Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 11

Lösungsvorschläge

Kryptokomplexität II

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

Aufgabe 1: Quadratische Reste und DLOGBIT

(a) ▶ Bestimmen Sie alle Elemente in $\mathbb{Z}_{18}^*$, die quadratische Reste modulo 18 sind.

(b) ▶ Bestimmen Sie DLOGBIT$(\langle 23, 5, 9, 1\rangle)$ und DLOGBIT$(\langle 37, 8, 5, 1\rangle)$. Überprufen Sie dabei die Gültigkeit der betrachteten Instanzen.

Lösungsvorschlag:

(a) Damit ein Element $x \in \mathbb{Z}_{18}^*$ ein quadratischer Rest modulo 18 ist, muss ein $w \in \mathbb{Z}_{18}$ existieren, so dass $x \equiv w^2 \mod n$ gilt.

w	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$w^2 \mod 18$	1	4	9	16	7	0	13	10	9	10	13	0	7	16	9	4	1

Mit $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$ sind 1, 7 und 13 die einzigen quadratischen Reste modulo 18.

(b) Es gilt $\alpha \in \mathrm{QR}_p \iff$ DLOGBIT$(\langle p, \gamma, \alpha, 1\rangle) = 0 \iff \alpha^{\frac{(p-1)}{2}} \equiv 1 \mod p$.

Für $p = 23$, $\gamma = 5$, $\alpha = 9$ gilt: $9^{11} \equiv 1 \mod 23$, also ist DLOGBIT$(\langle 23, 5, 9, 1\rangle) = 0$.

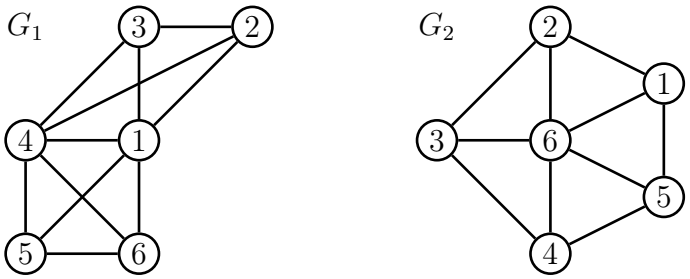
Für $p = 37$, $\gamma = 8$, $\alpha = 5$ gilt: $8^{12} \equiv 1 \mod 37$, also ist γ kein primitives Element und die Instanz nicht gültig.

Aufgabe 2: Uncolorability und Komplementklassen

(a) Betrachten Sie folgendes Problem:

MINIMAL-3-UNCOLORABILITY	
Gegeben:	Ein ungerichteter Graph G.
Frage:	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 $\mathcal{C} = \text{co}\mathcal{C}$.

Lösungsvorschlag:

(a) G_1 ist eine NEIN-Instanz, da etwa durch das Entfernen von Knoten 2 der Graph immer noch nicht 3-färbbar ist.

G_2 ist eine JA-Instanz, da der Graph nicht 3-färbbar ist, aber durch das Entfernen eines beliebigen Knotens 3-färbbar wird.

(b) Wir wissen bereits, dass $\mathcal{C} \subseteq \text{co}\mathcal{C}$ gilt. Um die umgekehrte Inklusion $\text{co}\mathcal{C} \subseteq \mathcal{C}$ zu zeigen, sei L ein beliebiges Problem in co$\mathcal{C}$. Dann ist das Komplement $\overline{L}$ in $\mathcal{C}$ (nach Definition von co$\mathcal{C}$) und somit auch in co$\mathcal{C}$ (wegen $\mathcal{C} \subseteq \text{co}\mathcal{C}$). Nach Definition von co$\mathcal{C}$ ist dann L in $\mathcal{C}$. Somit gilt co$\mathcal{C} \subseteq \mathcal{C}$, also $\mathcal{C} = \text{co}\mathcal{C}$.

Aufgabe 3: INDEPENDENTSET $\leq_m^p$ 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	
Gegeben:	Ein Graph $G = (V, E)$ und eine natürliche Zahl $k \leq \|V\|$.
Frage:	Besitzt G eine unabhängige Menge der Größe mindestens k?

Weiter ist das Entscheidungsproblem SETPACKING wie folgt definiert.

SetPacking	
Gegeben:	Eine endliche Menge U, eine Menge $S \subseteq 2^U$ von Teilmengen von U und eine natürliche Zahl $k \leq \lvert S \rvert$.
Frage:	Gibt es eine Teilmenge $S' \subseteq S$ mit $\lvert S' \rvert \geq k$, 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.

Lösungsvorschlag:

Wir beschreiben zuerst die Funktionsweise der Reduktion f. Sei dazu $I = (G, k)$ eine IndependentSet Instanz mit $G = (V, E)$ und $V = \{v_1, \ldots, v_n\}$. Dann konstruiert f aus I wie folgt eine SetPacking Instanz $I' = (U, S, k')$: Es gilt $U = E$, $k' = k$ und $S = \{S_i \mid v_i \in V\}$ mit

$$S_i = \{e \in E \mid e \cap \{v_i\} \neq \emptyset\}.$$

Offensichtlich kann $f(I)$ in Zeit polynomiell in $\lvert I \rvert$ berechnet werden: Für U und k müssen wir nur Kopieren. Für S konstruieren wir n Mal eine Menge S_i, wobei wir jedes Mal alle $\lvert E \rvert$ Kanten durchlaufen. Damit brauchen wir insgesamt eine Zeit in $\mathcal{O}(\lvert E \rvert + \lvert V \rvert \lvert E \rvert) \subseteq \mathcal{O}(\lvert V \rvert^3) \subseteq \mathcal{O}(\lvert I \rvert^2)$.
Wir argumentieren für jede Richtung der Äquivalenz einzeln:

"⇒" Sei I eine ja-Instanz für IndependentSet. Dann existiert eine unabhängige Menge $W \subseteq V$ in G mit $\lvert W \rvert \geq k$. Füge nun zu S' genau die Mengen S_i aus S hinzu, für die $v_i \in W$ gilt. Offensichtlich gilt dann $\lvert S' \rvert \geq k$. Angenommen es gibt S_i, S_j in S' mit $S_i \cap S_j \neq \emptyset$. Dann existiert eine Kante $\{v_i, v_j\} \in E$. Das ist aber ein Widerspruch dazu, dass $v_i, v_j \in W$ gelten und W eine unabhängige Menge ist. Folglich müssen alle $S_i \in S'$ paarweise disjunkt sein. Damit gilt also, dass $f(I)$ auch eine ja-Instanz für SetPacking ist.

"⇐" Sei $I = (G, k)$ eine IndependentSet Instanz und $f(I) = (U, S, k)$ eine ja-Instanz für SetPacking. Dann existiert eine Menge $S' \subseteq S$ mit $\lvert S' \rvert \geq k$ und alle Elemente S_i in S' sind paarweise disjunkt. Für jedes Element $S_i \in S'$ fügen wir v_i zu W hinzu. Offensichtlich gilt dann $W \subseteq V$ sowie $\lvert W \rvert \geq k$. Für $v_i, v_j \in W$ mit $v_i \neq v_j$ muss $\{v_i, v_j\} \notin E$ gelten, da S_i und S_j paarweise disjunkt sind. Demgemäß ist W eine unabhängige Menge in G und I folglich eine ja-Instanz.

Aufgabe 4: DirectedHamiltonCircuit $\leq_m^p$ HamiltonCircuit

► Geben Sie eine polynomialzeit-beschränkte Many-one Reduktion f von DirectedHamiltonCircuit auf HamiltonCircuit an und beweisen Sie die Korrektheit Ihrer Reduktion.

Lösungsvorschlag:

Wir beschreiben zuerst die Funktionsweise der Reduktion f. Sei dazu $I = G$ eine DHC Instanz mit $G = (V(G), E(G))$. Dann konstruiert f aus I wie folgt eine HC Instanz $I' = G'$: Für jeden Knoten $v \in V(G)$ gibt es drei Knoten in $V(G') : v^{in}, v', v^{out}$. Dabei ist v' jeweils zu den anderen beiden Knoten adjazent, also $\{\{v^{in}, v'\}, \{v^{out}, v'\}\} \in E(G')$. Weiterhin gibt es für jede Kante $(v_i, v_j) \in E(G)$ eine Kante $\{v_i^{out}, v_j^{in}\} \in E(G')$.
Offensichtlich kann $f(I)$ in Zeit polynomiell in $|I|$ berechnet werden.
Wir argumentieren für jede Richtung der Äquivalenz einzeln:

"$\Rightarrow$" Sei I eine JA-Instanz für DHC. Also existiert ein Hamiltonkreis $(v_1, v_2, \ldots, v_n)$ in G. Dann ist $(v_1^{in}, v_1', v_1^{out}, v_2^{in}, v_2', v_2^{out}, \ldots, v_n^{in}, v_n', v_n^{out})$ ein Hamiltonkreis in G'.

"$\Leftarrow$" Sei $I = G$ eine DHC Instanz und $f(I) = G'$ eine JA-Instanz für HC. Es gibt also einen Hamiltonkreis in G'. Da jeder Knoten v_i' nur mit v_i^{out} und v_i^{in} benachbart ist, und da sonst nur Kanten zwischen einem v_i^{out} und einem v_j^{in} existieren, muss der Kreis die Form $(v_1^{in}, v_1', v_1^{out}, v_2^{in}, v_2', v_2^{out}, \ldots, v_n^{in}, v_n', v_n^{out})$ oder $(v_1^{out}, v_1', v_1^{in}, v_2^{out}, v_2', v_2^{in}, \ldots, v_n^{out}, v_n', v_n^{in})$ haben. Da G' ungerichtet ist, ist der anderen Kreis identisch zu dem Kreis $(v_n^{in}, v_n', v_n^{out}, v_{n-1}^{in}, v_{n-1}', v_{n-1}^{out}, \ldots, v_1^{in}, v_1', v_1^{out})$. Aus dem ersten Kreis können wir den Kreis $(v_1, v_2, \ldots, v_n)$ und aus dem anderen den Kreis $(v_n, v_{n-1}, \ldots, v_1)$ in G extrahieren.