Prof. T. Nipkow
M. Eberl, J. Rädle, S. Wimmer
Technische Universität München
HANDSCHRIFTLICHE ABGABE **4 Punkte**
Abgabefrist: Montag, 15.07.2019, 14 Uhr

Einführung in die theoretische Informatik

Sommersemester 2019 – Hausaufgabenblatt Lösungsskizze 11

Handschriftliche Abgabe

Formale Kriterien zu handschriftlichen Abgaben entnehmen Sie bitte der Website `https://www21.in.tum.de/teaching/theo/SS19`.

AUFGABE 11.1. (*Kurzfragen*)

2 Punkte

(a) Seien A, B Sprachen mit $A \leq_p B$ und B NP-vollständig. Gilt dann A NP-vollständig?

(b) Jedes Problem ist entweder in P oder in NP.

(c) H_0 (das Halteproblem auf leerem Band) ist NP-schwer.

(d) Ist ntime_M für jede nichtdeterministische Turingmaschine M berechenbar?

Lösungsskizze

(a) Nein. Aus $A \leq_p B$ können wir nur folgern, dass $A \in \mathsf{NP}$ ist ("A ist höchstens so schwer wie B" und B ist ja schon in NP). Für NP-Vollständigkeit benötigen wir jedoch auch die NP-Schwere von A, und die kann man aus $A \leq_p B$ nicht folgern.

(b) Nein. Zum Beispiel sind alle nicht berechenbaren Probleme weder in P noch in NP. (Außerdem ist P eine Teilmenge von NP, sodass die Frage sich zu "Sind alle Probleme in NP?" vereinfacht, was offensichtlich falsch ist)

(c) Ja. Wir können jedes Problem $A \in \mathsf{NP}$ (sogar jedes entscheidbare Porblem) in polynomieller Zeit auf H_0 reduzieren: Sei M eine TM, die A entscheidet. Für eine Eingabe w bauen wir nun eine TM $M'(w)$, die folgendes tut:

1. Schreibe w auf das Band
2. Simuliere M
3. Wenn M ja zurückgibt, halten wir. Ansonsten gehen wir in eine Endlosschleife.

Dann hält M' auf leerem Band gdw. $w \in A$ ist. Die (offensichtlich polynomiell berechenbare) Abbildung $w \mapsto \text{enc}(M'(w))$ stellt also eine Reduktion $A \leq_p H_0$ dar.

(d) Nein. Wenn dies der Fall wäre, könnten wir das Halteproblem $\{w \mid M[w]\downarrow\}$ für jede fixe Maschine M entscheiden:

$$M[w]\downarrow \;\longleftrightarrow\; \text{ntime}_M(w) > 0 \vee M[w] \text{ hält nach 0 Schritten}$$

Dies funktioniert, weil (per Definition) $\text{ntime}_M(w) = 0$ ist gdw. entweder M auf w gar nicht hält oder bereits nach 0 Schritten hält.

In der Tat kann man aber *nicht* für jede Maschine das Halteproblem entscheiden, z.B.

- wenn M die universelle Turingmaschine ist (dann ist die Frage, ob M mit Eingabe w hält genau das allgemeine Halteproblem)
- wenn M eine Maschine ist, die das PCP löst (und nicht terminiert, wenn das PCP nicht lösbar ist)

AUFGABE 11.2. (*Abschlusseigenschaften von NP*)

Sei $A \subseteq \Sigma^*$ eine Sprache in NP. Zeigen Sie, dass A^* ebenfalls in NP liegt. Geben Sie hierfür an, wie geeignete polynomiell verifizierbare Zertifikate für A^* aussehen (unter Verwendung entsprechender Zertifikate für A).

0.5 Punkte

0.5P + 1P

Lösungsskizze
Sei $w \in A^*$ mit $|w| = n$. Dann gibt es eine Aufteilung von w in höchstens n nichtleere Wörter $w_1, \ldots, w_k$ mit $w = w_1 \ldots w_k$ und $\forall i.\ w_i \in A$. Somit gibt es für jedes i ein Zertifikat c_i für $w_i \in A$. Das Zertifikat für $w \in A^*$ ist dann die Liste der Paare $(w_1, c_1), \ldots, (w_k, c_k)$ in geeigneter Kodierung (z.B. $w_1 \# c_1 \# \ldots \# w_k \# c_k$.
Hinweis: Die Zerlegung *muss* im Zertifikat stehen. Im Verifikator alle Zerlegungen durchzuprobieren ist nicht möglich, da es hiervon exponentiell viele gibt. Der Verifikator ist offensichtlich wieder polynomiell.

AUFGABE 11.3. (*Tagungsproblem*)
Auf einer Tagung sollen Teilnehmer*innen (gegeben durch die endliche Menge P) an Diskussionsgruppen zu verschiedenen Themen (gegeben durch die endliche Menge T) teilnehmen. Dabei kann jede Person angeben, bei welchen Themen sie auf jeden Fall mitdiskutieren möchte. Diese Einschränkungen drücken wir durch eine Relation $R \subseteq P \times T$ aus. Die Themen sollen nun auf Zeitslots (gegeben durch die endliche Menge Z) verteilt werden. Gegeben eine solche Probleminstanz (P, R, T, Z) wollen wir die Frage stellen, ob es eine Verteilung der Themen auf Zeitslots geben kann, so dass alle Teilnehmer*innen an den von ihnen gewünschten Diskussionsrunden ohne Überschneidungen teilnehmen können. D.h. gibt es eine Funktion $f : T \to Z$ mit

$$\forall p \in P.\ \forall (p, t_1) \in R.\ \forall (p, t_2) \in R.\ f(t_1) = f(t_2) \longrightarrow t_1 = t_2\ ?$$

Wir bezeichnen dieses Problem als TAGUNG.
(a) Zeigen Sie TAGUNG $\in$ NP.
(b) Zeigen Sie mit Hilfe einer Reduktion von 3-COL, dass TAGUNG auch NP-schwer ist.

Lösungsskizze

(a) Ein Zertifikat ist die Zuordnung f. Eine solche Zuordnung können wir als Relation beschreiben, die höchstens $|T| \times |Z|$ viele Paare, also polynomiell viele Elemente enthält. Ein solches Zertifikat kann auch in polynomieller Zeit zertifiziert werden, indem wir zuerst prüfen, dass das Zertifikat eine Funktion beschreibt, und anschließend einmal über R iterieren, um sicherzustellen, dass alle Einschränkungen erfüllt wurden.
(b) Gegeben eine Probleminstanz (V, E), definieren wir die folgende Probleminstanz für TAGUNG:
- $Z = \{1, 2, 3\}$
- $T = V$
- $P = E$
- $R = \{(\{u, v\}, p) \mid p \in \{u, v\} \wedge \{u, v\} \in E\}$

Diese Reduktion bezeichnen wir nun als g. Sie ist offensichtlich in polynomieller Zeit in $|(V, E)|$ berechenbar. Korrektheit: Sei $f : V \to \{1, 2, 3\}$. Dann ist f eine Lösung des Färbbarkeitsproblems (V, E), genau dann wenn f eine Lösung von $g((V, E))$ darstellt:

$$\begin{aligned} & \forall p \in P.\ \forall (p, t_1) \in R.\ \forall (p, t_2) \in R.\ f(t_1) = f(t_2) \longrightarrow t_1 = t_2 \\ \iff & \forall \{u, v\} \in E.\ \forall (\{u, v\}, v_1) \in R.\ \forall (\{u, v\}, v_2) \in R.\ f(v_1) = f(v_2) \longrightarrow v_1 = v_2 \\ \iff & \forall \{u, v\} \in E.\ f(u) = f(v) \longrightarrow u = v \end{aligned}$$

Damit haben wir gezeigt: 3-COL $\leq_p$ TAGUNG. Da 3-COL NP-schwer ist, muss auch TAGUNG NP-schwer sein.