Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 1 / 03. April 2012

Abgabe: 17. April 2012, 9 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

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

(a) $L_1 = \{x \in \{0,1\}^* \mid x = w11w'\}$ (d.h. x enthält 2 unmittelbar aufeinanderfolgende 1en)

(b) $L_2 = \{x \in \{0,1\}^* \mid x = (01)^n(10)^m, n \geq 0, m \geq 0\}$.

Wählen Sie dazu jeweils geeignete Bandalphabete und Zustandsmengen. Um kurz zu erläutern, wie Ihre DTM funktioniert, geben Sie bitte an, welche Bedeutung die Zustände aus der Zustandsmenge jeweils haben (z.B. „suche linkeste 1“).
Schätzen Sie weiterhin die Zeitkomplexität $T_{M_i}(n)$ bei Eingabe der Länge $\leq n$ der von Ihnen angegebenen Turing-Maschinen sinnvoll nach oben ab.

AUFGABE 2 (5 Punkte)**:**

Sei für $w = w_1 \dots w_t \in \{0,1\}^t$ 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 $w \in \{0,1\}^*$. Gegeben ist die Sprache $\textsc{Spiegel} = \{x \in \{0,1\}^* \mid x = ww^S\}$ aller Spiegelzahlen. D.h. z.B. sind $\epsilon, 1001, 011110 \in \textsc{Spiegel}$, aber $0001, 101 \notin \textsc{Spiegel}$. Zeigen Sie: $\textsc{Spiegel} \in \mathcal{P}$.

Hinweis: Sie sollten zur Lösung dieser Aufgabe einen Algorithmus angeben und dessen Laufzeit analysieren. Es ist Ihnen überlassen, ob Sie dazu DTMs oder geeigneten Pseudocode verwenden.

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 $L_1 \cup L_2$ 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 $x = a^2 + b^2 + c^2$ als Summe 3er Quadratzahlen darstellen lässt mit $a, b, c \in \mathbb{N}_{\geq 0}$. Betrachten Sie die Sprache

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

Zeigen Sie durch Angabe eines polynomiellen Verifizierers, dass 3-Quadrat $\in \mathcal{NP}$.