite a  $+\infty$ , ma è sufficiente che esse siano **definitivamente positive**, ovvero

$$\exists x_n : \forall x > x_n, f(x) > 0 \wedge g(x) > 0$$

In questo caso, pertanto, affermare che  $f(x)$  “assomiglia” a  $g(x)$  significa affermare che  $f(x)$  appartiene alla stessa **classe di equivalenza** di  $g(x)$  (ovvero la classe delle funzioni che rassomigliano a  $g(x)$ ), che si indica come segue

$$f(x) \in \Theta(g(x))$$

che, generalmente, verrà denotato con

$$f(x) = \Theta(g(x))$$

nonostante sia più propriamente corretto impiegare un segno di appartenza in luogo di uno di uguaglianza.

### APPARTENENZA ALLA CLASSE DI EQUIVALENZA DI UNA FUNZIONE

Si considerino due funzioni  $f(x)$  e  $g(x)$  **definitivamente positive**; si dirà che  $f(x)$  appartiene alla stessa classe di equivalenza di  $g(x)$  e si scriverà

$$f(x) = \Theta(g(x))$$

se

$$\exists c_1 > 0, c_2 > 0, \bar{x} : c_1 \cdot g(x) \leq f(x) \leq c_2 \cdot g(x), \quad \forall x \geq \bar{x}$$

ovvero si riesce a descrivere ipoteticamente, con la funzione  $g(x)$ , una guaina all'interno della quale racchiudere la funzione  $f(x)$ .

**Osservazione:** Dalla definizione appena fornita, appare evidente come questa sia a tutti gli effetti una **relazione di equivalenza**, in quanto è soddisfatta la proprietà **riflessiva**

$$g(x) = \Theta(g(x))$$

in quanto basta considerare  $c_1 = c_2 = 1$ ; inoltre è soddisfatta anche la proprietà **simmetrica**:

$$f(x) = \Theta(g(x)) \longrightarrow g(x) = \Theta(f(x))$$

giacché se si ha che

$$c_1 \cdot g(x) \leq f(x) \leq c_2 \cdot g(x)$$

allora si può scrivere

$$\frac{1}{c_2} \cdot f(x) \leq g(x) \leq \frac{1}{c_1} \cdot f(x)$$

e infine quella **transitiva**

$$f(x) = \Theta(g(x)), g(x) = \Theta(h(x)) \longrightarrow f(x) = \Theta(h(x))$$

in quanto se

$$c_1 \cdot g(x) \leq f(x) \leq c_2 \cdot g(x) \quad \text{e} \quad c_3 \cdot h(x) \leq g(x) \leq c_4 \cdot h(x)$$

è facile concludere che

$$c_1 \cdot c_3 \cdot h(x) \leq c_1 \cdot g(x) \leq f(x) \quad \text{e} \quad f(x) \leq c_2 \cdot g(x) \leq c_2 \cdot c_4 \cdot h(x)$$

per cui si ottiene che

$$c_1 \cdot c_3 \cdot h(x) \leq f(x) \leq c_2 \cdot c_4 \cdot h(x)$$

**Esempio:** Si consideri la classe di equivalenza

$$\Theta(1)$$

Allora ad essa vi apparterranno tutte le costanti positive, così come le funzioni oscillanti che assumono valori positivi, come  $f(x) = 2 + \sin(x)$ , in quanto

$$2 \cdot 1 \leq f(x) \leq 3 \cdot 1, \quad \text{con } g(x) = 1$$

**Osservazione:** Si osservi che se due funzioni hanno lo stesso ordine di infinito, allora appartengono alla stessa classe di equivalenza. Tuttavia non è vero il contrario.

Si considerino, infatti, due funzioni  $f(x)$  e  $g(x)$  tali che

$$\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = \alpha \in \mathbb{R}^+ - \{0\}$$

quindi definitivamente, per  $x \geq \bar{x}$ , si ha che

$$\alpha - \epsilon \leq \frac{f(x)}{g(x)} \leq \alpha + \epsilon$$

dal momento che dalla definizione di limite sia  $\forall \epsilon > 0$ , è possibile anche considerare  $\epsilon = \frac{\alpha}{2}$ , da cui

$$\frac{\alpha}{2} \leq \frac{f(x)}{g(x)} \leq \frac{3}{2}\alpha$$

ma allora, moltiplicando ambo i membri per  $g(x)$ , essendo per definizione necessariamente definitivamente positiva, la diseguaglianza si conserva e diviene

$$\frac{\alpha}{2} \cdot g(x) \leq f(x) \leq \frac{3}{2} \cdot \alpha \cdot g(x)$$

che corrisponde esattamente alla definizione di due funzioni che appartengono alla stessa classe di equivalenza, con

$$c_1 = \frac{\alpha}{2} \quad \text{e} \quad c_2 = \frac{3}{2}\alpha$$

Per cui si è dimostrato che avere lo stesso ordine di infinito significa anche appartenere alla stessa classe di equivalenza, ma non è vero il contrario.

### 4.3 Funzioni di complessità

Si consideri una funzione di complessità temporale  $f(n)$  definita in funzione  $n$  della lunghezza dell'input: presumibilmente, al crescere di  $n$ , ossia al crescere della lunghezza dell'input, aumenta anche il valore della funzione stessa.

Le funzioni con cui si sta lavorando sono **definitivamente positive** e, generalmente, sono infinite per  $x \rightarrow +\infty$  e vengono studiate per  $x \geq 0$ .

Com'è noto, è stata definita la classe  $\Theta(f(n))$  come l'insieme di tutte le funzioni che rassomigliano alla funzione  $f(n)$ . In questo caso, in particolare, affermare che

$$g(n) = \Theta(f(n))$$

significa affermare che  $\exists c_1 > 0, c_2 > 0, \bar{n}$  tali che

$$c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n), \quad \forall n \geq \bar{n}$$

in cui  $\Theta(f(n))$  è, a tutti gli effetti, una classe di equivalenza, in quanto gode della proprietà di **riflessività, simmetria e transitività**.

Se si considera una lunghezza  $l = 5$  in base 10, una lunghezza effettiva senza zeri in testa, allora il numero  $n$  che si può descrivere con lunghezza  $l = 5$  è compreso tra

$$10000 \leq n \leq 100000 - 1 \longrightarrow 10^{l-1} \leq n < 10^l$$

e passando ai logaritmi in base 10, ciò si traduce in

$$l_{10}(n) \leq \log_{10}(n) < l_{10}(n)$$

in cui  $\log_{10}(n)$  viene considerata la lunghezza pratica da considerare come utilizzabile, per quanto differisca dalla lunghezza effettiva. Naturalmente si può scrivere che

$$\frac{1}{2} \cdot l_{10}(n) \leq l_{10}(n) \leq \log_{10}(n) \leq l_{10}(n)$$

per cui si può osservare come  $l_{10}(n)$  e  $\log_{10}(n)$  appartengono alla stessa classe di equivalenza  $\Theta(l_{10}(n))$  in quanto sono state usate le costanti  $c_1 = \frac{1}{2}$  e  $c_2 = 1$ .

Quando si impiega la notazione  $\Theta$  si osservi che una funzione  $f(n)$  e  $\alpha \cdot f(n)$  appartengono alla stessa classe  $\Theta$  ed è per questo che normalmente viene omessa la base dei logaritmi, la quale è ininfluente.

Inoltre si è osservato come due funzioni che hanno lo stesso ordine di infinito appartengono anche alla stessa classe  $\Theta$ , semplicemente applicando la definizione di limite. Pertanto, le 3 funzioni

$$3n^2 + 1 \quad \frac{n^2}{1000} \quad 8945n^2$$

appartengono alla stessa classe  $\Theta(n^2)$ .

Si consideri una funzione  $f(n)$  infinita per  $x \rightarrow +\infty$  e la funzione  $g(n) = f(n) \cdot [\sin(n) + 2]$  anch'essa infinita per  $x \rightarrow +\infty$  che appartengono alla stessa classe  $\Theta$ ; tuttavia, si ha che

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} = \lim_{n \rightarrow +\infty} \frac{f(n)}{f(n) \cdot [\sin(n) + 2]} = \frac{1}{[\sin(n) + 2]} \neq \frac{1}{2}$$

per cui due funzioni che appartengono alla stessa classe di equivalenza  $\Theta$  non è detto che abbiano lo stesso ordine di infinito.

**Notazione:** Si osservi che indicare

$$f(n) = O(g(n))$$

significa affermare che definitivamente si ha che

$$f(n) \leq g(n)$$

...continua...

per cui se  $f(n)$  è o grande di  $g(n)$  e  $g(n)$  è o grande  $f(n)$  allora  $f(n)$  e  $g(n)$  appartengono alla stessa classe di equivalenza. ... continua ...

Si osservi, inoltre, che quando

$$\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = +\infty$$

significa affermare che  $g(n) = O(f(n))$ .

**Osservazione:** Si osservi, per quanto si è detto, che

$$\begin{cases} f(n) = O(g(n)) \\ g(n) = O(f(n)) \end{cases}$$

se e solo se appartengono alla stessa classe  $\Theta$ .

Analogamente si ha che

$$\begin{cases} f(n) = O(g(n)) \\ g(n) = O(h(n)) \end{cases}$$

allora si ha che  $f(n) = O(h(n))$ .

**Notazione:** Si osservi che indicare

$$f(n) = \Omega(g(n))$$

significa affermare che definitivamente si ha che

$$f(n) \geq g(n)$$

Per cui si evince che

$$f(n) = \Omega(g(n))$$

se e solo se

$$g(n) = O(f(n))$$

Analogamente si ha che

$$\begin{cases} f(n) = O(g(n)) \\ f(n) = \Omega(g(n)) \end{cases}$$

se e solo se appartengono alla stessa classe  $\Theta$ .

#### 4.4 Classi di complessità

Le tre classi  $\Theta$  che si incontreranno maggiormente saranno

1. La classe **lineare**  $\Theta(n)$
2. La classe **log-lineare**  $\Theta(n \cdot \log(n))$
3. La classe **quadratica**  $\Theta(n^2)$

in cui si ha che

$$\Theta(n) = O\Theta(n \cdot \log(n)) = O\Theta(n^2)$$

ovvero la complessità log-lineare è comunque poco più complessa rispetto a quella lineare, in quanto la crescita all'infinito è molto lenta.

**Osservazione:** Si osservi che la funzione

$$10^{10^{80}} n = \Theta(n)$$

anche se il suo coefficiente è estremamente elevato. Analogamente, se si ha una funzione

$$2^{0,00000\dots 1} = \Theta(2^n)$$

nonostante la sua crescita è estremamente lenta rispetto ad una funzione esponenziale normale. Infatti, tali tipologie di funzioni sono impossibili tra trovare nella vita reale, secondo una valenza empirica.

---

**Algorithm 8** Esempio

---

```
1:  $s = 0$ 
2: for  $i = 1$  to  $k$ 
3:   for  $j = 1$  to  $k$ 
4:      $s = s + a_{i,j}$ 
5:      $a_{i,j} = s$ 
6:   next  $i$ 
7: next  $j$ 
```

---

Naturalmente il numero di iterazioni è  $k^2$ , ma se esse fossero  $2 + 2k^2$ , la notazione  $\Theta$  fa sì che in ogni caso la complessità sia  $k^2 \dots$  continua... anche se il numero di iterazioni è differente, l'orine si mantiene inalterato.

**Osservazione:** Si osservi che nel caso dell'algoritmo **insertion-sort**, il numero di iterazioni nel caso migliore è pari a  $\Theta(n)$ , in quanto le iterazioni sono  $n-1$ , mentre nel caso peggiore la complessità è  $\Theta(n^2)$ , in quanto le iterazioni sono  $\frac{n \cdot (n-1)}{2}$ . Per quanto concerne la complessità tipica, ovverosia la complessità media, dal punto di vista empirico si osserva che essa è  $\Theta(n^2)$ .

Per quanto concerne l'algoritmo di Euclide, il numero di iterazioni, nel caso peggiore era di  $1 + 2 \cdot \log_2(\min(m, n))$ , per cui si ha che la complessità effettiva sia  $O(\log(n))$ .

Merge-Sort L'algoritmo **merge-sort** è un algoritmo la cui idea alla base è molto più complessa dell'algoritmo **insertion-sort**.

L'input, come di consueto, è dato da un **array**  $A$  di lunghezza  $\text{length}(A) = n$ , per cui si dovranno ordinare  $n$  numeri. Inoltre, due altri input sono  $p, r$  le quali sono delle posizioni dell'array intermedie, tali che  $1 \leq p \leq r \leq n$

---

**Algorithm 9** Merge-sort

---

```
1: MERGE-SORT( $A, p, r$ )
2: if  $p < r$ 
3:   then  $q = \text{parte intera inferiore} \left[ \frac{p+r}{2} \right]$ 
4:   MERGE-SORT( $A, p, q$ )
5:   MERGE-SORT( $A, q+1, r$ )
6:   MERGE( $A, p, q, r$ )
```

---

... continua ... In cui la procedura *MERGE* non è ricorsiva, ma presenta due cicli for. Tale procedura inizia ad operare sui due insiemi di valori che sono già stati ordinati separatamente, con lo scopo di ricavare un unico insieme di valori ordinati, sfruttando l'ordinamento dell'insieme dei valori su cui si sta operando; dopodiché si confrontano tutti i valori in testa, prendendo sempre il più piccolo tra i due che vengono confrontati, fino ad arrivare all'ultimo valore (necessariamente molto elevato) che viene appositamente posto alla fine in modo da segnalare il termine dell'insieme di valori; in particolare si ha che  $p < q < r$ , in cui i valori che stanno tra  $[p - q]$  e  $[q - r]$  sono già stati ordinati. La procedura viene esposta di seguito

**Algorithm 10** Merge

---

```
1: MERGE( $A, p, q, r$ )
2:  $n_1 = q - p + 1$ 
3:  $n_2 = r - q$ 
4: Create two new arrays  $L$  and  $R$ 
5: for  $i = 1$  to  $n_1$ 
6:   do  $L[i] = A[p + i - 1]$ 
7:      $R[j] = A[q + j]$ 
8:    $L = [n_1 + 1] = +\infty, R[n_2 + 1] = +\infty$ 
9:    $i = 1, j = 1$ 
10:  for  $k = p$  to  $r$ 
11:    do if  $L[i] \leq R[j]$ 
12:      then  $A[k] = L[i]$ 
13:         $i = i + 1$ 
14:      else  $A[k] = R[j]$ 
15:         $j = j + 1$ 
```

---

In cui le iterazioni coinvolte, naturalmente, fino alla riga 9 sono

$$n_1 + n_2 = q - p + 1 + r - q = r - p + 1$$

ovverosia il numero delle posizioni che vanno da  $p$  a  $r$ .

Mentre dalle righe 9 in poi il numero di iterazioni è, ovviamente, ancora una volta  $r - p + 1$ ; pertanto il numero di iterazioni complessive è pari al doppio di  $r - p + 1$ , quindi la complessità è dell'ordine

$$\Theta(r - p + 1)$$

**Esempio:** Si consideri il seguente array

4	5	3	1	7	2	0	9
---	---	---	---	---	---	---	---

in cui  $n = 8$ . Per l'ordinamento di tale array, si divide lo stesso in due parti e poi successivamente ogni parte in ancora due parti e nuovamente in due parti fino ad ottenere una divisione dell'ordinamento riducendosi all'unità, in cui i singoli valori saranno automaticamente ordinati. Dopodiché si utilizza la procedura *Merge* per ordinare i blocchi di due, ottenenendo

4	5	1	3	2	7	0	9
---	---	---	---	---	---	---	---

e poi procedendo con i blocchi di 4, ottenendo

1	3	4	5	0	2	7	9
---	---	---	---	---	---	---	---

e infine si ordina il blocco completo

0	1	2	3	4	5	7	9
---	---	---	---	---	---	---	---

Questa, naturalmente, è una esecuzione parallela, mentre quella dell'algoritmo è lineare, in quanto va ad analizzare progressivamente ogni ramo di un albero binario, risalendolo progressivamente.

**Osservazione:** Tale algoritmo è **profondamente rigido**, in quanto il numero delle iterazioni che si devono eseguire è sempre lo stesso, indipendente dal caso migliore, peggiore e generale.

Questa non è una buona caratteristica, la quale rende ragionevole l'utilizzo di tale algoritmo quando i numeri sono inizialmente fortemente disordinati; se i numeri iniziali sono parzialmente ordinati è più conveniente impiegare l'algoritmo di insertion-sort.

La sua complessità è **log-lineare** ed è estremamente ottima in quanto è una complessità generale, che nessun altro algoritmo può batterla. La tecnica impiegata per la risoluzione di tale problema prende il nome di *Divide et impera* (o *Divide and conquer*).