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

Präsenzübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 1 / 10./11. April 2012

AUFGABE 1:

Betrachten Sie die deterministische Turing-Maschine M mit Zustandsmenge $Q = \{q_0, q_1, q_a, q_r\}$, Startzustand $s = q_0$, Eingabealphabet $\Sigma = \{0, 1\}$, Bandalphabet $\Gamma = \{0, 1, \sqcup, \rhd\}$ und der folgenden Übergangsfunktion δ:

δ	0	1	$\rhd$	$\sqcup$
q_0	$(q_0, 0, R)$	$(q_0, 1, R)$	$(q_0, \rhd, R)$	$(q_1, \sqcup, L)$
q_1	$(q_a, 0, L)$	$(q_r, 1, R)$	$(q_0, \rhd, R)$	$(q_r, \sqcup, L)$

(a) Geben Sie die aufeinanderfolgenden Konfigurationen der DTM M jeweils bei Eingabe $w = 01$ und bei Eingabe $w = 110$ an.

(b) Was ist die von der DTM M akzeptierte Sprache L? Entscheidet M die Sprache $L = L(M)$?

(c) Ist L rekursiv aufzählbar? Ist L entscheidbar?

AUFGABE 2:

Geben Sie deterministische Turing-Maschinen an, die die folgenden Sprachen über dem Eingabealphabet $\Sigma = \{0, 1\}$ entscheiden. Schätzen Sie weiterhin die Zeitkomplexität $T_{M_i}(n)$ bei Eingaben der Länge $\leq n$ der von Ihnen angegebenen Turing-Maschinen nach oben ab. Gilt $L_1 \in \mathcal{P}$? Gilt $L_2 \in \mathcal{P}$?

(a) $L_1 = \{x \in \{0, 1\}^* \mid x \text{ enthält mindestens zwei Einsen}\}$

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

AUFGABE 3:

Sei $\text{POTENZ} = \{m \in \mathbb{N} \mid m = a^t,\ \text{für } a, t \in \mathbb{N}, a \geq 2, t \geq 2\}$.

Zeigen Sie $\text{POTENZ} \in \mathcal{NP}$ durch Angabe eines *polynomiellen Verifizierers.*

Anmerkung: Sie wissen aus der Vorlesung, dass jede RAM mit Laufzeit $\mathcal{O}(t(n))$ durch eine DTM in Laufzeit $\mathcal{O}(t(n)^3)$ simuliert werden kann. Es genügt also eine RAM (in Pseudocode) anzugeben und zu zeigen, dass die Laufzeit der RAM polynomiell in der Eingabelänge ist. Messen Sie die Laufzeit Ihrer RAM in durchgeführten Bitoperationen. Benutzen Sie, dass die Addition und Subtraktion von zwei Zahlen $a, b \in \mathbb{N}$ auf Ihrer RAM in Laufzeit $\mathcal{O}(\log(\max\{a, b\}))$, der Vergleich der beiden Zahlen in Zeit $\mathcal{O}(\log(\min\{a, b\}))$ und die Multiplikation der Zahlen in Zeit $\mathcal{O}(\log(a) \cdot \log(b))$ durchgeführt werden kann.

AUFGABE 4:

Zeigen Sie, dass für jede Sprache $L \subset \Sigma^*$ die folgenden beiden Aussagen äquivalent sind:

(1) L ist entscheidbar.

(2) Sowohl L als auch $\bar{L} = \Sigma^* \setminus L$ sind rekursiv aufzählbar.