

Lösungsvorschlag zur Übung 11 zur Vorlesung
Theoretische Informatik für Studierende der Medieninformatik

TIMI11-1 PCP-Varianten

(2 Punkte)

- a) Wir betrachten das 456PCP-Problem, eine Variante von PCP, bei der die ‚Spielsteine‘ auf das Alphabet $\Sigma = \{4, 5, 6\}$ beschränkt sind. Eine Instanz von 456PCP ist also eine endliche Folge von Paaren $(x_1, y_1), \dots, (x_n, y_n)$ mit $x_i, y_i \in \{4, 5, 6\}^+$ für $i = 1, \dots, n$. Eine Lösung der Instanz K ist wie bei PCP eine endliche Folge von Indices $i_1, \dots, i_m \in \mathbb{N}$, sodass $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$.

Zeigen Sie durch Reduktion von PCP auf 456PCP, dass 456PCP unentscheidbar ist.

LÖSUNGSVORSCHLAG:

Wir zeigen $\text{PCP} \leq 456\text{PCP}$. Da PCP unentscheidbar ist, ist damit auch 456PCP unentscheidbar.

Sei $K = ((x_1, y_1), \dots, (x_n, y_n))$ eine Instanz von PCP mit Alphabet $\Sigma = \{a_1, \dots, a_j\}$. Wir definieren $f(a_i) = 45^i$ für die Elemente aus Σ und $f(\varepsilon) = \varepsilon$, $f(a_i w) = f(a_i) f(w)$ für Wörter aus Σ^* , sowie schließlich $f(K) = (f(x_1), f(y_1)), \dots, (f(x_n), f(y_n))$ für Instanzen. Da 45^i ein Wort aus $\{4, 5, 6\}^+$ darstellt, überführt f Instanzen von PCP in Instanzen von 456PCP. Damit ist f auch offensichtlich total und berechenbar.

Weiter gilt:

- 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

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

und es ist also $i_1, \dots, i_m$ eine Lösung für $f(K)$, somit $f(K) \in 456\text{PCP}$.

- Wenn $f(K) \in 456\text{PCP}$ ist, dann hat $f(K)$ eine Lösung $i_1, \dots, i_m$ mit $f(x_{i_1}) \cdots f(x_{i_m}) = f(y_{i_1}) \cdots f(y_{i_m})$. Die Zuordnung 45^i zu Buchstaben a_i ist eindeutig für ein gegebenes Alphabet Σ , damit können wir eine Funktion g angeben die sich invers zu f verhält. 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 $K \in \text{PCP}$.

- b) Wir betrachten das PCP4-Problem, eine Variante von PCP, bei der die Spielsteine aus vier Wörtern bestehen. Eine Instanz von PCP4 ist also eine endliche Folge von 4-Tupeln $(x_1, y_1, z_1, u_1), \dots, (x_n, y_n, z_n, u_n)$ mit $x_i, y_i, z_i, u_i \in \Sigma^+$ für $i = 1, \dots, n$. Eine Lösung der Instanz K ist ähnlich zu PCP eine endliche Folge von Indices $i_1, \dots, i_m \in \mathbb{N}$, sodass $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m} = z_{i_1} \cdots z_{i_m} = u_{i_1} \cdots u_{i_m}$.

Zeigen Sie durch Reduktion von PCP auf PCP4, dass PCP4 unentscheidbar ist.

LÖSUNGSVORSCHLAG:

Wir zeigen $\text{PCP} \leq \text{PCP4}$. Da PCP unentscheidbar ist, folgt daraus, dass auch PCP4 unentscheidbar ist.

Sei $K = ((x_1, y_1), \dots, (x_n, y_n))$ eine Instanz von PCP mit Alphabet Σ . Wir definieren $f(K) = f((x_1, y_1), \dots, f((x_n, y_n))$ und $f((x_i, y_i)) = (x_i, y_i, x_i, x_i)$. Damit ist $f(K)$ auf jeden Fall eine Instanz von PCP4 und f ist offensichtlich total und berechenbar.

Es gilt somit:

- Wenn $K \in \text{PCP}$ ist, dann hat K eine Lösung $i_1, \dots, i_m$ mit $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$. Da $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m} = x_{i_1} \cdots x_{i_m} = x_{i_1} \cdots x_{i_m}$, ist $i_1, \dots, i_m$ auch eine Lösung für $f(K)$, somit $f(K) \in \text{PCP4}$.
- Wenn $f(K) \in \text{PCP4}$ ist, dann hat $f(K)$ eine Lösung $i_1, \dots, i_m$ mit $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m} = x_{i_1} \cdots x_{i_m} = x_{i_1} \cdots x_{i_m}$. Somit gilt auch bereits $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$ und $i_1, \dots, i_m$ ist auch eine Lösung für K und $K \in \text{PCP}$.

- c) Sind die folgenden Instanzen K_1, K_2 von PCP4 lösbar? Wenn ja, geben Sie eine Lösung (also eine geeignete Folge von Indizes) an. Wenn nein, beweisen Sie, dass die Instanz keine Lösung hat.

$$K_1 = \left(\begin{bmatrix} bbc \\ bca \\ cab \\ bbca \end{bmatrix}, \begin{bmatrix} a \\ ab \\ abb \\ a \end{bmatrix}, \begin{bmatrix} cca \\ ca \\ a \\ ca \end{bmatrix}, \begin{bmatrix} abc \\ bcc \\ ccc \\ bcc \end{bmatrix} \right)$$

$$K_2 = \left(\begin{bmatrix} c \\ b \\ bab \\ cc \end{bmatrix}, \begin{bmatrix} acb \\ baa \\ aaa \\ acba \end{bmatrix}, \begin{bmatrix} bca \\ caaaa \\ b \\ c \end{bmatrix}, \begin{bmatrix} b \\ ba \\ b \\ bab \end{bmatrix} \right)$$

LÖSUNGSVORSCHLAG:

K_1 hat die Lösung 2, 1, 4, 3, also

$$\begin{bmatrix} a \\ ab \\ abb \\ a \end{bmatrix}, \begin{bmatrix} bbc \\ bca \\ cab \\ bbca \end{bmatrix}, \begin{bmatrix} abc \\ bcc \\ ccc \\ bcc \end{bmatrix}, \begin{bmatrix} cca \\ ca \\ a \\ ca \end{bmatrix}$$

K_2 hat keine Lösung: Mit den Spielsteinen 1, 2 und 3 kann man nicht beginnen, da alle mindestens ein Wort haben das bereits im ersten Symbol nicht mit den anderen übereinstimmt. Betrachten wir also den Fall, dass wir mit

dem Spielstein $\begin{bmatrix} b \\ ba \\ b \\ bab \end{bmatrix}$ anfangen. Wenn wir mit $\begin{bmatrix} c \\ b \\ bab \\ cc \end{bmatrix}$ oder $\begin{bmatrix} acb \\ baa \\ aaa \\ acba \end{bmatrix}$ wei-

ter machen wollen, passen die ersten beiden Wörter nicht zusammen, da bc kein Präfix von bab bzw. ba kein Präfix von $baaa$ ist, also können diese

keine Weiterführungen sein. Mit $\begin{bmatrix} bca \\ caaa \\ b \\ c \end{bmatrix}$ haben wir allerdings in den letz-

ten beiden Wörtern einen Unterschied, da bb kein Präfix von $babc$ ist. Somit

gibt es keine mögliche Weiterführung und da $\begin{bmatrix} b \\ ba \\ b \\ bab \end{bmatrix}$ auch alleine noch kei-

ne Lösung ist, kann K_2 keine Lösung haben.

TIMI11-2 Beweise prüfen

(0 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 .

LÖSUNGSVORSCHLAG:

Der Beweis enthält zwei Fehler:

- $w \in D$ bedeutet, dass M_w die Eingabe w *nicht* akzeptiert. Die Lösung geht in den zwei Stichpunkten aber davon aus, dass $w \in D$ das Gegenteil bedeutet.
- Selbst wenn wir diesen Fehler beheben, nimmt die Lösung an, dass ein M mit der gewünschten Eigenschaft existiert, aber wir haben das nie gezeigt. Der Beweis ist also zirkulär: „Unter der Annahme, dass M existiert, existiert M .“

Tatsächlich ist D nicht semi-entscheidbar, d.h. die Aussage ist falsch. Intuition: Die einzige Möglichkeit, zu testen, ob M_w das Wort w nicht akzeptiert, ist, M_w auf w auszuführen. Wenn M_w dann beliebig lange läuft, kann man nie sagen, ob M_w noch halten (und damit akzeptieren) wird oder nicht.

- 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

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

Dabei ist M_3 eine Turingmaschine, die die reguläre Sprache $\{0,1\}^*$ akzeptiert. M_4 ist eine Turingmaschine, die die nichtreguläre Sprache $\{0^n 1^n \mid n \in \mathbb{N}\}$ akzeptiert. w_{M_i} 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 $L_u \leq L_r$.

LÖSUNGSVORSCHLAG:

Die Reduktionsfunktion f ist nicht berechenbar. Um zu entscheiden, ob $f(v) = w_{M_3}$ oder $f(v) = w_{M_4}$, müssen wir entscheiden, ob M_w das Wort x akzeptiert. Das ist aber bekanntermaßen unentscheidbar.

- 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 $f : \{0,1\}^* \rightarrow \{0,1\}^*$ 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:

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

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

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.