Technische Universität Berlin, 05.04.2024

**Name:** ........................ **Matr.-Nr.:** ........................

# Schriftlicher Test: Berechenbarkeit und Komplexität (Wiederholung)

(Weller/Froese/Kellerhals/Kunz, Wintersemester 2023/2024)

| | |
|---|---|
| Bearbeitungszeit: | 60 Minuten |
| Max. Punktzahl: | 50 Punkte |

| Aufgabe Nr.: | 1 | 2 | 3 | **Summe** |
|---|---|---|---|---|
| Punktzahl: | 16 | 16 | 18 | 50 |
| Davon erreicht: | | | | |

**Allgemeine Hinweise:**

- Es sind keinerlei Hilfsmittel erlaubt.
- Benutzen Sie einen dokumentenechten Stift in der Farbe schwarz oder blau. Insbesondere also keinen Bleistift, sondern einen Kugelschreiber.
- Beschriften Sie jedes Blatt mit ihrem Vor- und Nachnamen und ihrer Matrikelnummer.
- **Falls es in der Aufgabenstellung nicht explizit ausgeschlossen wird, so sind alle Antworten zu begründen! Antworten ohne Begründung erhalten 0 Punkte.**
- Sie dürfen alle Aussagen **und Mitteilungen** aus den Vorlesungsfolien als bekannt annehmen, es sei denn der Beweis einer solchen Aussage ist explizit gefordert (dies schließt Forderungen nach logisch äquivalenten Aussagen wie der Kontraposition der Aussage mit ein).

**Erinnerung an Erkenntnisse der Vorlesung:**

- $Q$ ist in NP, falls Ja-Instanzen von $Q$ in Polynomzeit verifizierbar sind, d.h. es existiert eine deterministische, polynomzeitbeschränkte TM $M$, sodass für alle $x$ gilt
$$x \in Q \iff \exists_{u \in \Sigma^{\mathrm{poly}(|x|)}} \langle x, u \rangle \in T(M).$$
$Q$ ist in coNP, falls Nein-Instanzen von $Q$ in Polynomzeit verifizierbar sind (analog zu oben).
- Für alle $\mathcal{X} \in \{\mathrm{NP}, \mathrm{coNP}, \mathrm{PSPACE}\}$ ist $Q$ $\mathcal{X}$-schwer (-vollständig), falls $\forall_{L \in \mathcal{X}}\ L \leq_m^p Q$ (und $Q \in \mathcal{X}$).
- Die Menge TQBF aller wahren quantifizierten aussagenlogischen Formeln ist PSPACE-vollständig und entscheidbar.
- $\leq_m^p$ ist transitiv.
- $\mathrm{coNP} = \{L \mid \overline{L} \in \mathrm{NP}\}$
- $\mathrm{PSPACE} = \{L \mid L \leq_m^p \mathrm{TQBF}\}$
- 2-SAT $\in$ P
- $\overline{\mathrm{SAT}}$ und TAUT sind coNP-vollständig.
- SAT, Vertex Cover und Clique sind NP-vollständig.
- P = coP

**Viel Erfolg!**

Aufgabe 1: **Vermischtes** (16 Punkte)

(a) Geben Sie für jede der folgenden Aussagen an, ob diese korrekt ist oder nicht (ohne Begründung). (4 P)

(1) $2^n \in O(2^{n/2})$

(2) $n \log n \in O(2n)$

(3) $2^n n^2 \in O(3^n)$

(4) $n! \in O(n^n)$

—————Lösungsskizze—————

(3) und (4) sind wahr.

---

(b) Beweisen Sie **drei** der folgenden Aussagen. (Für die anderen Aussagen brauchen Sie nichts beweisen, manche Aussagen sind auch nicht wahr. Das Widerlegen von falschen Aussagen gibt keine Punkte) (12 P)

(1) $\mathrm{SAT} \leq_m^p \overline{\mathrm{SAT}}$

(2) Eine Sprache $A$ ist genau dann NP-schwer, wenn $\overline{A}$ coNP-schwer ist.

(3) $\mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$

(4) Wenn eine NP-schwere Sprache in P liegt, dann gilt P = NP.

(5) $\mathrm{P} \neq \mathrm{PSPACE} \implies \mathrm{P} \neq \mathrm{NP}$

(6) $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP}$

—————Lösungsskizze—————

**(2)**:

$$\begin{aligned} A \text{ ist NP-schwer} &\iff \forall_{L \in \mathrm{NP}}\ L \leq_m^p A \\ &\overset{\text{VL}}{\iff} \forall_{L \in \mathrm{NP}}\ \overline{L} \leq_m^p \overline{A} \\ &\iff \forall_{\overline{L} \in \mathrm{coNP}}\ \overline{L} \leq_m^p \overline{A} \\ &\iff \overline{A} \text{ ist coNP-schwer} \end{aligned}$$

**(4)**: Sei $A \in \mathrm{P}$, d.h. es gibt einen Algorithmus $Q$, der $A$ in polynomieller Zeit $q(n)$ entscheidet. Sei $A$ NP-schwer. Da $\mathrm{P} \subseteq \mathrm{NP}$ bekannt aus VL, zeigen wir nur $\mathrm{NP} \subseteq \mathrm{P}$. Sei dazu $L \in \mathrm{NP}$. Nach Vorraussetzung $L \leq_m^p A$, d.h. es gibt eine Funktion $f$ sodass für alle $x \in \Sigma^*$ gilt $x \in L \iff f(x) \in A$ und $f$ ist berechenbar in polynomieller Zeit $p(n)$. Insbesondere ist dann $|f(x)| \leq p(|x|)$. Da $A \in \mathrm{P}$ gibt es einen Algorithmus $Q$, der $f(x) \in A$ in polynomieller Zeit $q(n)$ entscheidet. Indem wir für Eingabe $x$ erst $f(x)$ berechnen und dann $f(x) \in A$ entscheiden haben wir $x \in L$ in Zeit $q(p(|x|))$, also polynomiell in $|x|$ Zeit entschieden, also $L \in \mathrm{P}$.

**(6)**: (a) $\mathrm{P} \subseteq \mathrm{NP}$ gilt, da jede deterministische Turing-Maschine auch eine nichtdeterministische Turing-Maschine ist, die von ihrem Nichtdeterminismus keinen Gebrauch macht.

(b) $\mathrm{P} \subseteq \mathrm{coNP}$ gilt, da $\mathrm{P} = \mathrm{coP} = \{L \mid \overline{L} \in \mathrm{P}\} \subseteq \{L \mid \overline{L} \in \mathrm{NP}\} = \{L \mid L \in \mathrm{coNP}\} = \mathrm{coNP}$.

---

**Name: ..............................** **Matr.-Nr.: .......................**

*(Leere Seite für Notizen oder Ähnliches; bei Lösungen bitte zugehörige Aufgabe klar kennzeichnen!)*

Aufgabe 2: **Polynomzeitreduktionen** (16 Punkte)

(a) Beweisen oder widerlegen Sie jeweils, dass $\leq_m^p$ ... (10 P)

(i) ... transitiv ist.

(ii) ... symmetrisch ist.

*Hinweis*: Eine binäre Relation $R$ ist *symmetrisch*, falls für alle $x, y$ gilt: $xRy \iff yRx$.

——————Lösungsskizze——————

(i) $\leq_m^p$ ist transitiv. Sein dazu $A, B, C \in \Sigma^*$ mit $A \leq_m^p B$ und $B \leq_m^p C$ vermöge Reduktionsfunktionen $f_A$ und $f_B$, berechenbar in polynomieller Zeit $p_A(n)$ bzw. $p_B(n)$. Dann lässt sich $f_B \circ f_A$ in polynomieller Zeit berechnen, da $p_B(p_A(n))$ ein Polynom ist (Totalität folgt aus der Totalität von $f_A$ und $f_B$). Für die Reduktionseigenschaft sei $x \in \Sigma^*$ beliebig. Dann gilt

$$x \in A \overset{\text{Red.Eig. } f_A}{\iff} f_A(x) \in B \overset{\text{Red.Eig.} f_B}{\iff} f_B(f_A(x)) \in C$$

(ii) $\leq_m^p$ ist nicht symmetrisch. Zum Beispiel gilt $\emptyset \leq_m^p H_0$ via Reduktion $f(x) = 0 \notin H_0$, aber nicht $H_0 \leq_m^p \emptyset$ da die leere Menge keine Ja-Instanzen hat, $H_0$ aber schon (Bilder von Wörtern in $H_0$ müssen auf Wörter in $\emptyset$ abgebildet werden, die aber gibt es nicht).

---

(b) Wir definieren eine *Spezialreduktion* von einer Sprache $A \subseteq \Sigma^*$ auf eine Sprache $B \subseteq \Sigma^*$ als eine polynomzeitberechenbare Funktion $f \colon \Sigma^* \to \Sigma^*$, für die $w \in B$ und $w' \in \Sigma^* \setminus B$ existieren, sodass für alle $x \in \Sigma^*$ gilt: (6 P)

$$f(x) = \begin{cases} w, & x \in A \\ w', & x \notin A \end{cases}.$$

Falls so eine Spezialreduktion von $A$ auf $B$ existiert, so schreiben wir $A \preceq B$.

Beweisen Sie: Falls $A \preceq B$ für Sprachen $A$ und $B$ gilt, so liegt $A$ in P.

——————Lösungsskizze——————

Um $A$ zu akzeptieren simulieren wir $f$ und akzeptieren genau dann wenn $f$ das Wort $w$ ausgibt, also wenn $f(x) = w$, was genau dann passiert wenn $x \in A$. Dabei wird $w$ im Algorithmus fest verdrahtet. Dieser Algorithmus arbeitet in polynomieller Zeit, da $f$ dies auch tut.

---

**Name: ..............................** **Matr.-Nr.: ......................**

*(Leere Seite für Notizen oder Ähnliches; bei Lösungen bitte zugehörige Aufgabe klar kennzeichnen!)*

Aufgabe 3: **NP-vollständige Probleme** (18 Punkte)

Betrachten Sie die folgenden Probleme:

NOT-ALL-EQUAL-SAT

*Eingabe:* Eine aussagenlogische Formel $\varphi$ in konjunktiver Normalform.

*Frage:* Existiert eine Belegung der Variablen von $\varphi$, sodass $\varphi$ erfüllt ist und in keiner Klausel alle Literale den gleichen Wert annehmen?

SET SPLITTING

*Eingabe:* Eine Zahl $n \in \mathbb{N}$ und $m$ Teilmengen $X_1, \ldots, X_m$ von $\{1, \ldots, n\}$.

*Frage:* Gibt es disjunkte Teilmengen $P, Q \subseteq \{1, \ldots, n\}$ mit $P \cup Q = \{1, \ldots, n\}$ und $X_j \nsubseteq P$ und $X_j \nsubseteq Q$ für alle $1 \leq j \leq m$?

Betrachten Sie die totale Funktion $f$, die bei Eingabe einer kodierten KNF-Formel $F$ mit Klauseln $C_1, \ldots, C_m$ und Variablen $x_1, \ldots, x_n$ die Kodierung von $m + n$ Teilmengen $X_1, \ldots, X_{m+n} \subseteq \{1, \ldots, 2n\}$ ausgibt, die wie folgt definiert sind:

- Für alle $1 \leq j \leq m$, sei $X_j := \{i \mid C_j \text{ enthält } x_i\} \cup \{n + i \mid C_j \text{ enthält } \overline{x}_i\}$.
- Für alle $1 \leq i \leq n$, sei $X_{m+i} := \{i, n + i\}$.

(a) Geben Sie $f(\varphi)$ für $\varphi := (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3)$ an und zeigen Sie, dass sowohl $\varphi$ eine Ja-Instanz von NOT-ALL-EQUAL-SAT als auch $f(\varphi)$ eine Ja-Instanz von SET SPLITTING ist. (6 P)

——————Lösungsskizze——————

$f(\varphi) = (6, \{\{1, 2\}, \{4, 3\}, \{1, 2, 3\}, \{1, 4\}, \{2, 5\}, \{3, 6\}\})$

Eine Lösung für $\varphi$ ist $x_1 = 1$, $x_2 = 0$, $x_3 = 1$ (oder invertiert). Unter dieser Belegung hat keine Klausel nur gleich belegte Literale.

Eine LÖsung für $f(\varphi)$ ist $P = \{1, 5, 3\}$, $Q = \{2, 4, 6\}$. Keine der Mengen von $f(\varphi)$ ist Teilmenge von $P$ oder $Q$.

---

(b) Zeigen Sie, dass es sich bei $f$ um eine Polynomzeitreduktion von NOT-ALL-EQUAL-SAT auf SET SPLITTING handelt. (12 P)

——————Lösungsskizze——————

Polynomzeit und Totalität von $f$ sind klar. Wir zeigen die Reduktionseigenschaft.

„$\Rightarrow$“: Sei $\varphi \in$ NOT-ALL-EQUAL-SAT. Dann gibt es eine Belegung $\beta$ sodass keine Klausel nur gleich belegte Literale hat. Sei $P := \{i \mid \beta(x_i) = 1\} \cup \{n + i \mid \beta(x_i) = 0\}$ und $Q := \{1, \ldots, 2n\} \setminus P$. Wenn das keine Lösung für $f(\varphi)$ ist, so gibt es eine Menge $X_j$ mit $X_j \subseteq P$ oder $X_j \subseteq Q$. Sei oBdA $X_j \subseteq P$.

**Fall 1**: $j > m$. Dann ist $X_j = \{i, n + i\}$ für ein $i \leq n$ aber dann $i, n + 1 \in P$, also $\beta(x_i) = 1$ und $\beta(x_i) = 0$, ein Widerspruch.

**Fall 2**: $j \leq m$. Für alle $x_i$ in $C_i$ ist also $i \in P$ und, für alle $\neg x_i$ in $C_i$ ist $n + i \in P$. Das heißt aber $\beta$ belegt alle Literale von $C_i$ gleich, im Widerspruch zur Not-All-Equal Bedingung.

„$\Leftarrow$“: Sei $f(\varphi) \in$ SET SPLITTING mit Lösung $(P, Q)$. Wir zeigen, dass $\beta(x_i) := 1 \iff i \in P$ (für alle $i \leq n$) eine gültige Belegung für $\varphi$ ist. Nehmen wir an, es gäbe eine Klausel $C_i$ in der alle Literale unter $\beta$ gleich belegt sind, oBdA alle 0. Für alle positiven Literale $x_i$ von $C_j$ ist dann $\beta(x_i) = 0$, also $i \notin P$ und damit $i \in Q$ da $Q = \{1, \ldots, 2n\} \setminus P$. Für alle negativen Literale $\neg x_i$ von $C_j$ ist $\beta(x_i) = 1$, also $i \in P$ und, da $\{i, n + i\} \nsubseteq P$ gilt $n + i \in Q$. Dann ist aber $X_j \subseteq Q$, im Widerspruch dazu, dass $(P, Q)$ eine Lösung für $f(\varphi)$ ist.

---