Prof. Dr. M. Grohe E. Fluck, A. Riazsadri, J. Feith

Übungsblatt Weihnachten mit Lösungen

Abgabetermin: Mittwoch, der 11. Januar 2023 um 14:30

Aufgabe 1 5* Punkte

Es ist kurz vor Weihnachten, und die Wichtel sind auf dem Weg zum Nordpol, um auch dieses Jahr wieder fleissig Geschenke für die Kinder der Welt zu produzieren. Leider ist ihr Zug jedoch im Schnee steckengeblieben, und sie entschliessen sich, ein paar Übungsaufgaben für ihre BuK-Klausur zu machen...

Zeigen Sie mit Hilfe des Satzes von Rice, dass folgende Sprachen unentscheidbar sind, oder begründen sie, warum der Satz von Rice nicht anwendbar ist.

a) $L_1 = \{\langle M\rangle w \mid M \text{ hält auf } w \text{ nach höchstens } |w| \text{ Schritten}\}$

b) $L_2 = \{\langle M\rangle \mid \langle M\rangle \text{ besteht aus ungerade vielen Symbolen}\}$

c) $L_3 = \{\langle M\rangle \mid M \text{ erkennt } H_\varepsilon\}$

d) $L_4 = \{\langle M\rangle \mid M \text{ erkennt } \overline{H_\varepsilon}\}$

Lösung:

a) L_1 ist keine Sprache von Gödelnummern, und somit ist der Satz von Rice nicht anwendbar. Weiterhin ist L_1 entscheidbar, da wir eine gegebene TM M auf einer gegebenen Eingabe w für $|w|$ Schritte simulieren können.

b) L_2 ist entscheidbar, da wir prüfen können, ob eine Eingabe eine Gödelnummer ist und ob eine Eingabe gerade Länge hat. Somit kann der Satz von Rice nicht angewendet werden.

c) Wir definieren

$$\mathcal{S} = \{f \mid f(w) \text{ beginnt mit 1 genau dann, wenn } w = \langle M\rangle \text{ gilt und } M \text{ auf } \varepsilon \text{ hält}\}.$$

Dann gilt $\emptyset \neq \mathcal{S} \neq \mathcal{R}$, da H_ε semi-entscheidbar ist und die konstante Nullfunktion nicht in $\mathcal{S}$ liegt. Weiterhin haben wir

$$\begin{aligned}
L(\mathcal{S}) &= \{\langle M\rangle \mid M \text{ berechnet eine Funktion aus } \mathcal{S}\}\\
&= \{\langle M\rangle \mid M \text{ akzeptiert } w \text{ genau dann, wenn } w \in H_\varepsilon\}\\
&= \{\langle M\rangle \mid M \text{ erkennt } H_\varepsilon\}\\
&= L_3,
\end{aligned}$$

weswegen L_3 nach dem Satz von Rice nicht entscheidbar ist.

d) L_4 ist entscheidbar, da L_4 leer ist. Dies folgt daraus, dass $\overline{H_\varepsilon}$ nicht semi-entscheidbar ist und somit von keiner TM erkannt wird.

Aufgabe 2 **5* Punkte**

Im Weihnachtsdorf angekommen machen sich die Wichtel sogleich an die Arbeit. Dieses Jahr haben sich alle Kinder die Lernbox "Berechenbarkeit" gewünscht, und jeder dieser Boxen soll eine magische Turingmaschine (MTM) beigelegt werden. Damit die Boxen aber nicht alle gleich sind, soll die Box jeder Turingmaschine eine andere Funktion berechnen.

Nach einiger Zeit stellen die QA-Wichtel jedoch fest, dass es einen Fehler in der Produktion gab und manche Boxen magische Turingmaschinen enthalten, welche die gleiche Funktion berechnen. Da sie unmöglich alle bereits produzierten magischen Turingmaschinen von Hand prüfen können, wollen sie die Prüfung automatisieren und wiederum von einer Turingmaschine durchführen lassen...

Wir betrachten die folgende Sprache:

$$L = \{\langle M\rangle\langle M'\rangle \mid M \text{ und } M' \text{ berechnen die gleiche Funktion}\}$$

a) Zeigen oder widerlegen Sie, dass L entscheidbar ist.

b) Geben Sie für L und $\overline{L}$ an, ob sie semi-entscheidbar sind. Beweisen Sie ihre Behauptungen.

Lösung:

a) L ist unentscheidbar. Dazu zeigen wir $H_{\text{all}} \leq L$.

Wir definieren eine Reduktionsabbildung $f\colon \Sigma^* \to \Sigma^*$ mit

$$f(w) = \begin{cases} \varepsilon, & \text{falls } w \text{ keine Gödelnummer ist} \\ \langle M^*\rangle\langle M_1\rangle, & \text{falls } w = \langle M\rangle \end{cases}$$

wobei M_1 auf jeder Eingabe 1 ausgibt und M^* zunächst M auf der gegebenen Eingabe simuliert, und 1 ausgibt, falls die Simulation von M hält. Diese Funktion ist berechenbar.

Sei w eine Eingabe, welche keine Gödelnummer ist. Dann gilt $w \notin H_{\text{all}}$, und $f(w) = \varepsilon \notin L$.

Betrachten wir nun eine Eingabe $w = \langle M\rangle$. Dann gibt M^* genau dann auf jeder Eingabe 1 aus, wenn M auf jeder Eingabe hält. Folglich gilt $\langle M\rangle \in H_{\text{all}}$ genau dann, wenn $f(\langle M\rangle) = \langle M^*\rangle\langle M_1\rangle \in L$ gilt, da genau in diesem Fall M^* und M_1 die gleiche Funktion berechnen.

Damit folgt $H_{\text{all}} \leq L$, und somit die Unentscheidbarkeit von L.

b) Da H_{all} nicht semi-entscheidbar ist, folgt mit der obrigen Reduktion auch, dass L nicht semi-entscheidbar ist. Weiterhin erhalten wir auch $\overline{H_{\text{all}}} \leq \overline{L}$, womit auch $\overline{L}$ nicht semi-entscheidbar ist, da $\overline{H_{\text{all}}}$ nicht semi-entscheidbar ist.

Aufgabe 3 **5* Punkte**

Munter haben die Wichtel trotz der Rückschläge Geschenke produziert. Heute gönnen sie sich eine Pause, und geraten ins Gespräch über Komplexitätstheorie...

a) Zeigen Sie: P ist abgeschlossen unter Komplementbildung, d.h. wenn $L \in \mathsf{P}$ gilt, dann auch $\overline{L} \in \mathsf{P}$.

b) Wir definieren $\mathsf{coNP} = \{\overline{L} \mid L \in \mathsf{NP}\}$, die Klasse der Komplemente aller Sprachen, welche in NP liegen. Zeigen oder widerlegen Sie: Wenn $\mathsf{P} = \mathsf{NP}$ gilt, dann gilt $\mathsf{NP} = \mathsf{coNP}$.

c) Zeigen Sie: Eine Sprache L ist genau dann NP-vollständig, wenn $\overline{L}$ coNP-vollständig ist.

Lösung:

a) Sei L in P, d.h. es existiert ein Polynomialzeitalgorithmus A, welcher L entscheidet. Wir betrachten nun den Algorithmus B, welcher zunächst A simuliert und die Ausgabe von A invertiert. Somit ist B ein Polynomialzeitalgorithmus, welcher $\overline{L}$ entscheidet, womit $\overline{L} \in \mathsf{P}$ folgt.

b) Angenommen, es gilt $\mathsf{P} = \mathsf{NP}$. Dann gilt $L \in \mathsf{P}$ für jede Sprache $L \in \mathsf{NP}$, und folglich auch $\overline{L} \in \mathsf{P}$ aufgrund der obrigen Überlegungen. Somit haben wir $\mathsf{coNP} \subseteq \mathsf{P}$.

Weiterhin gilt $\mathsf{P} \subseteq \mathsf{NP}$. Somit gilt für jede Sprache $L \in \mathsf{NP}$ und damit nach den obrigen Überlegungen auch $\overline{L} \in \mathsf{NP}$, woraus $L \in \mathsf{coNP}$ folgt. Folglich haben wir auch $\mathsf{P} \subseteq \mathsf{coNP}$ und damit $\mathsf{P} = \mathsf{coNP}$

Insgesamt gilt $\mathsf{NP} = \mathsf{P} = \mathsf{coNP}$.

c) Sei L NP-vollständig, d.h. es gilt $L' \leq_p L$ für alle $L' \in \mathsf{NP}$. Damit gilt auch $\overline{L'} \leq_p \overline{L}$, womit L coNP-vollständig ist.

Analog erhalten wir, dass L NP-vollständig ist, falls $\overline{L}$ coNP-vollständig ist.

Somit folgt die Aussage.

Aufgabe 4 **5* Punkte**

Die Wichtel beraten, was sie mit den bereits hergestellten magischen Turingmaschinen anstellen sollen. Ihnen kommt die Idee, dass sie die Lernboxen mit den MTMs einfach an Kinder verschenken, welche einander nicht kennen. Dazu konstruieren sie einen "Bekanntheitsgraphen", dessen Knoten die Kinder repräsentieren und welcher eine Kante vw besitzt, wenn die Kinder v und w einander kennen.

MTM-Verteilung

Eingabe: Ein "Bekanntheitsgraph" G und eine Zahl $k \in \mathbb{N}$.

Frage: Existiert eine Menge von mindestens k Kindern, welche einander paarweise nicht kennen?

Zeigen Sie, dass MTM-Verteilung NP-vollständig ist.

Lösung:

Zunächst zeigen wir MTM-Verteilung $\in$ NP. Sei also G ein Graph auf n Knoten und $I \subseteq V(G)$ eine Menge von k Kindern, welche einander nicht kennen. Wir definieren für $I = \{i_1, \dots, i_k\}$ das Zertifikat

$$C(I) = \text{bin}(i_1)\# \dots \# \text{bin}(i_k)$$

und sehen, dass $|C(I)| = O(k \log n) = O(n \log n)$ gilt, womit das Zertifikat polynomielle Länge hat.

Um ein gegebenes Zertifikat C für eine Instanz (G, k) zu verifizieren, gehen wir wie folgt vor:

- Prüfe, ob $C = C(I)$ für eine Menge $I \subseteq V(G)$ der Größe mindestens k gilt.
- Prüfe für alle Paare $v, w \in I$, ob $vw \notin E(G)$ gilt, d.h. ob v und w einander nicht kennen.

Dieses Verfahren ist offensichtlich korrekt und läuft in Polynomialzeit. Somit haben wir MTM-Verteilung $\in$ NP.

Um zu zeigen, dass MTM-Verteilung auch NP-schwer ist, reduzieren wir von Clique.

Sei also (G, k) eine Clique-Instanz. Wir definieren den Komplementgraphen $\overline{G} = (V(G), \{vw \in V(G)^2 \mid vw \notin E(G)\})$ von G und betrachten die Reduktionsabbildung f mit

$$f(G, k) = (\overline{G}, k).$$

Offensichtlich kann f in Polynomialzeit berechnet werden.

Wir zeigen nun, dass G genau dann eine k-Clique besitzt, wenn eine Menge $I \subseteq V(G)$ der Größe mindestens k existiert, sodass in $\overline{G}$ keine Kanten zwischen Knoten von I verlaufen.

Sei also K eine k-Clique von G. Dann gilt $vw \in E(G)$ für alle $v, w \in K$, und somit $vw \notin E(\overline{G})$ für alle $v, w \in K$. Folglich ist K in $\overline{G}$ eine Menge von k Knoten, sodass keine Kanten zwischen den Knoten in K verlaufen.

Analog ist eine Menge $I \subseteq V(G)$ mit den oben genannten Eigenschaften auch eine k-Clique von G, da alle Knoten von I in G benachbart sind.

Damit haben wir Clique $\leq_p$ MTM-Verteilung, und wir folgern, dass MTM-Verteilung NP-schwer ist. Insgesamt ist MTM-Verteilung also NP-vollständig.