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

Präsenzübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 2 / 24./25. April 2012

AUFGABE 1:

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

$$\textsc{Clique} := \{(G, k) \mid G \text{ besitzt eine } \textit{Clique} \text{ der Größe mindestens } k.\}$$

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

AUFGABE 2:

Ein ungerichteter Graph $H = (W, F)$, $W = \{1, \dots, n\}$ heißt *Teilgraph* eines ungerichteten Graphen $G = (V, E)$, wenn es paarweise verschiedene Knoten $\{v_1, \dots, v_n\} \subseteq V$ gibt, so dass für alle $1 \leq i < j \leq n$

$$\{i, j\} \in F \Rightarrow \{v_i, v_j\} \in E$$

gilt. Sei

$$\textsc{Teilgraph} := \{(H, G) \mid H \text{ ist } \textit{Teilgraph} \text{ von } G.\}$$

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

AUFGABE 3:

Zeigen Sie $\textsc{Clique} \leq_p \textsc{Teilgraph}$. Geben Sie dazu eine Funktion f in Pseudocode an. Zeigen Sie dann (wie in jeder Reduktion):

(i) $(G,k) \in \textsc{Clique} \;\Rightarrow\; (H',G') = f((G,k)) \in \textsc{Teilgraph}$

(ii) $(G,k) \notin \textsc{Clique} \;\Rightarrow\; (H',G') = f((G,k)) \notin \textsc{Teilgraph}$
oder alternativ
$(H',G') = f((G,k)) \in \textsc{Teilgraph} \;\Rightarrow\; (G,k) \in \textsc{Clique}$

(iii) Die Funktion f ist in Zeit polynomiell in der Eingabelänge berechenbar.

AUFGABE 4:

Es gilt

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

Sei

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

Es gilt z.B. für $\phi_1 = \neg(x_1 \vee x_2) \wedge x_3$, dass $\phi_1 \in \text{SAT}$, aber $\phi_1 \notin \textsc{Doppel}\text{SAT}$, da $(x_1, x_2, x_3) = (0,0,1)$ die einzige erfüllende Belegung ist. Es gilt allerdings für $\phi_2 = (x_1 \vee x_2) \wedge \neg x_3$ sowohl $\phi_2 \in \text{SAT}$ als auch $\phi_2 \in \textsc{Doppel}\text{SAT}$, da z.B. $(x_1, x_2, x_3) = (0,1,0)$ und $(x_1, x_2, x_3) = (1,1,0)$ verschiedene erfüllende Belegungen sind.

Zeigen Sie $\text{SAT} \leq_p \textsc{Doppel}\text{SAT}$.