Prof. Dr. Jasmin Blanchette
Jannis Limperg
Lydia Kondylidou

Ludwig-Maximilians-Universität München
Institut für Informatik
Abgabe bis 12. Juli 2023, 10:00 Uhr

Übung 12 zur Vorlesung
Formale Sprachen und Komplexität

FSK12-1 ***PCP-Varianten*** (2 Punkte)

a) Wir betrachten das LPCP-Problem, eine Variante von PCP, bei der die ‚Spielsteine' auch das leere Wort enthalten können. Eine Instanz von LPCP mit Alphabet Σ ist also eine endliche Folge von Paaren $(x_1, y_1), \ldots, (x_n, y_n)$ mit $x_i, y_i \in \Sigma^*$ für $i = 1, \ldots, n$ (wohingegen bei PCP gilt: $x_i, y_i \in \Sigma^+$). Eine Lösung der Instanz K ist wie bei PCP eine endliche Folge von Indices $i_1, \ldots, i_m \in \mathbb{N}$ sodass $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$.

   Zeigen Sie durch Reduktion von PCP auf LPCP, dass LPCP für $|\Sigma| \geq 2$ unentscheidbar ist.

b) Sind die folgenden Instanzen K_1, K_2 von LPCP lösbar? Wenn ja, geben Sie eine Lösung (also eine geeignete Folge von Indizes) an. Wenn nein, beweisen Sie, dass die Instanz keine Lösung hat.

$$K_1 = \left(\begin{bmatrix} ab \\ aba \end{bmatrix}, \begin{bmatrix} bab \\ ba \end{bmatrix}, \begin{bmatrix} aa \\ \varepsilon \end{bmatrix}, \begin{bmatrix} \varepsilon \\ bb \end{bmatrix} \right)$$
$$K_2 = \left(\begin{bmatrix} a \\ ba \end{bmatrix}, \begin{bmatrix} bc \\ cbaa \end{bmatrix}, \begin{bmatrix} baa \\ \varepsilon \end{bmatrix}, \begin{bmatrix} \varepsilon \\ aab \end{bmatrix} \right)$$

c) Wir betrachten das EVENPCP-Problem, eine Variante von LPCP, bei der die Wörter auf den Spielsteinen gerade Länge haben müssen. Eine Instanz von EVENPCP ist also eine endliche Folge von Paaren $(x_1, y_1), \ldots, (x_n, y_n)$ mit $x_i, y_i \in \{w \mid w \in \Sigma^* \text{ und } |w| \text{ gerade}\}$ für $i = 1, \ldots, n$. Beispielsweise ist $(ab, aaba)$ ein erlaubter Spielstein; (ab, aab) aber nicht.

   Zeigen Sie durch Reduktion von PCP auf EVENPCP, dass EVENPCP für $|\Sigma| \geq 2$ unentscheidbar ist.

d) Für Mengen Σ und Δ nennen wir eine Funktion $f : \Sigma^* \to \Delta^*$ einen *Homomorphismus* (siehe auch Aufgabe FSK6-4), wenn gilt:

$$f(\varepsilon) = \varepsilon$$
$$f(u \circ v) = f(u) \circ f(v) \quad \forall u, v \in \Sigma^*$$

   Wir definieren das Problem HOMPCP. Eine Instanz dieses Problem ist ein 4-Tupel (Σ, Δ, f, g), wobei Σ und Δ endliche Mengen sind und $f, g : \Sigma^* \to \Delta^*$ Homomorphismen. Eine Lösung der Instanz ist ein Wort $w \in \Sigma^+$ sodass gilt: $f(w) = g(w)$.

Zeigen Sie durch Reduktion von LPCP auf HOMPCP, dass HOMPCP für $|\Delta| \geq 2$ unentscheidbar ist.

FSK12-2 ***Beweise prüfen*** (2 Punkte)

In den folgenden Teilaufgaben betrachten wir jeweils einen Beweis, der einen Fehler enthält. Identifizieren Sie diesen Fehler (mit kurzer Begründung).

a) Beweisen oder widerlegen Sie: Die Sprache

$$D = \{w \in \{0,1\}^* \mid M_w \text{ akzeptiert } w \text{ nicht}\}$$

ist semi-entscheidbar.

Beweis:
D ist semi-entscheidbar. Um das zu zeigen, konstruieren wir eine DTM M, die D semi-entscheidet. Das heißt, dass M für alle Eingaben $w \in D$ hält und für alle Eingaben $w \notin D$ nicht hält.

Angenommen, es gäbe so eine Turingmaschine M. Betrachte ein Wort $w \in \{0,1\}^*$.

- Wenn $w \in D$ ist, dann akzeptiert M_w die Eingabe w. Somit akzeptiert auch M das Wort w.
- Wenn $w \notin D$ ist, dann hält M_w mit Eingabe w nicht. Somit akzeptiert auch M das Wort w nicht.

M semi-entscheidet also D.

b) Sei $L_u = \{w\#x \mid w, x \in \{0,1\}^* \text{ und } x \in L(M_w)\}$. Diese Sprache ist semi-entscheidbar, aber nicht entscheidbar.

Zeigen Sie: Die Sprache $L_r = \{w \in \{0,1\}^* \mid L(M_w) \text{ ist regulär}\}$ ist unentscheidbar.

Beweis:
Wir reduzieren L_u auf L_r. Da L_u unentscheidbar ist, folgt daraus, dass L_r unentscheidbar ist.

Sei $v \in \{0,1,\#\}^*$. Wir definieren die Reduktionsfunktion f durch

$$f(v) = \begin{cases} \langle M_3 \rangle & \text{falls } v = w\#x \text{ und } M_w \text{ akzeptiert } x \\ \langle M_4 \rangle & \text{sonst} \end{cases}$$

Dabei ist M_3 eine Turingmaschine, die die reguläre Sprache $\{0,1\}^*$ akzeptiert. M_4 ist eine Turingmaschine, die die nicht-reguläre Sprache $\{0^n1^n \mid n \in \mathbb{N}\}$ akzeptiert. $\langle M_i \rangle$ ist die Binärkodierung der jeweiligen Turingmaschine.

M_3, M_4 und die Binärkodierungen sind offensichtlich berechenbar, also ist f berechenbar (und offensichtlich total). Weiterhin gilt:

$$\begin{array}{ll} & v \in L_u \\ \text{g.d.w.} & v = w\#x \text{ und } x \in L(M_w) \\ \text{g.d.w.} & M_{f(v)} \text{ akzeptiert eine reguläre Sprache} \\ \text{g.d.w.} & f(v) \in L_r \end{array}$$

Somit ist f eine valide Reduktionsfunktion und $L_u \leq L_r$.

c) Sei $A = \{w \in \{0,1\}^* \mid M_w \text{ hält bei Eingabe 36 mit Ausgabe 42 an}\}$. Zeigen Sie durch Reduktion von H_0 auf A, dass A unentscheidbar ist.

Beweis:
Wir zeigen $H_0 \leq A$. Da H_0 unentscheidbar ist, folgt daraus, dass auch A unentscheidbar ist.

Wir definieren die Reduktionsfunktion $f : \{0,1\}^* \to \{0,1\}^*$ wie folgt. Für $w \in \{0,1\}^*$ berechnet f zunächst die Turingmaschine M_w, erstellt daraus eine Turingmaschine T und berechnet anschließend deren Binärcodierung $\langle T \rangle$. Dabei verhält sich T wie folgt:

- Prüfe, ob auf dem Band die Zahl 36 (in Binärdarstellung) steht. Falls nein, gehe in eine Endlosschleife über.
- Führe M_w aus.
- Falls M_w anhält, schreibe die Zahl 42 (in Binärdarstellung) auf das Band und akzeptiere.

Die Funktion f ist offensichtlich total. Sie ist auch berechenbar, da T konstruierbar ist. Weiterhin gilt:

$$\begin{array}{ll} & w \in H_0 \\ \text{g.d.w.} & M_w \text{ hält auf leerem Band} \\ \text{g.d.w.} & M_{f(w)} \text{ hält für Eingabe 36 mit Ausgabe 42} \\ \text{g.d.w.} & f(w) \in A \end{array}$$

Somit ist f eine valide Reduktionsfunktion und $H_0 \leq A$.

FSK12-3 $\mathcal{P}$ ***und*** $\mathcal{NP}$ (0 Punkte)

a) Zeigen Sie, dass $\mathcal{P}$ unter Vereinigung abgeschlossen ist.

b) Zeigen Sie, dass $\mathcal{P}$ unter Schnitt abgeschlossen ist.

c) Zeigen Sie, dass $\mathcal{NP}$ unter Vereinigung abgeschlossen ist.

d) Zeigen Sie, dass $\mathcal{NP}$ unter Schnitt abgeschlossen ist.

FSK12-4 ***PCP und DFA*** (0 Punkte)

Betrachten Sie das folgende Verfahren V:

V berechnet für eine PCP-Instanz K über einem Alphabet Σ (d. h. $K = ((x_1, y_1), \dots, (x_k, y_k))$ mit $x_i, y_i \in \Sigma^+$) und einen deterministischen endlichen Automaten $A = (Z, \Sigma, \delta, z_0, E)$ einen Wahrheitswert.

Dafür wird zunächst die Menge $M \subseteq Z \times Z$ folgendermaßen iterativ bestimmt:

- Anfangs ist $M = \varnothing$
- In jedem Schritt wird für alle $(z_i, z_j) \in M$, sowie für (z_0, z_0) (selbst, wenn es nicht in M enthalten ist) und jedes Wortpaar/Spielstein $T = (x_l, y_l)$ aus K bestimmt, welcher Zustand $z_{i'}$ von z_i aus mit dem oberen Wort von T erreicht wird (d.h. $z_{i'} = \widehat{\delta}(z_i, x_l)$) und welcher Zustand $z_{j'}$ von z_j aus mit dem unteren Wort von T erreicht wird (d.h. $z_{j'} = \widehat{\delta}(z_j, y_l)$).

  Das Tupel $(z_{i'}, z_{j'})$ wird zu M hinzugefügt, wenn es nicht bereits in M vorhanden ist.
- Wenn sich die Menge M nicht mehr ändert, ist dies die engültige Gestalt von M und die Berechnung von M ist beendet.

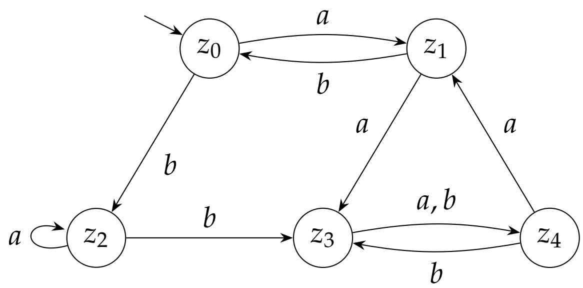
Gibt es nun einen Zustand $z \in Z$ mit $(z, z) \in M$, so wird „wahr“ zurückgegeben, ansonsten „falsch“.

Hinweis: Die Endzustandsmenge E wird vom Verfahren V nicht verwendet.

a) Berechnen Sie die Menge M für die PCP-Instanz K:

$$\left\{ \begin{bmatrix} bba \\ bb \end{bmatrix}, \begin{bmatrix} abba \\ abbab \end{bmatrix}, \begin{bmatrix} aba \\ bab \end{bmatrix}, \begin{bmatrix} abaaba \\ bbb \end{bmatrix}, \begin{bmatrix} ba \\ bbaabbab \end{bmatrix} \right\}$$

und den Automaten A:



Was gibt das Verfahren zurück?

b) Wenn V auf einer PCP-Instanz K gelaufen ist, was kann man dann aus einer „wahr"- und was aus einer „falsch"-Antwort für die PCP-Instanz schlussfolgern?

Bestimmen Sie mit Begründung getrennt für den „wahr"- und „falsch"-Fall die richtige Antwortkategorie:

- K hat sicher eine Lösung
- K hat sicher keine Lösung
- Man kann damit noch nicht sicher sagen, ob K eine Lösung hat

c) Zeigen Sie, dass es PCP-Instanzen K gibt, die keine Lösung haben, bei denen es aber dennoch keinen Automaten A gibt, sodass $V(K, A)$ mit „falsch" antwortet.

Hinweis: Die Unentscheidbarkeit von PCP kann Ihnen beim Beweis helfen