Hausaufgabenblatt

Hinweise:

- Die Hausaufgabe kann ab dem **12.01.2023, 00:00 Uhr** bis zum **13.01.2023, 23:59 Uhr** auf ISIS hochgeladen werden.
- Die Hausaufgabe muss in Dreiergruppen bearbeitet werden.[1] Bitte tragen Sie sich in ISIS bis zum **11.01.2023, 23:59 Uhr** in der Gruppenwahl ein. Die Hausaufgabe kann nur von eingetragenen Gruppen abgegeben werden.
- Bitte verwenden Sie die LaTeX-Vorlage auf ISIS für Ihre Abgabe.
- Plagiate werden nicht toleriert und werden scharf geahndet.
- Es können bis zu **25 Portfoliopunkte** erreicht werden.
- Alle Antworten sind zu begründen. Antworten ohne Begründung erhalten **0 Punkte**. Achten Sie insbesondere darauf, die Korrektheit Ihrer angegebenen Lösungen (Algorithmen, Reduktionen etc.) zu begründen.
- Um zu zeigen, dass eine Sprache (semi-)entscheidbar ist, reicht es aus, die prinzipielle Arbeitsweise eine(r/s) Turing-Maschine/Algorithmus/WHILE-/GOTO-Programmes zu beschreiben, welche(r) die Sprache (semi-)entscheidet (die (halbe) charakteristische Funktion berechnet). Falls Sie in einer Reduktion eine Turing-Maschine konstruieren, so reicht es ebenfalls aus, ihr Verhalten algorithmisch zu beschreiben.
- Sätze, die in der Vorlesung oder Modulkonferenz *bewiesen* wurden (auch skizzenhaft) dürfen verwendet werden (unbewiesene Mitteilungen nicht).
- Erstellen Sie für jede Aufgabe ein separates Dokument und laden Sie es in der jeweiligen Dokumentabgabe in ISIS hoch.
- Wir empfehlen pro erreichbarem Punkt nicht mehr als 1/3 Seite zu schreiben. Wir behalten uns vor, nur die ersten 6 Seiten jedes Dokuments zu lesen.

Aufgabe 1. *(Semi-)Entscheidbarkeit von Sprachen* 10 P.

Betrachten Sie die folgenden Sprachen:

$$A \coloneqq \{w \in \{0,1\}^* \mid T(M_w) \cap \{0,1\}^n \neq \emptyset \text{ für alle } n \in \mathbb{N}\},$$
$$B \coloneqq \left\{ w \in \{0,1\}^* \;\middle|\; \begin{array}{l} M_w \text{ berechnet die charakteristische Funktion} \\ \text{einer unentscheidbaren Sprache} \end{array} \right\}$$
$$C \coloneqq \{w \in \{0,1\}^* \mid \text{die Anzahl der Zustände von } M_w \text{ ist größer als } |T(M_w)|\}$$

(a) Ist A semi-entscheidbar?

(b) Ist A co-semi-entscheidbar?

(c) Ist B semi-entscheidbar?

(d) Ist B co-semi-entscheidbar?

(e) Ist C semi-entscheidbar?

(f) Ist C co-semi-entscheidbar?

[1] In begründeten Ausnahmen schreiben Sie bitte eine E-Mail an `bk@akt.tu-berlin.de`

Lösung:

(a) Nein. Wir zeigen $\overline{H_0} \leq A$. Da $\overline{H_0}$ nicht semi-entscheidbar ist (VL), folgt daraus, dass auch A nicht semi-entscheidbar ist.

Reduktion: Für eine gegebene TM $M = (Z, \Sigma, \Gamma, \delta, z_0, \Box, E)$ sei $\tau(M) = (Z', \{0,1\}, \Gamma', \delta', z', \Box, E')$ eine TM, die auf Eingabe $x \in \{0,1\}^*$ wie folgt arbeitet: Simuliere M auf leerem Band für $n := |x|$ Schritte. Falls M innerhalb von n Schritten hält, gehe in eine Endlosschleife. Falls M nicht in n Schritten hält, gehe in einen Endzustand.

$f\colon \{0,1\}^* \to \{0,1\}^*$, $w \mapsto \langle \tau(M_w) \rangle$ ist total und berechenbar (Kodierung von TM).

Es gilt:

$w \in \overline{H_0} \implies M_w$ hält nicht auf leerer Eingabe $\implies T(\tau(M_w)) = \{0,1\}^* \implies f(w) \in A$.

$w \notin \overline{H_0} \implies \exists n \in \mathbb{N} : M_w$ hält auf leerer Eingabe nach n Schritten $\implies \tau(M_w)$ akzeptiert kein Wort, das länger als n ist $\implies f(w) \notin A$.

(b) Nein, denn wir zeigen $H_0 \leq A$. Da H_0 nicht co-semi-entscheidbar ist (VL), folgt daraus, dass auch A nicht co-semi-entscheidbar ist.

Reduktion: Für eine gegebene TM $M = (Z, \Sigma, \Gamma, \delta, z_0, \Box, E)$ sei $\alpha(M) = (Z', \{0,1\}, \Gamma, \delta', z', \Box, E')$ eine TM, die auf Eingabe $x \in \{0,1\}^*$ wie folgt arbeitet: Lösche die Eingabe (neuer Startzustand) und simuliere dann M auf leerem Band. Falls M hält, gehe in einen (neuen) Endzustand über.

$f\colon \{0,1\}^* \to \{0,1\}^*$ ist definiert als $w \mapsto \langle \alpha(M_w) \rangle$ und ist total und berechenbar (Kodierung von TM).

Es gilt:

$w \in H_0 \implies M_w$ hält auf leerer Eingabe $\implies T(\alpha(M_w)) = \{0,1\}^* \implies f(w) \in A$.

$w \notin H_0 \implies T(\alpha(M_w)) = \emptyset \implies f(w) \notin A$.

(c) Ja, denn $B = \emptyset$, also entscheidbar.

(d) Ja, siehe (c).

(e) Nein. Wir zeigen $\overline{H_0} \leq C$ mithilfe der Funktion f aus Aufgabe (b).

Es gilt:

$w \in \overline{H_0} \implies M_w$ hält nicht auf leerer Eingabe $\implies |T(\alpha(M_w))| = 0 \implies f(w) \in C$.

$w \notin \overline{H_0} \implies M_w$ hält auf leerer Eingabe $\implies |T(\alpha(M_w))| = \infty \implies f(w) \notin C$.

(f) Ja. Eine TM M, die $\overline{C}$ akzeptiert, arbeitet bei Eingabe w wie folgt: Sei Σ das Eingabealphabet von M_w und Z die Zustandsmenge. Simuliere M_w auf allen Eingabewörtern "parallel". Das heißt, in der i-ten Iteration wird M_w für jedes der ersten i Wörter aus Σ^* für i Schritte simuliert. Sobald in einer Iteration mindestens $|Z|$ Wörter von M_w akzeptiert wurden, akzeptiert M das Wort w.

Korrektheit: Falls $w \notin \overline{C}$, dann geht M in eine Endlosschleife. Also gilt $w \notin T(M)$. Falls $w \in \overline{C}$, dann existiert ein $i \in \mathbb{N}$, sodass in der i-ten Iteration von M mindestens $|Z|$ Wörter aus $T(M_w)$ in i Schritten akzeptiert wurden. Somit gilt $w \in T(M)$.

Aufgabe 2. *Varianten des Postschen Korrespondenzproblems* 6 P.

Für eine Sequenz $i_1, \dots, i_n \in \mathbb{N}$ sei $\#_x(i_1, \dots, i_n) := |\{j \in \{1, \dots, n\} \mid i_j = x\}|$ die Anzahl der Vorkommen von $x \in \mathbb{N}$. Zum Beispiel $\#_2(1, 1, 2, 3, 1, 2, 2, 4) = 3$, da die 2 genau 3 mal in der Sequenz vorkommt.

Wir betrachten die folgenden zwei Varianten des Postschen Korrespondenzproblems (mit Alphabet Σ).

$$P_{\leq 2} := \left\{ \begin{array}{r|l} & k \geq 1, x_i, y_i \in \Sigma^* \text{ für alle } i \in \{1, \dots, k\}, \\ \langle (x_1,y_1), (x_2, y_2), & \text{und es existieren } n \geq 1 \text{ und } i_1, \dots, i_n \in \{1, \dots, k\}, \\ \dots, (x_k, y_k) \rangle & \text{sodass } x_{i_1} \cdot \dots \cdot x_{i_n} = y_{i_1} \cdot \dots \cdot y_{i_n} \text{und} \\ & \#_i(i_1, \dots, i_n) \leq 2 \text{ für jedes } i \in \{1, \dots, k\} \end{array} \right\}$$

$$P_{\text{even}} := \left\{ \begin{array}{r|l} & k \geq 1, x_i, y_i \in \Sigma^* \text{ für alle } i \in \{1, \dots, k\}, \\ \langle (x_1,y_1), (x_2, y_2), & \text{und es existieren } n \geq 1 \text{ und } i_1, \dots, i_n \in \{1, \dots, k\}, \\ \dots, (x_k, y_k) \rangle & \text{sodass } x_{i_1} \cdot \dots \cdot x_{i_n} = y_{i_1} \cdot \dots \cdot y_{i_n} \text{ und} \\ & \#_i(i_1, \dots, i_n) \text{ für jedes } i \in \{1, \dots, k\} \text{ gerade ist} \end{array} \right\}$$

Zeigen Sie für jede der beiden Sprachen $P_{\leq 2}$ und P_{even}, ob diese entscheidbar ist oder nicht.

Lösung:

$P_{\leq 2}$ ist entscheidbar, da jede Lösung höchstens Länge $n \leq 2k$ hat und somit nur endlich viele mögliche Lösungen existieren. Diese können einfach alle ausprobiert werden, um festzustellen, ob eine gültige Lösung existiert.

P_{even} ist unentscheidbar. Wir zeigen PCP $\leq P_{\text{even}}$.
$f\colon \{0,1\}^* \to \{0,1\}^*$, $w \mapsto w$. (total und berechenbar).
Sei $w = \langle (x_1, y_1), \dots, (x_k, y_k) \rangle$. Dann gilt:

$w \in$ PCP $\implies$ es existiert Lösung $i_1, \dots, i_n$ $\implies$ $i_1, \dots, i_n, i_1, \dots, i_n$ ist auch eine Lösung, in der jeder Index in gerader Anzahl vorkommt $\implies$ $w \in P_{\text{even}}$

$w \in P_{\text{even}} \implies w \in$ PCP klar

Aufgabe 3. *Dichte von Sprachen* 9 P.

Die *Dichte* einer Sprache $L \subseteq \{0, 1\}^*$ sei definiert durch

$$\rho(L) := \lim_{n \to \infty} \frac{|L \cap \{0, 1\}^n|}{2^n},$$

falls dieser Grenzwert existiert. Falls er nicht existiert, ist die Dichte von L undefiniert.

Für jede reelle Zahl $x \in [0, 1]$ existiert bekanntlich eine eindeutige Folge $(x_k)_{k \in \mathbb{N}}$ mit $x_k \in \{0, 1\}$ für alle $k \in \mathbb{N}$, sodass:

- $\displaystyle\sum_{k=0}^{\infty} x_k \cdot 2^{-k} = x$ und
- $x_k = 0$ für unendliche viele $k \in \mathbb{N}$.

Diese Folge ist die *Binärentwicklung* von x. Definiere die Funktion $f_x\colon \mathbb{N} \to \{0, 1\}$ durch $f_x(k) := x_k$. Die Funktion f_x gibt bei Eingabe k also die k-te Stelle der Binärentwicklung von x aus. Wir nennen die Zahl x *berechenbar*, falls f_x berechenbar ist.

Beweisen Sie die folgenden Aussagen:

(a) Es gibt eine entscheidbare Sprache $L \subseteq \{0, 1\}^*$, deren Dichte undefiniert ist.

(b) Es gibt eine entscheidbare Sprache $L \subseteq \{0, 1\}^*$ mit $\rho(L) = \frac{1}{2}$.

(c) Es gibt eine unberechenbare Zahl $x \in [0,1]$.

(d) Falls $x \in [0,1]$ berechenbar ist, dann existiert eine entscheidbare Sprache $L \subseteq \{0,1\}^*$ mit $\rho(L) = x$. (*Tipp*: L enthält für jedes $n \in \mathbb{N}$ einen Anteil von $\sum_{k=0}^{n} x_k \cdot 2^{-k}$ aller Wörter der Länge n.)

Lösung:

(a) Sei $L = \{w \in \{0,1\}^{2n} \mid n \in \mathbb{N}\}$. Dann ist L klar entscheidbar, da eine TM nur überprüfen muss, ob das Eingabewort gerade Länge hat. Es gilt

$$\frac{|L \cap \{0,1\}^n|}{2^n} = \begin{cases} 1, & \text{falls } n \text{ gerade} \\ 0, & \text{sonst} \end{cases},$$

und somit ist die Dichte von L undefiniert.

(b) Die Sprache $L = \{1x \mid x \in \{0,1\}^*\}$ ist klar entscheidbar und es gilt

$$\frac{|L \cap \{0,1\}^n|}{2^n} = 1/2$$

für alle $n \geq 1$. Somit gilt $\rho(L) = 1/2$.

(c) $[0,1]$ ist überabzählbar, es kann aber nur abzählbar viele berechenbare Zahlen geben.

(d) Definiere L wie folgt. Für jedes $n \in \mathbb{N}$ sei $a_n := \sum_{k=0}^{n} x_k \cdot 2^{n-k}$ und L_n enthalte die ersten a_n Wörter der Länge n nach der lexikographischen Ordnung. Sei $L := \bigcup_{n=0}^{\infty} L_n$. Es gilt:

$$\frac{|L \cap \{0,1\}^n|}{2^n} = \frac{a_n}{2^n} = \sum_{k=0}^{n} x_k \cdot 2^{-k}$$

und folglich

$$\rho(L) = \lim_{n \to \infty} \sum_{k=0}^{n} x_k \cdot 2^{-k} = x.$$

Ferner ist L entscheidbar: Ein Algorithmus berechnet auf Eingabe w der Länge n zunächst die Werte $x_0, \ldots, x_n$. (Das ist aufgrund der Berechenbarkeit von x möglich.) Mit diesen Werten kann a_n berechnet werden und dann kann überprüft werden ob w eines der ersten a_n Wörter der Länge n nach der lexikographischen Ordnung ist.