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 3 / 20./21. Mai 2014

Abgabe: 20. Mai 2014, 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

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 $\{i, j\} \notin E$. Betrachten Sie die Sprachen Independent (Hausübung 2) und

$$\textsc{Half-Independent} := \{G \mid G = (V, E), |V| \text{ gerade, hat } \textit{unabhängiges } U \subseteq V \text{ mit } |U| = \frac{|V|}{2}.\}$$

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

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

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

Sie dürfen verwenden, dass Independent $\mathcal{NP}$-vollständig ist.

AUFGABE 2 (5 Punkte)**:**

Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $U \subseteq V$ mit $|U| = k$ heißt *k-Knotenüberdeckung*, falls $e \cap U \neq \emptyset$ für alle $e \in E$. Sei

$$\textsc{Knotenüberdeckung} := \{(G, k) | G \text{ besitzt eine k-Knotenüberdeckung}\}.$$

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

Sie dürfen verwenden, dass 3-Sat $\leq_p$ Knotenüberdeckung gilt (siehe Folie 62) und dass 3-Sat $\mathcal{NP}$-vollständig ist (siehe Folie 59).

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

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

(a) Teilung $\in \mathcal{NP}$.

(b) SubsetSum $\leq_p$ Teilung.

Sie dürfen verwenden, dass SubsetSum $\mathcal{NP}$-vollständig ist (siehe Folie 67).

AUFGABE 4 (5 Punkte)**:**

Sei $M = \{1, \ldots, m\}$ und $F = \{S_1, \ldots, S_n\} \subseteq \mathsf{P}(M)$, d. h. $S_i \subseteq M$. Eine Menge $C \subseteq \{1, \ldots, n\}$ mit $|C| = k$ heißt *k-Mengenüberdeckung* von (M, F), falls

$$\bigcup_{i \in C} S_i = M$$

Wir definieren

$$\textsc{Mengenüberdeckung} := \{(M, F, k) \mid (M, F) \text{ besitzt eine } k\text{-}\textit{Mengenüberdeckung.}\}$$

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

(a) Mengenüberdeckung $\in \mathcal{NP}$.

(b) Knotenüberdeckung $\leq_p$ Mengenüberdeckung.

Sie dürfen verwenden, dass Knotenüberdeckung $\mathcal{NP}$-vollständig ist (siehe Aufgabe 3).