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 3 / 13./14. Mai 2014

AUFGABE 1:

Sei $M = \{m_1, \ldots, m_n\} \subset \mathbb{N}$, $t \in \mathbb{N}$, $S \in \{0,1\}^n$ mit $S = s_1 s_2 \ldots s_3$ und $s_i \in \{0,1\}$. Es gilt $\overline{s_i} = s_i + 1 \mod 2$. Wir betrachten die Sprache SubsetSum (Hausübung 2, Aufgabe 3) und definieren die Sprache

$$\textsc{Teilung} := \{M \mid \text{ es existiert ein } S \text{ mit } \sum_{i=1}^{n} s_i m_i = \sum_{i=1}^{n} \overline{s_i} m_i\}$$

Zeigen Sie, dass Teilung $\leq_p$ SubsetSum.

AUFGABE 2:

Betrachten Sie die Sprache

$$\textsc{Half-Clique} := \{G \mid G = (V,E),\ |V| \text{ ist gerade und } G \text{ besitzt eine } \frac{|V|}{2}\text{-Clique.}\}$$

Zeigen Sie, dass Half-Clique $\mathcal{NP}$-vollständig ist, d. h. zeigen Sie zunächst:

(a) Half-Clique $\in \mathcal{NP}$.

(b) Clique $\leq_p$ Half-Clique.

Benutzen Sie dann, dass Clique $\mathcal{NP}$-vollständig ist.

Bitte wenden!

AUFGABE 3:

Wir betrachten die Sprachen

$$\text{SAT} := \{\phi \mid \phi \text{ ist eine Boolesche Formel mit mindestens einer erfüllenden Belegung.}\}$$

und

$$\textsc{DoppelSat} := \{\phi \mid \phi \text{ ist eine Boolesche Formel mit mindestens zwei erfüllenden Belegungen.}\}$$

Es gilt $\textsc{DoppelSat} \in \mathcal{NP}$. Zeigen Sie, dass $\textsc{DoppelSat}$ $\mathcal{NP}$-vollständig ist.

AUFGABE 4:

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

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

Zeigen Sie, dass $\textsc{Independent}$ $\mathcal{NP}$-vollständig ist.