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 2 / 6./7. Mai 2014

Abgabe: 6. Mai 2014, 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

Betrachten Sie folgende *nicht*-deterministische Turingmaschine N mit Zustandsmenge $Q = \{q_0, q_1, q_2, q_a, q_r\}$, 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	$\{(q_0, 0, R), (q_1, 0, R)\}$	$\{(q_0, 1, R)\}$	$\{(q_0, \rhd, R)\}$	$\{(q_r, \sqcup, L)\}$
q_1	$\{(q_2, 0, R)\}$	$\{(q_r, 1, R)\}$	$\{(q_r, \rhd, R)\}$	$\{(q_r, \sqcup, L)\}$
q_2	$\{(q_r, 0, R)\}$	$\{(q_a, 1, R)\}$	$\{(q_r, \rhd, R)\}$	$\{(q_r, \sqcup, L)\}$

(a) Zeichnen Sie den Baum der möglichen Berechnungspfade der NTM bei Eingabe 10010. Akzeptiert N die Eingabe 10010? Was ist die maximale Anzahl Rechenschritte $T_N(10010)$ von N auf 10010?

(b) Geben Sie eine möglichst einfache Beschreibung der von N akzeptierten Sprache an. Gibt es eine DTM, welche diese Sprache entscheidet? Bitte begründen Sie ihre Aussage.

AUFGABE 2:

Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $U \subseteq V$ heißt *unabhängig*, falls keine zwei Knoten $i, j \in U$ durch eine Kante $\{i, j\} \in E$ verbunden sind. Es gilt also für alle Knoten $i, j \in U$, dass $\{i, j\} \notin E$. Sei

Independent $:= \{(G, k) | G = (V, E)$ besitzt eine *unabhängige* Menge $U \subseteq V$ mit $|U| \geq k\}$.

Zeigen Sie Independent $\in \mathcal{NP}$ durch Angabe einer NTM.

Bitte wenden!

AUFGABE 3:

Sei $M = \{m_1, \ldots, m_n\} \subset \mathbb{N}$, $t \in \mathbb{N}$ und $S \in \{0,1\}^n$ mit $S = s_1 s_2 \ldots s_n$ und $s_i \in \{0,1\}$.

Wir definieren die Sprache

$$\textsc{SubsetSum} := \{(M,t) |\text{ es existiert ein } S \text{ mit } \sum_{i=1}^{n} s_i m_i = t\}.$$

Zeigen Sie SubsetSum $\in \mathcal{NP}$ durch Angabe eines polynomiellen Verifizierers.

AUFGABE 4:

Betrachten Sie die Definitionen von Clique (Präsenzübung 2, Aufgabe 2) und Independent (Aufgabe 2 dieses Blatts).

Zeigen Sie Independent $\leq_p$ Clique.