

UNIVERSITÀ DEGLI STUDI DI VERONA

---

# **Complessità**

---

RIASSUNTO DEI PRINCIPALI ARGOMENTI

*Matteo Danzi, Davide Bianchi*

23 maggio 2018

# Indice

<b>1</b>	<b>Introduzione</b>	<b>2</b>
1.1	Cos'è la complessità computazionale . . . . .	2
1.2	Problemi <i>facili</i> e <i>difficili</i> . . . . .	2
1.3	Risolvere vs Verificare . . . . .	3
<b>2</b>	<b>Problema computazionale</b>	<b>3</b>
2.1	Risolvere un problema computazionale . . . . .	3
2.2	Complessità di un problema computazionale . . . . .	4
2.3	Trattabilità di un problema. . . . .	4
<b>3</b>	<b>Le classi di problemi computazionali</b>	<b>4</b>
3.1	Classe <b>P</b> . . . . .	5
3.2	Classe <b>Exp</b> . . . . .	5
3.3	Classe Time(n) . . . . .	6
3.4	Classe <b>NP</b> . . . . .	7
<b>4</b>	<b>Riduzione alla Karp tra problemi di decisione</b>	<b>8</b>
4.1	Problema SAT . . . . .	8
4.2	Alcuni esempi di riduzioni tra problemi . . . . .	9
4.3	Problema NAE-K-SAT . . . . .	11
4.4	Transitività della riduzione alla Karp . . . . .	12
4.5	Problema Reachability . . . . .	13
<b>5</b>	<b>Riduzione alla Turing tra problemi di decisione</b>	<b>13</b>
<b>6</b>	<b>Classe di problemi NP-Completi</b>	<b>13</b>
6.1	Circuito Booleano . . . . .	13
6.2	Problema Circuit-SAT . . . . .	14
6.3	Relazione tra <b>P</b> , <b>NP</b> , e <b>NP-completo</b> . . . . .	15
<b>7</b>	<b>Classe di problemi CO-NP</b>	<b>16</b>
7.1	Relazione tra <b>P</b> , <b>NP</b> e <b>CO-NP</b> . . . . .	16
7.2	Problema Minimo circuito booleano . . . . .	17
<b>8</b>	<b>Gerarchia Polinomiale</b>	<b>17</b>
8.1	Funzione time-costruibile . . . . .	18
8.2	Problema Catch 22 . . . . .	19
<b>9</b>	<b>Teorema di Ladner</b>	<b>19</b>
9.1	Problema Clique . . . . .	20
9.2	Problema Independent Set . . . . .	21
<b>10</b>	<b>Ricavare problemi di ottimizzazione e ricerca</b>	<b>23</b>
10.1	Independent Set . . . . .	23
10.2	Problema SAT-Search . . . . .	24
10.3	Self Reducibility . . . . .	24
10.4	Problema Graph Isomorphism . . . . .	25

## 1 Introduzione

### 1.1 Cos'è la complessità computazionale

Nella teoria della complessità ci si pone la seguente domanda:

*Come scalano le risorse necessarie per risolvere un problema all'aumentare delle dimensioni del problema?*

La teoria della *complessità computazionale* è una parte dell'informatica teorica che si occupa principalmente di classificare i problemi in base alla quantità di *risorse computazionali* (come il tempo di calcolo e lo spazio di memoria) che essi richiedono per essere risolti. Tale quantità è detta anche *costo computazionale* del problema.

### 1.2 Problemi *facili* e *difficili*

Vediamo quattro esempi di problemi che classificheremo come facili o difficili:

1. (**Eulerian Cycle**) Esiste un modo per attraversare ogni arco di un grafo una e una sola volta?

- Il problema si può vedere anche nella forma più piccola del problema dei *sette ponti di Königsberg*:

A Königsberg ci sono 7 ponti, esiste un percorso che attraversa tutti i ponti una e una sola volta per poi tornare al punto di partenza?

Se avessi  $n$  ponti e su ogni riva partissero 2 ponti avrei  $2^n$  possibili percorsi.

- La **soluzione di Eulero** dice che un grafo connesso non orientato ha un percorso che parte e inizia esattamente nello stesso vertice e attraversa ogni arco esattamente una volta se e solo se ogni vertice ha grado dispari (grado = numero di archi uscenti).  
Se ci sono esattamente due vertici  $v$  e  $u$ , di grado dispari, allora esiste un percorso che parte da  $u$  e attraversa ogni arco esattamente una volta e finisce in  $v$ .
- Seguendo quindi la soluzione di Eulero, *quanto costa decidere se un grafo  $G$  ha un tour Euleriano?*

```
odd-vertex-num = 0;
foreach vertex v of G
    if (deg(v) is odd)
        increment odd-vertex-num
If(odd-vertex-num is neither 0 nor 2)
    output no Eulerian tour
output Eulerian
```

Questo algoritmo ha complessità:  $O(|E| + |V|)$

Il costo e l'algoritmo sono gli stessi se vogliamo *provare* che  $G$  non ha un tour Euleriano.

2. (**Hamiltonian Cycle**) Esiste un modo per attraversare ogni nodo di un grafo una e una sola volta?

Esistono diverse soluzioni:

- Provo tutte le possibilità ogni volta, costo:  $O(2^n)$
- Provo tutte le possibili permutazioni, costo:  $O(n!)$
- La soluzione migliore ad oggi è:  $O(1.657^n)$

Alla domanda: *Quanto costa decidere se un grafo ha un tour hamiltoniano?* Non sappiamo rispondere. Non sappiamo dire se il problema ha una soluzione non esponenziale. Per quanto ne sappiamo meglio di  $O(1.657^n)$  non sappiamo fare.

Non sappiamo nemmeno dire se Hamiltonian Cycle è più difficile di Eulerian Cycle.

3.  $N$  è un numero primo?

Il migliore algoritmo conosciuto per decidere se  $N$  è un numero primo impiega  $O((\log N)^{6+\epsilon})$

## 4. Quali sono i fattori primi di un numero?

Ad oggi non conosciamo una procedura per fattorizzare un numero molto grande nei suoi divisori, che non sia provare tutte le possibilità.

### 1.3 Risolvere vs Verificare

La seguente tabella riassume in modo generico quanto detto nella sezione precedente riguardo alla difficoltà di risolvere problemi e verificare tali problemi su un istanza.

Tabella 1: Risolvere vs Verificare

Problema	Risolvere	Verificare
Eulerian Cycle	<i>facile</i>	<i>facile</i>
Hamiltonian Cycle	<i>difficile?</i>	<i>facile</i>
N è primo?	<i>facile</i>	<i>facile</i>
N ha un numero piccolo di fattori?	<i>difficile?</i>	<i>facile</i>

## 2 Problema computazionale

Un problema computazionale è una semplice relazione  $p$  che mappa l'insieme *infinito* di possibili input (domande o istanze) con un insieme *finito* (non vuoto) di output, cioè di risposte o soluzioni alle istanze.

$$p : \text{istanze infinite} \mapsto \text{soluzioni finite alle istanze}$$

Un problema computazionale non è una singola domanda, ma è una **famiglia di domande**:

- Una domanda per ogni possibile istanza
- Ogni domanda è dello stesso tipo (appartiene alla stessa classe)

**Esempio 2.0.1.** Il seguente esempio è un problema computazionale:

- Input: Qualsiasi grafo  $G$
- Domanda: Il grafo  $G$  contiene un ciclo Euleriano?

**Esempio 2.0.2.** Il seguente esempio *non* è un problema computazionale:

- Domanda: È vero che il bianco vince sempre a scacchi, sotto l'ipotesi della giocata perfetta?

Non è un problema computazionale perché non ho un insieme infinito di possibili partite in input.

### 2.1 Risolvere un problema computazionale

Risolvere un problema computazionale significa trovare un **algoritmo**, cioè una procedura che risolve il problema matematico in un numero finito di passi (di computazione elementare), che solitamente include la ripetizione di un'operazione. È un procedimento deterministico che mappa l'input sull'output.

Un algoritmo è una procedura *finita*, *definita*, *efficace* e con un input e un output.

Donald Knuth – *The Art of Computer Programming*

## 2.2 Complessità di un problema computazionale

**Misura della complessità.** Come misuro la complessità di un problema computazionale? Come faccio a dire quanto è facile rispetto ad altri problemi?

- Do un **upper bound**: trovo un algoritmo qualsiasi che risolve il problema in modo da calcolare qual è il suo costo.
- Do un **lower bound**: trovo la minima quantità di risorse che ogni algoritmo utilizza per risolvere il problema. Tutti gli algoritmi sono *al minimo* complessi come il limite inferiore che abbiamo stabilito. Nessuno può fare di meglio.



## 2.3 Trattabilità di un problema.

La crescita della complessità di un problema è riducibile a 2 categorie fondamentali.

**Crescita polinomiale.** Un problema ha crescita polinomiale quando le risorse necessarie alla sua risoluzione sono limitate ad  $n^k$ , per qualche  $k$ . Se la taglia del problema aumenta, la sua complessità aumenta di un qualche fattore costante. Infatti, se la taglia dell'input va da  $n$  a  $2n$  allora la complessità del problema si modifica in  $(2n)^k = 2^k n^k$ , ovvero aumenta di un fattore  $2^k$  (costante). Raggruppiamo nella classe **P** i problemi di questo tipo.

**Crescita esponenziale.** Un problema ha crescita esponenziale la necessità di risorse necessarie alla sua risoluzione è proporzionale a  $c^n$ , per qualche costante  $c > 1$ . Se la taglia dell'input va da  $n$  a  $2n$  allora la richiesta di risorse si diventa  $c^{2n} = c^n * c^n$ , aumentando quindi di un fattore che cresce con l'aumentare di  $n$ . Raggruppiamo nella classe **Exp** i problemi di questo tipo.

## 3 Le classi di problemi computazionali

**Notazione e idee di base.** Formalmente definiamo un problema come un elemento  $\mathbb{A}$  di una relazione

$$\mathcal{R} \subseteq \mathcal{I}(\mathbb{A}) \times \text{Sol}$$

dove:

- $\mathcal{I}(\mathbb{A})$  è l'insieme delle istanze del problema  $\mathbb{A}$
- $\text{Sol}$  è l'insieme delle soluzioni delle istanze di  $\mathbb{A}$

Si può quindi dire che

$$\forall x \in \mathcal{I}(\mathbb{A}), \text{Sol}(x) = \{\text{Soluzioni di } x\}$$

Non è restrittivo restringersi ai **problemi di tipo decisionale**, ovvero quei problemi che hanno come soluzione una risposta del tipo *si* o *no*, quindi i problemi del tipo

$$\mathbb{A} : \mathcal{I}(\mathbb{A}) \rightarrow \{\text{yes}, \text{no}\}$$

L'algoritmo  $\mathcal{A}$  per un problema  $\mathbb{A}$  è un algoritmo che dato il problema,  $\forall x \in \mathcal{I}(\mathbb{A}), \mathcal{A}(x) = \mathbb{A}(x)$ . Inoltre, dato un algoritmo  $\mathcal{A}$ , definiamo  $T_{\mathcal{A}}(|x|)$  la sua **complessità**, cioè il *tempo che impiega*  $\mathcal{A}$  sull'istanza di taglia  $|x|$ . Notare che  $|x|$  è la taglia dell'istanza  $x$ .

### 3.1 Classe P

Intuitivamente la classe **P** è definita come la classe di problemi di **complessità polinomiale**. Introduciamo qui la definizione formale.

**Definizione 3.1.1** (Classe P). Definiamo la classe di problemi **P** come l'insieme dei problemi di complessità polinomiale, ovvero

$$\mathbf{P} = \{ \mathbb{A} \mid \exists \mathcal{A} \text{ t.c. } \exists c \text{ costante e } \forall x \in \mathcal{I}(\mathbb{A}), \mathcal{A}(x) = \mathbb{A}(x) \text{ e } T_{\mathcal{A}}(|x|) \leq |x|^c \}$$

**Esempio 3.1.1** (Eulerian Cycle). Un semplice esempio di problema appartenente alla classe **P** è il problema del tour euleriano. Per questo problema infatti abbiamo che è un problema computazionale di decisione:

- Input: grafo  $G$
- Output:  $\text{yes} \Leftrightarrow \exists \text{ Eulerian Cycle in } G$ .

Come abbiamo già visto quindi:

$$\exists \mathcal{A} \text{ t.c. } T_{\mathcal{A}}(|G|) = O(|E| + |V|) = O(|G|)$$

$\text{Eulerian Cycle} \in \mathbf{P}$  perché  $\exists \mathcal{A}$  che impiega un tempo che è nell'ordine della taglia di  $G$ , in particolare  $\exists c$  costante dove  $c = 1$ .

**Esempio 3.1.2** (Hamiltonian Cycle). Ci chiediamo allora se anche  $\text{Hamiltonian Cycle} \in \mathbf{P}$ ? La risposta è che non lo sappiamo dire. Quello che sappiamo per questo problema è che:

$$\exists \mathcal{A} \text{ t.c. } T_{\mathcal{A}}(|G|) = O(a^{|G|})$$

dove  $a$  è costante.

### 3.2 Classe Exp

Dal momento che non sappiamo se alcuni problemi stiano oppure no nella classe **P** (dal momento che non si conosce un algoritmo che li risolva in tempo polinomiale), si definisce la classe **Exp**, che racchiude tutte le istanze di questa tipologia di problemi di **complessità esponenziale**.

**Definizione 3.2.1** (Classe Exp). Definiamo la classe di problemi **Exp** come la classe di problemi di complessità esponenziale, ovvero

$$\mathbf{Exp} = \{ \mathbb{A} \mid \exists \mathcal{A} \text{ t.c. } \forall x \in \mathcal{I}(\mathbb{A}), \mathcal{A}(x) = \mathbb{A}(x) \text{ e } T_{\mathcal{A}}(|x|) \leq 2^{|x|^c} \}$$

**Esempio 3.2.1** (Hamiltonian Cycle). Ci chiediamo se  $\text{Hamiltonian Cycle} \in \mathbf{Exp}$ ? Se prendiamo l'algoritmo che prova tutte le combinazioni di archi cioè  $\binom{|E|}{n}$  per vedere se formano un ciclo hamiltoniano. La complessità di quest'algoritmo è al massimo  $2^{|E|^2}$ .

Se invece prendiamo l'algoritmo che considera tutte le possibili permutazioni dei vertici del grafo abbiamo che la complessità è  $n!$ . Quindi il problema  $\text{Hamiltonian Cycle} \notin \mathbf{Exp}$

**Relazione tra P ed Exp.** La domanda che sorge spontanea è  $\mathbf{P} \subseteq \mathbf{Exp}$ ?

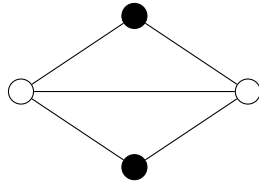
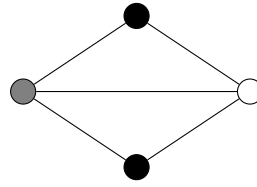
La risposta alla domanda è banalmente **si**, in quanto, dato un algoritmo  $\mathcal{B}$  con complessità  $T_{\mathcal{B}}(|x|)$ , possiamo dire che

$$T_{\mathcal{B}}(|x|) = O(|x|^c) = O(2^{|x|^c}) \Rightarrow \mathbb{A} \in \mathbf{Exp}$$

**Problema K-Graph-Colouring.** Analizziamo ora il problema della K-colorabilità di un grafo  $G$ :

- Input:  $G$  non orientato.
- Output:  $\text{yes} \Leftrightarrow \exists \text{ colorazione propria dei vertici di } G \text{ ovvero:}$

$$\exists f : v \mapsto \{0, \dots, k-1\} \text{ t.c. } \forall (u, v) \in E(G) \quad f(u) \neq f(v)$$

(a) Grafo con colorazione *non* propria

(b) Grafo con colorazione propria

**Problema 2-Graph-Colouring.** Consiste nel trovare se esiste una 2 colorazione del grafo dato in input in modo tale che un arco non si trovi tra due vertici dello stesso colore. Questo problema corrisponde a dire se il grafo è **bipartito**, cioè se *posso suddividere il grafo in due classi diverse*. Per vedere se è bipartito si effettua una **BFS**, cioè una visita in ampiezza, e si controlla se c'è un ciclo dispari. Se c'è allora non è bipartito e quindi nemmeno 2-colorabile.

È 2-colorabile  $\Leftrightarrow$  è Bipartito  $\Leftrightarrow$  non contiene un ciclo dispari. La visita BFS ha una complessità pari a  $O(|E| + |V|)$ , perciò il problema è risolvibile in tempo polinomiale, perciò possiamo concludere che 2-Graph-Colouring  $\in \mathbf{P}$ .

**Problema 3-Graph Colouring** Il problema 3-Graph Colouring  $\in \mathbf{P}$ ? Non sappiamo rispondere a questa domanda, poiché non sappiamo se esiste un algoritmo che lo svolga in tempo polinomiale. Il problema 3-Graph Colouring  $\in \mathbf{Exp}$ ? Se consideriamo l'algoritmo che prova tutte le possibili colorazioni abbiamo che:

$$3^n \text{ sono le colorazioni dei vertici, dove } n = |V(G)|$$

Bisogna vedere se ci sono archi monocolori e quindi la complessità diventa:

$$O(3^n \cdot |E|) = O(3^{2n}) = O((2^{\log_2 3})^{2n}) = O(2^{2n \log_2 3})$$

Perciò possiamo concludere che il problema 3-Graph Colouring  $\in \mathbf{Exp}$ .

### 3.3 Classe Time(n)

**Definizione 3.3.1** (Classe Time(n)). Definiamo la classe **Time(n)** come l'insieme dei problemi di complessità lineare, ovvero

$$\mathbf{Time}(n) = \{ \mathbb{A} \mid \exists \mathbb{B} \text{ per } \mathbb{A} \text{ t.c. } \forall x \in \mathcal{I}(\mathbb{A}) \quad T_{\mathbb{B}}(|x|) = O(n) = O(f(|x|)) \}$$

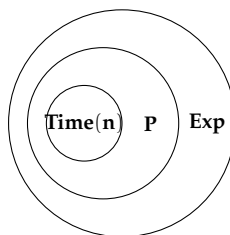
**Teorema 3.3.1.**  $\forall \mathbb{B} \text{ t.c. } \mathbb{B}(x) = \mathbb{A}(x) \quad T_{\mathbb{B}}(|x|) > |x|^c \quad \forall c \text{ costante}$

**Teorema 3.3.2.** *Qualsiasi algoritmo di ordinamento che usa confronti su  $n$  elementi ha tempo di esecuzione pari a*

$$\Omega(n \log n)$$

Possiamo dire quindi che:

- **Eulerian Cycle**  $\in \mathbf{Time}(n)$  perché esiste un problema che lo risolve in tempo lineare.
- **Sorting**  $\notin \mathbf{Time}(n)$  per il teorema 3.3.2.



Possiamo riassumere quindi che:

- **Eulerian Cycle**  $\in P$ , **Eulerian Cycle**  $\in \text{Time}(n)$ .
- **Hamiltonian Cycle**  $\in \text{Exp}$
- **Hamiltonian Cycle**  $\in P$  ? non lo sappiamo dire.
- **K-Colouring**  $\in \text{Exp}$
- **K-Colouring**  $\in P$ ?  
per  $k \geq 3$  non lo sappiamo dire  
per  $k = 2$  sì.

Inoltre, con la definizione della classe **Time**(n) si può dire che:

$$P = \bigcup_{k \geq 0} \text{Time}(n^k)$$

$$\text{Exp} = \bigcup_{k \geq 0} \text{Time}(2^{n^k})$$

### 3.4 Classe NP

La classe **NP** (*non deterministic polynomial time*) è la classe di problemi tali che se la soluzione per un'istanza del problema è *yes*, allora è facile verificarlo.

**Definizione 3.4.1.** (Classe NP)

$$\text{NP} = \{ \mathbb{A} \mid \exists \mathcal{B}(\cdot, \cdot) \text{ t.c. } T_{\mathcal{B}}(|x| + |w|) = O((|x| + |w|)^c) \\ \forall x \in \mathcal{I}(\mathbb{A}) \quad \mathbb{A}(x) = \text{yes} \Leftrightarrow \exists w \text{ t.c. } |w| = O(|x|^d) \text{ e } \mathcal{B}(x, w) = \text{yes} \}$$

dove:

- $\mathcal{B}(\cdot, \cdot)$  è detto **verificatore** per  $\mathbb{A}$ . Se la risposta di  $\mathbb{A}$  esiste, allora  $\mathcal{B}$  dice *yes*. Il verificatore impiega **tempo polinomiale** nella taglia dell'istanza per rispondere.
- $x$  è l'istanza
- $w$  è il certificato.

**Hamiltonian Cycle**  $\in \text{NP}$  ? Per vedere se il problema Hamiltonian cycle appartiene alla classe NP dobbiamo costruire un verificatore  $\mathcal{B}$  che agisca in tempo polinomiale.

Algorithm 1: Verificatore per HamCycle

---

```

VerifyHamCycle ( $G = (V, E)$ ,  $C = x_1, \dots, x_n$ )
    if  $r \neq |V|$ : return no
    foreach  $v \in V$ 
        if  $v$  non appare in  $C$ : return no
    for  $i=1$  to  $n-1$ 
        if  $(x_i, x_{i+1}) \notin E$ : return no
    if  $(x_1, x_n) \notin E$ : return no
    return yes

```

---

$\left. \begin{array}{l} \} O(|w|) \\ \} O(|V| \cdot |C|) \\ \} O(|C|) \\ \} O(1) \end{array} \right\}$

Il tempo di esecuzione del verificatore è polinomiale e quindi posso dire che **Hamiltonian Cycle**  $\in \text{NP}$ .



**K-Colouring**  $\in$  **NP**? Per vederlo costruisco il verificatore:

Algorithm 2: Verificatore per K-Colouring

---

```

VerifyK-Colouring( $G = (V, E), f(v_1), \dots, f(v_n)$ )
  foreach  $E(u, v)$ 
    if  $f(u) = f(v)$ : return no
  for  $i=1$  to  $n$ 
    if  $f(v_i) \geq K$ : return no
  return yes

```

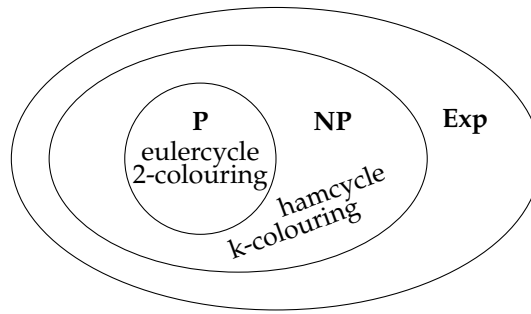
---

Il tempo di esecuzione del verificatore è polinomiale e quindi posso dire che **K-Colouring**  $\in$  **NP**.

**P**  $\subseteq$  **NP**? Vogliamo capire in che classe è **NP**. Se include la classe **P** allora significa che un problema che appartiene a quest'ultima, se lo sappiamo risolvere, lo sappiamo anche verificare. Infatti se  $A \in P$  dobbiamo dimostrare che esiste un verificatore. Tale verificatore per  $A$  sarà:  $B'(x, w) = B(x)$  privo di certificato. Dobbiamo dimostrare che se l'istanza è *yes* allora  $B(x) = \text{yes}$  altrimenti  $B(x) = \text{no}$ .

**NP**  $\subseteq$  **Exp**? Vogliamo capire in che classe è **NP**

Possiamo supporre che **P**  $\subseteq$  **NP**  $\subseteq$  **Exp**.



## 4 Riduzione alla Karp tra problemi di decisione

**Definizione 4.0.2** (Riduzione alla Karp). Un problema di decisione  $A$  si riduce alla Karp al problema  $B$ :  $A \leq_K B$  se esiste un algoritmo polinomiale  $\mathcal{A}$  tale che

$$\forall x \in \mathcal{I}(A), B(\mathcal{A}(x)) = \text{yes} \Leftrightarrow A(x) = \text{yes}$$

**Proposizione 4.0.1.** Se  $A \leq_K B$  e  $B \in P \Rightarrow A \in P$

**Proposizione 4.0.2.** Se  $A \leq_K B$  e  $B \notin P \Rightarrow A \notin P$

Come effettivamente svolgiamo le trasformazioni?

### 4.1 Problema SAT

**Definizione 4.1.1** (SAT). Il problema di soddisfacibilità di una formula booleana è definito nel seguente modo:

- Input: formula booleana :  $\phi(x_1, \dots, x_n) = C_1 \wedge C_2 \wedge \dots \wedge C_n$   
Dove:
  - $C_i = l_{i1} \vee l_{i2} \vee \dots \vee l_{ik}$  (clausola)
  - $l_{ij} = x_k$  oppure  $\bar{x}_k$  (letterale)

- Output:  $yes \Leftrightarrow \exists a_1 \dots a_n \in T, F^n \text{ t.c. } \phi(a_1, \dots, a_n) = T$

**Esempio 4.1.1.**  $\phi(x_1, x_2, x_3) = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \wedge (x_1 \vee \bar{x}_3)$   
 Assegnamento che soddisfa la formula booleana  $\phi(x_1, x_2, x_3)$ :

$$\begin{array}{lll} x_1 = T & x_2 = F & x_3 = F \\ a_1 = T & a_2 = F & a_3 = F \end{array}$$

**SAT  $\in$  NP ?** Ci chiediamo se il problema SAT sta nella classe NP. Vediamo dunque se esiste un certificato e un verificatore che attesta, dato una formula booleana, se essa è soddisfacibile in tempo polinomiale.

- Si può notare facilmente che il certificato è un assegnamento per la formula booleana, dunque è polinomialmente correlato alla grandezza delle variabili della formula, sarà al massimo  $n$ .
- Il verificatore viene costruito analizzando la formula booleana, controllando ogni letterale di ciascuna clausola. Ho quindi  $m \times n \times n$  controlli, dove  $m$  = numero di clausole,  $n$  = numero di letterali. Il verificatore è quindi polinomiale.

Possiamo concludere che il problema SAT  $\in$  NP. Questa affermazione si può tradurre con: *data una formula booleana di cui sappiamo essere soddisfacibile, allora è facile (polytime) costruire un verificatore che attesta che essa è SAT.*

**Problema K-SAT:** è il problema SAT in cui l'input ha come restrizione il vincolo che ogni clausola ha esattamente  $k$  letterali.

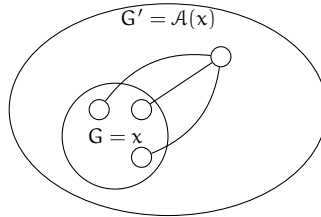
**Esempio 4.1.2 (3-SAT).**  $\phi(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3)$

## 4.2 Alcuni esempi di riduzioni tra problemi

**K-colouring  $\leq_K$  (K+1)-colouring** Vediamo se il problema (K+1)-colouring non è più facile del problema K-colouring. Dobbiamo in sostanza dimostrare che decidere se possiamo colorare un grafo con  $k + 1$  colori non è più facile che decidere se possiamo colorare un grafo con  $k$  colori. **N.B.:** da notare che i due grafi non sono necessariamente uguali, parliamo di qualsiasi grafo che appartiene al problema.

$$\begin{array}{ll} \mathcal{A} : x \in \mathcal{I}(K - \text{COL}) & \mapsto \mathcal{A}(x) \in \mathcal{I}((K + 1) - \text{COL}) \\ K - \text{COL}(x) = \text{yes} & \Leftrightarrow (K + 1) - \text{COL}(\mathcal{A}(x)) = \text{yes} \end{array}$$

Prendiamo quindi il grafo  $G'$ :



per cui

$$\begin{array}{l} G = (V, E) \\ G' = (V \cup \{v'\}, E \cup \{(v, v') \mid v \in V\}) \end{array}$$

in tempo lineare e quindi sotto il polinomiale riesco a costruire il grafo  $G'$ .

Se  $G$  è  $K$ -colorabile allora  $G'$  è  $(K+1)$ -colorabile. Mi basta assegnare a  $v'$  il colore  $k$  (il  $k+1$ -esimo colore) e mantenere la colorazione di  $G$ .

Se  $G$  non è  $K$ -colorabile allora  $G'$  non è  $K+1$ -colorabile. Equivale a dire che se  $G'$  è  $K+1$ -colorabile allora  $G$  è  $k$ -colorabile. Quindi se  $v'$  ha un colore  $f(v') = x$  allora ogni  $v \in V(G)$  ha un colore  $f(v) \neq x$ , al più usano  $k$  colori.

Da questa dimostrazione ricaviamo anche che  $2\text{-col} \leq_K 3\text{-col} \leq_K 4\text{-col} \leq_K 5\text{-col}$

**SAT  $\leq_K$  3-SAT** Vogliamo dimostrare che data una formula booleana  $\phi$  CNF esiste una trasformazione polytime che mi porta a una formula booleana  $\phi'$  3CNF (ogni clausola ha esattamente 3 letterali). E inoltre che  $\phi$  è soddisfacibile se e solo se  $\phi'$  è soddisfacibile.

Possiamo iniziare dicendo che  $(x_1 \vee x_2) \equiv (x_1 \vee x_1 \vee x_2)$ . Le clausole più piccole possono essere espanse. Seguendo questa intuizione arriviamo a dire che:

$$(l_1 \vee l_2 \vee l_3 \vee \dots \vee l_k) \rightsquigarrow (l_1 \vee l_2 \vee z_1) \wedge (\bar{z}_1 \vee l_3 \vee z_2) \wedge (\bar{z}_2 \vee l_4 \vee z_3) \wedge (\bar{z}_3 \vee l_5 \vee z_4) \wedge \dots \wedge (\bar{z}_{k-1} \vee l_{k+1} \vee z_k)$$

Dimostriamo che se  $\phi$  non è soddisfacibile allora non lo è neanche  $\phi'$ .

- Prendiamo  $\phi = (x_1, \dots, x_n)$ . Per questa formula prendiamo un assegnamento  $a_1, \dots, a_n$  che non la rende soddisfacibile, quello in cui ogni letterale viene assegnato a F.
- Prendiamo dunque  $\phi' = (x_1, \dots, x_n, z_1, \dots, z_r)$ . Per questa formula prendiamo lo stesso assegnamento di  $\phi$  e vediamo cosa succede con i letterali  $z$ :

$$\begin{array}{cccccccccccccccc} (l_1 \vee l_2 \vee z_1) \wedge (\bar{z}_1 \vee l_3 \vee z_2) \wedge (\bar{z}_2 \vee l_4 \vee z_3) \wedge (\bar{z}_3 \vee l_5 \vee z_4) \wedge \dots \wedge (\bar{z}_{k-1} \vee l_{k+1} \vee z_k) \\ \text{F} \quad \text{F} \quad \text{V} \quad \text{F} \quad \text{F} \quad \text{V} \quad \text{F} \quad \text{F} \quad \text{V} \quad \text{F} \quad \text{F} \quad \text{V} \quad \text{F} \quad \text{F} \quad \text{V} \quad \text{F} \quad \text{F} \quad \text{V} \end{array}$$

risulta che l'ultimo letterale  $z_k$  è falso, e quindi  $\phi'$  non è soddisfacibile.

**K-COL  $\leq_K$  K-SAT** Vogliamo dimostrare che il problema di colorare un grafo con  $k$  colori è riducibile al problema di soddisfacibilità di una formula booleana  $k$ -CNF.

Cerchiamo un modo per esprimere in modo logico il fatto che due nodi adiacenti non abbiano lo stesso colore. Supponiamo che il nodo  $v$  abbia colore  $i$  e il nodo  $u$  abbia colore  $i$  con  $i = 0, 1, \dots, k-1$ . Per ogni  $v \in V$ :  $x_0^{(v)} x_1^{(v)} x_2^{(v)} \dots x_{k-1}^{(v)}$  dove  $x_i^{(v)} = T$  se il vertice  $v$  ha colore  $i$ .

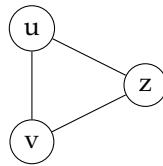
Ci chiediamo quindi quand'è che la formula è  $K$ -colorabile?

$$\forall v \in V \begin{cases} x_0^{(v)} \vee x_1^{(v)} \vee x_2^{(v)} \vee \dots \vee x_{k-1}^{(v)} & \text{ogni vertice ha un colore} \\ \overline{x_i^{(v)} \wedge x_j^{(v)}} = \overline{x_i^{(v)}} \vee \overline{x_j^{(v)}} & \forall i, j \end{cases}$$

$\forall e = (u, v) \in E$  i due vertici non devono avere lo stesso colore

$$\forall i \quad \overline{x_i^{(v)} \wedge x_i^{(u)}} = \overline{x_i^{(v)}} \vee \overline{x_i^{(u)}}$$

**Esempio 4.2.1.** Prendiamo per esempio il seguente grafo:



La formula booleana corrispondente sarà:

Un vertice non può avere 2 colori

$$\begin{array}{l} \text{Ogni vertice ha un colore} \left\{ \begin{array}{l} (x_0^{(u)} \vee x_1^{(u)} \vee x_2^{(u)}) \wedge (\overline{x_0^{(u)}} \vee \overline{x_1^{(u)}}) \wedge (\overline{x_0^{(u)}} \vee \overline{x_2^{(u)}}) \wedge (\overline{x_1^{(u)}} \vee \overline{x_2^{(u)}}) \wedge \\ (x_0^{(v)} \vee x_1^{(v)} \vee x_2^{(v)}) \wedge (\overline{x_0^{(v)}} \vee \overline{x_1^{(v)}}) \wedge (\overline{x_0^{(v)}} \vee \overline{x_2^{(v)}}) \wedge (\overline{x_1^{(v)}} \vee \overline{x_2^{(v)}}) \wedge \\ (x_0^{(z)} \vee x_1^{(z)} \vee x_2^{(z)}) \wedge (\overline{x_0^{(z)}} \vee \overline{x_1^{(z)}}) \wedge (\overline{x_0^{(z)}} \vee \overline{x_2^{(z)}}) \wedge (\overline{x_1^{(z)}} \vee \overline{x_2^{(z)}}) \wedge \end{array} \right. \\ \text{Ogni arco ha colori diversi} \left\{ \begin{array}{l} (\overline{x_0^{(v)}} \vee \overline{x_0^{(u)}}) \wedge (\overline{x_1^{(v)}} \vee \overline{x_1^{(u)}}) \wedge (\overline{x_2^{(v)}} \vee \overline{x_2^{(u)}}) \wedge \\ (\overline{x_0^{(v)}} \vee \overline{x_0^{(z)}}) \wedge (\overline{x_1^{(v)}} \vee \overline{x_1^{(z)}}) \wedge (\overline{x_2^{(v)}} \vee \overline{x_2^{(z)}}) \wedge \\ (\overline{x_0^{(z)}} \vee \overline{x_0^{(u)}}) \wedge (\overline{x_1^{(z)}} \vee \overline{x_1^{(u)}}) \wedge (\overline{x_2^{(z)}} \vee \overline{x_2^{(u)}}) \end{array} \right. \end{array}$$

La trasformazione è polinomiale? La complessità della trasformazione è:

$$|V| \cdot \left( K + 2 \binom{K}{2} \right) + |E|K \cdot 2 \leq (|E| + |V|)K^2$$

Quindi è polinomiale.

### 4.3 Problema NAE-K-SAT

**NAE-K-SAT (Not All Equivalent-K-SAT):**

- Input:  $\phi$  K-CNF  $\phi : \{T, F\}^n \mapsto \{T, F\}$
- Output:  $\text{yes} \Leftrightarrow \exists \underline{a} \in \{T, F\}^n$  t.c.  $\phi(\underline{a}) = T$  e, in ogni clausola  $C_i = l_1^{(i)} \vee l_2^{(i)} \vee \dots \vee l_k^{(i)}$  con  $\underline{a}$ , almeno un  $l_j^{(i)}$  è vero e almeno un  $l_j^{(i)}$  è falso.

**Esempio 4.3.1.**

$$\phi(x_1, x_2, x_3) = (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})$$

$$x_1 = F \quad x_2 = F \quad x_3 = F \quad \text{non è NAE-K-SAT}$$

$$x_1 = F \quad x_2 = T \quad x_3 = F \quad \text{è NAE-K-SAT}$$

**Proposizione 4.3.1.** Se  $\underline{a}$  è un assegnamento che soddisfa  $\phi$  (è NAE), allora anche il negato  $\overline{\underline{a}}$  soddisfa  $\phi$  (è NAE).

**3-SAT  $\leq_K$  NAE-4-SAT** Vogliamo dimostrare che data una qualsiasi formula  $\phi$  3-CNF la trasformo in una formula  $\psi$  4-CNF in tempo polinomiale.

$$\phi \text{ 3-CNF} \mapsto \psi \text{ 4-CNF}$$

$$\phi = C_1 \wedge C_2 \wedge \dots \wedge C_n \quad C_i = l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)} \quad i = 1 \dots n$$

$$\psi = C'_1 \wedge C'_2 \wedge \dots \wedge C'_n \quad C'_i = l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)} \vee z \quad i = 1 \dots n$$

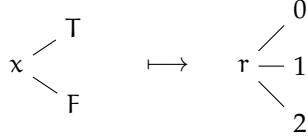
Per creare  $\psi$  espando le variabili e ne aggiungo sempre una. La trasformazione da  $\phi$  a  $\psi$  è polinomiale nella taglia della formula  $\phi$ , perché la scorro tutta per creare  $\psi$ .

Ora dobbiamo dimostrare che se  $\phi$  è soddisfacibile allora anche  $\psi$  è soddisfacibile:

- $\phi$  è soddisfacibile  $\Rightarrow \exists \underline{a} \in \{T, F\}^n$  t.c.  $\phi(\underline{a}) = T$ .
- Se prendiamo l'assegnamento  $\underline{b} = \underline{a} \quad z = F$   $\psi(\underline{b}) = T$  e ogni clausola ha un letterale a FALSE.
- Vogliamo dimostrare che se esiste un assegnamento  $\underline{b}$  che soddisfa  $\psi$  allora esiste un assegnamento  $\underline{a}$  che soddisfa  $\phi$ .
- Se secondo  $\underline{b} \quad z = F$  allora, la parte rimanente di  $\underline{b}$  soddisfa  $\psi$
- Se secondo  $\underline{b} \quad z = T$  allora, lo nego e torno al primo caso. Perciò se  $\psi$  è nae-soddisfatta con  $z = F$  allora  $\phi$  è soddisfatta.

**NAE-3-SAT  $\leq_K$  3-COL** Vogliamo dimostrare che data la formula  $\phi$  3-CNF esiste una trasformazione polinomiale che la rende un grafo  $G$  tale che  $\phi$  è NAE-soddisfacibile se e solo se il grafo  $G$  è 3-colorabile.

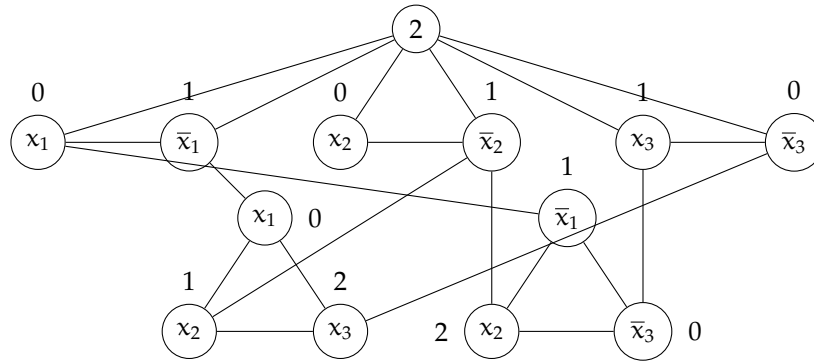
Mappo variabili (letterali) che possono valere T o F, su vertici (elementi del grafo) che hanno colore 0, 1, 2.



Partendo dalla formula  $\phi(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3)$  costruiamo il grafo nel seguente modo:

- Creo un nodo per ogni letterale e per il suo negato, poi aggiungo un vertice perché per ogni vertice  $x$  uso la stessa coppia di colori.
- Per ogni clausola metto un triangolo che corrisponde ai letterali della clausola
- Se ho una 3-colorazione ho un assegnamento corrispondente per la clausola che mi mette un letterale T e uno F.
- Ora aggiungo gli archi, collego i letterali che hanno valori di verità opposti.

Se associamo  $0 \mapsto T$ ,  $1 \mapsto F$ , e 2 libero, abbiamo il seguente risultato:



Perciò la trasformazione garantisce che se  $\exists \underline{a}$  t.c.  $\phi(\underline{a})$  è nae-soddisfatta allora esiste una 3-colorazione per il grafo  $G$  che associa ai valori di verità i colori in modo tale da rendere  $G$  3-colorabile. È facile vedere anche l'implicazione nel verso opposto.

#### 4.4 Transitività della riduzione alla Karp

La riduzione  $\leq_K$  è transitiva, ciò implica che:

$$A \leq_K B \text{ e } B \leq_K C \Rightarrow A \leq_K C$$

in particolare abbiamo che:

$$\begin{aligned} A \leq_K B \quad \exists \mathcal{A} \text{ polytime } x \in \mathcal{I}(A), \mathcal{A}(x) \in \mathcal{I}(B) \quad \mathcal{A}(x) = \text{yes} &\Leftrightarrow B(\mathcal{A}(x)) = \text{yes} \\ B \leq_K C \quad \exists \mathcal{B} \text{ polytime } y \in \mathcal{I}(B), \mathcal{B}(y) \in \mathcal{I}(C) \quad \mathcal{B}(y) = \text{yes} &\Leftrightarrow C(\mathcal{B}(y)) = \text{yes} \end{aligned}$$

Perciò

$$\forall x \in \mathcal{I}(A), \mathcal{B}(\mathcal{A}(x)) \in \mathcal{I}(C) \quad \mathcal{A}(x) = \text{yes} \Leftrightarrow C(\mathcal{B}(\mathcal{A}(x))) = \text{yes} \Rightarrow C(x) = \mathcal{B}(\mathcal{A}(x))$$

## 4.5 Problema Reachability

- Input: Grafo  $G$  diretto, due nodi  $s$  e  $t$ .
- Output:  $\text{yes} \Leftrightarrow$  esiste un cammino che va da  $s$  a  $t$ .

Quanto costa risolvere Reachability?

Una possibile soluzione potrebbe essere applicare BFS partendo da  $s$ . Se si trova  $t$ , allora ritorno  $\text{yes}$ , altrimenti  $\text{no}$ . Questo procedimento richiede  $O(|V| + |E|)$ . Quindi  $\text{Reachability} \in \mathbf{P}$

## 5 Riduzione alla Turing tra problemi di decisione

**Definizione 5.0.1** (Riduzione alla Turing).  $\mathbb{A} \leq_T \mathbb{B}$  se esiste un algoritmo con complessità polinomiale  $\mathcal{A}$  che data un'istanza  $x \in \mathcal{I}(\mathbb{A})$  utilizzando chiamate ad un *oracolo* per  $\mathbb{B}$  che hanno costo  $O(1)$ ,  $\mathcal{A}(x) = \mathbb{A}(x)$ .

## 6 Classe di problemi NP-Completi

**Definizione 6.0.2.** (Classe NPC) Un problema  $\mathbb{A}$  è NP-completo (NPC) se

- $\mathbb{A} \in \mathbf{NP}$
- $\mathbb{A}$  è *NP-hard*, cioè se  $\forall \mathbb{B} \in \mathbf{NP} \quad \mathbb{B} \leq_K \mathbb{A}$

### 6.1 Circuito Booleano

**Definizione 6.1.1** (Circuito Booleano). Un circuito booleano è un grafo aciclico orientato (DAG)  $C_n$  con  $n$  input e ha le seguenti caratteristiche:

- $\exists n$  vertici che hanno  $\text{in-degree} = 0$
- $\exists 1$  vertice che ha  $\text{out-degree} = 0$
- Ogni altro vertice ha  $\text{in-degree} = 1$  o  $2$  ed è etichettato con *and*, *or*, *not*.
- La taglia di  $C_n$  è il numero di vertici.

**Esempio 6.1.1.** Per  $n = 4$  abbiamo  $C_4(x_1, x_2, x_3, x_4)$ :

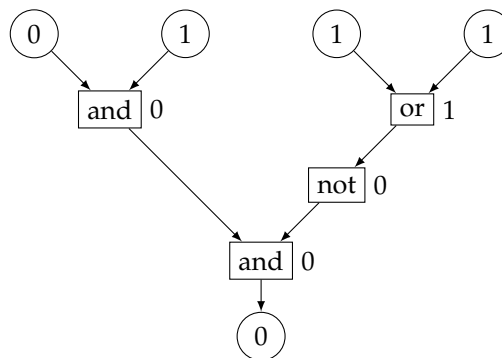


Figura 2: Esempio di circuito booleano con 4 input, il nodo finale di output è detto nodo *sink*.

## 6.2 Problema Circuit-SAT

- Input: Circuito booleano  $C_n$
- Output:  $\text{yes} \Leftrightarrow \exists \underline{x} \text{ t.c. } C(\underline{x}) = 1$  (il circuito booleano è soddisfacibile).

Definiamo una famiglia di circuiti  $C_{n \geq 0}$  (per ogni numero di input) di complessità  $T(n)$  tale che la taglia di  $C_n$  è  $O(T(n))$ .

Vogliamo mappare il verificatore di ogni problema in **NP** in un circuito:

$$\mathbb{A} \longmapsto V(\cdot, \cdot)$$

$$\mathbb{A}(\underline{x}) = \text{yes} \Leftrightarrow \exists w \text{ t.c. } V(\underline{x}, w) = \text{yes}$$

Dove  $V(\underline{x}, w)$  è un circuito che prende  $\underline{x}$  in input e che mi dice se esiste un certificato  $w$  tale che rende soddisfatto il circuito.

**Teorema 6.2.1.** Se  $\mathbb{A} \in \text{TIME}(f(n))$  allora esiste una famiglia di circuiti  $C_{n \geq 0}$  di complessità  $T(n) = O(f(n)^2)$  tale che  $\forall \underline{x} \in \mathcal{I}(\mathbb{A})$  e  $n = |\underline{x}|$   $C_n(\underline{x}) = \mathbb{A}(\underline{x})$  e  $C_n$  è costruibile in tempo polinomiale.

**Corollario 6.2.1.** Se  $\mathbb{A} \in \mathbf{P}$  ( $f(n)$  è un polinomio in  $\text{TIME}(f(n))$ ) allora esiste una famiglia di circuiti di complessità polinomiale ( $T(n) = n^k$ ) tale che  $\forall \underline{x} \in \mathcal{I}(\mathbb{A})$  e  $n = |\underline{x}|$   $C_n(\underline{x}) = \mathbb{A}(\underline{x})$  e  $C_n$  è costruibile in tempo polinomiale in  $|\underline{x}| = n$ .

**Circuit SAT è NP-completo** Dimostriamo prima a parole che Circuit-SAT  $\in \mathbf{NP}$ . Forniamo il verificatore  $V(\underline{x}, w)$  verifica se un'istanza soddisfa il problema. Il certificato  $w$  è l'assegnamento che soddisfa il circuito, mentre il verificatore scorre ogni nodo e ne valuta il valore, ritorna  $\text{yes}$  se il nodo finale (sink) è a 1, altrimenti no.

Ora dimostriamo che Circuit-SAT è NP-hard, ovvero che  $\forall \mathbb{A} \in \mathbf{NP}$   $\mathbb{A} \leq_K \text{Circuit-SAT}$ . Dobbiamo mostrare dunque che esiste tale trasformazione polinomiale:

$$\underline{x} \in \mathcal{I}(\mathbb{A}) \longmapsto C \in \mathcal{I}(\text{Circuit-SAT})$$

e vale anche che:

$$\mathbb{A} = \text{yes} \Leftrightarrow \exists w \text{ t.c. } C(w) = 1 \text{ (C è soddisfacibile)}$$

Sia  $\mathbb{A} \in \mathbf{NP}$  allora  $\exists V_{\mathbb{A}}(\underline{x}, w)$  per le istanze  $\underline{x} \in \mathcal{I}(\mathbb{A})$ , tale che  $V_{\mathbb{A}}$  ha complessità  $O(p(|\underline{x}|)) = |w|$  (polinomiale). Allora per il teorema 6.2.1 sappiamo che esiste una famiglia di circuiti  $C_m$  che fa esattamente ciò che fa il verificatore  $V_{\mathbb{A}}$ :

$$C_m = V_{\mathbb{A}} \quad m = |\underline{x}| + p(|\underline{x}|)$$

perciò, se consideriamo  $C'_x(\underline{x}) = C_m(\underline{x}, w)$

$$\mathbb{A}(\underline{x}) = \text{yes} \Leftrightarrow \exists w \text{ t.c. } V_{\mathbb{A}}(\underline{x}, w) = \text{yes} \Leftrightarrow \exists w \text{ t.c. } C_m(\underline{x}, w) = 1 \Leftrightarrow \exists w \text{ t.c. } C'_x(\underline{x}) = 1$$

**SAT è NP-completo** Vogliamo dimostrare che dato un circuito booleano soddisfacibile esiste una riduzione che lo trasforma in tempo polinomiale in una formula booleana soddisfacibile.

$$\text{Circuit-SAT} \leq_K \text{SAT}$$

$$\forall C \in \mathcal{I}(\text{Circuit-SAT}) \longmapsto \phi(\dots)$$

$$C \text{ è soddisfacibile} \Leftrightarrow \phi \text{ è soddisfacibile}$$

**Osservazione 6.2.1.** Ogni funzione di gate (and, or, not, ...) può essere espressa con una formula booleana CNF  $\phi$ :

$$\begin{aligned} c = a \text{ and } b & \quad (\bar{c} \vee a) \wedge (\bar{c} \vee b) \wedge (c \vee \bar{a} \vee \bar{b}) \\ c = a \text{ or } b & \quad (\bar{c} \vee a \vee b) \wedge (c \vee \bar{b}) \wedge (c \vee \bar{a}) \\ c = \text{not } a & \quad (\bar{c} \vee \bar{a}) \wedge (c \vee a) \end{aligned}$$

Quindi un circuito booleano è soddisfatto quando ogni formula è soddisfatta e il nodo sink è soddisfatto (= 1).

Perciò se ogni funzione di gate sottoforma di circuito booleano rappresenta ogni clausola della formula CNF  $\phi$ , allora possiamo mettere in and tutte le clausole e dire che il circuito C è soddisfatto se e solo se  $\phi$  è soddisfatta.

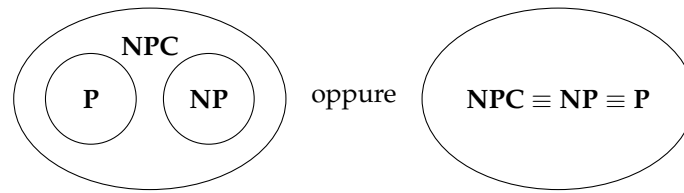
Con questo e con la dimostrazione che Circuit-SAT è NP-completo possiamo dire che

$$\forall \mathbb{B} \in \mathbf{NP} \quad \mathbb{B} \leq_K \text{Circuit-SAT} \leq_K \text{SAT}$$

Perciò, per la proprietà transitiva della riduzione alla Karp tra problemi di decisione, deduciamo che SAT è NP-completo.

### 6.3 Relazione tra P, NP, e NP-completo

Distinguiamo principalmente due casi che rappresentano le relazioni tra le classi di problemi P, NP e NP-completo:



**Teorema 6.3.1.** Se  $\mathbf{NPC} \cap \mathbf{P} \neq \emptyset$  e  $\mathbb{A} \in \mathbf{NP}$  t.c.  $\mathbb{A}$  *non è banale*, ovvero

$$\exists x \in \mathcal{I}(\mathbb{A}) \quad \text{t.c. } \mathbb{A}(x) = \text{yes}$$

$$\exists y \in \mathcal{I}(\mathbb{A}) \quad \text{t.c. } \mathbb{A}(y) = \text{no}$$

Allora  $\mathbb{A} \in \mathbf{NPC}$

*Dimostrazione.* Se  $\mathbf{NPC} \cap \mathbf{P} \neq \emptyset \quad \exists \mathbb{B} \text{ Np-hard} \quad \text{t.c. } \mathbb{B} \in \mathbf{P} \wedge \forall \mathbb{C} \in \mathbf{NP} \quad \mathbb{C} \leq_K \mathbb{B}$ . Perciò deduciamo che  $\mathbb{C} \in \mathbf{P}$ , quindi ogni problema che è in NP è anche in P e viceversa. Quindi  $\mathbf{P} \equiv \mathbf{NP}$ .

Dobbiamo quindi dimostrare che ogni problema in NP si riduce polinomialmente ad  $\mathbb{A}$ . Prendiamo come esempio il seguente problema *bit*:

- Input: Bit b
- Output: yes  $\Leftrightarrow b = 1$

Sia  $\mathbb{D}$  un problema  $\mathbb{D} \in \mathbf{NP}$  e quindi  $\mathbb{D} \in \mathbf{P}$  (c'è un risolutore polinomiale per  $\mathbb{D}$ ). Dobbiamo trovare una trasformazione  $f(x)$  tale che riduce il problema  $\mathbb{D}$  al problema *bit*:

$$f(x) = \begin{cases} 1 & \text{se } \mathbb{D}(x) = \text{yes} \\ 0 & \text{altrimenti} \end{cases}$$

dove  $x \in \mathcal{I}(\mathbb{D})$ .

Sappiamo quindi risolvere  $f(x)$  in tempo polinomiale perché sappiamo risolvere  $\mathbb{D}$  in tempo polinomiale poiché  $\mathbb{D} \in \mathbf{NP} \wedge \mathbb{D} \in \mathbf{P}$ . Quindi siano  $x$  e  $y$

$$x_{\text{yes}} \in \mathcal{I}(\mathbb{A}) \quad \text{t.c. } \mathbb{A}(x_{\text{yes}}) = \text{yes}$$

$$x_{\text{no}} \in \mathcal{I}(\mathbb{A}) \quad \text{t.c. } \mathbb{A}(x_{\text{no}}) = \text{no}$$

allora la trasformazione  $f(x)$  sarà:

$$f(x) = \begin{cases} x_{\text{yes}} & \text{se } \mathbb{D}(x) = \text{yes} \\ x_{\text{no}} & \text{se } \mathbb{D}(x) = \text{no} \end{cases}$$

□



## 7 Classe di problemi CO-NP

**Definizione 7.0.1.** (Classe CO-NP) L'insieme dei problemi CO-NP è definito nel seguente modo:

$$\text{CO-NP} = \{A \mid \bar{A} \in \text{NP}\}$$

Sono quei problemi per cui è "facile" verificare le istanze no.

Di seguito forniamo un paio di esempi di problemi:

**Esempio 7.0.1.** Problema:

- Input: Grafo G
- Output: yes se G non è colorabile con 7 colori.

Questo problema è il complemento del problema 7-COL. Quest'ultimo appartiene alla classe NP quindi il problema in esempio è in CO-NP.

**Esempio 7.0.2.** Problema:

- Input: formula booleana  $\phi$
- Output: yes se  $\forall a \phi(a) = T$

Per questo problema è facile vedere che esiste un'istanza no poiché basta che ci sia almeno una clausola con tutti i letterali a false. Quindi appartiene a CO-NP.

### 7.1 Relazione tra P, NP e CO-NP

**Teorema 7.1.1.** Se  $\exists A$  t.c.  $A \in \text{NPC} \cap \text{CO-NP}$  allora  $\text{NP} \equiv \text{CO-NP}$ .

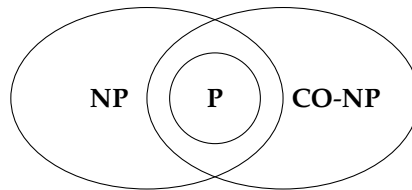
$\text{CO-NP} \subseteq \text{NP}$ . Supponiamo che  $A \in \text{NPC}$  allora  $A \in \text{NP}$  e  $\forall C \in \text{NP} \quad C \leq_K A$ .

Se prendiamo il problema  $B \in \text{CO-NP}$   $\bar{B} \in \text{NP}$ .

Allora esiste una riduzione alla Karp  $\bar{B} \leq_K A$  che mappa le istanze yes di B alle istanze no di A ed esiste anche una riduzione  $B \leq_K \bar{A}$  che è duale alla precedente.

Poiché  $A \in \text{CO-NP}$  allora  $\bar{A} \in \text{NP}$ . Quindi B si riduce polinomialmente ad un problema in NP. Quindi  $B \in \text{NP}$ . Quindi per estensione  $\text{CO-NP} \subseteq \text{NP}$ .  $\square$

$\text{NP} \subseteq \text{CO-NP}$ . Sia  $C \in \text{NP}$   $C \leq_K A$   $\bar{C} \leq_K \bar{A}$ . Poiché  $A \in \text{CO-NP}$  allora  $\bar{A} \in \text{NP}$ . Quindi  $\bar{C} \in \text{NP} \Rightarrow C \in \text{CO-NP} \Rightarrow \text{NP} \subseteq \text{CO-NP}$ .  $\square$



**Cosa succede se  $P \equiv \text{CO-NP}$ ?** Se abbiamo l'equivalenza di queste due classi di problemi si ha che:

$$\begin{aligned} A(x) \in \text{NP} & \quad \mathcal{A}(x) = \exists w B(x, w) \in P \\ A(x) \in \text{CO-NP} & \quad \mathcal{A}(x) = \forall w B(x, w) \in P \end{aligned}$$

- Se  $\text{NP} \neq \text{CO-NP} \Rightarrow P \neq \text{NP}$
- Se  $P = \text{NP}$  siccome  $P = \text{CO-NP}$   $\forall A \in \text{NP}, A \in P \Rightarrow \bar{A} \in P = \text{NP} \Rightarrow \text{NP} = \text{CO-NP}$

**Definizione 7.1.1** (Hardness del problema  $\mathbb{A}$  nella classe **CO-NP**).  $\mathbb{A}$  è **CO-NP-completo** se  $\mathbb{A} \in \text{CO-NP}$  e  $\forall \mathbb{B} \in \text{CO-NP} \quad \mathbb{B} \leq_K \mathbb{A}$ .

**Teorema 7.1.2.** Se  $\mathbb{A}$  è **NP-completo** allora  $\overline{\mathbb{A}}$  è **CO-NP-completo** e viceversa.

*Dimostrazione.* Se  $\mathbb{A}$  è **NP-completo**, allora

- $\mathbb{A} \in \text{NP}$
- $\forall \mathbb{B} \in \text{NP} \quad \mathbb{B} \leq_K \mathbb{A}$

Dalla prima deduciamo che  $\Rightarrow \overline{\mathbb{A}} \in \text{CO-NP}$

Dalla seconda invece, se  $\mathbb{C} \in \text{CO-NP}$ ,  $\overline{\mathbb{C}} \in \text{CO-NP} \Rightarrow \overline{\mathbb{C}} \leq_K \mathbb{A} \Rightarrow \mathbb{C} \leq_K \overline{\mathbb{A}}$

$\Rightarrow \forall \mathbb{C} \in \text{CO-NP} \Rightarrow \mathbb{C} \leq_K \overline{\mathbb{A}}$

Da queste due deduzioni abbiamo quindi la definizione di **CO-NP-completo** per  $\overline{\mathbb{A}}$  □

1. Se vogliamo dimostrare che è **CO-NP-completo** possiamo dimostrare che *il complemento è NP-completo*.
2. Per dimostrare che  $\mathbb{A}$  è **NP-completo**
  - (a)  $\mathbb{A} \in \text{NP}$
  - (b)  $\forall \mathbb{B} \quad \mathbb{B} \leq_K \mathbb{A}$

## 7.2 Problema Minimo circuito booleano

- Input: Circuito booleano  $C_n$  (con  $n$  input)
- Output: yes  $\Leftrightarrow \nexists$  circuito  $C'$  t.c.  $\forall x \quad C'(x) = C(x)$  con  $|C'| < |C|$

Consideriamo l'algoritmo  $\mathcal{A}$

$$\mathcal{A}(x) = \forall w_1 \exists w_2 \quad B(x, w_1, w_2) = \text{yes} \quad \text{con } B \in \mathbf{P} \text{ e } |w_i| = O(p_i(|x|))$$

Se minimo circuito booleano  $\in \text{NP}$  allora:  $\forall w_1 \exists w_2 \quad B(x, w_1, w_2) \equiv \exists w' \quad B'(x, w')$ .

Se minimo circuito booleano  $\in \text{CO-NP}$  allora:  $\forall w'' \quad B''(x, w'')$ .

## 8 Gerarchia Polinomiale

**Definizione 8.0.1** (Classe di problemi  $\Pi_i \mathbf{P}$ ).

$$\Pi_i \mathbf{P} = \{ \mathcal{A}(x) = \forall w_1 \exists w_2 \forall w_3 \exists w_4 \dots Q_i w_i \quad B(x, w_1, \dots, w_i) \quad \text{dove } |w_i| = O(p_i(|x|)) \text{ e } B \in \mathbf{P} \}$$

**Definizione 8.0.2** (Classe di problemi  $\Sigma_i \mathbf{P}$ ).

$$\Sigma_i \mathbf{P} = \{ \mathcal{A}(x) = \exists w_1 \forall w_2 \exists w_3 \forall w_4 \dots Q_i w_i \quad B(x, w_1, \dots, w_i) \quad \text{dove } |w_i| = O(p_i(|x|)) \text{ e } B \in \mathbf{P} \}$$

Dalla definizione di queste classi di problemi deduciamo che:

$$\Pi_0 \mathbf{P} = \Sigma_0 \mathbf{P} = \mathbf{P} \quad \mathcal{A}(x) = B(x) \text{ non ho quantificatori}$$

$$\Pi_1 \mathbf{P} = \text{NP}$$

$$\Sigma_1 \mathbf{P} = \text{CO-NP}$$

$$\text{Minimo circuito booleano} \in \Pi_2 \mathbf{P}$$

**Osservazione 8.0.1.**  $\mathcal{A}(x) \in \Pi_i \mathbf{P} \Leftrightarrow \overline{\mathcal{A}(x)} \in \Sigma_i \mathbf{P}$ .

**Osservazione 8.0.2.**  $\Pi_i \mathbf{P} \subseteq \Sigma_{i+1} \mathbf{P}$  e  $\Sigma_i \mathbf{P} \subseteq \Pi_{i+1} \mathbf{P}$ .

Infatti se aggiungo un quantificatore all'inizio, ho che

$$\mathcal{A}(x) \in \Pi_i \mathbf{P}$$

$$\mathcal{A}(x) = \forall w_1 \exists w_2 \dots Q_i w_i \quad B(x, w_1, w_2, \dots, w_i)$$

$$\Sigma_{i+1} \mathbf{P} = \exists w^* \forall w_1 \exists w_2 \dots Q_i w_i \quad B'(x, w^*, w_1, w_2, \dots, w_i)$$

Perciò  $B'(\dots) = B(\dots)$

**Osservazione 8.0.3.** Per lo stesso motivo dell'osservazione precedente vale che:  
 $\Pi_i P \subseteq \Pi_{i+1} P$  e  $\Sigma_i P \subseteq \Sigma_{i+1} P$ .

**Osservazione 8.0.4.** Se  $P \equiv NP \Rightarrow \forall i \Sigma_i P = P \wedge \Pi_i P = P$   
 cioè abbiamo che:

$$B(x, w_1, w_2, \dots, w_i) = B'(x) \text{ (elimino tutte le quantificazioni)}$$

**Proposizione 8.0.1.** Se  $NP = CO-NP \Rightarrow \Sigma_1 P = \Pi_1 P$ .

Quindi  $\Sigma_i P = \Pi_i P = \Sigma_1 P = \Pi_1 P \quad \forall i \geq 1$ .

Tutte le classi sopra collassano sulla classe 1.

*Dimostrazione.* Assumiamo che  $NP \equiv CO-NP$ :

$$A(x) = \exists w_1 B(x, w_1) \Leftrightarrow A(x) = \forall w_1 B'(x, w_1)$$

$$\text{Sia } A'(x) \in \Sigma_1 P \quad A'(x) = \exists w_1 \forall w_2 C(x, w_1, w_2) = \mathcal{D}_{w_2}(x).$$

$\mathcal{D}_{w_2}(x) \in CO-NP \equiv NP$  quindi  $\mathcal{D}_{w_2}(x) = \exists w'_1 C'(x, w'_1, w_2)$  perciò diventa:

$$\begin{aligned} A'(x) &= \exists w_2 \exists w'_1 C'(x, w'_1, w_2) \\ &= \exists w_{12} C'(x, w_{12}) \in NP \end{aligned}$$

Quindi deduciamo che se  $NP \equiv CO-NP \Rightarrow \Sigma_2 P = \Sigma_1 P$  □

**Definizione 8.0.3** (Gerarchia Polinomiale). Definiamo gerarchia polinomiale la classe **PH** delle proprietà  $\mathbb{A}$  che possono essere espresse da una formula con quantificatori contenente un numero costante di quantificatori alternati:

$$PH = \bigcup_k \Sigma_k P = \bigcup_k \Pi_k P$$

**Teorema 8.0.1** (Collasso della gerarchia polinomiale). Se

$$P = NP \Rightarrow NP = CO-NP = P \Rightarrow \Sigma_i P = \Pi_i P = P \quad \forall i$$

la gerarchia polinomiale collassa in  $P$ .

Se  $NP = CO-NP \Rightarrow PH = NP = CO-NP$ .

**Teorema 8.0.2.** Se  $\Pi_i P = \Sigma_i P \Rightarrow PH = \Pi_i P = \Sigma_i P$

## 8.1 Funzione time-costruibile

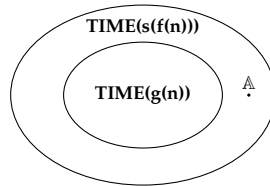
**Proposizione 8.1.1.** Nel modello computazionale in oggetto è possibile simulare  $t$  passi di un algoritmo (programma) mentre controlliamo che  $\leq t$  passi sono fatti in  $s(t)$  passi.

**Esempio 8.1.1.** Se il modello computazionale è la Macchina di Turing, allora  $s(t) = O(t \log t)$ .

**Esempio 8.1.2.** Se il modello computazionale è la RAM, allora  $s(t) = O(t)$

**Definizione 8.1.1.** Diciamo che  $f(n)$  è **Time-costruibile** se esiste un programma (algoritmo) che calcola  $f(n)$  in  $O(f(n))$ .

**Teorema 8.1.1.** Data l'assunzione precedente, per ogni funzione  $f(n)$  time-costruibile e per ogni  $g(n) = o(f(n))$  la classe  $TIME(g(n)) \subset TIME(s(f(n)))$



## 8.2 Problema Catch 22

- Input:  $\Pi$  (programma)
- Output: se  $\Pi(\Pi)$  termina in meno di  $f(|\Pi|)$  passi allora ritorna  $\overline{\Pi(\Pi)}$  altrimenti ritorna 0.

Supponiamo che esista un algoritmo  $\Pi_{22}$  tale che risolve il problema Catch 22 in  $g(n)$  passi, dove  $g(n) < f(n)$ . Questo è equivalente a dire che  $\text{Catch 22} \in \mathbf{TIME}(g(n))$ .

Se  $\Pi_{22}(\Pi_{22}) = \text{Catch 22}(\Pi_{22})$  siccome ci mette meno di  $f(\Pi_{22})$  passi, allora è uguale a  $\overline{\Pi_{22}(\Pi_{22})}$ . Questo è assurdo perché non può essere che  $\Pi_{22}(\Pi_{22}) = \overline{\Pi_{22}(\Pi_{22})}$ , quindi *non* esiste l'algoritmo  $\Pi_{22}$  che impiega  $g(n) < f(n)$  passi.

Supponiamo che il programma  $\Pi$  risolve Catch 22 se e solo se  $\forall x \in \mathcal{I}(\text{Catch 22}) \quad \Pi(x) = \text{Catch 22}(x)$ . Se  $\Pi$  termina in  $\leq f(n)$  passi per ogni  $x$ , allora  $\exists x$  t.c.  $\Pi(x) \neq \text{Catch 22}(x)$ .

**Proposizione 8.2.1.** Per ogni algoritmo esistono infiniti programmi  $\Pi$  che implementano l'algoritmo (fanno la stessa cosa) di lunghezza arbitrariamente grandi.

**Proposizione 8.2.2.** Per ogni  $n \geq |\Pi_{22}|$  fissato esiste un altro  $\Pi'_{22}$  tale che  $|\Pi'_{22}| = n$ . Quindi  $\Pi'_{22}(\Pi'_{22}) = \Pi_{22}(\Pi_{22})$ .

## 9 Teorema di Ladner

Ci chiediamo se esiste un problema **NP** che non appartiene né alla classe **P** né alla classe **NPC**.

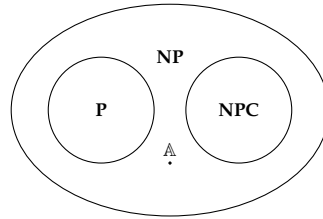


Figura 3: Esiste il problema  $\mathbb{A}$ ?

**Teorema 9.0.1** (Teorema di Ladner). Se  $P \neq NP$  allora esiste un problema  $\mathbb{A} \in NP \setminus (P \cup NPC)$ .

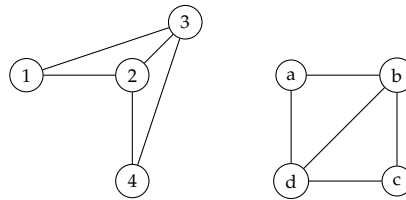
*Dimostrazione.* Vediamo un problema esempio che soddisfa il teorema di Ladner:

### Graph Isomorphism

- Input:  $G_1, G_2$  grafi
- Output:  $\text{yes} \Leftrightarrow G_1$  è isomorfo a  $G_2$ .

**Definizione 9.0.1** (Isomorfismo).  $\exists f: V(G_1) \mapsto V(G_2)$   
t.c.  $(v, u) \in E(G_1) \Leftrightarrow (f(v), f(u)) \in E(G_2)$

**Esempio 9.0.1** (Grafici isomorfi). Ecco un esempio di due grafi isomorfi:



$$\begin{aligned} f(1) &= a & f(2) &= b \\ f(3) &= c & f(4) &= d \end{aligned}$$

$$A(x) = \begin{cases} \text{SAT}(x) & \text{se } f(|x|) \text{ è pari} \\ 0 & \text{se } f(|x|) \text{ è dispari} \end{cases}$$

Vogliamo far vedere che:

1.  $A \in \mathbf{NP}$
2.  $A \notin \mathbf{P}$ , cioè  $\forall \Pi$  polinomiale  $\exists x$  t.c.  $\Pi(x) \neq A(x)$ .
3.  $A \notin \mathbf{NPC}$ , cioè  $\forall \Pi$  polinomiale  $\exists x$  t.c.  $\text{SAT}(x) \neq A(\Pi(x))$ .  
Se SAT è NPC sappiamo che  $\text{SAT} \leq_K A$

□

## 9.1 Problema Clique

- Input: grafo  $G = (V, E), K$
- Output: yes  $\Leftrightarrow G$  contiene una clique di taglia  $K$

**Clique** è un insieme di vertici tutti connessi a due a due da un arco.

**Clique**  $\in \mathbf{NPC}$  Facciamo vedere che il problema Clique appartiene alla classe **NPC** e che quindi appartiene alla classe **NP** e che esiste la riduzione  $3\text{-SAT} \leq_K \text{Clique}$  che trasforma in tempo polinomiale una formula  $\phi$  CNF in un grafo per il problema Clique.

**Clique**  $\in \mathbf{NP}$  Creiamo un verificatore per il problema Clique:

- Conta i vertici del grafo  $C$ .  $[O(n)]$
- Per ogni  $(u, v) \in C$  verifica che  $(u, v) \in E$ .  $[O(|K|^2 \times |E|)]$

Questo verificatore è polinomiale.

Il certificato per il verificatore è una clique  $C$  di taglia  $K$  in  $G$ , tale clique ha taglia polinomiale perché  $K$  può essere al massimo  $n$ . Perciò **Clique**  $\in \mathbf{NP}$ .

**3-SAT**  $\leq_K$  **Clique** Vediamo la seguente riduzione che mappa la formula

$$\phi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3)$$

in un grafo che soddisfa il problema Clique.

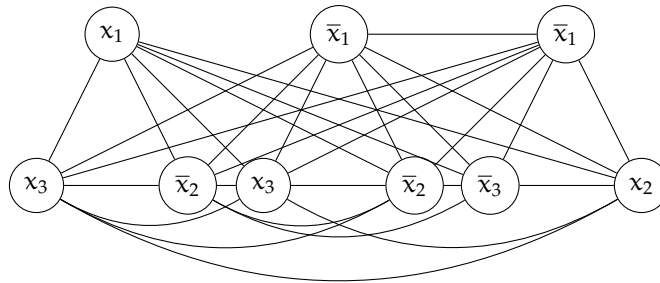


Figura 4: Grafo in cui c'è un arco per ogni letterale diverso dal proprio negato

Il grafo mostra le seguenti caratteristiche:

- Numero di vertici:  $|V| = 3m$  con  $\phi = C^{(1)} \wedge \dots \wedge C^{(m)}$ .

- Numero di archi:  $|E| \leq 9m^2$

Quindi il grafo, e di conseguenza la riduzione, è costruibile in tempo polinomiale.

Dimostriamo ora che se  $\phi$  è soddisfacibile allora esiste un assegnamento  $a_1, a_2, \dots, a_n$  per  $x_1, \dots, x_n$  tale che in ogni clausola un letterale è posto a T.

Siano  $v_{i1}^{(1)} v_{i2}^{(2)} \dots v_{in}^{(n)}$  i vertici corrispondenti ai letterali posti a T dell'assegnamento (uno per clausola). Tali vertici rappresentano nel grafo una clique.

Dimostriamo ora che se  $G$  ha una clique di taglia  $m$  allora  $\phi$  è soddisfacibile. Supponiamo che  $G$  abbia una clique  $C$  di taglia  $m$ .

1. Gli  $m$  vertici di  $C$  sono uno per tripla. Le triple corrispondono alle clausole.
2. Due vertici in  $C$  non corrispondono a letterali opposti di  $\phi$ .

Dall'ultimo punto in questione costruiamo un assegnamento che soddisfa  $\phi$ . Se prendiamo i vertici di  $C$  e li assegniamo a T, gli altri vengono assegnati di conseguenza:

$$\begin{aligned} \bar{x}_2 = T \quad x_2 = F \\ \bar{x}_3 = T \quad x_3 = F \\ x_1 = F \end{aligned}$$

Perciò abbiamo che

$$\phi(F, F, F) = (x_1 \underset{F}{\vee} \bar{x}_2 \underset{T}{\vee} x_3 \underset{F}{\vee}) \wedge (\bar{x}_1 \underset{T}{\vee} x_2 \underset{F}{\vee} x_3 \underset{F}{\vee}) \wedge (\bar{x}_1 \underset{T}{\vee} x_2 \underset{F}{\vee} x_3 \underset{F}{\vee}) = T$$

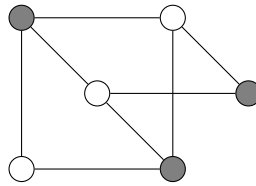
## 9.2 Problema Independent Set

- Input: Grafo  $G = (V, E), k$
- Output: yes  $\Leftrightarrow$  in  $G$  c'è un Independent Set di taglia  $\geq k$ .

**Definizione 9.2.1** (Independent Set). Un independent set è un insieme  $I$ :

$$I \subseteq V \quad \text{t.c.} \quad \forall (u, v) \in I \quad (u, v) \notin E$$

**Esempio 9.2.1** (Independent Set). Vediamo un esempio di independent set:



**IndSet**  $\in$  NPC Esiste una riduzione  $\text{Clique} \leq_K \text{IndSet}$  tale che

$$(G = (V, E), k) \mapsto (G' = (V, E), k)$$

**Problema TreeIndependentSet** Dimostriamo che il seguente problema appartiene alla classe P:

- Input: grafo *connesso* e *aciclico*  $G = (V, E), k$ .
- Output: yes  $\Leftrightarrow$   $G$  ha un Independent Set di taglia  $k$ .

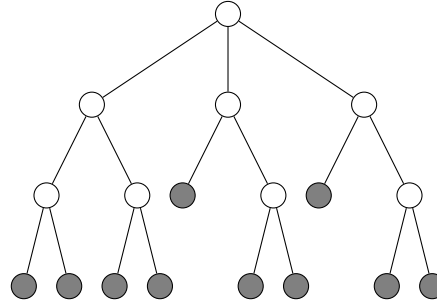


Figura 5: Esempio di Tree independent Set

**Osservazione 9.2.1.** Si può osservare che le *foglie* di un albero (grafo connesso e aciclico) rappresentano un independent set massimo.

Costruiamo quindi l'algoritmo che dimostra che il problema è in **P**:

Algorithm 3: Algoritmo che risolve TreeIndependentSet

---

```

TreeIndSetSolver( $G = (V, E)$ ,  $k$ )
   $I \leftarrow \emptyset$ 
  while  $V \neq \emptyset$ :
    foreach  $v$  t.c.  $d(v) \leq 1$ :
       $I \leftarrow I \cup \{v\}$ 
      remove i vicini  $v$  da  $G$ 
  if  $|I| \geq k$  return yes
  else return no

```

---

**Problema Only Small Independent Set** Vediamo ora il problema OSIS:

- Input:  $G = (V, E)$ ,  $k$
- Output: yes  $\Leftrightarrow$  ogni Independent Set  $I$ ,  $|I| \leq k$ .

Se esiste un algoritmo  $\mathcal{A}$  che risolve questo problema in tempo polinomiale allora

$$\mathbf{NP} \cap \mathbf{P} \neq \emptyset \Rightarrow \mathbf{P} = \mathbf{NP}$$

Perciò avremmo che

$$\forall (G, k) \quad \mathcal{A}(G, k) = \text{yes} \Leftrightarrow \text{OSIS}(G, k) = \text{yes}$$

dove la taglia di  $\mathcal{A}$  è  $T_{\mathcal{A}} = \left( O(|G| + (\log |k|)^c) \right)$ .

Abbiamo dunque un algoritmo  $\mathcal{B}^{\text{IndSet}} = \overline{\mathcal{A}(G, k-1)}$ .

**Osservazione 9.2.2.** Osserviamo che è facile verificare il no di istanze del problema OSIS, inoltre si può vedere che tale problema è il duale di IndSet, il quale appartiene alla classe **NPC**. Concludiamo dunque dicendo che  $\text{OSIS} \in \mathbf{CO-NPC}$ .

## 10 Ricavare problemi di ottimizzazione e ricerca

### 10.1 Independent Set

Vediamo ora diverse formulazioni per il problema Independent Set:

- **Optimization Problem: IndSet-Opt**
  - Input:  $G$
  - Output: un IndSet di massima cardinalità
- **Decision Problem: IndSet-Dec**
  - Input:  $G, k \in \mathbb{N}$
  - Output:  $\text{yes} \Leftrightarrow G$  ha un IndSet di cardinalità  $\geq k$
- **Search Problem: IndSet-Search**
  - Input:  $G, k \in \mathbb{N}$
  - Output: un IndSet di  $G$  t.c.  $|I| \geq k$  se esiste, altrimenti no.

Dimostriamo che se  $P = NP$  allora esiste un algoritmo che in tempo polinomiale trova un Independent Set di taglia massima in  $G$ .

Se  $P = NP$  allora esiste un algoritmo  $\mathcal{A}$  polinomiale per **IndSet-Dec**:

$\Rightarrow \forall (G, k) \quad \mathcal{A}(G, k) = \text{yes} \Leftrightarrow$  esiste in  $G$  un IndSet di taglia  $k$ .

$\Rightarrow$  In tempo polinomiale posso trovare  $k^*$  tale che esiste un IndSet in  $G$  di taglia  $k^*$  e ogni IndSet di  $G$  ha taglia al più

$$k^* = \max\{k \mid \exists I, \text{IndSet di } G, |I| = k\}$$

Per  $v \in V$  se in  $G - v - \{u \mid (u, v) \in E\}$  (i vicini di  $u$ ) non esiste un IndSet di taglia  $k^* - 1$  allora nessun IndSet di taglia  $k^*$  contiene  $v$ .

Per  $v \in V$  se in  $G - v - \{u \mid (u, v) \in E\}$  contiene un IndSet  $I'$  di taglia  $k^* - 1$  allora  $I' \cup \{v\}$  è un IndSet di  $G$ . Dove  $|I \cup \{v\}| = k^*$

Vediamo ora l'algoritmo che permette di costruire un IndSet:

Algorithm 4: Algoritmo di Ottimizzazione per IndSet

---

```

CostruisciIndSet( $G, k^*$ )
  if  $\mathcal{A}(G, k^*) = \text{no}$ :
    return no
  else
     $\tilde{G} \leftarrow G, I \leftarrow \emptyset$ 
    foreach  $v \in V$ :
      if  $\mathcal{A}(\tilde{G} - v - N(v), k - 1) = \text{yes}$ :
         $I \leftarrow I \cup \{v\}$ 
         $\tilde{G} \leftarrow \tilde{G} - v - N(v)$ 
         $k \leftarrow k - 1$ 
    return  $I$ 

```

---

Dove  $N(v) = \{u \mid (u, v) \in E\}$

Se  $\mathcal{A}$  utilizza tempo  $T_{\mathcal{A}}(G)$ , il tempo di **CostruisciIndSet** è  $O(nT_{\mathcal{A}}(G))$

Quindi sapendo risolvere il problema di decisione in tempo polinomiale, riusciamo a risolvere il problema di ottimizzazione in tempo polinomiale.



## 10.2 Problema SAT-Search

- Input:  $\phi$  CNF
- Output: assegnamento  $\underline{a}$  t.c.  $\phi(\underline{a}) = T$ , se esiste, altrimenti no.

Vediamo ora che dato un algoritmo polinomiale  $\mathcal{A}$  per il problema **SAT-Dec**, riusciamo a trovare un algoritmo polinomiale per **SAT-Search**.

L'idea è di procedere per passi. Prendiamo la seguente formula booleana CNF:

$$\phi(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \overline{x_3})$$

Assegniamo  $x_1 = T$  ed eliminiamo così la prima clausola, poiché è sempre vera dato l'assegnamento:

$$\phi'(x_2, x_3) = (\overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_3})$$

L'algoritmo procede facendo lo stesso per  $x_2$  e  $x_3$ . Infine otteniamo la formula  $\phi_{x_1=a_1 \dots x_i=a_i}$  ottenuta dopo aver fissato ogni variabile.

---

### Algorithm 5: Algoritmo di Ricerca per SAT

---

```

SAT-Solver( $\phi$ )
  if  $\mathcal{A}(\phi) = \text{no}$ :
    return no
  for  $i = 1$  to  $n$ :
     $a_i \leftarrow T$ 
    if  $\mathcal{A}(\phi_{x_1=a_1 \dots x_i=a_i}) = \text{no}$ :
       $a_i \leftarrow F$ 
  return  $a_1, a_2, \dots, a_i$ 

```

---

Qual è la complessità?  $T_{\text{SAT-Solver}}(|\phi|) = O(|\phi| \cdot T_{\mathcal{A}}(|\phi|))$ , è quindi polytime.

Abbiamo dimostrato quindi che se sappiamo risolvere il problema di decisione in tempo polinomiale, allora sappiamo risolvere anche il relativo problema di ricerca in tempo polinomiale.

## 10.3 Self Reducibility

**Proposizione 10.3.1.** Abbiamo visto che per ogni problema **NPC**, se esiste un algoritmo polinomiale per il problema di *decisione*, esiste un algoritmo polinomiale per il problema di *ricerca* corrispondente.

Se  $P \neq NP$  esiste un problema in **NP** per cui *non* vale "quanto sopra".

**Decision e search per i problemi in NP** Vediamo le definizioni dei problemi di decisione e di ricerca per i problemi della classe **NP**, cioè i problemi per cui

$$\mathbb{A} \in \mathbf{NP} \Leftrightarrow \exists V_{\mathbb{A}}(\cdot, \cdot) \text{ t.c. } \mathbb{A}(x) = \text{yes} \Leftrightarrow \exists w V_{\mathbb{A}}(x, w) = \text{yes}$$

Dato  $\mathbb{A} \in \mathbf{NP}$  e il verificatore  $V_{\mathbb{A}}(\cdot, \cdot)$ :

**Definizione 10.3.1** (problema di decisione- $\mathbb{A}$ ). Dato  $x \quad \exists w \quad \text{t.c.} \quad V_{\mathbb{A}}(x, w) = \text{yes}$

**Definizione 10.3.2** (problema di ricerca- $\mathbb{A}$ ). Dato  $x$  produci  $w$ , se esiste, t.c.  $V_{\mathbb{A}}(x, w) = \text{yes}$

**Definizione 10.3.3** (Self Reducible).  $\mathbb{A} \in \mathbf{NP}$  (rispetto a  $V_{\mathbb{A}}$ ) è **self reducible** se, dato un **oracolo** per il problema di decisione- $\mathbb{A}$ , esiste un algoritmo polinomiale per il problema di ricerca- $\mathbb{A}$ .

**Definizione 10.3.4** (Oracolo). Un **oracolo** è una black box che prende in input un'istanza di decisione- $\mathbb{A}$  e ritorna in tempo costante  $O(1)$  la soluzione (è specifico per il problema  $\mathbb{A}$ ).

Abbiamo visto che **IndSet** è *Self Reducible* e **SAT** è *Self Reducible*.

**Teorema 10.3.1.** *Ogni problema NPC è Self Reducible*

Con la seguente dimostrazione vediamo come sfruttare un algoritmo "debole" (decision) per costruirne uno "forte" (search).

*Dimostrazione. Assunzione:* assumiamo che esista un oracolo  $\mathcal{O}_{\mathbb{A}}$  per il problema  $\mathbb{A}$ .  
Data l'istanza  $x \in \mathcal{I}(\mathbb{A})$  vogliamo un certificato  $w$  tale che  $V_{\mathbb{A}}(x, w) = \text{yes}$ , se  $w$  esiste.

Sappiamo che se  $\mathbb{A} \in \mathbf{NPC}$  allora  $\mathbb{A} \leq_K \text{SAT}$ .

Partiamo dal teorema *Cook-Levin* per cui  $\text{Circuit-Sat} \in \mathbf{NPC}$  e  $\text{SAT} \in \mathbf{NPC}$ . Abbiamo che la riduzione da  $\mathbb{A}$  a  $\text{SAT}$  è tale che il certificato per l'istanza prodotta di  $\text{SAT}$  è un certificato per il verificatore  $V_{\mathbb{A}}$ . Inoltre sappiamo che possiamo trovare un certificato per  $\text{SAT}$  se abbiamo un oracolo per  $\text{SAT}$ .

Se  $\mathbb{A} \in \mathbf{NPC}$  allora  $\text{SAT} \leq_K \mathbb{A}$  e quindi un oracolo per  $\mathbb{A}$  implica un oracolo per  $\text{SAT}$ .

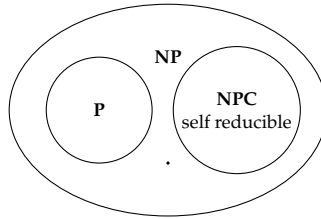
Prendiamo  $x \in \mathcal{I}(\mathbb{A})$  e lo trasformiamo in  $\phi^{(x)}$  di  $\text{SAT}$  utilizzando il teorema *Cook-Levin*. Sappiamo che

$$\begin{aligned} \text{SAT}(\phi^{(x)}) = \text{yes} &\Leftrightarrow \mathbb{A}(x) = \text{yes} \\ V_{\mathbb{A}}(x, w) = \text{yes} &\Leftrightarrow V_{\text{SAT}}(\phi^{(x)}, \underline{w}) = \text{yes} \end{aligned}$$

Possiamo produrre  $w$  usando l'algoritmo  $\text{SAT-Solver}$  (5). La risposta di tale algoritmo sarà uguale alla risposta dell'oracolo

$$\mathcal{O}_{\mathbb{A}}(f(\phi_{x_1=a_1, \dots, x_i=a_i}))$$

dove  $f$  è la riduzione polinomiale da  $\text{SAT}$  a  $\mathbb{A}$ . In questo modo il certificato  $w$  che costruisce  $\text{SAT-solver}$  è lo stesso che serve a  $V_{\mathbb{A}}$ .  $\square$



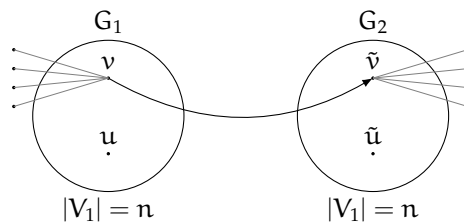
Vediamo ora un problema in  $\mathbf{NP}$  che non crediamo sia in  $\mathbf{NPC}$ .

**10.4 Problema Graph Isomorphism**

Versione Graph Isomorphism-Search:

- Input:  $G_1 = (V_1, E_1)$ ,  $G_2 = (V_2, E_2)$  semplici e non diretti
- Output: una funzione  $f : v_1 \mapsto v_2$  t.c.  $\forall (v, u) \in E_1$   
 $(u, v) \in E_1 \Leftrightarrow (f(u), f(v)) \in E_2$ . Se esiste una tale  $f$ , altrimenti no.

Dato un oracolo  $\mathcal{O}_{\text{GI-Dec}}$  per il problema Graph-Isomorphism-Decision, allora esiste un algoritmo polinomiale (che usa  $\mathcal{O}_{\text{GI-Dec}}$ ) per il problema di ricerca Graph-Isomorphism-Search.



## Algorithm 6: Graph Isomorphism Search

---

```

GraphIsomorphismSearch( $G_1, G_2$ )
  if  $\mathcal{O}^{\text{GI-Decision}}(G_1, G_2) = \text{no}$ :
    return no
  foreach  $v_i \in V_1$ : // Fissiamo  $v \in V_1, \tilde{v} \in V_2$ 
    foreach  $\tilde{v}_i \in V_2$ :
       $\tilde{G}_1 \leftarrow$  aggiungiamo  $n$  vertici a  $V_1$  come vicini di  $v$ 
       $\tilde{G}_2 \leftarrow$  aggiungiamo  $n$  vertici a  $V_2$  come vicini di  $\tilde{v}$ 
      if  $\mathcal{O}^{\text{GI-Decision}}(G_1, G_2) = \text{yes}$ :
         $f(v) = \tilde{v}$ 
         $G_1 \leftarrow \tilde{G}_1, G_2 \leftarrow \tilde{G}_2$ 
        break

```

---

**Teorema 10.4.1.** Se  $\text{NP} \cup \text{CO-NP} \neq \text{P}$  allora esiste un problema non self-reducible di ricerca il cui problema di decisione è in  $\text{NP}$ .

*Dimostrazione.* Partiamo dunque dall'ipotesi che

$$\exists \mathbb{A} \in (\text{NP} \cap \text{CO-NP}) \setminus \text{P} \quad \mathbb{A} \notin \text{P}, \mathbb{A} \in \text{NP}, \mathbb{A} \in \text{CO-NP}$$

$\rightarrow \mathbb{A} \in \text{NP}$  esiste un verificatore  $V_{\text{yes}}(x, w)$  polinomiale per le istanze yes tale che

$$\forall x \in \mathcal{I}(\mathbb{A}), \mathbb{A}(x) = \text{yes} \Leftrightarrow \exists w \ V_{\text{yes}}(x, w) = \text{yes}$$

$\rightarrow \mathbb{A} \in \text{CO-NP}$  esiste un verificatore  $V_{\text{no}}(x, w')$  polinomiale per le istanze no tale che

$$\forall x \in \mathcal{I}(\mathbb{A}), \mathbb{A}(x) = \text{no} \Leftrightarrow \exists w' \ V_{\text{no}}(x, w') = \text{yes}$$

Definiamo  $\forall x \in \mathcal{I}(\mathbb{A})$  un verificatore

$$V^*(x, w) = \text{yes} \Leftrightarrow V_{\text{yes}}(x, w) = \text{yes} \quad \text{OR} \quad V_{\text{no}}(x, w) = \text{yes}$$

$V^*$  è polinomiale perché  $V_{\text{yes}}$  e  $V_{\text{no}}$  sono polytime. Questo verificatore è associato al problema  $\mathbb{B} \in \text{NP}$  per cui  $\mathcal{I}(\mathbb{A}) = \mathcal{I}(\mathbb{B}), \forall x \in \mathcal{I}(\mathbb{B}) \ \mathbb{B}(x) = \text{yes}$ .

Il problema di ricerca associato a  $V^*$  è dato per qualche  $w$  tale che  $V^*(x, w) = \text{yes}$ .

Se in tempo polinomiale, dato  $x$ , trovo un certificato  $w$  tale che  $V^*(x, w) = \text{yes}$

se  $V_{\text{yes}}(x, w) = \text{yes}$  allora  $\mathbb{A}(x) = \text{yes}$

se  $V_{\text{no}}(x, w) = \text{yes}$  allora  $\mathbb{A}(x) = \text{no}$

Perciò risolvo  $\mathbb{A}$  in tempo polinomiale. Questa è una *contraddizione* perché  $\mathbb{A} \notin \text{P}$ . Perciò il problema non è self reducible.  $\square$