RUHR-UNIVERSITÄT BOCHUM
LEHRSTUHL FÜR KRYPTOLOGIE UND IT-SICHERHEIT
Prof. Dr. Alexander May
Stefan Hoffmann

Präsenzübungen zur Vorlesung

Diskrete Mathematik 2
Einführung in die theoretische Informatik

Sommersemester 2014

Blatt 1 / 15./16. April 2014

AUFGABE 1:

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) $L_2 = \{x \in \{0, 1\}^* \mid x = (101)^n, n \geq 0\}$

AUFGABE 2:

Gegeben ist die Sprache $\textsc{Hamming}_3 = \{x \in \{0, 1\}^* \mid \mathsf{wt}(x) = 3\}$. Die Funktion $\mathsf{wt}(x)$ beschreibt die Anzahl der Einsen in x, das sogenannte Hamming-Gewicht.

Zeigen Sie, dass $\textsc{Hamming}_3 \in \mathcal{P}$. Geben Sie dazu eine DTM M an, die $\textsc{Hamming}_3$ entscheidet und analysieren Sie die Laufzeit von M.

Bitte wenden!

AUFGABE 3:

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

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

Anmerkung: Jede RAM kann mit Laufzeit $\mathcal{O}(t(n))$ durch eine DTM in Laufzeit $\mathcal{O}(t(n)^3)$ simuliert werden. 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.