

Übung zur Vorlesung Kryptokomplexität II

Bearbeitungszeit: 18. Juni bis 28. Juni
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1: Quadratische Reste und DLOGBIT

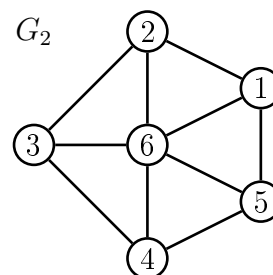
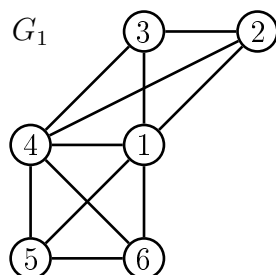
- (a) ► Bestimmen Sie alle Elemente in $\mathbb{Z}_{18}^*$, die quadratische Reste modulo 18 sind.
- (b) ► Bestimmen Sie $\text{DLOGBIT}(\langle 23, 5, 9, 1 \rangle)$ und $\text{DLOGBIT}(\langle 37, 8, 5, 1 \rangle)$. Überprüfen Sie dabei die Gültigkeit der betrachteten Instanzen.

Aufgabe 2: Uncolorability und Komplementklassen

- (a) Betrachten Sie folgendes Problem:

MINIMAL-3-UNCOLORABILITY	
<i>Gegeben:</i>	Ein ungerichteter Graph G .
<i>Frage:</i>	Ist es wahr, dass G nicht legal 3-färbbar ist, aber durch das Entfernen eines beliebigen Knotens (und seiner inzidenten Kanten) entsteht ein legal 3-färbbarer Graph?

- Sind die folgenden Graphen JA- oder NEIN-Instanzen von MINIMAL-3-UNCOLORABILITY?



- (b) ► Zeigen Sie, dass wenn für eine Komplexitätsklasse $\mathcal{C}$ die Inklusion $\mathcal{C} \subseteq \text{co}\mathcal{C}$ gilt, dann gilt auch die Gleichheit $\mathcal{C} = \text{co}\mathcal{C}$.

Aufgabe 3: $\text{INDEPENDENTSET} \leq_m^p \text{SETPACKING}$

Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $I \subseteq V$ der Knoten von G heißt *unabhängige Menge* in G , falls für alle Knoten $x, y \in I$ mit $x \neq y$ gilt $\{x, y\} \notin E$. Das entsprechende Entscheidungsproblem INDEPENDENTSET ist wie folgt definiert.

INDEPENDENTSET	
<i>Gegeben:</i>	Ein Graph $G = (V, E)$ und eine natürliche Zahl $k \leq V $.
<i>Frage:</i>	Besitzt G eine unabhängige Menge der Größe mindestens k ?

Weiter ist das Entscheidungsproblem SETPACKING wie folgt definiert.

SETPACKING	
<i>Gegeben:</i>	Eine endliche Menge U , eine Menge $S \subseteq 2^U$ von Teilmengen von U und eine natürliche Zahl $k \leq S $.
<i>Frage:</i>	Gibt es eine Teilmenge $S' \subseteq S$ mit $ S' \geq k$, so dass alle Mengen in S' paarweise disjunkt sind?

- Geben Sie eine polynomialzeit-beschränkte Many-one Reduktion f von INDEPENDENTSET auf SETPACKING an und beweisen Sie die Korrektheit Ihrer Reduktion.

Aufgabe 4: $\text{DIRECTEDHAMILTONCIRCUIT} \leq_m^p \text{HAMILTONCIRCUIT}$

- Geben Sie eine polynomialzeit-beschränkte Many-one Reduktion f von $\text{DIRECTEDHAMILTONCIRCUIT}$ auf HAMILTONCIRCUIT an und beweisen Sie die Korrektheit Ihrer Reduktion.