

11. Aufgabenblatt

(Besprechung in den Tutorien 15.01.2024–19.01.2024)

Aufgabe 1. Polynomzeitreduktionen und NP

Sei Σ ein endliches Alphabet und bezeichne $A \leq_m^p B$ die Relation „ A ist polynomiell reduzierbar auf B “. Diskutieren Sie die Korrektheit folgender Behauptungen.

- (a) Für alle $A, B, C \subseteq \Sigma^*$ gilt, falls $A \leq_m^p B$ und $A \leq_m^p C$, dann $B \leq_m^p C$.
- (b) Wenn $P = NP$, dann gilt für alle $A \in NP \setminus \{\Sigma^*, \emptyset\}$, dass A NP-schwer ist.
- (c) Für alle $A, B \in NP$ gilt, wenn $A \leq_m^p B$, dann $B \leq_m^p A$.

—————Lösungsskizze—————

- (a) Nein. $A = \emptyset = C$, $B = \text{SAT}$ ist ein Gegenbeispiel.
(Alternative: Sei $A, C \in P \setminus \{\Sigma^*, \emptyset\}$ und B NP-vollständig. Es gilt $A \leq_m^p B$ und $A \leq_m^p C$, aber nicht $B \leq_m^p C$, es sei denn $P = NP$.)
- (b) Ja. Für alle $A \in NP \setminus \{\Sigma^*, \emptyset\}$ gilt die Aussage. Da $A \neq \emptyset$, existiert ein $w_1 \in A$. Da $A \neq \Sigma^*$, existiert ein $w_2 \in \bar{A}$. Sei also $B \in NP$ beliebig. Wir müssen zeigen, dass $B \leq_m^p A$. Da $B \in NP$ und nach Annahme $P = NP$, gilt dann auch $B \in P$. Dann ist f mit $f(x) := w_1$, falls $x \in B$, und $f(x) := w_2$, falls $x \notin B$, eine Polynomzeitreduktion von B auf A .
- (c) Nein, $A = \emptyset$, $B = \text{SAT}$ ist ein Gegenbeispiel.

Aufgabe 2. Polynomzeitreduktionen und Halteproblem

Sei $H = \{w\#x \mid M_w \text{ hält auf Eingabe } x\}$ das allgemeine Halteproblem. Welche der folgenden Aussagen gelten?

1. $H \leq_m^p \text{SAT}$
2. $\text{SAT} \leq_m^p H$
3. H ist NP-schwer
4. H ist NP-vollständig

—————Lösungsskizze—————

1. Nein. H ist nicht reduzierbar auf SAT und folglich auch nicht polynomiell reduzierbar auf SAT, da H unentscheidbar ist, während SAT entscheidbar ist.
2. Ja. Sei M eine DTM, die, gegeben eine Kodierung einer aussagenlogische Formel F , über alle möglichen Variablenbelegungen iteriert (endlich viele) und prüft, ob eine erfüllende Belegung für die Formel F existiert. Falls keine solche Belegung existiert, geht M in eine Endlosschleife. Die Turing-Maschine M hält also genau dann, wenn F erfüllbar ist.

Jede Kodierung $\langle F \rangle$ kann in polynomieller Zeit auf eine Instanz $\langle M \rangle \# \langle F \rangle$ reduziert werden, da $\langle M \rangle$ eine konstante Größe (d.h. unabhängig von der Länge von $\langle F \rangle$) hat. Es gilt:

$$\langle F \rangle \in \text{SAT} \Leftrightarrow F \text{ ist erfüllbar} \Leftrightarrow M \text{ hält auf der Eingabe } \langle F \rangle \Leftrightarrow \langle M \rangle \# \langle F \rangle \in H$$

3. Ja. Es gilt $\text{SAT} \leq_m^p H$ und SAT ist NP-schwer. Folglich ist auch H NP-schwer.
4. Nein. NP ist eine Klasse von entscheidbaren Sprachen. Da H unentscheidbar ist, gilt $H \notin \text{NP}$. Folglich ist H nicht NP-vollständig.

Aufgabe 3. Polynomzeitreduktion I

Betrachten Sie die beiden folgenden Probleme.

VERTEX COVER

Eingabe: Ein ungerichteter Graph $G = (V, E)$ und eine natürliche Zahl k .

Frage: Existiert eine Teilmenge $X \subseteq V$ mit $|X| \leq k$, sodass für jede Kante $\{v, w\} \in E$ einer der beiden Endpunkte in X enthalten ist, d.h. $v \in X$ oder $w \in X$?

STEINERBAUM

Eingabe: Ein ungerichteter Graph $G = (V, E)$, eine Teilmenge von Knoten $T \subseteq V$ und eine natürliche Zahl k .

Frage: Existiert eine Kantenteilmenge $E' \subseteq E$ mit $|E'| \leq k$, sodass im Graph $G' = (V, E')$ alle Knoten in T in derselben Zusammenhangskomponente sind?

Gegeben sei die Funktion f , die für eine VERTEX COVER-Instanz $\langle G = (V, E), k \rangle$ eine STEINERBAUM-Instanz $f(\langle G, k \rangle) = \langle G^* = (V^*, E^*), T^*, |E| + k \rangle$ liefert, die wie folgt definiert ist:

$$\begin{aligned} V^* &:= \{v^* \mid v \in V\} \cup \{e^* \mid e \in E\} \cup \{z\}, \\ E^* &:= \{\{z, v^*\} \mid v \in V\} \cup \{\{e^*, v^*\}, \{e^*, w^*\} \mid e = \{v, w\} \in E\}, \\ T^* &:= \{e^* \mid e \in E\} \cup \{z\}. \end{aligned}$$

Beweisen Sie, dass die gegebene Funktion f eine polynomielle Reduktion von VERTEX COVER auf STEINERBAUM ist.

Lösungsskizze

Die Reduktion kann in $O(|V| + |E| + \log k)$ Schritten berechnet werden (Linearzeit).

Korrektheit:

(\Rightarrow): Sei $X \subseteq V$ ein Vertex Cover der Größe $\leq k$. Wir fixieren für jede Kante $e \in E$ eine Kante $\{e^*, v^*\} \in E^*$ mit $v \in X \cap e$. Sei Y die Menge dieser Kanten. Wir setzen $E' := Y \cup \{\{z, v^*\} \mid v \in X\}$ und behaupten, dass E' eine Lösung der STEINERBAUM-Instanz ist.

Es gilt $|E'| = |Y| + |X| \leq |E| + k$. Von jedem $e^* \in T^* \setminus \{z\}$ kann man z in G' erreichen, indem man die für die Kante e fixierte Kante $\{e^*, v^*\}$ und die Kante $\{v^*, z\}$ wählt. Daher ist E' eine Lösung der STEINERBAUM-Instanz.

(\Leftarrow): Sei E' eine Lösung der STEINERBAUM-Instanz. Dann gibt es für jeden Knoten e^* aus T^* eine inzidente Kante zu einem Knoten v^* (da e^* sonst nicht in der gleichen Zusammenhangskomponente mit z sein kann). Falls nun die Kante $\{v^*, z\}$ nicht in E' enthalten ist, so muss es von mindestens einem weiteren Nachbarn e'^* von v^* einen Pfad zu z geben, der nicht über v^* geht. Wir ersetzen die Kante $\{e'^*, v^*\}$ in E' durch die Kante $\{v^*, z\}$. Dies ändert die Zusammenhangskomponenten von G' nicht, da die Kante $\{e'^*, v^*\}$ in jedem Kantenzug durch den e'^* - z -Pfad und $\{v^*, z\}$ ersetzt werden kann. Durch diese Modifikationen gilt nun, dass $X := \{v \in V : \{v^*, z\} \in E'\}$ ein Vertex Cover für G ist.

Da $|E|$ Kanten aus E' zu Knoten e^* inzident sind, hat der Knoten z in G' höchstens Grad $|E'| - |E| = k$, und somit gilt $|X| \leq k$.