Richiami di teoria della complessità

Ottimizzazione discreta

Giovanni Righini

UNIVERSITÀ DEGLI STUDI DI MILANO

Le classi $\mathcal{P}$ e $\mathcal{NP}$

Un problema di decisione ha un output binario: o “sì” o “no”.

Sia X l’insieme delle possibili istanze e sia Y l’insieme delle istanze “sì”.

La classe di complessità $\mathcal{P}$ contiene i problemi la cui risposta si può determinare con complessità (in spazio e in tempo, nel caso peggiore) polinomiale, assumendo come esecutore dell’algoritmo una macchina di Turing.

La classe di complessità $\mathcal{NP}$ contiene i problemi la cui risposta

- si può determinare con complessità polinomiale con una macchina di Turing non-deterministica (con oracolo);
- si può verificare, quando è “sì”, con complessità polinomiale con una macchina di Turing.

Riduzioni polinomialie e classe $\mathcal{NP}c$

Un problema $P_1(X_1, Y_1)$ si riduce polinomialmente ad un problema $P_2(X_2, Y_2)$,

$$P_1 <_{poly} P_2$$

se e solo se

$$\exists f : X_1 \mapsto X_2 : f(X_1) \in Y_2 \Leftrightarrow x_1 \in Y_1$$

e f è calcolabile in tempo polinomiale.

La classe di complessità $\mathcal{NP}c$ comprende i problemi $\mathcal{NP}$-completi

$$P \in \mathcal{NP}c \Leftrightarrow \begin{cases} P \in \mathcal{NP} \\ Q <_{poly} P \quad \forall Q \in \mathcal{NP} \end{cases}$$

Dimostrazioni di $\mathcal{NP}$-completezza

Certamente $\mathcal{P} \subseteq \mathcal{NP}$ e $\mathcal{NP}c \subseteq \mathcal{NP}$.
Famoso problema aperto: $\mathcal{P} = \mathcal{NP} = \mathcal{NP}c$ o $\mathcal{P} \subset \mathcal{NP}$?

Come conseguenza di $P_1 <_{poly} P_2$,

- se P_2 è polinomiale, allora P_1 è polinomiale;
- se P_1 è $\mathcal{NP}$-completo, allora P_2 è $\mathcal{NP}$-completo.

Le dimostrazioni di $\mathcal{NP}$-completezza si ottengono tramite riduzioni polinomiali da problemi $\mathcal{NP}$-completi.

Punto di partenza (Cook, 1971): $SAT \in \mathcal{NP}c$.

Riferimento classico: Garey, Johnson, *Computers and intractability*, 1979.

Esempio 1: *STABLE SET*

Il problema *STABLE SET* è $\mathcal{NP}$-completo (Karp, 1972):

$$SAT <_{poly} STABLE\ SET.$$

PROBLEMA: *STABLE SET*.
INPUT: un grafo G e un numero naturale k.
DOMANDA: esiste in G uno stable set di cardinalità k?

PROBLEMA: *SATISFIABILITY*(*SAT*).
INPUT:

- un insieme X di variabili booleane;
- una collezione Z di clausole $Z_1, Z_2, \ldots, Z_m$ in congiunzione ($\wedge$) tra loro; ogni clausola $Z_i = \{\lambda_i^1, \lambda_i^2, \ldots, \lambda_i^{n_i}\}\ \forall i = 1, \ldots, m$ è una disgiunzione ($\vee$) di letterali. Ogni letterale λ_i^j è $\lambda_i^j = x_u$ oppure $\lambda_i^j = \overline{x}_u$ per una $x_u \in X$.

DOMANDA: esiste un assegnamento di valori x che soddisfa Z?

Esempio 1: riduzione polinomiale

Da una generica istanza di *SAT* con m clausole, costruiamo un'istanza di *STABLE SET* che ha uno stable set di cardinalità m se e solo se Z è soddisfacibile.

Per ogni clausola $i = 1, \ldots, m$ definiamo una clique di G con n_i vertici. Inseriamo edges tra vertici incompatibili.

$$V = \{v_{ij} : i \in [1, \ldots, m], j \in [1, \ldots, n_i]\}$$

$$E = \{[v_{ij}, v_{i'j'}] : ((i = i') \wedge (j \neq j')) \vee (\exists x \in X : (\lambda_i^j = x) \wedge (\lambda_{i'}^{j'} = \overline{x}))\}$$

Ogni stable set può avere al massimo un vertice in ogni clique. Quindi, se esiste una stable set di cardinalità m, Z è soddisfacibile.

Solo vertici incompatili sono connessi.
Se Z è soddisfacibile, esiste almeno un letterale vero in ogni clique. Quindi, scegliendone uno in ogni clique, si ha uno stable set di cardinalità m.

Esempio 2: *CLIQUE*

PROBLEMA: *CLIQUE*.
INPUT: un grafo G e un numero naturale k.
DOMANDA: esiste in G una clique di cardinalità k?

Una clique in G è uno stable set nel grafo complementare $\overline{G}$.

$$V(\overline{G}) = V(G)$$

$$E(\overline{G}) = \{[i,j] \in V(\overline{G}) \times V(\overline{G}) : (i \neq j) \wedge [i,j] \notin E(G)\}.$$

Quindi, se esiste uno stable set di cardinalità k in $\overline{G}$, allora esiste una clique di cardinalità k in G e viceversa.

Esempio 3: *VERTEX COVER* (Karp, 1972)

PROBLEMA: *VERTEX COVER*.
INPUT: un grafo G e un numero naturale k.
DOMANDA: esiste in G un *vertex cover* di cardinalità k?

Vertex cover: sottoinsieme di vertici che "coprono" tutti gli edges.

X è un vertex cover di $G = (V, E)$ se e solo se $V \setminus X$ è uno stable set in G.

Esempio 4: $3-$ *DIMENSIONAL MATCHING*

PROBLEMA: $3-$ *DIMENSIONAL MATCHING* ($3DM$).
INPUT: tre insiemi U, V e W di cardinalità m e un set di terne $T \subseteq U \times V \times W$.
DOMANDA: esiste un *matching 3-dimensionale* di cardinalità m?

Matching 3-dimensionale: insieme di terne $M \subseteq T$ tale che per ogni coppia di terne distinte (u, v, w) e (u', v', w') in M,

$$(u \neq u') \wedge (v \neq v') \wedge (w \neq w').$$

La riduzione polinomiale è da *SAT* (Karp, 1972):

$$SAT <_{polyu} 3DM$$

Da una generica istanza di *SAT* descritta da $X = \{x_1, \ldots, x_n\}$ e $Z = \{Z_1, \ldots, Z_m\}$, costruiamo un'istanza di $3DM$, descritta da (U, V, W, T) tale che Z è soddisfacibile se e solo se $\exists M$ con $|M| = m$.

Esempio 4: riduzione polinomiale

$$
\begin{aligned}
U =& \{x_i^j, \overline{x}_i^j \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m\} \\
V =& \{a_i^j \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m\} \cup \\
& \{v^j \ \forall j = 1, \ldots, m\} \cup \\
& \{c_k^j \ \forall k = 1, \ldots, n-1 \ \forall j = 1, \ldots, m\} \\
W =& \{b_i^j \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m\} \cup \\
& \{w^j \ \forall j = 1, \ldots, m\} \cup \\
& \{d_k^j \ \forall k = 1, \ldots, n-1 \ \forall j = 1, \ldots, m\} \\
T_1 =& \{(x_i^j, a_i^j, b_i^j), (\overline{x}_i^j, a_i^{j+1}, b_i^j) \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m\} \\
T_2 =& \{(x_i^j, v^j, w^j) \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m, \forall x_i \in Z_j\} \cup \\
& \{(\overline{x}_i^j, v^j, w^j) \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m, \forall \overline{x}_i \in Z_j\} \\
T_3 =& \{(x_i^j, c_k^j, d_k^j), (\overline{x}_i^j, c_k^j, d_k^j) \ \forall i = 1, \ldots, n \ \forall j = 1, \ldots, m \ \forall k = 1, \ldots, n-1\} \\
T =& T_1 \cup T_2 \cup T_3
\end{aligned}
$$

Esempio 5: *SUBSET SUM*

PROBLEMA: *SUBSET SUM*.
INPUT: $N = \{c_1, c_2, \ldots, c_n\} \in \mathbb{Z}^n$ e $K \in \mathbb{Z}$.
DOMANDA: esiste $S \subseteq N : \sum_{i \in S} c_i = K$?

$$3DM <_{poly} SUBSET\ SUM.$$

Generica istanza di $3DM$: (U, V, W, T) con $|U| = |V| = |W| = m$.
Per ogni tripla $t \in T$, mettiamo in sequenza i tre vettori caratteristici di $U \cap T$, $V \cap T$ e $W \cap T$, formando un vettore di $3m$ cifre binarie (3 di esse sono pari a 1, le altre $3m - 3$ sono pari a 0).
Interpretiamolo come un numero scritto in una certa base b:

$$c_t = \sum_{i=1}^{3m} b^{i-1} t_i.$$

Scegliamo $K = \sum_{i=1}^{3m} b^{i-1}$: vettore con $3m$ componenti pari a 1.
Scegliamo base $b = |T| + 1$: la somma di terne non provoca riporti.

Esempio 6: *PARTITION*

PROBLEMA: *PARTITION*.
INPUT: $N = \{c_1, c_2, \ldots, c_n\} \in \mathbb{Z}^n$.
DOMANDA: esiste $S \subseteq N : \sum_{i \in S} c_i = \sum_{i \notin S} c_i$?

$$\textit{SUBSET SUM} <_{poly} \textit{PARTITION}.$$

Generica istanza di *SUBSET SUM*: $\{c_1, c_2, \ldots, c_n\}$ e K.

Aggiungiamo un altro numero $c_{n+1} = |\sum_{i=1}^{n} c_i - 2K|$.

Esempio 6: *PARTITION*

Consideriamo i tre casi possibili:

1. Se $\sum_{i=1}^{n} c_i = 2K$, allora $c_{n+1} = 0$ e i due problemi sono equivalenti (caso banale).
2. Se $\sum_{i=1}^{n} c_i > 2K$, allora $c_{n+1} = \sum_{i=1}^{n} c_i - 2K$ e quindi

$$\sum_{i \in S} c_i = K \Leftrightarrow \sum_{i \in S \cup \{n+1\}} c_i = \sum_{i \notin S} c_i.$$

   Infatti $C_S + C_T - 2K = C_T - C_S \Leftrightarrow C_S = K$.
3. Se $\sum_{i=1}^{n} c_i < 2K$, allora $c_{n+1} = 2K - \sum_{i=1}^{n} c_i$ e quindi

$$\sum_{i \in S} c_i = K \Leftrightarrow \sum_{i \in S} c_i = \sum_{i \in N \cup \{n+1\} \setminus S} c_i.$$

   Infatti $C_S = C_T + (2K - C_T) - C_S \Leftrightarrow C_S = K$.

Esempio 7: *HAMILTONIAN CYCLE*

PROBLEMA: *HAMILTONIAN CYCLE*.
INPUT: un grafo $G(V, E)$.
DOMANDA: esiste un ciclo Hamiltoniano in G?

Riduzione da $3 - SAT$ (Papadimitriou, Steiglitz, 1982):

$$3 - SAT <_{poly} HAMILTONIAN\ CYCLE.$$

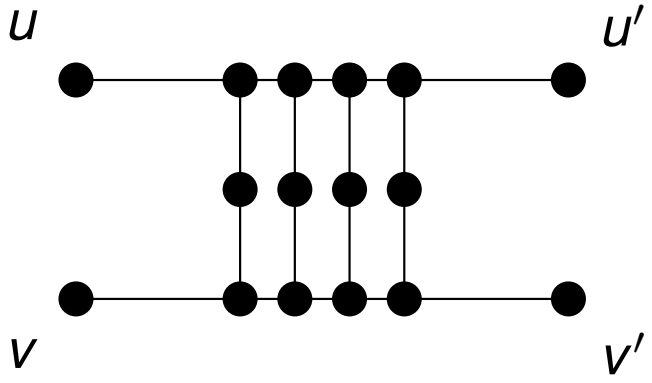
Generica istanza di $3 - SAT$: $\{Z_1, Z_2, \ldots, Z_m\}$ con $|Z_i| = 3 \ \ \forall i = 1, \ldots, m$.

Costruiamo un grafo G che ammette un ciclo Hamiltoniano se e solo se Z è soddisfacibile.

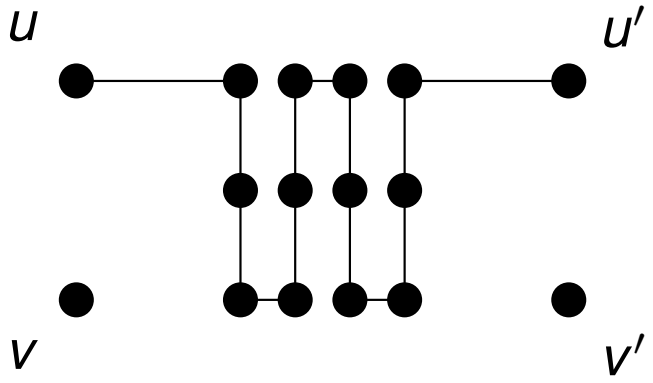
Il grafo è composto da sottografi (*gadgets*) di due tipi, A e B.

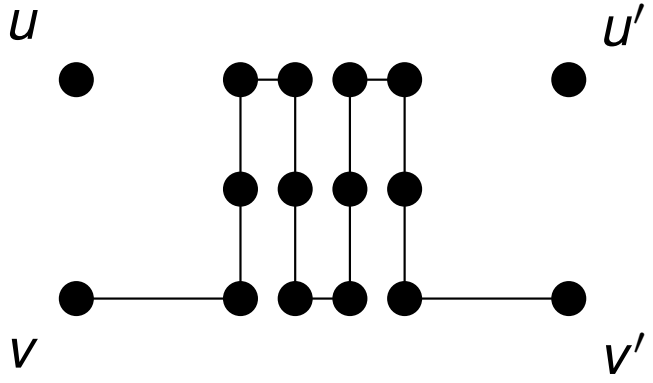
Esempio 7: riduzione polinomiale

Gadget A

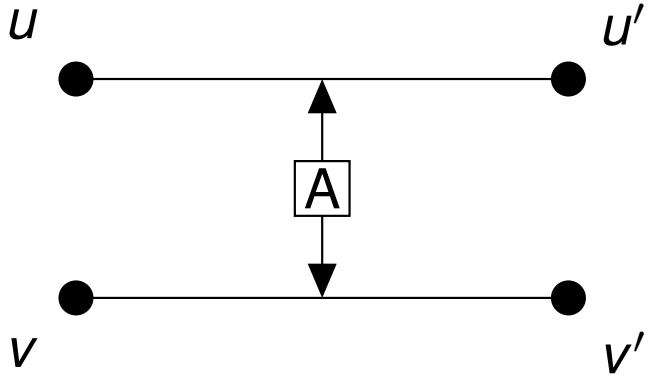


Il gadget A può essere attraversato solo in due modi:



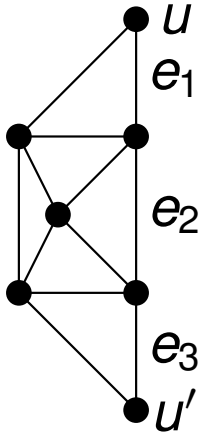


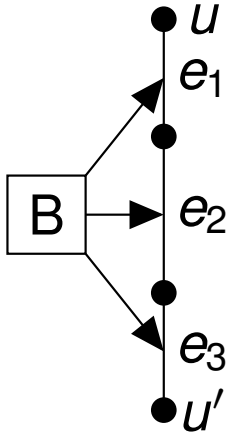
Il gadget A impone un XOR tra $[u, u']$ e $[v, v']$.

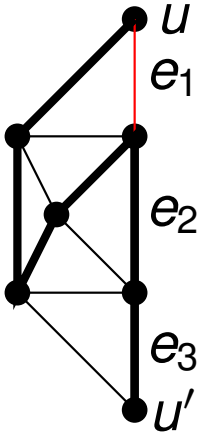


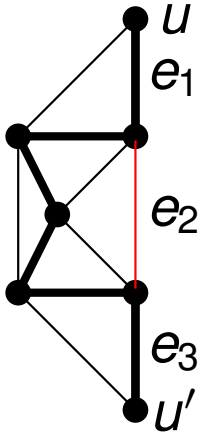
Esempio 7: riduzione polinomiale

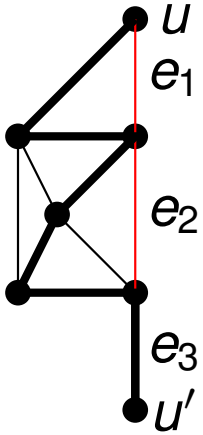
Gadget B: attraversabile se e solo se uno dei tre edges è escluso.

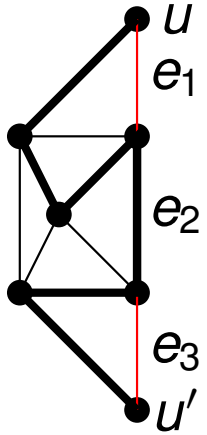


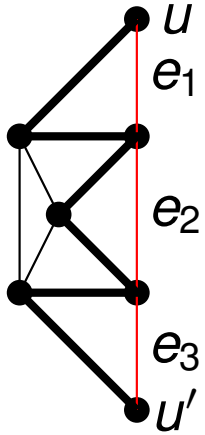












Esempio 7: riduzione polinomiale