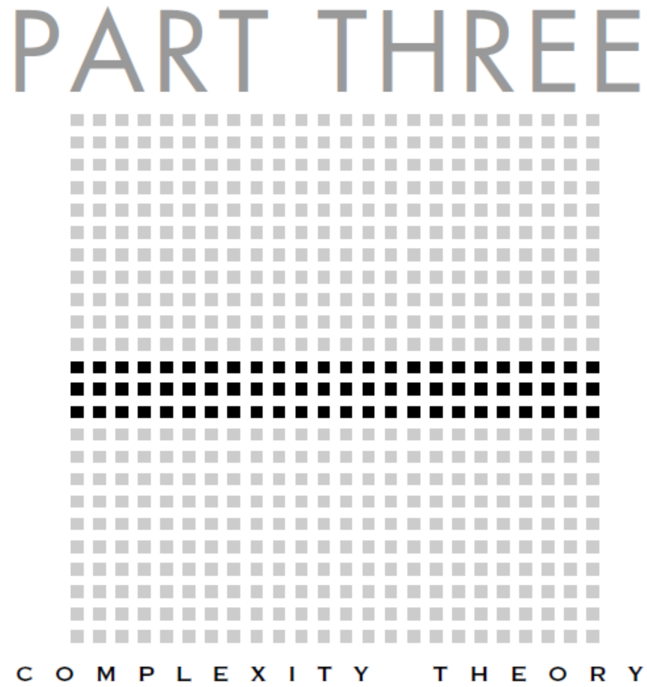

TEORIA DELLA COMPLESSITA'

NP-completezza

19 maggio 2022

Teoria della complessità: argomenti trattati

Scorse lezioni:

- Definizione di complessità di tempo
- La complessità di tempo dipende dal modello di calcolo; useremo decisori e modelli polinomialmente equivalenti
- La complessità di tempo dipende dalla codifica utilizzata: useremo codifica in binario o polinomialmente correlata
- TIME (f(n)) = insieme dei linguaggi decisi in tempo O(f(n))
- La classe $P = \bigcup_{k \geq 0} \text{TIME}(n^k)$ e sua robustezza
- La classe EXPTIME
- Algoritmi di verifica e la classe NP
- Il concetto di riduzione polinomiale

Oggi:

- Il concetto di NP-completezza

Definizione

Siano A, B linguaggi sull'alfabeto Σ.

Una riduzione in tempo polinomiale f di A in B è

- una funzione $f : \Sigma^* \rightarrow \Sigma^*$
- calcolabile in tempo polinomiale
- tale che per ogni $w \in \Sigma^*$

$$w \in A \Leftrightarrow f(w) \in B$$

Definizione

Un linguaggio $A \subseteq \Sigma^*$ è riducibile in tempo polinomiale a un linguaggio $B \subseteq \Sigma^*$, e scriveremo $A \leq_p B$, se esiste una riduzione di tempo polinomiale di A in B.

Nota.

- Se A è un linguaggio su un alfabeto Σ e A è associato a un problema di decisione $\mathbb{P}_D$, le stringhe w in Σ^* si dividono in tre gruppi:
  1. w è la codifica di un'istanza di $\mathbb{P}_D$ per la quale $\mathbb{P}_D$ ammette risposta "sì" (e quindi $w \in A$);
  2. w è la codifica di un'istanza di $\mathbb{P}_D$ per la quale $\mathbb{P}_D$ ammette risposta "no" (e quindi $w \notin A$);
  3. w non è la codifica di un'istanza di $\mathbb{P}_D$ (e quindi $w \notin A$).
- In generale nelle prove di riduzione di tempo polinomiale di A a un altro linguaggio B, vengono considerate solo le stringhe dei primi due gruppi e si assume implicitamente che la riduzione f associa alle stringhe w del terzo gruppo (stringhe che non sono codifiche di istanze di $\mathbb{P}_D$) una stringa $f(w)$ che non è in B.

Teorema

$$\boxed{3SAT \leq_P CLIQUE}$$

$3SAT = \{\langle \phi \rangle \mid \phi$ è una formula 3CNF soddisfacibile$\}$

Una formula 3CNF è un *AND* di clausole e tutte le clausole hanno tre letterali.

$CLIQUE =$
$\{\langle G, k \rangle \mid G$ è un grafo non orientato in cui esiste una k-clique$\}$

Ricorda:
Una clique (o cricca) in un grafo non orientato G è un sottografo G' di G in cui ogni coppia di vertici è connessa da un arco.
Una k-clique è una clique che contiene k vertici.

3SAT $\leq_p$ *CLIQUE*

Dobbiamo dimostrare che esiste una funzione $f : \Sigma^* \to \Sigma^*$

- calcolabile in tempo polinomiale
- tale che per ogni $w \in \Sigma^*$ $w \in 3SAT \Leftrightarrow f(w) \in CLIQUE$

Convenzione: non specificheremo il valore di f sulle stringhe che non rappresentano un'istanza del problema.

Quindi definiremo la f solo su stringhe che codificano formule booleane in 3CNF ϕ e ad esse associeremo stringhe che codificano (G, k).

$$f : \langle \phi \rangle \to \langle G, k \rangle$$

$$\langle \phi \rangle \in 3SAT \Leftrightarrow \langle G, k \rangle \in CLIQUE$$

$3SAT \leq_p CLIQUE$

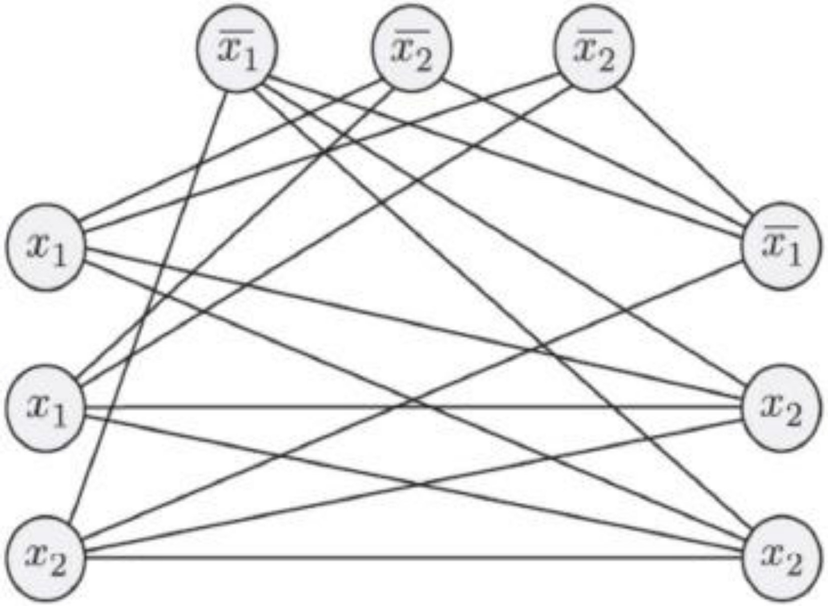

FIGURA 7.33
Il grafo che la riduzione produce per $\phi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$

3SAT $\leq_p$ *CLIQUE*

I risultati precedenti ci dicono che:

se *CLIQUE* fosse decidibile in tempo polinomiale anche *3SAT* lo sarebbe.

Questa connessione tra i due linguaggi sembra veramente notevole perché i linguaggi sembrano piuttosto differenti.

Riducibilità in tempo polinomiale: teoremi

Teorema

Se $A \leq_p B$ e $B \in P$, allora $A \in P$.

Dimostrazione

- Per ipotesi $B \in P$, quindi esiste un algoritmo M, di complessità $O(m^t)$, che decide B.
- Inoltre $A \leq_p B$: sia f la riduzione di tempo polinomiale di A in B e sia F l'algoritmo, di complessità $O(n^k)$, che calcola la funzione f .
- Consideriamo l'algoritmo N che sull'input w:
  - simula F su w e calcola f (w)
  - simula M sull'input f (w) per decidere se f $(w) \in B$
  - N accetta w se M accetta f (w), N rifiuta w se M rifiuta f (w)

$$N : w \to \boxed{\boxed{F} \to f(w) \to \boxed{M}}$$

Riducibilità in tempo polinomiale: teoremi

$$N : w \to \boxed{\boxed{F} \to f(w) \to \boxed{M}}$$

N decide A (correttezza dell'algoritmo N).

N è un decider. Infatti N si ferma su w se si fermano F ed M. Ora, per ogni w, F si ferma con $f(w)$ sul nastro e per ogni w, M si ferma su $f(w)$ perché M è un decider.

Inoltre N riconosce A. Infatti

$$\begin{aligned} w \in L(N) \quad & \Leftrightarrow \quad f(w) \in L(M) \text{ (per la definizione di } N) \\ & \Leftrightarrow \quad f(w) \in B \text{ (perché } M \text{ decide } B) \\ & \Leftrightarrow \quad w \in A \text{ (perché } f \text{ è una riduzione polinomiale} \\ & \qquad \text{di } A \text{ a } B) \end{aligned}$$

Riducibilità in tempo polinomiale: teoremi

$$N : w \to \boxed{\boxed{F} \to f(w) \to \boxed{M}}$$

- N è un algoritmo polinomiale in $n = |w|$.

  Infatti, F calcola $f(w)$ in $O(n^k)$ passi (primo passo dell'algoritmo: polinomiale).

  Inoltre risulta $|f(w)| = O(n^k)$ (cioè, per n sufficientemente grande, $|f(w)| \leq cn^k$ perché **la lunghezza dell'output di F è limitata dalla complessità di tempo di F**)

  Al secondo passo M viene eseguito sull'input $f(w)$ e si arresterà dopo $c'|f(w)|^t \leq c'(cn^k)^t$ passi, cioè dopo $O(n^{kt})$ passi (c', c, k, t costanti. Secondo passo dell'algoritmo: polinomiale, composizione dei due polinomi).

  In conclusione N ha complessità $O(n^k) + O(n^{kt}) = O(n^{kt})$.
- Quindi $A \in P$.

Transitività

Teorema

Se $A \leq_p B$ e $B \leq_p C$, allora $A \leq_p C$.

Dimostrazione

- Per ipotesi: esiste una riduzione di tempo polinomiale $f : \Sigma^* \to \Sigma^*$ di A a B ed esiste una riduzione di tempo polinomiale $g : \Sigma^* \to \Sigma^*$ di B a C.
- Consideriamo la composizione $g \circ f : \Sigma^* \to \Sigma^*$ delle funzioni f e g, definita da $(g \circ f)(w) = g(f(w))$.
- Risulta, per ogni $w \in \Sigma^*$:

$$\begin{aligned} w \in A \quad &\Leftrightarrow \quad f(w) \in B \text{ (perché } f \text{ è una riduzione polinomiale di } A \text{ a } B) \\ &\Leftrightarrow \quad g(f(w)) \in C \text{ (perché } g \text{ è una riduzione polinomiale di } B \text{ a } C) \end{aligned}$$

- Inoltre la funzione $g \circ f$ è una funzione calcolabile in tempo polinomiale.

Transitività

- Infatti, sia F l'algoritmo di complessità $O(n^k)$ che calcola la funzione f, sia G l'algoritmo di complessità $O(m^t)$ che calcola la funzione g.
- Consideriamo l'algoritmo GF che sull'input w:
  1. simula F su w e calcola $f(w)$,
  2. simula G sull'input $f(w)$ e calcola $g(f(w))$
  3. fornisce in output l'output di G.

- L'algoritmo GF calcola $g \circ f$ perchè prima esegue F su w calcolando $f(w)$ (primo passo dell'algoritmo) e poi G su $f(w)$ (secondo passo dell'algoritmo) fornendo quindi in output $g(f(w))$.

- Quindi $g \circ f$ è una riduzione di tempo polinomiale di A a C.

P = la classe dei linguaggi L per i quali l'appartenenza di una stringa w ad L può essere decisa da un algoritmo polinomiale in |w|.

NP = la classe dei linguaggi L per i quali l'appartenenza di una stringa w ad L può essere verificata da un algoritmo polinomiale in |w|.

Teorema 7.20
Un linguaggio L è in NP se e solo se esiste una macchina di Turing non deterministica che decide L in tempo polinomiale.

Teorema
$P \subseteq NP$

Uno dei più grandi problemi aperti dell'informatica teorica:

$$P = NP\ ?$$

Uno dei più grandi problemi aperti dell'informatica teorica:

$$P = NP\ ?$$

Come affrontare il problema? Approccio seguito:

Cerchiamo i problemi più difficili della classe NP.
Così se L è (il linguaggio associato a) uno dei problemi più difficili di NP:

1. Dovrebbe essere più semplice dimostrare che non è in P, e quindi concludere che: $P \neq NP$
2. Se, invece, riuscissimo a dimostrare che L è in P (cioè trovare un algoritmo polinomiale per decidere L) anche tutti gli altri linguaggi di NP (che sono meno difficili), dovrebbero essere in P e potremmo concludere che $NP = P$

Un progresso importante sulla questione ‘’P = NP?" ci fu all'inizio degli anni '70 con il lavoro di Stephen Cook e Leonid Levin.

Essi definirono i linguaggi «più difficili» della classe NP e li chiamarono linguaggi NP-completi.

Il fenomeno della NP-completezza è importante sia per ragioni teoriche che pratiche.

Il primo linguaggio NP-completo che fu (da loro) scoperto è SAT, il problema della soddisfacibilità di una formula booleana.

Vogliamo definire quando un linguaggio B è uno dei linguaggi «più difficili» della classe NP.

Abbiamo visto un modo per definire quando B è «più difficile» di A, ovvero quando A è di difficoltà «minore o uguale» a B:

$$A \leq_p B$$

Quindi B è uno dei linguaggi «più difficili» della classe NP…..

Definizione

Un linguaggio B è *NP-completo* se soddisfa le seguenti due condizioni:

1. B appartiene a NP
2. Per ogni linguaggio A in NP, $A \leq_p B$ (ovvero B è NP-hard)

NP – completezza: teoremi fondamentali

Teorema

Se B è NP-completo e B è in P allora $P = NP$.

Dimostrazione.

- Siccome B è NP-completo, per ogni $A \in NP$, risulta $A \leq_P B$
- Ma abbiamo provato che se $A \leq_P B$ e $B \in P$ allora $A \in P$
- Quindi $NP \subseteq P$ e siccome $P \subseteq NP$ risulta $P = NP$.

NP – completezza: teoremi fondamentali

Ma esistono linguaggi NP-completi?

Ma esistono linguaggi indecidibili?

Come abbiamo dimostrato che A_{TM}, $HALT_{TM}$, E_{TM}, $REGULAR_{TM}$, EQ_{TM} e tanti altri linguaggi sono indecidibili?

Abbiamo provato che:

1. A_{TM} è indecidibile, dalla definizione, per assurdo
2. Se B è indecidibile e B $\leq_m$ C allora anche C è indecidibile

Analogamente dimostreremo che:

1. SAT è NP-completo (Teorema di Cook-Levin)
2. Se B è NP-completo e B $\leq_p$ C, con C $\in$ NP, allora anche C è NP-completo.

Nota: $\leq_m$ e $\leq_p$

Teorema (Cook-Levin)
SAT è NP-completo.

La dimostrazione è complessa (non è in programma).
L'idea è la seguente.
Sappiamo che SAT $\in$ NP.
Occorre poi mostrare che **per ogni** A $\in$ NP (e sappiamo solo questo) si ha $A \leq_p SAT$.
La riduzione di tempo polinomiale si ottiene definendo per ogni input w una formula booleana che simula la macchina di Turing non deterministica che decide A sull'input w.

Conseguenza: il teorema non dice che SAT non si possa risolvere in tempo polinomiale, ma che:

SAT $\in$ P se e solo se P = NP.

NP – completezza: teoremi fondamentali

Teorema

Se B è NP-completo e $B \leq_p C$, con $C \in NP$, allora C è NP-completo.

Dimostrazione

Per ipotesi:

1. $C \in NP$
2. Per ogni $A \in NP$, $A \leq_p B$ (B è NP-completo)
3. $B \leq_p C$

Allora, utilizzando la proprietà transitiva di $\leq_p$:

1. $C \in NP$

5.(=2+3) Per ogni $A \in NP$, $A \leq_p C$

Cioè C è NP-completo.

Provare la *NP* – completezza

Teorema

Se B è NP-completo e $B \leq_p C$, con $C \in NP$, allora C è NP-completo.

Una possibile strategia per provare che un linguaggio C è NP-completo:

1. Mostrare che $C \in NP$
2. Scegliere un linguaggio B che sia NP-completo
3. Definire una riduzione di tempo polinomiale di B in C.

Provare la *NP* – completezza

Una possibile strategia per provare che un linguaggio C è NP-completo:

1. Mostrare che $C \in NP$
2. Scegliere un linguaggio B che sia NP-completo
3. Definire una riduzione di tempo polinomiale di B in C.

Proveremo che alcuni linguaggi sono NP-completi mostrando una riduzione di tempo polinomiale da 3SAT che utilizza la tecnica di ‘’riduzione mediante progettazione di componenti" o ‘’gadgets".

Occorre prima dimostrare che 3SAT è NP-completo.

3SAT è *NP* – completo

Occorre prima dimostrare che 3SAT è NP-completo.

- 3SAT $\in$ NP. Infatti 3SAT è verificabile in tempo polinomiale perché è un caso particolare di SAT (che sappiamo essere in NP).

- E' possibile dimostrare poi che:

$$\text{SAT} \leq_p \text{SAT}_{\text{CNF}} \leq_p 3\ \text{SAT}$$

Nota: 3SAT pur essendo un caso particolare di SAT è di «difficoltà maggiore o uguale» a SAT.

Esercizio

La seguente affermazione è vera?

''Comunque prendo due linguaggi NP-completi A e B, si ha:

$$A \leq_p B \quad \text{e} \quad B \leq_p A \text{ .''}$$

Cioè, i linguaggi NP-completi hanno tutti la «uguale difficoltà».

SAT_{CNF} è NP – completo

$$SAT_{CNF} = \{\langle \phi \rangle \mid \phi \text{ è una formula booleana soddisfacibile in } CNF\}$$

$SAT_{CNF} \in NP$,

SAT è riducibile in tempo polinomiale a SAT_{CNF}

$$SAT \leq_P SAT_{CNF}$$

Teorema

SAT_{CNF} è NP-completo.

- Nota: la trasformazione classica di un'espressione booleana nella sua forma normale congiuntiva non definisce, in generale, una riduzione di tempo polinomiale.

$3SAT$ è NP-completo

3CNF = formula booleana in forma normale 3-congiuntiva

$$3SAT = \{\langle\phi\rangle \mid \phi \text{ è una formula 3CNF soddisfacibile}\}$$

Teorema
$3SAT$ è NP-completo.

Dimostrazione

- 3SAT è in NP.
- Per provare che 3SAT è NP-completo basta dimostrare che $SAT_{CNF} \leq_P 3SAT$.
- La prova consiste nel costruire, a partire da ϕ in CNF, una formula booleana ψ in 3CNF tale che ϕ è soddisfacibile se e solo se ψ è soddisfacibile.
- Inoltre ψ può essere costruita a partire da ϕ in tempo polinomiale.

$CLIQUE$ è NP-completo

Teorema

$CLIQUE$ è NP-completo.

Dimostrazione.

- Sappiamo che $CLIQUE \in NP$.
- Inoltre, $3SAT$ è NP-completo e $3SAT \leq_P CLIQUE$
- Quindi $CLIQUE$ è NP-completo.

$\square$

Esercizio svolto

La seguente affermazione è vera o falsa?

''Se A $\leq_p$ B,   B $\leq_p$ C, C è decidibile allora anche (complemento di B) è decidibile''