Strukturelle Komplexitätstheorie

Prof. Dr. Meer, Dr. Gengler

Aufgabenblatt 2

Die folgenden Aufgaben behandeln Stoff, der aus den vorhergehenden Semestern bekannt sein sollte. Gegebenenfalls sollten Sie Lücken nacharbeiten.

Aufgabe 1
Zeigen Sie, dass die beiden folgenden Aussagen äquivalent sind ($L \subseteq \Sigma^*$ und $\# \notin \Sigma$):

1. L wird von einer nichtdeterministische Turing-Maschine in Polynomialzeit erkannt.
2. Es gibt $B \in \mathrm{P}$, es gibt ein Polynom p mit $L = \{w \mid \exists y : w\#y \in B \wedge |y| \leq p(|w|)\}$

Aufgabe 2
Wir betrachten die folgenden Sprachen L_1 und L_2 ($\mathrm{bin}(n)$ bezeichnet die Binärdarstellung von n, niederwertigste Bits hinten, ohne führende Nullen):

$$L_1 := \{a^n c a^m c a^k \mid n, m, k \in \mathbb{N} \setminus \{0\} \;\wedge\; k = n \cdot m\}$$
$$L_2 := \{\mathrm{bin}(n) c\, \mathrm{bin}(m) c\, \mathrm{bin}(k) \mid n, m, k \in \mathbb{N} \setminus \{0\} \;\wedge\; k = n \cdot m\}$$

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 verworfern. (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 3
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 4
Zeigen Sie: (Σ endliches Alphabet, $A, B, L \subseteq \{0,1\}^*$)

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

Aufgabe 5
Zeigen Sie: (Σ endliches Alphabet, $A, B \subseteq \{0,1\}^*$, vollständig jeweils bezüglich $\leq_{\text{mo}}^{\text{poly}}$)

1. (A NP-vollständig und $A \leq_{\text{mo}}^{\text{poly}} B$ und $B \in \text{NP}$) $\Longrightarrow$ B NP-vollständig.
2. Keine nichtentscheidbare Sprache ist NP-vollständig.

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

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

1. Zeigen Sie: $L_1 \in \text{NP}$ und $L_2 \in \text{NP}$.
2. Zeigen Sie: $L_1 \equiv_{\text{mo}}^{\text{poly}} L_2$.

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

Aufgabe 7
Zeigen Sie:

1. $A \leq_{\text{mo}}^{\text{poly}} B \iff \overline{A} \leq_{\text{mo}}^{\text{poly}} \overline{B}$.
2. $(A \in \text{NPC} \land \text{NP} \neq \text{co-NP}) \Longrightarrow (\{1\}\cdot A \cup \{2\}\cdot \overline{A} \notin \text{NP} \ \cup\ \text{co-NP})$.