Tutorato di Automi e Linguaggi Formali

Homework 10: Riducibilità mediante Funzione e Classe P

Gabriel Rovesti
Corso di Laurea in Informatica - Università degli Studi di Padova

Tutorato 10 - 26-05-2025

1 Riducibilità mediante Funzione

Esercizio 1. Sia $HALF_{TM} = \{\langle M \rangle \mid M$ è una TM che accetta almeno la metà delle stringhe di lunghezza n per qualche $n \geq 1\}$.

a) Dimostrare che $A_{TM} \leq_m HALF_{TM}$ fornendo una funzione di riduzione esplicita f tale che per ogni coppia $\langle M, w \rangle$, si ha $\langle M, w \rangle \in A_{TM}$ se e solo se $f(\langle M, w \rangle) \in HALF_{TM}$.

b) Utilizzare la riduzione precedente per dimostrare che $HALF_{TM}$ è indecidibile.

c) Analizzare se $HALF_{TM}$ è Turing-riconoscibile o co-Turing-riconoscibile. Giustificare la risposta.

Esercizio 2. Consideriamo il problema $REGULAR_{TM} = \{\langle M \rangle \mid M$ è una TM tale che $L(M)$ è un linguaggio regolare$\}$.

a) Costruire una riduzione da A_{TM} a $\overline{REGULAR_{TM}}$ (il complemento di $REGULAR_{TM}$). Specificare la funzione di riduzione e dimostrare la sua correttezza.

b) Utilizzare il teorema di Rice per fornire una dimostrazione alternativa dell'indecidibilità di $REGULAR_{TM}$.

c) Confrontare le due dimostrazioni: quale fornisce più informazioni sulla natura computazionale del problema?

Esercizio 3. Sia $PREFIX_{TM} = \{\langle M_1, M_2 \rangle \mid M_1, M_2\{$ sono TM tali che $L(M_1)$ è un prefisso proprio di $L(M_2)\}$, dove A è un prefisso proprio di B se $A \subset B$ e per ogni $w \in A$, nessuna estensione propria di w appartiene ad A.

a) Dimostrare che $E_{TM} \leq_m PREFIX_{TM}$ costruendo una riduzione appropriata.

b) Dimostrare che $PREFIX_{TM}$ è indecidibile utilizzando la riduzione precedente.

c) Spiegare perché questo risultato è significativo nel contesto dell'analisi delle relazioni tra linguaggi.

2 Classe P e Algoritmi Polinomiali

Esercizio 4. Sia $MODEXP = \{\langle a, b, c, p\rangle \mid a, b, c, p$ sono numeri interi positivi in rappresentazione binaria tali che $a^b \equiv c \pmod{p}\}$.

a) Dimostrare che $MODEXP \in P$ fornendo un algoritmo polinomiale esplicito. Analizzare attentamente la complessità temporale considerando la rappresentazione binaria degli input.

b) Spiegare perché un approccio naive di calcolare a^b e poi ridurre modulo p non è polinomiale nella dimensione dell'input.

c) Descrivere l'algoritmo di esponenziazione modulare veloce e dimostrare formalmente che la sua complessità temporale è $O((\log b)^3)$.

Esercizio 5. Considerare il problema $COMPOSITE = \{n \mid n$ è un numero composto rappresentato in binario $\}$.

a) Fornire un algoritmo deterministico polinomiale per $COMPOSITE$ o una variante deterministica appropriata. Analizzare la complessità temporale.

Esercizio 6. Sia $BIPARTITE = \{\langle G\rangle \mid G$ è un grafo non diretto bipartito $\}$.

a) Dimostrare che $BIPARTITE \in P$ fornendo un algoritmo basato sulla colorazione a 2 colori. Analizzare la complessità temporale in termini del numero di vertici $|V|$ e archi $|E|$.

3 Problemi Avanzati su P e Riducibilità

Esercizio 7. Consideriamo il problema della equivalenza di DFA: $EQDFA = \{\langle A, B\rangle \mid A, B$ sono DFA tali che $L(A) = L(B)\}$.

a) Dimostrare che $EQDFA \in P$ utilizzando l'algoritmo di minimizzazione dei DFA. Fornire un'analisi dettagliata della complessità temporale.

b) Fornire un algoritmo alternativo basato sulla costruzione del prodotto cartesiano dei due automi e sulla verifica della vuotezza di linguaggi derivati. Confrontare le complessità.

c) Spiegare perché $EQNFA$ (equivalenza di NFA) è considerato significativamente più difficile e discutere lo stato attuale della conoscenza su questo problema.

Esercizio 8. Un linguaggio A è *star-closed* se $A = A^*$. Sia $STAR\text{-}CLOSED_{DFA} = \{\langle M \rangle \mid M \text{ è un DFA che riconosce un linguaggio star-closed}\}$.

a) Caratterizzare algebraicamente quando un linguaggio regolare è star-closed in termini delle proprietà del suo automa minimo.

b) Utilizzare questa caratterizzazione per fornire un algoritmo polinomiale che decide se un DFA riconosce un linguaggio star-closed.

c) Analizzare la complessità temporale dell'algoritmo e dimostrare che $STAR\text{-}CLOSED_{DFA} \in P$.

4 Problemi di Sintesi e Approfondimento

Esercizio 9. Consideriamo la relazione tra riducibilità mediante funzione e riducibilità in tempo polinomiale.

a) Dimostrare che se $A \leq_p B$ (riducibilità polinomiale) e $B \in P$, allora $A \in P$. Confrontare questo risultato con il teorema analogo per la decidibilità.

b) Fornire un esempio di linguaggi A e B tali che $A \leq_m B$ ma non necessariamente $A \leq_p B$. Spiegare la differenza fondamentale tra i due tipi di riducibilità.

c) Discutere l'importanza della riducibilità polinomiale nella definizione delle classi di complessità come NP e l'ipotesi P vs NP.