RUHR-UNIVERSITÄT BOCHUM
LEHRSTUHL FÜR KRYPTOLOGIE UND IT-SICHERHEIT
Prof. Dr. Alexander May
Ilya Ozerov

**Hausübungen zur Vorlesung**

# Diskrete Mathematik II

**SS 2012**

Blatt 3 / 08. Mai 2012

Abgabe: 22. Mai 2012, 9 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 $\{i, j\} \notin E$. Sei

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

Betrachten Sie die Sprache

HALF-INDEPENDENT $:= \{G \mid G = (V, E), |V|$ gerade, hat *unabhängiges* $U \subseteq V$ 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.

Benutzen Sie dann, dass INDEPENDENT $\mathcal{NP}$-vollständig ist (siehe Präsenzübung).

Bitte wenden!

**AUFGABE 2** (5 Punkte)**:**

Sei $M = \{m_1, \ldots, m_n\} \subset \mathbb{N}$ und $t \in \mathbb{N}$. Wir definieren die Sprache

$$\textsc{SubsetSum} := \{(M,t) \mid \text{ es existiert ein } S \subseteq \{1,\ldots,n\} \text{ mit } \sum_{i \in S} m_i = t\}$$

und die Sprache

$$\textsc{Teilung} := \{M \mid \text{ es existiert ein } S \subseteq \{1,\ldots,n\} \text{ mit } \sum_{i \in S} m_i = \sum_{i \in \{1,\ldots,n\} \setminus S} m_i\}$$

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

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

(b) SubsetSum $\leq_p$ Teilung.

Benutzen Sie dann, dass SubsetSum $\mathcal{NP}$-vollständig ist (siehe Vorlesung).

**AUFGABE 3** (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

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

**Zeigen Sie**, dass Knotenüberdeckung $\mathcal{NP}$-vollständig ist. Zeigen Sie dazu zunächst, dass Knotenüberdeckung $\in \mathcal{NP}$.

In der Vorlesung wurde bereits 3-SAT $\leq_p$ Knotenüberdeckung gezeigt. Benutzen Sie schließlich, dass 3-SAT $\mathcal{NP}$-vollständig ist (siehe Vorlesung).

**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.

Benutzen Sie dann, dass Knotenüberdeckung $\mathcal{NP}$-vollständig ist (Aufgabe 3).