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

Präsenzübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 3 / 15./16. Mai 2012

AUFGABE 1:

- 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 $|U| \geq k.\}$.

- Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $U \subseteq V$ mit $|U| = k$ heißt *Clique* der Größe k (oder auch k-*Clique*), wenn für alle $i, j \in U$ mit $i \neq j$ gilt $\{i, j\} \in E$, d.h. zwischen allen Knoten aus U gibt es Kanten. Sei

  CLIQUE := $\{(G, k) \mid G$ besitzt eine *Clique* der Größe mindestens $k.\}$

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

(a) INDEPENDENT $\in \mathcal{NP}$. [Bereits in Hausaufgabe 2, Aufgabe 1 gezeigt.]

(b) CLIQUE $\leq_p$ INDEPENDENT. [Noch zu zeigen.]

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

AUFGABE 2:

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 $\textsc{Teilung} \leq_p \textsc{SubsetSum}$.

AUFGABE 3:

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

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

(b) $\textsc{Clique} \leq_p \textsc{Half-Clique}$.

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

Für die Hausaufgabe:

- 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

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

- 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

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

- 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

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