

Lösungsvorschlag zur Klausurvorbereitungsaufgabe zur Übung 11 zur
Vorlesung
Formale Sprachen und Komplexität

Klausurvorbereitung FSK-11-K

- a) 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 $(x_1, y_1), \dots, (x_n, y_n)$ mit $x_i, y_i \in \{w \mid w \in \Sigma^* \text{ und } |w| \text{ gerade}\}$ für $i = 1, \dots, n$. Beispielsweise ist $(ab, aaba)$ ein erlaubter Spielstein; (ab, aab) aber nicht.

Zeigen Sie durch Reduktion von PCP auf EVENPCP, dass EVENPCP unentscheidbar ist.

LÖSUNGSVORSCHLAG:

Wir zeigen $\text{PCP} \leq \text{EVENPCP}$. Da PCP unentscheidbar ist, folgt daraus, dass auch EVENPCP unentscheidbar ist.

Sei $K = ((x_1, y_1), \dots, (x_n, y_n))$ eine Instanz von PCP mit Alphabet Σ . Wir definieren für jedes Wort $w = z_1 \cdots z_p$ mit $z_i \in \Sigma$ das Wort $f(w) = z_1 z_1 \cdots z_p z_p$. Damit ist $|f(w)|$ gerade. Definiere nun die EVENPCP-Instanz $f(K) = ((f(x_1), f(y_1)), \dots, (f(x_n), f(y_n)))$. Offensichtlich ist f total und berechenbar. Außerdem ist f kompatibel mit Konkatination: $f(u \circ v) = f(u) \circ f(v)$ für alle $u, v \in \Sigma^*$. Es gilt somit:

- Wenn $K \in \text{PCP}$ ist, dann hat K eine Lösung $i_1, \dots, i_m$ mit $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$. Dann ist auch

$$f(x_{i_1}) \cdots f(x_{i_m}) = f(x_{i_1} \cdots x_{i_m}) = f(y_{i_1} \cdots y_{i_m}) = f(y_{i_1}) \cdots f(y_{i_m})$$

und es ist also $i_1, \dots, i_m$ eine Lösung für $f(K)$, somit $f(K) \in \text{EVENPCP}$.

- Wenn $f(K) \in \text{EVENPCP}$ ist, dann hat $f(K)$ eine Lösung $i_1, \dots, i_m$ mit $f(x_{i_1}) \cdots f(x_{i_m}) = f(y_{i_1}) \cdots f(y_{i_m})$. Wir definieren die Funktion g , die aus einem Wort mit gerader Länge p jeden zweiten Buchstaben entfernt: $g(z_1 z_2 z_3 \cdots z_{p-1} z_p) = z_1 z_3 \cdots z_{p-1}$. Damit ist g linksinvers zu f ,

d.h. $g(f(w)) = w$ für alle $w \in \Sigma^*$. Es gilt also:

$$\begin{aligned} x_{i_1} \cdots x_{i_m} &= g(f(x_{i_1} \cdots x_{i_m})) = g(f(x_{i_1}) \cdots f(x_{i_m})) = \\ &g(f(y_{i_1}) \cdots f(y_{i_m})) = g(f(y_{i_1} \cdots y_{i_m})) = y_{i_1} \cdots y_{i_m} \end{aligned}$$

Somit ist $i_1, \dots, i_m$ auch eine Lösung für K und $K \in \text{PCP}$.

- b) Sei $A = \{w \in \{0,1\}^* \mid M_w \text{ hält bei Eingabe 36 mit Ausgabe 42 an}\}$. Der folgende Beweis zur Unentscheidbarkeit von A ist falsch. Lokalisieren Sie den Fehler und begründen Sie, wieso der Beweis falsch ist.

Beweis:

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

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

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

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

LÖSUNGSVORSCHLAG:

Die von f für w konstruierte Turingmaschine löscht nicht das Band, bevor sie M_w ausführt. Somit testet sie nicht, ob M_w auf dem leeren Band hält. Die Aussage „ M_w hält auf dem leeren Band g.d.w. $M_{f(w)}$ für Eingabe 36 mit Ausgabe 42 hält“ ist also falsch.