Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

**Hausübungen zur Vorlesung**

# Diskrete Mathematik II

**SS 2011**

Blatt 2 / 12. April 2011 / Abgabe **bis spätestens 26.April, 09:00 Uhr in den Übungskästen**

## AUFGABE 1:

Sei $G = (V, E)$ ein (ungerichteter, schleifenfreier) 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. die zwischen allen Knoten aus $U$ gibt es Kanten.

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

Zeigen sie:

(a) Zeigen Sie, $\textsc{Clique} \in \mathcal{NP}$, indem Sie einen polynomiellen Verfizierer angeben. [3P]

(b) Zeigen Sie: Falls $\textsc{Clique} \in \mathcal{P}$, so gibt es auch einen Algorithmus, der zu einem gegebenen Graphen $G = (V, E)$ in Zeit polynomiell in $|V| + |E|$ eine größte Clique in $G$ findet. [5P]

Bemerkung zu (b): Falls es mehrere größte Cliquen in $G$ geben sollte, soll der Algorithmus irgendeine beliebige davon ausgeben.

## AUFGABE 2:

Eine natürliche Zahl $x \geq 0$ heiße 3-*Quadrat*, wenn sich $x = a^2 + b^2 + c^2$ als Summe 3er Quadratzahlen darstellen lässt mit $a, b, c \in \mathbb{N}_{\geq 0}$. Betrachten Sie die Sprache

$$\text{3-}\textsc{Quadrat} = \{x \mid x \text{ is 3-Quadrat.}\}.$$

Zeigen Sie durch Angabe einer NTM[1], dass 3-$\textsc{Quadrat} \in \mathcal{NP}$.[3P]

Bitte wenden!

[1]Sie müssen keine formale NTM mit Übergangsfunktion angeben. Es genügt ein Computerprogramm, in dem „Rate nichtdeterministisch ein $i \in \{1, \ldots, n\}$“ eine zulässige Operation ist.

**AUFGABE 3:**

Seien $L_1, L_2 \subset \Sigma^*$ Sprachen. Zeigen Sie:

(a) Gilt $L_1 \in \mathcal{P}$ und $L_2 \in \mathcal{P}$, so ist auch $L_1 \cup L_2 \in \mathcal{P}$.[3P]

(b) Gilt $L_1 \in \mathcal{NP}$ und $L_2 \in \mathcal{NP}$, so ist auch $L_1 \cup L_2 \in \mathcal{NP}$.[4P]

**AUFGABE 4:**

Betrachten Sie die *nicht*deterministische Turing-Maschine $M$ mit Zustandmenge $Q = \{q_0, q_1, q_{\text{accept}}, q_{\text{reject}}\}$, Startzustand $s = q_0$, Eingabealphabet $\Sigma = \{0, 1\}$, Bandalphabet $\Gamma = \{0, 1, \sqcup, \triangleright\}$ und der folgenden Übergangsfunktion $\delta$:

| $\delta$ | $0$ | $1$ | $\triangleright$ | $\sqcup$ |
|---|---|---|---|---|
| $q_0$ | $\{(q_0, 0, R)\}$ | $\{(q_0, 1, R), (q_1, \sqcup, L)\}$ | $\{(q_0, \triangleright, R)\}$ | $\{(q_{\text{reject}}, \sqcup, R)\}$ |
| $q_1$ | $\{(q_1, 0, L), (q_0, 1, r)\}$ | $\{(q_{\text{accept}}, 1, R)\}$ | $\{(q_{\text{reject}}, \triangleright, R)\}$ | $\{(q_{\text{reject}}, \sqcup, L)\}$ |

(a) Zeichnen Sie den Baum der möglichen Berechnungspfade der NTM bei Eingabe 101. Akzeptiert M die Eingabe 101? [2P]

(b) Geben Sie eine möglichst einfache Beschreibung der von $M$ akzeptierten Sprache an. Die Richtigkeit der Aussage ist zu beweisen. [2P]

Bemerkung zu Teil b: Sie dürfen (ohne Beweis) als gegeben voraussetzen, dass $M$ bei jeder Eingabe und jedem Berechnungspfad nach endlich vielen Schritten anhält.