Berlin, 27.07.2015

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

Klausur: Berechenbarkeit und Komplexität

(Niedermeier/Chen/Froese, Sommersemester 2015)

1	
2	
3	
4	
5	
6	
Σ	

Einlesezeit:	15 min.
Bearbeitungszeit:	60 min.
max. Punktezahl:	80 Punkte

Allgemeine Hinweise:

- Es sind keinerlei Hilfsmittel erlaubt.
- Benutzen Sie keinen Bleistift, sondern einen Kugelschreiber oder Füller in der Farbe schwarz oder blau.
- Beschriften Sie jedes Blatt mit Vor- und Nachnamen sowie Matrikelnummer.
- **Falls in der Aufgabenstellung nicht explizit ausgeschlossen, sind alle Antworten zu begründen! Antworten ohne Begründung erhalten 0 Punkte.**

Viel Erfolg!

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

Aufgabe 1: **Analyse einer Turingmaschine** (3+5+5 Punkte)

Gegeben sei die Turingmaschine $M = (\{q_0, q_1, q_2, q_3, q_4\}, \Sigma = \{a, b, c\}, \Gamma = \{a, b, c, \Box\}, \delta, q_0, \Box, \{q_4\})$, wobei δ wie folgt definiert ist:

δ	a	b	c	$\Box$
q_0	(q_0, a, R)	(q_1, b, R)	(q_2, c, R)	$(q_3, \Box, L)$
q_1	–	(q_1, b, R)	(q_2, c, R)	$(q_3, \Box, L)$
q_2	–	–	(q_2, c, R)	$(q_3, \Box, L)$
q_3	(q_3, b, L)	(q_3, b, L)	(q_3, c, L)	$(q_4, \Box, R)$

a) Geben Sie die Konfigurationsfolge (beginnend mit der Startkonfiguration q_0abc) der Turingmaschine M bei Eingabe abc an (ohne Begründung).

b) Welche Funktion f berechnet die Turingmaschine M? Dabei ist der Funktionswert $f(w)$ definiert als das Wort, das rechts vom Lesekopf auf dem Band steht, falls M einen Endzustand erreicht. Andernfalls ist der Funktionswert undefiniert ($\perp$).

c) Sei w ein beliebiges Wort der Länge n bei dem die Turingmaschine M den Endzustand q_4 erreichen kann. Gilt dann immer, dass M auf Eingabe w nach höchstens $1{,}5 \cdot n + 5$ Schritten den Endzustand erreicht?

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

Aufgabe 2: **μ-Rekursion und LOOP-Programme** (3+5 Punkte)

Für eine Funktion $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ ist der μ-Operator gemäß Vorlesung wie folgt definiert:

$$\mu(f)(x_1,\ldots,x_k) :=\begin{cases} n, & f(n,x_1,\ldots,x_k)=0 \text{ und} \\ & f(n',x_1,\ldots,x_k)\neq 0 \text{ und def. für } n'<n, \\ \perp, & \text{sonst.}\end{cases}$$

Im Folgenden sei $\mathrm{sub}\colon \mathbb{N}^2 \to \mathbb{N}$ mit $\mathrm{sub}(x,y) := \max(0, x-y)$ die modifizierte Subtraktionsfunktion und $\mathrm{mult}\colon \mathbb{N}^2 \to \mathbb{N}$, $\mathrm{mult}(x,y) := x \cdot y$ die Multiplikationsfunktion.

Außerdem sei $g\colon \mathbb{N}^3 \to \mathbb{N}$ definiert als $g(x,y,z) := \mathrm{sub}(\mathrm{mult}(y,z),x)$.

a) Wieviele Argumente hat die Funktion $\mu(g)$?

b) Ist $\mu(g)$ primitiv-rekursiv? Falls ja, geben Sie ein LOOP-Programm (ohne Begründung) an, das $\mu(g)$ berechnet.

Hinweis: LOOP-Programme sind wie folgt aufgebaut.

- Variablen: $x_0, x_1, \ldots$
- Konstanten: $0, 1, 2, \ldots$
- Trennsymbole: $;\,,\,:=$
- Operationen: $+, -$
- Schlüsselwörter: **LOOP**, **DO**, **END**

- Für konstante $c \in \mathbb{N}$ sind $x_i := x_j + c$ und $x_i := x_j - c$ LOOP-Programme.
- Für LOOP-Programme P_1 und P_2 ist $P_1; P_2$ ein LOOP-Programm.
- Für LOOP-Programm P und Variable x_i ist **LOOP** x_i **DO** P **END** ein LOOP-Programm.

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

Aufgabe 3: **Entscheidbarkeit** (6+6 Punkte)

Der Reißverschlussoperator „$\propto$" konstruiert aus zwei Sprachen $L_1 \subseteq \Sigma^*$ und $L_2 \subseteq \Gamma^*$ eine neue Sprache

$$\begin{aligned} L_1 \propto L_2 \coloneqq \{w = a_1 b_1 a_2 b_2 \dots a_n b_n \mid n \geq 1 \wedge (\forall i \in \{1, 2, \dots, n\} \colon a_i \in \Sigma \wedge b_i \in \Gamma) \\ \wedge\, a_1 a_2 \dots a_n \in L_1 \wedge b_1 b_2 \dots b_n \in L_2\}. \end{aligned}$$

a) Nehmen Sie an, dass L_1 und L_2 entscheidbar sind. Argumentieren Sie, dass dann auch $L_1 \propto L_2$ entscheidbar ist.

b) Ist $L_1 \propto L_2$ immer entscheidbar, falls L_2 entscheidbar ist?

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

Aufgabe 4: **Post'sches Korrespondenzproblem** (4+4+4 Punkte)

Für ein endliches Alphabet Σ ist das Post'sche Korrespondenzproblem über Σ die Menge

$$\mathrm{PCP} := \{\langle (x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k) \rangle \mid k \geq 1 \wedge x_i, y_i \in \Sigma^* \wedge \exists n \geq 1 \exists i_1, i_2, \ldots, i_n \in \{1, \ldots, k\} \colon x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}\}.$$

a) Geben Sie für die beiden folgenden Tupelmengen über $\Sigma = \{a, b\}$ an, ob sie in der Menge PCP sind, das heißt, ob eine Lösung existiert. Falls eine Lösung existiert, dann geben Sie eine an. Begründen Sie andernfalls, warum keine Lösung existiert.

   (i) $\{(aa, ba), (ba, aa), (ba, b)\}$

   (ii) $\{(baa, ba), (a, abaa), (bab, bb), (baa, a)\}$

b) Das Post'sche Korrespondenzproblem ist im Allgemeinen nicht entscheidbar. Gilt das auch für den Spezialfall, dass für jedes Eingabetupel (x_i, y_i) die Wörter x_i und y_i gleich lang sind?

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

Aufgabe 5: **Problemvarianten von Subset Sum** (6+3+4+7 Punkte)

Betrachten Sie das aus der Vorlesung bekannte NP-vollständige Subset Sum-Problem:

Subset Sum
Eingabe: Eine Multimenge $U := \{u_1, \dots, u_m\}$ von natürlichen Zahlen und eine Zahl B.
Frage: Existiert ein $W \subseteq U$ mit $\sum_{u \in W} u = B$?

a) Beweisen Sie, dass Subset Sum $\in$ DTIME(n) falls $B = (\sum_{u \in U} u) - 1$ gilt, wobei n die Gesamtlänge der kodierten Eingabe sei. Gehen Sie dabei davon aus, dass
   - die Eingabe nur aus den Zahlen $u_1, u_2, \dots, u_m$ besteht und
   - die Eingabezahlen binär kodiert und durch ein „#"-Symbol getrennt sind.

b) Das spezielle Subset Sum-Problem Half Sum, bei dem $S := \sum_{u \in U} u$ geradzahlig ist und $B = S/2$ gilt, ist NP-schwer. Betrachten Sie folgende Polynomzeitkonstruktion.
   Konstruktion: Definiere die Abbildung $f(U, B) = U \cup \{S - B, B\}$.
   (i) Sei $I := (\{3, 3, 11, 11, 20\}, 30)$ eine Instanz für Subset Sum.
   Geben Sie $f(I)$ an (ohne Begründung).
   (ii) Begründen Sie anhand des Beispiels aus Teilaufgabe b(i), warum die Konstruktion *keine* Reduktion von Subset Sum auf Half Sum ist.
   (iii) Korrigieren Sie die Konstruktion indem Sie die Zahlen $S - B$ und B durch zwei andere Zahlen ersetzen, wobei eine davon $S - B + 1$ ist. Beweisen Sie anschließend die Korrektheit der korrigierten Konstruktion f', d.h. zeigen Sie, dass für alle $I = (U, B)$ gilt,

$$I \text{ ist eine Ja-Instanz für Subset Sum} \Leftrightarrow f'(I) \text{ ist eine Ja-Instanz für Half Sum.}$$

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

Aufgabe 6: **Vermischtes zur Komplexität** (3+3+3+3+3 Punkte)

Begründen oder widerlegen Sie (in jeweils maximal 3 Sätzen) die folgenden Aussagen.

a) Jede Sprache, die sowohl in NP als auch in coNP enthalten ist, ist nicht in P.

b) Jede Sprache, die nicht in NP liegt, ist in PSPACE.

c) Wenn eine Sprache $A \in \mathrm{P}$ existiert, sodass $L \leq_m^p A$ für alle $L \in \mathrm{NP}$ gilt, dann folgt $\mathrm{P} = \mathrm{NP}$.

d) Unter der Annahme $\mathrm{P} = \mathrm{NP}$ ist jede Sprache $A \subseteq \Sigma^*$ mit $A \neq \emptyset$ und $A \neq \Sigma^*$ NP-schwer.

e) Unter der Annahme $\mathrm{P} \neq \mathrm{NP}$ gilt, dass 2-SAT nicht von einer deterministischen Turingmaschine in Polynomzeit gelöst werden kann.