Übung zur Vorlesung
Kryptokomplexität 1

Ausgabe: 9. Januar
Besprechung: 24.-26. Januar
Verantwortlich: Roman Zorn

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

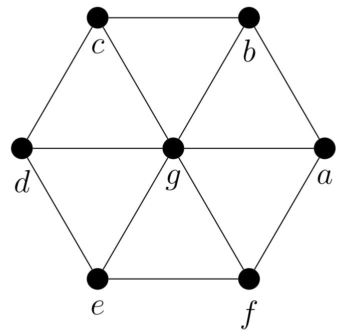
Aufgabe 1 : VertexCover und SetCover

Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $C \subseteq V$ heißt *Knotenüberdeckung* (engl. *vertex cover*) von G, falls für alle Kanten $\{x, y\} \in E$ gilt $\{x, y\} \cap C \neq \emptyset$. Das entsprechende Entscheidungsproblem VertexCover ist wie folgt definiert.

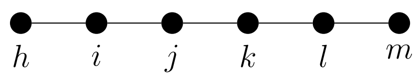
VertexCover	
Gegeben:	Ein Graph $G = (V, E)$ und eine Zahl $k \in \mathbb{N}$.
Frage:	Besitzt G eine Knotenüberdeckung $C \subseteq V$ der Größe höchstens k?

(a) Betrachten Sie die VertexCover-Instanzen

(i) $I = (G, 4)$ mit $G = (V, E)$ wie folgt:



(ii) und $I' = (H, 2)$ mit $H = (V', E')$ wie folgt:



▶ Entscheiden Sie, ob I und I' ja-Instanzen für VertexCover sind und begründen Sie Ihre Antworten.

(b) Sei $I = (G, k)$ eine VertexCover-Instanz mit $G = (V, E)$. Betrachten Sie die folgende SetCover-Instanz (siehe Blatt 11, Aufgabe 4) $I' = (E, \mathcal{S}, k)$ mit

$$\mathcal{S} = \{S_i \mid v_i \in V\} \text{ und } S_i = \{e \in E \mid e \cap \{v_i\} \neq \emptyset\}.$$

► Zeigen Sie: $I \in$ VertexCover *gilt genau dann, wenn* $I' \in$ SetCover.

Aufgabe 2 : Separationen von P, NP und coNP

Sei coNP $= \{\overline{L} \mid L \in \text{NP}\}$ die Menge der Komplemente der Sprachen aus NP.

► Zeigen Sie:

(i) P $\subseteq$ coNP *und*

(ii) falls NP $\neq$ coNP *gilt, so gilt auch* P $\neq$ NP.

Aufgabe 3 : IndependentSet und 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:	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:	Endliche Menge U, eine Menge $S \subseteq 2^U$ von Teilmengen von U und eine natürliche Zahl $k \leq \|S\|$.
Frage:	Gibt es eine Teilmenge $S' \subseteq S$ mit $\|S'\| \geq k$, so dass alle Mengen in S' paarweise disjunkt sind?

(a) ► Entscheiden und begründen Sie, ob folgende Instanzen ja- oder nein-Instanzen für IndependentSet sind.

(i) $I_1 = (G_1, k_1)$ mit $G_1 = (V_1, E_1)$ und $k_1 = 4$ sowie

$$V_1 = \{1, 2, 3, 4, 5, 6\} \text{ und}$$
$$E_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{4, 5\}, \{4, 6\}\},$$

(ii) $I_2 = (G_2, k_2)$ mit $G_2 = (V_2, E_2)$ und $k_2 = 3$ sowie

$$V_2 = \{1,2,3,4,5\} \text{ und}$$
$$E_2 = \{\{1,2\},\{1,4\},\{1,5\},\{2,3\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\}.$$

(b) ▶ Entscheiden und begründen Sie, ob folgende Instanzen JA- oder NEIN-Instanzen für SETPACKING sind.

(i) $I_1 = (U_1, S_1, k_1)$ mit $U_1 = \{1, \ldots, 11\}$,

$$S_1 = \{\{1,7,11\},\{3,6,9\},\{2,5,11\},\{2,4,6,8,10\},\{1,2,5,7\},\{2,5,8\},\{3,4,11\}\}$$

und $k_1 = 3$.

(ii) $I_2 = (U_1, S_1, k_2)$ mit $k_2 = 4$.

(c) ▶ Zeigen Sie, dass SETPACKING $\in$ NP gilt.

(d) ▶ Sei I_1 eine INDEPENDENTSET Instanz. Geben Sie eine bzgl. der Eingabe in polynomieller Zeit berechenbare Funktion f an, so dass $f(I_1)$ eine SETPACKING Instanz ist und

$$I_1 \in \text{INDEPENDENTSET} \iff f(I_1) \in \text{SETPACKING}$$

gilt. Beweisen Sie die obige Äquivalenz und erläutern Sie warum f in polynomieller Zeit berechenbar ist.

(e) ▶ Wenden Sie f auf die Instanzen aus (a) an und entscheiden Sie, ob die Ergebnisse JA- oder NEIN-Instanzen für SETPACKING sind.

Aufgabe 4 : PARTITION und MAXCUT

Die Entscheidungsprobleme PARTITION und WEIGHTED MAXCUT sind wie folgt definiert:

PARTITION	
Gegeben:	Eine Liste $A = (a_1, \ldots, a_n)$ positiver ganzer Zahlen mit $\sum_{i=1}^{n} a_i$ gerade.
Frage:	Kann man A so in zwei disjunkte Listen A_1, A_2 partitionieren, dass $\sum_{a_i \in A_1} a_i = \sum_{a_j \in A_2} a_j$ gilt?

WEIGHTED MAXCUT	
Gegeben:	Ein ungerichteter Graph $G = (V, E)$, eine Gewichtsfunktion $w\colon E \to \mathbb{N}_{\geq 0}$ und eine Schranke $k \in \mathbb{N}_{\geq 0}$.
Frage:	Gibt es eine Partition der Knotenmenge V in zwei disjunkte Teilmengen V_1, V_2, so dass $\sum_{\{u,v\} \in \{\{u,v\} \in E \mid u \in V_1, v \in V_2\}} w(\{u,v\}) \geq k$ gilt?

(a) ► Entscheiden und begründen Sie, ob folgende Instanzen JA- oder NEIN-Instanzen für PARTITION sind:

(i) $I_1 = (14, 5, 2, 6, 5, 8, 13, 7)$ und

(ii) $I_2 = (3, 12, 22, 17, 6)$.

(b) ► Zeigen Sie, dass PARTITION $\in$ NP gilt.

(c) Betrachten Sie die Funktion g, die eine PARTITION Instanz I auf eine WEIGHTED MAXCUT Instanz $g(I)$ wie folgt abbildet. Sei $I = \{a_1, \ldots, a_n\}$ eine PARTITION Instanz. Dann gilt $g(I) = (G, w, k)$ mit $G = (V, E)$, $w\colon E \to \mathbb{N}_{\geq 0}$ und

$$k = \left(\frac{\sum_{i=1}^{n} a_i}{2}\right)^2,$$

wobei $V = \{v_1, \ldots, v_n\}$, $E = V \times V \setminus \{\{v_i, v_i\} \mid 1 \leq i \leq n\}$ und $w(\{v_i, v_j\}) = a_i a_j$ sei.

► Zeigen Sie, dass für eine PARTITION Instanz I gilt

$$I \in \text{PARTITION} \iff g(I) \in \text{WEIGHTED MAXCUT}$$

und argumentieren Sie, weshalb g in Polynomialzeit bzgl. $|I|$ berechenbar ist.

(d) ► Wenden Sie g auf die Instanzen aus (a) an und entscheiden Sie, ob die resultierenden Instanzen JA- oder NEIN-Instanzen für WEIGHTED MAXCUT sind.