Theorie der Informatik

G. Röger
F. Pommerening
Frühjahrssemester 2020

Universität Basel
Fachbereich Informatik

Übungsblatt 11 — Lösungen

Aufgabe 11.1 (Unentscheidbarkeit; 1+3+2 Punkte)

(a) Zeigen Sie, dass es für jedes Alphabet Σ eine kontextfreie Grammatik $G_{\text{Palindrom}}(\Sigma)$ gibt, die genau die nichtleeren Palindrome über Σ erzeugt.

Lösung:

Die Grammatik $G_{\text{Palindrom}}(\Sigma) = \langle \Sigma, \{S\}, P, S\rangle$ mit $P = \{S \to x \mid x \in \Sigma\} \cup \{S \to xx \mid x \in \Sigma\} \cup \{S \to xSx \mid x \in \Sigma\}$ erzeugt genau die nicht-leeren Palindrome über Σ und ist kontextfrei.

(b) Betrachten Sie eine PCP-Instanz $\mathcal{I} = \langle (x_1, y_1), \ldots, (x_k, y_k)\rangle$ mit $x_i, y_i \in \Sigma^+$. Sei $\Sigma' = \Sigma \cup \{\#\}$, wobei $\#$ ein Zeichen ist, das in Σ nicht vorkommt. Geben Sie eine kontextfreie Grammatik $G_\mathcal{I}$ über Σ' an, welche die folgende Sprache erzeugt (mit $^{-1}$ bezeichnen wir hier die Umkehrung eines Wortes):

$$\mathcal{L}(G_\mathcal{I}) = \{x_{i_1} \ldots x_{i_n} \# y_{i_n}^{-1} \ldots y_{i_1}^{-1} \mid n \geq 1 \text{ und } i_1, \ldots, i_n \in \{1, \ldots, k\}\}$$

Zeigen Sie dann, dass $\mathcal{I}$ genau dann eine Lösung hat, wenn $\mathcal{L}(G_\mathcal{I})$ ein Palindrom enthält.

Lösung:

Die Grammatik $G_\mathcal{I} = \langle \Sigma', \{S, Z\}, P, S\rangle$ mit $P = \{S \to x_i Z y_i^{-1} \mid 1 \leq i \leq k\} \cup \{Z \to x_i Z y_i^{-1} \mid 1 \leq i \leq k\} \cup \{Z \to \#\}$ erzeugt die gesuchte Sprache und ist kontextfrei.

- Wenn $i_1, \ldots i_n$ eine Lösung von $\mathcal{I}$ ist, können wir ein Palindrom in $G_\mathcal{I}$ ableiten:
  Dazu wird zuerst die Regel $S \to x_1 Z y_1^{-1}$ angewendet und dann die Regeln $Z \to x_i Z y_i^{-1}$ für $i = i_2, \ldots, i = i_k$. Zuletzt wird dann noch $Z \to \#$ angewendet. Das so generierte Wort ist $x_{i_1} \ldots x_{i_n} \# y_{i_n}^{-1} \ldots y_{i_1}^{-1}$. Es erfüllt $x_{i_1} \ldots x_{i_n} = y_{i_1} \ldots y_{i_n} = (y_{i_n}^{-1} \ldots y_{i_1}^{-1})^{-1}$ (weil $i_1, \ldots i_n$ eine Lösung von $\mathcal{I}$ ist) und ist daher ein Palindrom.
- Wenn wir ein Palindrom in $G_\mathcal{I}$ ableiten können, dann gibt es eine Lösung von $\mathcal{I}$:
  Da es nur eine Regel gibt, mit der $\#$ eingefügt wird und diese Regel genau einmal angewendet werden muss, muss auch $\#$ genau einmal in jedem abgeleiteten Wort vorkommen. Wenn das abgeleitete Wort ein Palindrom ist, muss $\#$ in der Mitte stehen und das Palindrom muss die Form $x\#y$ mit $x, y \in \Sigma^+$ und $x = y^{-1}$ haben. Zudem muss es Indizes $i_1, \ldots, i_n$ geben, so dass $x = x_{i_1} \ldots x_{i_n}$ und $y = y_{i_n}^{-1} \ldots y_{i_1}^{-1}$, da das Wort sonst nicht in der Sprache wäre. Zusammen erhalten wir, dass $x_{i_1} \ldots x_{i_n} = x = y^{-1} = (y_{i_n}^{-1} \ldots y_{i_1}^{-1})^{-1} = y_{i_1} \ldots y_{i_n}$ gilt, also ist $i_1, \ldots, i_n$ eine Lösung für $\mathcal{I}$.

(c) Verwenden Sie die Ergebnisse aus den Teilaufgaben (a) und (b) um zu beweisen, dass das Schnittproblem für *kontextfreie* Grammatiken unentscheidbar ist.

SCHNITT$_{\text{KF}}$: Gegeben zwei kontextfreie Grammatiken G_1 und G_2, gilt $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \emptyset$?

Hinweis: Natürlich können Sie die Aussagen aus den Teilen (a) und (b) auch verwenden, wenn Sie die Aufgaben nicht gelöst haben.

Lösung:

Wir zeigen, dass $\overline{\text{PCP}} \leq \textsc{Schnitt}_{\text{KF}}$. Weil PCP unentscheidbar ist, ist auch das Komplement $\overline{\text{PCP}}$ unentscheidbar.

Wir verwenden die Reduktionsfunktion $f(\mathcal{I}) = \langle G_{\mathcal{I}}, G_{\text{Palindrom}}(\Sigma')\rangle$. Diese Funktion ist total und berechenbar da wir das Alphabet Σ' und die Grammatiken $G_{\mathcal{I}}$ und $G_{\text{Palindrom}}(\Sigma')$ für beliebige Instanzen $\mathcal{I}$ erstellen können.

Wir wissen aus Teilaufgabe (a), dass die kontext-freie Grammatik $G_{\text{Palindrom}}(\Sigma')$ genau die Sprache aller (nichtleeren) Palindrome über Σ' generiert. Aus Teilaufgabe (b) wissen wir, dass die kontext-freie Grammatik $G_{\mathcal{I}}$ für eine Instanz $\mathcal{I}$ des PCP eine Sprache generiert, die ein Palindrome enthäl gdw. es eine Lösung für $\mathcal{I}$ gibt. Also gilt $G_{\mathcal{I}} \cap G_{\text{Palindrom}}(\Sigma') \neq \emptyset$ gdw. $\mathcal{I}$ eine Lösung hat.

Zusammenfassend erhalten wir

$$\mathcal{I} \notin \text{PCP gdw. } G_{\mathcal{I}} \cap G_{\text{Palindrom}}(\Sigma') = \emptyset \text{ gdw. } f(\mathcal{I}) \in \textsc{Schnitt}_{\text{KF}}$$

Daher ist f eine Reduktion von $\overline{\text{PCP}}$ auf $\textsc{Schnitt}_{\text{KF}}$. Weil $\overline{\text{PCP}}$ unentscheidbar ist, impliziert das, dass auch $\textsc{Schnitt}_{\text{KF}}$ unentscheidbar ist.

Aufgabe 11.2 (Nicht-deterministische Algorithmen; 2+2 Punkte)

Geben Sie für die folgenden Probleme einen nichtdeterministischen, polynomiellen Algorithmus an. Damit zeigen Sie, dass die Probleme in der Komplexitätsklasse NP liegen, die wir nächste Woche kennenlernen werden.

(a) HittingSet:

- *Gegeben:* endliche Menge M, Menge $\mathcal{S} = \{S_1, \ldots, S_n\}$ mit $S_i \subseteq M$ für alle $i \in \{1, \ldots, n\}$, eine natürlich Zahl $k \in \mathbb{N}_0$
- *Gefragt:* Gibt es eine Menge H mit höchstens k Elementen, die aus jeder Menge aus $\mathcal{S}$ mindestens ein Element enthält?

  Formal: Gibt es eine Menge H mit $|H| \leq k$ und $H \cap S_i \neq \emptyset$ für alle $i \in \{1, \ldots, n\}$?

Lösung:

Eingabe: Menge M, Menge von Mengen $\mathcal{S}$, Zahl k

$$\begin{array}{l}
\mathit{hittingset} := \emptyset \\
\mathit{remaining} := M \\
\mathit{not_hit} := \mathcal{S} \\
\textbf{WHILE } |\mathit{hittingset}| < k : \\
\quad \textbf{GUESS } \mathit{next} \in \mathit{remaining} \\
\quad \mathit{remaining} := \mathit{remaining} \setminus \{\mathit{next}\} \\
\quad \mathit{hittingset} := \mathit{hittingset} \cup \{\mathit{next}\} \\
\quad \mathit{not_hit_prev} := \text{copy of } \mathit{not_hit} \\
\quad \textbf{FOR } s \in \mathit{not_hit_prev} : \\
\qquad \textbf{IF } \mathit{next} \in s \\
\qquad\quad \mathit{not_hit} := \mathit{not_hit} \setminus \{s\} \\
\quad \textbf{IF } \mathit{not_hit} = \emptyset : \\
\qquad \textbf{ACCEPT} \\
\textbf{REJECT}
\end{array}$$

(b) SetPacking:

- *Gegeben:* endliche Menge M, Menge $\mathcal{S} = \{S_1, \dots, S_n\}$ mit $S_i \subseteq M$ für alle $i \in \{1, \dots, n\}$, eine natürlich Zahl $k \in \mathbb{N}_0$
- *Gefragt:* Gibt es $\mathcal{S}' \subseteq \mathcal{S}$ mit $|\mathcal{S}'| \geq k$, so dass alle Mengen in $\mathcal{S}'$ paarweise disjunkt sind, d.h. für alle $S_i, S_j \in \mathcal{S}'$ mit $S_i \neq S_j$ gilt $S_i \cap S_j = \emptyset$?

Lösung:

Eingabe: Menge M, Menge von Mengen $\mathcal{S}$, Zahl k

$$
\begin{array}{l}
\mathit{chosen} := \emptyset \\
\mathit{remaining} := \mathcal{S} \\
\textbf{WHILE } |\mathit{chosen}| < k : \\
\quad \textbf{IF } \mathit{remaining} = \emptyset : \\
\quad\quad \textbf{REJECT} \\
\quad \textbf{GUESS } \mathit{next} \in \mathit{remaining} \\
\quad \textbf{FOR } \mathit{set} \in \mathit{chosen} : \\
\quad\quad \textbf{IF } \mathit{next} \cap \mathit{set} \neq \emptyset : \\
\quad\quad\quad \textbf{REJECT} \\
\quad \mathit{chosen} := \mathit{chosen} \cup \{\mathit{next}\} \\
\quad \mathit{remaining} := \mathit{remaining} \setminus \{\mathit{next}\} \\
\textbf{ACCEPT}
\end{array}
$$