Universität Leipzig
Institut für Informatik
Sommersemester 2025

Prof. Dr. Andreas Maletti,
Dr. habil. Karin Quaas,
Fabian Sauer

Aufgaben zur Lehrveranstaltung

# Berechenbarkeit

## Lösungen zu Serie 7

---

### Übungsaufgabe 7.1

Besitzen die folgenden Instanzen des Postschen Korrespondenzproblems (PCP) eine Lösung? Falls ja, geben Sie eine Lösung an. Falls nicht, begründen Sie, warum keine Lösung existieren kann.

(a) $\langle (ab, abb), (aab, ba), (ba, aa) \rangle$ Nein, es existiert keine Lösung: gäbe es eine Lösung, so müssten die beiden Wörter im letzten Index gleich enden; allerdings endet keines der Paare im gleichen Index gleich.

(b) $\langle (ab, abab), (b, a), (aba, b), (aa, a) \rangle$ Ja, die Indexfolge $4, 4, 2, 1$ ist eine Lösung, denn sie ergibt das Wort $aaaabab = aaaabab$.

### Übungsaufgabe 7.2

Gegeben sei das folgende Entscheidungsproblem $P_1$:

- Gegeben ein PCP $P = \langle (u_1, v_1), \ldots, (u_k, v_k) \rangle$ über $\Sigma = \{a\}$.
- Frage: Besitzt $P$ eine Lösung?

Zeigen Sie, dass $P_1$ deterministisch polynomiell entscheidbar ist.

Lösung: Sei $\langle (u_1, v_1), \ldots, (u_k, v_k) \rangle$ ein PCP über $\Sigma = \{a\}$. Wir unterscheiden vier Fälle:

(a) Falls es ein $1 \leq i \leq k$ gibt mit $u_i = v_i$, so ist die Indexfolge $i$ eine Lösung für $P$.

(b) Falls für alle $1 \leq i \leq k$ gilt, dass $|u_i| < |v_i|$, so kann es keine Lösung geben (das erste Wort ist notwendigerweise immer kürzer als das zweite Wort).

(c) Falls für alle $1 \leq i \leq k$ gilt, dass $|u_i| > |v_i|$, so kann es keine Lösung geben (das zweite Wort ist notwendigerweise immer kürzer als das erste Wort).

(d) Anderenfalls muss es $1 \leq i, j \leq k$ mit $i \neq j$ geben, sodass $|u_i| < |v_i|$ und $|u_j| > |v_j|$. Setze $J = |v_i| - |u_i|$ und setze $I = |u_j| - |v_j|$. Die Indexfolge $\underbrace{i, \ldots, i}_{\text{I-mal}}, \underbrace{j, \ldots, j}_{\text{J-mal}}$ ist eine Lösung für $P$.

Diese Tests können in Polynomialzeit von einer deterministischen Turingmaschine ausgeführt werden: Die TM geht von links nach rechts über das Eingabeband (mit der darauf gespeicherten Instanz des PCP). Das Problem ist also polynomiell entscheidbar.

## Übungsaufgabe 7.3 (NP)

Wir definieren das *Problem der zwei Fahrradtaschen* wie folgt.

- Gegeben: $n_1, n_2, \ldots, n_k$ in Binärkodierung
- Frage: Existieren nicht-leere $I, J \subseteq \{1, \ldots, k\}$ sodass $I \cap J = \emptyset$ und $\sum_{i \in I} n_i = \sum_{j \in J} n_j$?

(a) Geben Sie für die beiden folgenden Instanzen des Problems der zwei Fahrradtaschen an, ob es sich um positive oder negative Instanzen handelt (mit Begründung).

(i) $5, 7, 3, 17, 1, 2$

(ii) $1, 2, 4, 8, 16$

(b) Zeigen Sie, dass das Problem der zwei Fahrradtaschen nichtdeterministisch polynomiell entscheidbar ist.

LÖSUNG: Zertifikatrelation $R \subseteq (\{0,1\}^* \times \{0,1\}^*)$ definiert durch $(u, z) \in R$ gdw.

- $u = \text{bin}(n_1)\#\text{bin}(n_2)\#\ldots\#\text{bin}(n_k)$
- $z = i_1 i_2 \ldots i_k j_1 j_2 \ldots j_k$ ($i_p = 1$ bedeutet: $n_p \in I$, analog: $j_p = 1$ bedeutet $n_p \in J$)
- es existiert $1 \leq p \leq k$ mit $i_p = 1$ (mindestens ein Element in $I$)
- es existiert $1 \leq p \leq k$ mit $j_p = 1$ (mindestens ein Element in $J$)
- für alle $1 \leq p \leq k$ gilt $i_p = 1 \Rightarrow j_p = 0$
- für alle $1 \leq p \leq k$ gilt $j_p = 1 \Rightarrow i_p = 0$ (diese und vorherige Bedingung garantieren $I \cap J = \emptyset$)
- $\sum_{\substack{1 \leq p \leq k \\ i_p = 1}} n_p = \sum_{\substack{1 \leq p \leq k \\ j_p = 1}} n_p$
- $R$ ist polynomiell entscheidbar: die einzelnen Bedingungen müssen getestet werden. Dies kann in polynomieller Zeit geschehen.
- $u$ ist positive Instanz des Problems der zwei Fahrradtaschen gdw. es existiert $z \in \Gamma^{2k}$ mit $(u, z) \in R$, für alle $u \in \{0,1\}^*$:

- Angenommen, $u$ ist eine positive Instanz des Problems. Dann gibt es zwei nicht-leere disjunkte Mengen $I = \{\alpha_1, \ldots, \alpha_m\} \subseteq \{1, \ldots, k\}$ und $J = \{\beta_1, \ldots, \beta_n\} \subseteq \{1, \ldots, k\}$ mit $\sum_{\alpha_\ell \in I} n_{\alpha_\ell} = \sum_{\beta_\ell \in J} n_{\beta_\ell}$. Definiere das Zertifikat $z = i_1 i_2 \ldots i_k j_1 j_2 \ldots j_k$ durch $i_\ell = 1$ gdw. $\ell \in I$ und $j_\ell = 1$ gdw. $\ell \in J$. Da $I, J$ nicht leer, existieren $1 \leq p \leq k$ mit $i_p = 1$ und $1 \leq q \leq k$ mit $j_q = 1$. Da $I \cap J = \emptyset$, gilt für alle $1 \leq p \leq k$: falls $i_p = 1$, dann $j_p = 0$, und falls $j_p = 1$, dann $i_p = 0$. Die Summenbedingung gilt direkt nach Annahme. Also $(u, z) \in R$.
- Angenommen $(u, z) \in R$ mit $z = i_1 i_2 \ldots i_k j_i \ldots j_k$. Setze $I = \{\alpha \mid i_\alpha = 1\}$ und $J = \{\alpha \mid j_\alpha = 1\}$. Nach Annahme gibt es $1 \leq i \leq k$ mit $i_p = 1$, also $p \in I$, also $I \neq \emptyset$ (und analog für $J$). Weiterhin gilt für alle $p$, falls $i_p = 1$, dann $j_p = 0$, also: falls $p \in I$, dann $p \notin J$, und falls $j_p = 1$, dann $i_p = 0$, also: falls $p \in J$, dann $p \notin I$. Also $I \cap J \neq \emptyset$. Summe gilt auch, also $u$ positive Instanz.