Prof. Dr. M. Grohe

E. Fluck, A. Riazsadri, J. Feith

Übungsblatt 3 mit Lösungen

Abgabetermin: Mittwoch, der 9. November 2022 um 14:30

Aufgabe 4 (Abzählbare Vereinigung) **3 Punkte**

Sei

$$\mathbb{N}^* = \bigcup_{k \in \mathbb{N}} \mathbb{N}^k$$

die Menge der endlichen Tupel über $\mathbb{N}$. Zeigen Sie, dass $\mathbb{N}^*$ abzählbar ist.

Hinweis: Beachten Sie, dass $\mathbb{N}^0$ das leere Tupel $()$ enthält.

Lösung:

Sei $\Sigma = \{0, 1, \#\}$. Die Menge Σ^* ist bekanntermaßen abzählbar, d.h. es existiert eine Surjektion $f\colon \mathbb{N} \to \Sigma^*$; konkret etwa die lexikographische Aufzählung (bzgl. einer Ordnung $0 < 1 < \#$) mit $f(0) = \varepsilon$, $f(1) = 0$, $f(2) = 1$, $f(9) = 1\#$, etc. Wir konstruieren nun eine weitere Abbildung $g\colon \Sigma^* \to \mathbb{N}^*$ mit

$$g(w) = \begin{cases} (k_1, \dots, k_n) & \text{falls } w = \operatorname{bin}(k_1)\# \dots \# \operatorname{bin} k_n \\ () & \text{andernfalls.} \end{cases}$$

Aus dieser Definition folgt sofort die Surjektivität von g, womit auch die Komposition $h\colon \mathbb{N} \to \mathbb{N}^*$ mit $h = g \circ f$ (es ist also $h(n) = g(f(n))$) surjektiv ist. Somit ist $\mathbb{N}^*$ abzählbar.

Aufgabe 5 ((Un-)Entscheidbarkeit) **6 (3 + 3) Punkte**

Zeigen oder widerlegen Sie, dass folgende Sprachen entscheidbar sind.

a) $L_1 = \{\langle M\rangle \mid M \text{ akzeptiert genau 42 Wörter}\}$

b) $L_2 = \{\langle M\rangle w \mid M \text{ bewegt auf der Eingabe } w \text{ den Kopf nie nach links}\}$

Lösung:

a) Die Sprache L_1 ist unentscheidbar.

Angenommen, L_1 wäre entscheidbar. Dann existiert eine TM M_1, welche L_1 entscheidet. Wir konstruieren per Unterprogrammtechnik eine TM M_ε, welche das spezielle Halteproblem H_ε entscheiden soll.

Die TM M_ε verhält sich wie folgt:

- Zunächst wird geprüft, ob die Eingabe eine valide Gödelnummer ist. Falls nein, so verwirft M_ε sofort.
- Andernfalls hat die Eingabe die Form $\langle M\rangle$, und wir konstruieren eine TM M^* mit den folgenden Eigenschaften:
  - Auf ε simuliert M^* das Verhalten von M auf ε. Falls M hält, so akzeptiert M_ε.
  - Auf den Eingaben $1, 11, \ldots, 1^{41}$ akzeptiert M^*.
  - Alle anderen Eingaben verwirft M^*.
- Nun prüft M_ε mittels dem Unterprogram M_1 ob $\langle M^*\rangle \in L_1$ gilt. Falls ja, so akzeptiert M_ε, andernfalls verwirft M_ε.

Offensichtlich verhält sich M_ε auf Eingaben, welche keine validen Gödelnummern sind, korrekt. Ist die Eingabe hingegen eine Gödelnummer $\langle M\rangle$, so akzeptiert M^* exakt 42 Wörter genau dann, wenn M auf ε hält (andernfalls akzeptiert M_ε nur 41 Wörter). Da M_ε genau dann akzeptiert, wenn $\langle M^*\rangle \in L_1$ gilt, folgern wir, dass M_ε die Eingabe $\langle M\rangle$ genau dann akzeptiert, wenn M auf ε hält.

Somit entscheidet M_ε das spezielle Halteproblem, was aber bekannt unentscheidbar ist. Es folgt, dass L_1 nicht entscheidbar sein kann.

b) Die Sprache L_2 ist entscheidbar.

Sei M eine TM, welche auf einer Eingabe w den Kopf nie nach links bewegt. Folglich sind zwei Konfigurationen $\alpha q\beta$ und $\alpha' q' \beta'$, welche M auf w erreicht, bereits effektiv äquivalent (d.h. sie führen zum selbem Berechnungsergebnis) falls $q = q'$ und $\beta = \beta'$ gilt, da die Bandpositionen links des Kopfes nie wieder gelesen werden können.

Wir bemerken, dass M an jeder Position nach maximal $|\Gamma| \cdot |Q|$ Schritten entweder den Kopf nach rechts bewegt oder eine effektiv äquivalente Konfiguration wiederholt (und befindet sich somit in einer Endlosschleife). Somit erreicht M nach höchstens $|\Gamma| \cdot |Q| \cdot |w|$ Schritten ein Blank rechts der Eingabe, weswegen M nach spätestens $|\Gamma| \cdot |Q| \cdot (|w| + 1)$ Schritten hält – oder nie.

Um L_2 zu entscheiden reicht es daher, M für $|\Gamma| \cdot |Q| \cdot (|w| + 1)$ Schritte auf der Eingabe w zu simulieren; Eingaben mit anderem Format als $\langle M \rangle w$ werden sofort verworfen. Hält M während der Simulation, so wird $\langle M \rangle w$ akzeptiert, andernfalls verworfen.

Aufgabe 6 (Diagonalisierung) **6 (2 + 1 + 3) Punkte**

Zur Erinnerung: Ein *deterministischer endlicher Automat* (DFA) ist ein 5-Tupel

$$A = (Q, \Sigma, q_0, F, \delta).$$

a) Entwerfen Sie eine eindeutige, präfixfreie Kodierung (DFA-Gödelnummer), welche jedem DFA A ein Wort $\langle A \rangle$ über dem Alphabet $\{0,1\}^*$ zuordnet. Sie brauchen nicht zu zeigen, dass ihre Kodierung die gewünschten Eigenschaften besitzt.

b) Folgern Sie, dass die Menge $\{\langle A \rangle \mid A \text{ ist ein DFA über } \{0,1\}\}$ abzählbar ist.

c) Zeigen Sie mittels Diagonalisierung, dass die Sprache

$$L = \{\langle A \rangle \mid A \text{ ist ein DFA und } \langle A \rangle \notin L(A)\}$$

nicht regulär ist.

Hinweis: Die Definitionen von DFAs und regulären Sprachen finden Sie in den zur Verfügung gestellten Materialien der Vorlesung "Formale Systeme, Automaten, Prozesse".

Lösung:

a) Wir nutzen eine Abwandlung der Gödelnummern für Turingmaschinen. Zu beachten ist, dass wir die Menge der Endzustände zusätzlich kodieren müssen.

Sei also $A = (Q, \{0,1\}, q_1, F, \delta)$ ein DFA über dem Alphabet $\{0,1\}$ und Anfangszustand q_1. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass $Q = \{q_1, \dots, q_k\}$ durchnummeriert sind, wobei die Endzustandsmenge $F = \{q_{f_1}, \dots, q_{f_\ell}\}$ für geeignete Indizees $f_1, \dots, f_\ell \in \{1, \dots, k\}$ ist. Nun kodieren wir einen Übergang $\delta(q_i, \sigma) = q_j$ für ein $\sigma \in \{0,1\}$ mit dem Wort $0^i 1 0^{1+\sigma} 1 0^j$ und bezeichnen mit $\text{code}(t)$ die Kodierung des t-ten Übergangs. Die Übergangskodierungen trennen wir mit 11; die Endzustände, wiederum getrennt durch 11, kodieren wir wiederum durch eine entsprechende Sequenz von Nullen, wobei die Länge den Index des Zustandes angibt. Die beiden Teile (Transitionen und Endzustände) trennen wir durch 111 und schliesslich umrahmen wir die Kodierung von beiden Seiten durch 1111, un die Präfixfreiheit zu garantieren.

Somit erhalten wir für einen DFA mit s Übergängen die DFA-Gödelnummer

$$\langle A \rangle = 1111 \ \text{code}(1) \ 11 \ \text{code}(2) \ 11 \dots 11 \ \text{code}(s) \ 111 \ 0^{f_1} \ 11 \ 0^{f_2} \ 11 \dots 11 \ 0^{f_\ell} \ 1111.$$

b) Da jede DFA-Gödelnummer eine Binärzahl ist, trifft die Binärkodierung $\text{bin}\colon \mathbb{N} \to \{0,1\}^*$ bereits alle DFA-Gödelnummern. Um eine Surjektion nur in die Menge aller DFA-Gödelnummern zu konstruieren, fixieren wir eine beliebige DFA-Gödelnummer $\langle A_0 \rangle$ als Bild aller natürlichen Zahlen, deren Binärkodierung keine DFA-Gödelnummer ist.

Dadurch erhalten wir die Surjektion $f\colon \mathbb{N} \to \{\langle A\rangle \mid A \text{ ist ein DFA}\}$ mit

$$f(n) = \begin{cases} \mathrm{bin}(n) & \text{falls } \mathrm{bin}(n) \text{ eine DFA-Gödelnummer ist} \\ \langle A_0\rangle & \text{andernfalls.} \end{cases}$$

Daher ist die Menge der DFA-Gödelnummern abzählbar.

c) Angenommen, L wäre regulär. Dann existiert ein DFA A_L, welcher L entscheidet.

Wir betrachten nun zwei Fälle:

a) Es ist $\langle A_L\rangle \in L$. Dann gilt nach Definition von L auch $\langle A_L\rangle \notin L(A_L)$. Da aber $L = L(A_L)$ gilt, folgt $\langle A_L\rangle \notin L$ und somit ein Widerspruch.

b) Es ist $\langle A_L\rangle \notin L$. Dann gilt nach Definition von L also $\langle A_L\rangle \in L(A_L)$. Da aber $L = L(A_L)$ gilt, folgt $\langle A_L\rangle \in L$ und somit ein Widerspruch.

Beide möglichen Fälle führen also zu einem Widerspruch (zu der Existenz von A_L). Somit ist L nicht regulär.