Theoretische Informatik

Prof. Meer, Dr. Gengler

Aufgabenblatt 14

Abgabetermin: 31.01.2014

Heften Sie unbedingt alle Blätter Ihrer Lösung zusammen und geben Sie oben auf dem ersten Blatt Ihren Namen, Vornamen, und Ihre Übungsgruppe an.

Kriterium für erfolgreiche Bearbeitung des Übungsblattes:
Bearbeitung von:
- Aufgabe 1,
- Aufgabe 2, wird aber nicht korrigiert,
- Aufgaben 9, 10 und 11

Fragen zu den Aufgaben können auf `http://www.BTU-Forum.DE` in Unterforum "Theoretische Informatik, ..." gestellt werden.

Definitionen:

$$\begin{array}{lll} L \leq_m^{\text{poly}} L' & \iff & L \textbf{ (many-one) polynonial reduzierbar} \text{ auf } L' \\ & :\iff & \exists\, f : \Sigma_L^* \to \Sigma_{L'}^* \text{ total und polynomialzeit-berechenbar mit } \; (w \in L \iff f(w) \in L') \\ L \equiv_m^{\text{poly}} L' & :\iff & (L \leq_m^{\text{poly}} L' \;\wedge\; L' \leq_m^{\text{poly}} L) \end{array}$$

Für eine Sprachklasse $\mathcal{L}$ heisst eine Sprache A **$\mathcal{L}$-vollständig** bzgl. der Reduktion $\leq_m^{\text{poly}}$ genau dann, wenn $A \in \mathcal{L}$ und $\forall L \in \mathcal{L} : L \leq_m^{\text{poly}} A$.

$\text{NPC} := \{L \in \text{NP} \mid L \text{ ist NP-vollständig bzgl. der Reduktion } \leq_m^{\text{poly}}\}$

Aufgabe 1

Wir betrachten die folgenden Sprachen L_1 und L_2 ($\text{bin}(n)$ bezeichnet die Binärdarstellung von n, niederwertigste Bits hinten, ohne führende Nullen):

$$\begin{array}{l} L_1 := \{a^n c a^m c a^k \mid n, m, k \in \mathbb{N} \wedge k = n \cdot m\} \\ L_2 := \{\text{bin}(n) c \,\text{bin}(m) c \,\text{bin}(k) \mid n, m, k \in \mathbb{N} \wedge k = n \cdot m\} \end{array}$$

Zu L_1 und L_2 betrachten wir die im Folgenden kurz beschriebenen Turing-Maschinen M_1 und M_2, welche L_1 und L_2 entscheiden: im Wesentlichen subtrahieren die Turing-Maschinen n m-mal vom Startwert k; wird dadurch genau 0 erreicht, so wird akzeptiert ansonsten verworfen. (Natürlich müssen M_1 und M_2 auch prüfen, dass die Eingabe die korrekte Form hat.)

1. Wird durch die Turing-Maschinen M_1 und M_2 bezeugt, dass L_1 und L_2 in P liegen?
2. Liegen L_1 und L_2 in P?

Begründen Sie Ihre Antworten.

Aufgabe 2
Zeigen Sie, dass die folgenden Sprachen in P liegen:

$$
\begin{aligned}
L_1 &:= \{a^n b^n c^n \mid n \in \mathbb{N}\} \\
L_2 &:= \{a^n \mid \exists m \in \mathbb{N} : n = m^2\} \\
L_3 &:= \{\mathrm{bin}(n) \mid \exists m \in \mathbb{N} : n = m^2\} \\
L_4 &:= \{a^n \mid \exists m \in \mathbb{N} : n = 2^m\} \\
L_5 &:= \{\mathrm{bin}(n) \mid \exists m \in \mathbb{N} : n = 2^m\} \\
L_6 &:= \{wcvcu \mid w, v, u \in \{a, b\}^* \wedge (w = v \vee w = u)\} \\
L_7 &:= \{a^p \mid p \text{ ist Primzahl}\}
\end{aligned}
$$

Aufgabe 3
Zeigen Sie: (Σ endliches Alphabet, $A, B, L \subseteq \{0,1\}^*$)

1. $(A \leq_m^{\mathrm{poly}} B\,) \implies (A \leq_m B\,)$
2. $(A \leq_m^{\mathrm{poly}} B \wedge B \in \mathrm{P}\,) \implies A \in \mathrm{P}$
3. $(A \leq_m^{\mathrm{poly}} B \wedge A \notin \mathrm{NP}\,) \implies B \notin \mathrm{NP}$.
4. ($A \in \mathrm{P}$ entscheidbar, $B \neq \emptyset$, $B \neq \{0,1\}^*$, dann ist $A \leq_m^{\mathrm{poly}} B$.
5. (A NP-vollständig $\wedge\, A \in \mathrm{P}\,) \implies (\mathrm{P} = \mathrm{NP})$.

Aufgabe 4
Zeigen Sie: (Σ endliches Alphabet, $A, B, L \subseteq \{0,1\}^*$, vollständig jeweils bezüglich $\leq_m^{\mathrm{poly}}$)

1. (A NP-vollständig und $A \leq_m^{\mathrm{poly}} B$ und $B \in \mathrm{NP} \implies B$ NP-vollständig.
2. Keine nichtentscheidbare Sprache ist NP-vollständig.
3. Jede nicht-triviale Sprache in P ist P-vollständig.

Aufgabe 5
Welche der Eigenschaften "reflexiv", "symmetrisch", "antisymmetrisch", "transitiv" haben die Relationen $\leq_m^{\mathrm{poly}}$ bzw. $\equiv_m^{\mathrm{poly}}$ auf der Menge aller Sprachen über dem Alphabet $\{0,1\}^*$? Beweisen Sie jeweils Ihre Antwort.

Aufgabe 6
Wir betrachten die folgenden Sprachen L_1 und L_2 ($\mathrm{bin}(n)$ bezeichnet die Binärdarstellung von n, niederwertigste Bits hinten, ohne führende Nullen)::

$$
\begin{aligned}
L_1 := \{\mathrm{bin}(n_0)c \ldots c\,\mathrm{bin}(n_k) \mid \; & k \in \mathbb{N} \quad \text{und} \\
& \forall i \in \{0, \ldots, k\} : n_i \in \mathbb{N} \;\; \text{und} \\
& \exists J \subseteq \{1, \ldots, k\} : \sum_{i \in J} n_l = n_0 \;\; \} \\
L_2 := \{\mathrm{bin}(n_0)c \ldots c\,\mathrm{bin}(n_k) \mid \; & k \in \mathbb{N} \quad \text{und} \\
& \forall i \in \{0, \ldots, k\} : n_i \in \mathbb{N} \quad \text{und} \\
& \exists J \subseteq \{0, \ldots, k\} : \sum_{i \in J} n_i = \sum_{i \in \{0,\ldots,k\} \setminus J} n_i \;\; \}
\end{aligned}
$$

1. Zeigen Sie: $L_1 \in \mathrm{NP}$ und $L_2 \in \mathrm{NP}$.
2. Zeigen Sie: $L_1 \equiv_m^{\mathrm{poly}} L_2$.

Bemerkung: Sowohl L_1 als auch L_2 sind NP-vollständig (vgl. in der Literatur: Knappsack, Partition).

Aufgabe 7
Beweisen oder widerlegen Sie die folgenden Aussagen (Σ endliches Alphabet, $A, B, L \subseteq \{0,1\}^*$):

1. co-P $=$ P .
2. $A \leq_m^{\text{poly}} B \implies B \leq_m^{\text{poly}} A$.
3. $(L \in \mathrm{P} \setminus \{\emptyset, \Sigma^*\} \wedge L' \in \mathrm{P} \setminus \{\emptyset, \Sigma^*\}) \implies L \equiv_m^{\text{poly}} L'$.

Aufgabe 8
Zeigen Sie:

1. $A \leq_m^{\text{poly}} B \iff \overline{A} \leq_m^{\text{poly}} \overline{B}$.
2. $(A \in \mathrm{NPC} \wedge \mathrm{NP} \neq \text{co-NP}) \implies (\{1\} \cdot A \cup \{2\} \cdot \overline{A} \notin \mathrm{NP} \cup \text{co-NP})$.

Aufgabe 9
Zeichen Sie ein Venn-Diagramm mit den folgenden Sprachklasssen: CFL, P, NP, co-NP, REC und RE. Tragen Sie die Sprachen $\{a^n b^n \mid n \in \mathbb{N}\}$, $\{a^n b^n c^n \mid n \in \mathbb{N}\}$ und H in dieses Venndiagramm ein.

Aufgabe 10
Zeigen Sie, dass die Klassen P und NP unter Vereinigung, Schnittbildung, Konkatenation und inverserm Homomorphismus abgeschlossen sind.

Aufgabe 11
Zeigen Sie: (Σ endliches Alphabet, $A, B, L \subseteq \{0,1\}^*$)

1. $(A \leq_m^{\text{poly}} B \wedge B \in \mathrm{NP}) \implies A \in \mathrm{NP}$.
2. $(A \leq_m^{\text{poly}} B \wedge A \notin \mathrm{P}) \implies B \notin \mathrm{P}$.
3. $A \leq_m^{\text{poly}} B \iff \overline{A} \leq_m^{\text{poly}} \overline{B}$.
4. Sind A und B NP-vollständig, so gilt $A \equiv_m^{\text{poly}} B$.
5. $(\mathrm{NPC} \cap \mathrm{P} \neq \emptyset) \implies (\mathrm{NP} = \mathrm{P})$.
6. $(\mathrm{P} = \mathrm{NP}) \implies (\mathrm{NPC} = \mathrm{P} \setminus \{\emptyset, \Sigma^*\})$.
