Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann

Hausübungen zur Vorlesung

Diskrete Mathematik 2
Einführung in die theoretische Informatik

Sommersemester 2014

Blatt 1 / 22./23. April 2014

Abgabe: 22. April 2014, bis 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

Geben Sie deterministische Turing-Maschinen M_i an, die die folgenden Sprachen über dem Eingabealphabet $\Sigma = \{0, 1\}$ entscheiden:

(a) $L = \{x \in \{0,1\}^* \mid x = 1(10)^n 1,\ n \geq 0\}$
(d. h. x beginnt und endet mit einer 1 und enthält in der Mitte beliebig häufig das Wort 10.)

(b) $L = \{x \in \{0,1\}^* \mid x = (01)^m (10)^n,\ m \geq 0,\ n \geq 0\}$
(d. h. x beginnt mit m mal dem Wort 01, gefolgt von n mal dem Wort 10.)

Wählen Sie jeweils geeignete Bandalphabete und Zustandsmengen. Geben Sie auch bitte kurz an, welche Bedeutung die Zustände aus der Zustandsmenge jeweils haben (z. B. „suche ganz rechts stehende 1“).

AUFGABE 2 (5 Punkte)**:**

Sei für $w = w_1 \dots w_t \in \{0,1\}^t$ für $t \geq 0$ die *Spiegelung von w* als $w^S = w_t \dots w_1$ definiert (die Bitreihenfolge wird gedreht). Eine „Spiegelzahl“ sei ein Binärstring der Form ww^S für ein $w \in \{0,1\}^*$. Die Sprache $\textsc{Spiegel} = \{x \in \{0,1\}^* \mid x = ww^S\}$ ist die Menge aller Spiegelzahlen. D. h. beispielsweise $\epsilon, 1001, 011110 \in \textsc{Spiegel}$, aber $0001, 101 \notin \textsc{Spiegel}$.

Zeigen Sie: $\textsc{Spiegel} \in \mathcal{P}$.

Hinweis: Sie sollten zur Lösung dieser Aufgabe eine DTM angeben, welche Spiegel entscheidet und deren Laufzeit analysieren.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Seien $L_1, L_2 \subset \Sigma^*$ Sprachen. Zeigen Sie:

(a) Sind L_1 und L_2 entscheidbar, so ist auch $L_1 \cup L_2$ entscheidbar.

(b) Sind L_1 und L_2 rekursiv aufzählbar, so ist auch $L_1 \cup L_2$ rekursiv aufzählbar.

Hinweis: Geben Sie jeweils einen Algorithmus in Pseudocode an, der $L_1 \cup L_2$ entscheidet bzw. akzeptiert.

AUFGABE 4 (5 Punkte)**:**

Eine natürliche Zahl $x \geq 0$ heiße 3-*Quadrat*, wenn sich x als Summe dreier Quadratzahlen darstellen lässt, also als $x = a^2 + b^2 + c^2$ mit $a, b, c \in \mathbb{N}_{\geq 0}$. Betrachten Sie die Sprache

$$\text{3-}\textsc{Quadrat} = \{x \mid x \text{ ist ein 3-}\textit{Quadrat.}\}.$$

Zeigen Sie durch Angabe eines polynomiellen Verifizierers in Pseudocode, dass 3-Quadrat $\in \mathcal{NP}$. Weisen Sie nach, dass Ihr Verifizierer die für einen Verifizierer erforderlichen Eigenschaften besitzt.