Teorema di Rice e riduzioni

~~16~~ 18 maggio 2023

Contenuto del corso

Il corso è un'introduzione alle tre aree centrali della teoria della computazione:

- Teoria degli Automi (Linguaggi formali e modelli di calcolo)
- Teoria della Calcolabilità /Computabilità
- Teoria della Complessità

Le tre aree sono legate dalla domanda:

Quali sono le capacità e i limiti dei computer?

Oggi concludiamo la Teoria della computabilità col

Teorema di Rice

Indecidibilità

Un linguaggio L è indecidibile se non esiste una MdT che sia un decisore e riconosca L.

Ci sono 3 modi per provare indecidibilità:

1. Supporre per assurdo che L sia decidibile ed arrivare a una contraddizione, usando la diagonalizzazione (come visto per A_{TM})
2. Mostrare un linguaggio indecidibile L' , tale che $L' \leq_m L$.
3. Applicare (se possibile) il Teorema di Rice.

Definizione

Siano A, B linguaggi sull'alfabeto Σ.

Una riduzione mediante funzione di A in B è

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

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

Definizione

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

Teorema

Se $A \leq_m B$ e A è indecidibile allora B è indecidibile.

Teorema di Rice

Il Teorema di Rice è un risultato molto forte secondo cui qualsiasi proprietà non banale sul linguaggio accettato da una MdT è indecidibile.

Proprietà banale è una proprietà che è soddisfatta da tutte le MdT, oppure da nessuna. Non effettua alcuna discriminazione tra le MdT.

Esempio $L = \{\langle M \rangle \mid M$ è una MdT t.c. $L(M)$ è riconoscibile $\}$
$L' = \{\langle M \rangle \mid M$ è una MdT t.c. $L(M)$ è sia finito che infinito $\}$

Teorema di Rice. Sia

$$L = \{\langle M \rangle \mid M \text{ è una MdT che verifica la proprietà } \mathcal{P}\}$$

un linguaggio che soddisfa le seguenti due condizioni:

1. $\mathcal{P}$ è una proprietà del linguaggio $L(M)$, cioè: prese comunque due MdT M_1, M_2 tali che $L(M_1) = L(M_2)$ risulta

$$\langle M_1 \rangle \in L \Leftrightarrow \langle M_2 \rangle \in L$$

2. $\mathcal{P}$ è una proprietà non banale, cioè: esistono due MdT M_1, M_2 tali che

$$\langle M_1 \rangle \in L, \langle M_2 \rangle \notin L.$$

Allora L è indecidibile.

Teorema di Rice: osservazioni

- Nota la differenza tra una proprietà di $L(M)$ e una proprietà di M:
  - **Esempio:** $L(M) = \emptyset$ è una proprietà del linguaggio.
  - **Esempio:** "M ha almeno 1000 stati" è una proprietà della MdT, non del linguaggio.
  - "$L(M) = \emptyset$" è indecidibile; "M ha almeno 1000 stati" è facilmente decidibile, basta guardare la codifica di M e contare.

  - **Esempio:** "M rifiuta ab", oppure "M si arresta su ba" sono proprietà della MdT, non del linguaggio.
  - **Esempio:** "M accetta w" è una proprietà del linguaggio; è equivalente a "$L(M)$ contiene w".

Teorema di Rice: conseguenze

Non possiamo decidere se una MdT:

- Accetta $\emptyset$
- Accetta un linguaggio finito
- Accetta un linguaggio regolare, ecc.
- Ogni proprietà non banale del linguaggio di una MdT è indecidibile. Ecco perchè modelli limitati, come DFA per esempio, per i quali molte proprietà sono invece decidibili, diventano più realistici.

E' possibile mostrare che entrambe le condizioni del Teorema di Rice sono necessarie (vedi es.5.17 di [Sipser]).

CLIQUE

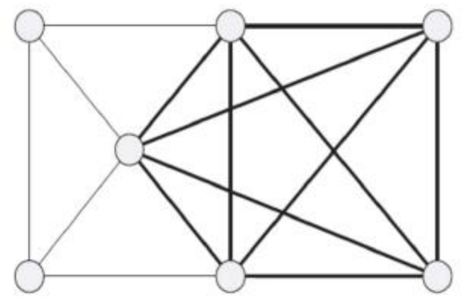

FIGURA 7.23
Un grafo con una 5-clique

Definizione

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

Il problema di stabilire se un grafo non orientato G contiene una k-clique si può formulare come un problema di decisione, il cui linguaggio associato è $CLIQUE$.

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

SAT

Una formula booleana ϕ è soddisfacibile se esiste un insieme di valori 0 o 1 per le variabili di ϕ (o assegnamento) che renda la formula uguale a 1 (assegnamento di soddisfacibilità). Diremo che tale assegnamento soddisfa ϕ o anche che rende vera ϕ.

Il problema della **soddisfacibilità di una formula booleana**:
Data una formula booleana ϕ, ϕ è soddisfacibile?

Il linguaggio associato è:

$$\boxed{SAT = \{\langle\phi\rangle \mid \phi \text{ è una formula booleana soddisfacibile}\}}$$

3 SAT

Definizione

Una clausola è un OR di letterali.

Esempio: $(\overline{x} \vee x \vee y \vee z)$

CNF

Definizione

Una formula booleana ϕ è in forma normale congiuntiva (o forma normale POS) se è un AND di clausole, cioè è un AND di OR di letterali.

Definizione

Una formula booleana è in forma normale 3-congiuntiva se è un AND di clausole e tutte le clausole hanno tre letterali.

Esempio:

$$(\overline{x_1} \vee x_2 \vee x_3) \wedge (x_3 \vee \overline{x_6} \vee x_6) \wedge (x_3 \vee \overline{x_5} \vee x_5)$$

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

Teorema

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

$3SAT = \{\langle \phi \rangle \mid \phi$ 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$\}$

$3SAT \leq_m CLIQUE$

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

- calcolabile
- 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).

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

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

3SAT $\leq_m$ *CLIQUE*

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

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

Poi dimostreremo che:

- f è calcolabile
- Se ϕ è soddisfacibile allora G ha una k-clique
- Se il grafo associato G ha una k-clique allora ϕ è soddisfacibile.

Vediamo come associare ad ogni formula in 3CNF un grafo e un intero.

$3SAT \leq_m CLIQUE$

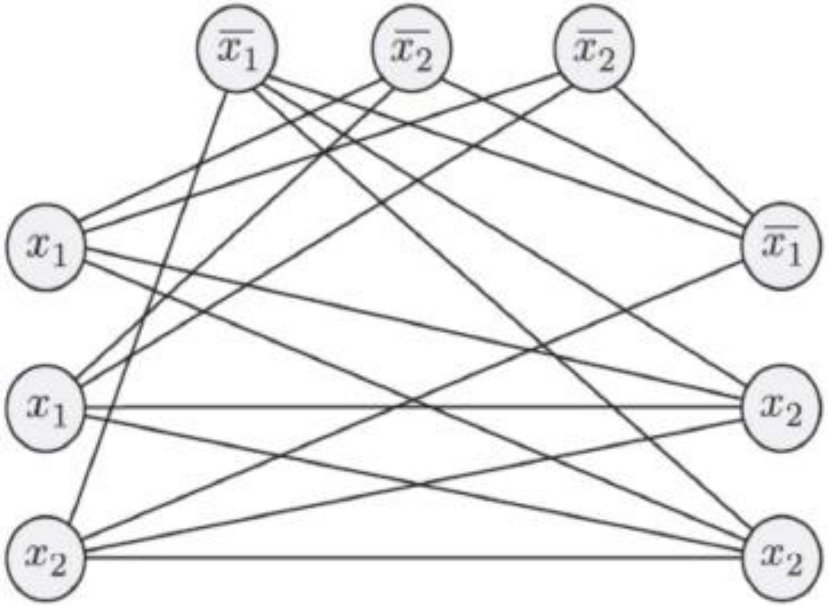

FIGURA 7.33
Il grafo che la riduzione produce per $\phi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$

$3SAT \leq_m CLIQUE$

Teorema

3SAT è riducibile mediante funzione a CLIQUE

Dimostrazione

- Sia ϕ una formula $3CNF$ con k clausole:

$$(a_1 \vee b_1 \vee c_1) \wedge (a_2 \vee b_2 \vee c_2) \wedge \ldots \wedge (a_k \vee b_k \vee c_k)$$

- Consideriamo la funzione f che associa a $\langle \phi \rangle$ la stringa $\langle G, k \rangle$ dove $G = (V, E)$ è il grafo non orientato definito come segue:
- V ha $3 \times k$ vertici. I vertici di G sono divisi in k gruppi di tre nodi (o **triple**) $t_1, \ldots, t_k$: t_j corrisponde alla clausola $(a_j \vee b_j \vee c_j)$ e ogni vertice in t_j corrisponde a un letterale in $(a_j \vee b_j \vee c_j)$. Quindi $V = \{a_1, b_1, c_1, \ldots, a_k, b_k, c_k\}$.
- Non ci sono archi tra i vertici in una tripla t_j, non ci sono archi tra un vertice associato a un letterale x e i vertici associati al letterale $\overline{x}$.
- Ogni altra coppia di vertici è connessa da un arco.

Nota: k è il numero di clausole in ϕ.

La funzione f è calcolabile (infatti….).

Per provare che f è una riduzione di *3SAT* in *CLIQUE* resta da dimostrare che

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

Cioè ϕ è soddisfacibile se e solo se G ha una k-clique.

- Supponiamo che ϕ abbia un assegnamento di soddisfacibilità. Questo assegnamento di valori alle variabili rende vera ogni clausola $(a_j \vee b_j \vee c_j)$ e quindi esiste almeno un letterale vero in ogni clausola $(a_j \vee b_j \vee c_j)$.
- Scegliamo un letterale vero in ogni clausola $(a_j \vee b_j \vee c_j)$ e consideriamo il sottografo G' di G indotto dai nodi corrispondenti ai letterali scelti.
- G' è una k-clique.
- Infatti G' ha k vertici poiché abbiamo scelto un letterale in ognuna delle k clausole e poi i k vertici di G corrispondenti a tali letterali.
- Due qualsiasi vertici in G' non si trovano nella stessa tripla (corrispondono a letterali in clausole diverse) e non corrispondono a una coppia $x, \overline{x}$ perché corrispondono a letterali veri nell'assegnamento di soddisfacibilità. Quindi due qualsiasi vertici in G' sono connessi da un arco in G.

- Viceversa, supponiamo che G abbia una k-clique G'.
- Poiché due nodi in una tripla non sono connessi da un arco, ognuna delle k triple contiene esattamente uno dei nodi della k-clique.
- Consideriamo l'assegnamento di valori alle variabili di ϕ che renda veri i letterali corrispondenti ai nodi di G'. Ciò è possibile perché in G' non ci sono archi che collegano una coppia $x, \overline{x}$.
- Ogni tripla contiene un nodo di G' e quindi ogni clausola contiene un letterale vero.
- Questo è un assegnamento di soddisfacibilità per ϕ cioè $\langle\phi\rangle \in 3SAT$.

$\square$

I risultati precedenti ci dicono che:

se *CLIQUE* è decidibile anche *3SAT* lo è, ma, in realtà…. Sono entrambi decidibili!

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

Passando alla teoria della complessità ci interesseremo soltanto a linguaggi decidibili e ne studieremo la loro…. complessità.

Esercizi svolti

Transitività delle riduzioni

Dimostrare chde se $A \leq_m B$ e $B \leq_m C$ allora $A \leq_m C$.

Riduzione da A_TM al complemento di EQ_TM

Esercizio (riduzione da A_{TM} a $\overline{EQ_{TM}}$)
Sia f_{A-NE} la funzione di riduzione esibita per dimostrare che $A_{TM} \leq_m \overline{E_{TM}}$ e sia f_{E-EQ} la funzione di riduzione esibita per dimostrare che $E_{TM} \leq_m EQ_{TM}$.

E' possibile utilizzare f_{A-NE} e f_{E-EQ} per esibire una funzione di riduzione f_{A-NEQ} per dimostrare che $A_{TM} \leq_m \overline{EQ_{TM}}$?

Se sì, la funzione f_{A-NEQ} è la stessa di quella esibita nelle slide precedenti per dimostrare che $A_{TM} \leq_m \overline{EQ_{TM}}$?

Riduzione da linguaggio diagonale

Sia $L_d = \{\langle M \rangle \mid M \notin L(M)\}$ il linguaggio diagonale e $L_{ne} = \{\langle M \rangle \mid L(M) \neq \emptyset\}$. Si dimostri che

$$\bar{L}_d \leq L_{ne}$$

Esercizio Sul Complemento di $HALT_{TM}$

Definire il linguaggio $HALT_{TM}$ e provare che il suo complemento $\overline{HALT_{TM}}$ non è Turing-riconoscibile, enunciando i risultati che vengono utilizzati, senza dimostrarli (si suggerisce l'utilizzo di riduzioni mediante funzioni studiate e di note proprietà delle riduzioni mediante funzione)

(a) Definire il linguaggio $HALT_{TM}$

$HALT_{TM} = \{ \langle M, w \rangle \mid M \textit{ è una } MdT \textit{ e } M \textit{ si arresta su } w\}$

(b)Dimostrare che $\overline{HALT_{TM}}$ non è Turing Riconoscibile

Problema accettazione di DFA

(a) Si descriva la relazione esistente tra un problema di decisione e il linguaggio associato.

(b) Dato il problema

> **Problema dell'accettazione di un DFA:** Sia $\mathcal{B}$ un DFA e w una parola. L'automa $\mathcal{B}$ accetta w?

definire il linguaggio associato A_{DFA}, spiegando la corrispondenza.

(c) Si consideri l'automa finito deterministico $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$, dove $Q = \{q_0, q_1\}$, $\Sigma = \{a, b\}$, $F = \{q_1\}$ e δ è tale che $\delta(q_0, a) = q_0$, $\delta(q_0, b) = q_1$, $\delta(q_1, a) = \delta(q_1, b) = q_1$. Precisare quali delle seguenti stringhe sono elementi di A_{DFA}:
$\langle \mathcal{A}, aa \rangle$, $\langle \mathcal{A}, aba \rangle$, $\langle \mathcal{A}, 00 \rangle$.

Esercizi da svolgere

Riduzione da $HALT_{TM}$

Si consideri il linguaggio

$$L = \{\langle M \rangle \mid M \text{ è una MdT che si arresta su 11 e non si arresta su 00}\}.$$

Definire il linguaggio $HALT_{TM}$ e dimostrare che $HALT_{TM} \leq_m L$.

Riduzione da A_{TM}

Si consideri il linguaggio

$$L = \{\langle M_1, M_2, w \rangle \mid M_1 \text{ ed } M_2 \text{ sono } TM,\ M_1 \text{ accetta } w \text{ ed } M_2 \text{ accetta } w\}.$$

Provare che $A_{TM} \leq L$.

Esercizio 5.11 da [Sipser]

Mostrare che A è decidibile se e soltanto se A si riduce mediante funzione al linguaggio 0*1*.

… etc, etc……