Institut für Informatik
M. Mutz

Übungsblatt 13

Theoretische Informatik

Bearbeitungszeit: 08.07.2024 bis 14.07.2024, 16:00 Uhr
Besprechung: 15.07.2024, 10:30 Uhr in Hörsaal 5E

Abgabe: als PDF über das ILIAS
Gruppenabgaben möglich und erwünscht

Aufgabe 1 ($\leq^{\mathrm{p}}_{\mathrm{m}}$-Relation)10P

Betrachten Sie die $\leq^{\mathrm{p}}_{\mathrm{m}}$-Relation aus der Vorlesung. Seien $A, B \subseteq \Sigma^*$ Mengen. Zeigen Sie die folgenden Aussagen aus der Vorlesung.

(a) $\leq^{\mathrm{p}}_{\mathrm{m}}$ ist reflexiv und transitiv, aber nicht antisymmetrisch.

(b) $A \leq^{\mathrm{p}}_{\mathrm{m}} B \Rightarrow \overline{A} \leq^{\mathrm{p}}_{\mathrm{m}} \overline{B}$.

Lösungsvorschlag:

(a) **Reflexiv:** Sei $A \subseteq \Sigma^*$, dann ist zu zeigen, dass $A \leq^{\mathrm{p}}_{\mathrm{m}} A$. Sei $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = x$. Offensichtlich ist f total und in Polynomialzeit berechenbar. Sei $i \in \mathbb{N}$. Dann ist $i \in A \Leftrightarrow f(i) = i \in A$. Somit ist $A \leq^{\mathrm{p}}_{\mathrm{m}} A$.

Transitiv: Seien $A, B, C \subseteq \Sigma^*$, dann ist zu zeigen, dass aus $A \leq^{\mathrm{p}}_{\mathrm{m}} B$ und $B \leq^{\mathrm{p}}_{\mathrm{m}} C$ folgt, dass $A \leq^{\mathrm{p}}_{\mathrm{m}} C$. Gelte also $A \leq^{\mathrm{p}}_{\mathrm{m}} B$ und $B \leq^{\mathrm{p}}_{\mathrm{m}} C$. Dann gibt es $f, g \in \mathrm{FP}$, sodass für jedes $x \in \Sigma^*$ gilt, dass $x \in A \Leftrightarrow f(x) \in B$ und $x \in B \Leftrightarrow g(x) \in C$. Sei $h : \Sigma^* \to \Sigma^*$ mit $h(x) = (g \circ f)(x) = g(f(x))$. Dann gilt $x \in A \Leftrightarrow f(x) \in B \Leftrightarrow h(x) = g(f(x)) \in C$.

Es bleibt zu zeigen, dass h total und in Polynomialzeit berechenbar ist. Ersteres ist offensichtlich. Für letzteres seien M_f und M_g Turingmaschinen, die jeweils f und g in Polynomialzeit berechnen. Dann gibt es eine Turingmaschine M_h, die h in Polynomialzeit berechnet, indem sie für Eingabe x zunächst M_f simuliert und für die Ausgabe von M_f dann M_g simuliert und dessen Ausgabe wiederum ausgibt.

Nicht antisymmetrisch: Es ist zu zeigen, dass $A, B \in \Sigma^*$ mit $A \neq B$ existieren mit $A \leq^{\mathrm{p}}_{\mathrm{m}} B$ und $B \leq^{\mathrm{p}}_{\mathrm{m}} A$. Sei $A = \{x \in \Sigma^* \mid |x| \text{ ist gerade}\}$, $B = \{x \in \Sigma^* \mid |x| \text{ ist ungerade}\}$ und $f : \Sigma^* \to \Sigma^*$ mit $f(x) = xy$ für ein $y \in \Sigma$. Offensichtlich ist f total und in Polynomialzeit berechenbar. Es gilt $A \neq B$,

$A \leq_{\mathrm{m}}^{\mathrm{p}} B$ via f und $B \leq_{\mathrm{m}}^{\mathrm{p}} A$ via f.

(b) Seien $A, B \subseteq \Sigma^*$ mit $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ via $f \in \mathrm{FP}$. Dann gilt $x \in A \Leftrightarrow f(x) \in B$. Dann gilt $x \in \overline{A} \Leftrightarrow x \notin A \Leftrightarrow f(x) \notin B \Leftrightarrow f(x) \in \overline{B}$. Somit ist $\overline{A} \leq_{\mathrm{m}}^{\mathrm{p}} \overline{B}$ via f.

Aufgabe 2 (Unentscheidbarkeitskriterium)10P

Zeigen Sie die Unentscheidbarkeit der Menge

$$L_1 = \{(w_1, w_2) \in \{0,1\}^* \times \{0,1\}^* \mid 0 \in L(M_{w_1}) \cup L(M_{w_2})\},$$

indem sie vom speziellen Halteproblem

$$K = \{w \in \{0,1\}^* \mid M_w \text{ angesetzt auf } w \text{ hält nach endlich vielen Schritten}\}$$

auf sie reduzieren.

Lösungsvorschlag:
Wir zeigen $K \leq_m L_1$. Für jedes $w \in \{0,1\}^*$ definieren wir die folgende Turingmaschine M:

Funktionsweise der Turingmaschine M für Eingabe X:
Für eine Eingabe x löscht M die Eingabe vom Band, schreibt stattdessen w darauf und simuliert M_w für Eingabe w. Dann akzeptiert M falls M_w für Eingabe w anhält.

Dann definieren wir die berechenbare und totale Funktion $f : \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^*$ durch $f(w) = (\text{code}(M), \text{code}(M))$
Es gilt für alle $w \in \{0,1\}^*$:

$$\begin{aligned}
w \in K &\Leftrightarrow M_w \text{ angesetzt auf } w \text{ hält nach endlich vielen Schritten}\\
&\Leftrightarrow f(w) = (\text{code}(M), \text{code}(M)) \text{ und } M \text{ angesetzt auf } 0 \text{ akzeptiert}\\
&\Leftrightarrow f(w) = (\text{code}(M), \text{code}(M)) \in L_1
\end{aligned}$$

Der erste Schritt folgt aus der Definition von K, der zweite aus der Definition von M und f (da M für jede Eingabe hält, falls M_w für Eingabe w anhält, also auch für Eingabe 0) und der dritte aus der Definition von L_1.

Aufgabe 3 (Wiederholung: Pumping-Lemma)10P

Zeigen Sie mit dem Pumping-Lemma für reguläre Sprachen, dass die folgenden Sprachen nicht regulär sind:

(a) $L_1 = \{\alpha \mid \alpha \text{ ist ein Palindrom}\} \subseteq \{0,1\}^*$

(b) $L_2 = \{y^k \mid y \in \{a,b\}^*, k \geq 2\} \subseteq \{a,b\}^*$

Hinweise: Achten Sie dabei auf eine gut ersichtliche Beweisstruktur (was ist zu zeigen, was wird zu einem Widerspruch geführt, etc.), darauf, dass alle Einzelschritte nachvollziehbar sind (führen Sie verwendete Regeln auf, begründen Sie, warum Sie mit diesem Wort/dieser Zahl argumentieren dürfen, welche Eigenschaften eine Variable hat, etc.), und definieren Sie alle verwendeten Variablen.

Lösungsvorschlag:

(a) Wir nehmen für einen Widerspruch an, L_1 wäre regulär. Dann existiert nach dem Pumping-Lemma für reguläre Sprachen eine Zahl $n \geq 1$, so dass für alle $x \in L_1$ mit $|x| \geq n$ eine Zerlegung $x = uvw$ existiert mit

(1) $|uv| \leq n$,

(2) $|v| \geq 1$,

(3) für alle $i \geq 0$ gilt $uv^iw \in L_2$.

Für den Widerspruch zeigen wir, dass ein $x \in L_1$ mit $|x| \geq n$ existiert, so dass für alle Zerlegungen $x = uvw$ mit (1) und (2) nicht (3) gilt.
Sei $x = 0^n10^n$. Es gelten $|x| = 2n + 1 > n$ und $x \in L_1$, da x ein Palindrom ist. Durch (1) und (2) gilt $v = 0^j$ mit $0 \leq j \leq n$. Damit gilt für $i = 2$: $uv^iw = uvvw = 0^{n+j}10^n$. Dies ist aber kein Palindrom, da wir nur eine 1 haben und dies somit die Mitte des Wortes sein müsste, aber links stehen mehr 0en als rechts, da $n + j \neq n$. Also $uv^2w \notin L_1$ Dies ist ein Widerspruch zur Annahme, also war diese falsch und es gilt $L_1 \notin \text{REG}$.

(b) Wir nehmen für einen Widerspruch an, L_2 wäre regulär. Dann existiert nach dem Pumping-Lemma für reguläre Sprachen eine Zahl $n \geq 1$, so dass für alle $x \in L_2$ mit $|x| \geq n$ eine Zerlegung $x = uvw$ existiert mit

(1) $|uv| \leq n$,

(2) $|v| \geq 1$,

(3) für alle $i \geq 0$ gilt $uv^iw \in L_2$.

Für den Widerspruch zeigen wir, dass ein $x \in L_2$ mit $|x| \geq n$ existiert, so dass für alle Zerlegungen $x = uvw$ mit (1) und (2) nicht (3) gilt.
Wähle $x = a^n b a^n b$. Es gilt $|x| = 2n + 2 > n$ und für $y = a^n b$ und $k = 2$ gilt $x \in L_2$.
Durch (1) und (2) gilt $uv = a^p$ mit $1 \leq p \leq n$. Demnach gilt $w = a^{n-p} b a^n b$. Wir benennen $u = a^\ell, \ell < p$.
Wähle $i = 0$. Es gilt $uv^0 w = a^\ell a^{n-p} b a^n b$.
Wir zeigen weiter, dass $uv^0 w \notin L_2$. Da in $uv^0 w$ genau zwei bs sind und $k \geq 2$ muss $k = 2$ gelten. Da $uv^0 w$ auf b endet, muss auch y auf b enden. Demnach muss $y = a^\ell a^{n-p} b = a^n b$ sein. Durch $\ell + n - p < n$ gilt $uv^0 w \neq y^2$ und damit $uv^0 q \notin L_2$.
Dies ist ein Widerspruch zur Annahme, also war diese falsch und es gilt $L_2 \notin$ REG.

Aufgabe 4 (Wiederholung: Pumping Lemma für kontextfreie Sprachen)5P
Zeigen Sie jeweils anhand des Pumping-Lemmas, dass die folgende Sprache nicht kontextfrei ist:

$L_1 = \{a^n \mid n \text{ ist Quadratzahl}\} \subseteq \{a\}^*$

Lösungsvorschlag:

Gegeben: Die Sprache $L_1 = \{a^n \mid n \text{ ist Quadratzahl}\}$
z.z.: L_1 ist keine kontextfreie Sprache.
Beweis: Wir zeigen $L_1 \notin$ CF durch Widespruchsbeweis. Wir nehmen an, dass L_1 eine kontextfreie Sprache ist. Sei n die Zahl, die nach dem Pumping-Lemma für kontextfreie Sprachen für L_1 existiert. Wir betrachten dann das Wort $z = a^{n^2} \in L_1$ mit $|z| = n^2 \geq n$. Nach dem Pumping-Lemma lässt sich das Wort z so zerlegen ($z = uvwxy = a^{n^2}$), dass die folgenden drei Bedingungen aus Satz 3.17 gelten:

1. $|vwx| \leq n$,
2. $|vx| \geq 1$ und
3. $(\forall i \geq 0)[uv^i wx^i y \in L_1]$.

Insbesondere gilt für $i = 2$:

$$n^2 < |uv^2 wx^2 y| = |uvwxy| + |vx| \overset{(1)}{\leq} n^2 + n < n^2 + n + (n + 1) = (n + 1)^2$$

Die Ungleichungen oben implizieren, dass die Länge von uv^2wx^2y eine Zahl zwischen n^2 und $(n+1)^2$ ist. Daraus folgt also, dass nach Definition von L_1 das Wort uv^2wx^2y kein Element von L_1 ist. Dies ist offenbar ein Widerspruch.

Aufgabe 5 (Wiederholung: Abschlusseigenschaften)5P

Zeigen Sie mit Hilfe der Abschlusseigenschaften von kontextfreien Sprachen, dass $L = \{0^m1^n \mid m, n \geq 1, n \neq m\} \subseteq \{0,1\}^*$ kontextfrei ist.

Hinweis: Sie dürfen die aus der Vorlesung bekannten Sprachen $\{0^n \mid n \geq 1\}$ und $\{0^m1^m \mid m \geq 1\}$ nutzen.

Lösungsvorschlag: Wir wissen, dass $\{a^n \mid n \geq 1\}$, $\{b^n \mid n \geq 1\}$ und $\{a^mb^m \mid m \geq 1\}$ kontextfrei sind. Durch Substitution des Alphabets und Abgeschlossenheit von CF unter Konkatenation sind also auch $\{0^n0^m1^m \mid n, m \geq 1\}$ und $\{0^m1^m1^n \mid n, m \geq 1\}$ kontextfrei. Es gilt außerdem

$$\{0^n0^m1^m \mid n, m \geq 1\} = \{0^{n+m}1^m \mid n, m \geq 1\} = \{0^p1^m \mid p, m \geq 1, p > m\}$$

und analog $\{0^m1^m1^n \mid n, m \geq 1\} = \{0^m1^p \mid m, p \geq 1, m < p\}$. Durch die Abgeschlossenheit von CF unter Vereinigung ist

$$\{0^p1^m \mid p, m \geq 1, p > m\} \cup \{0^m1^p \mid p, m \geq 1, m < p\} = \{0^m1^n \mid m, n \geq 1, n \neq m\}$$

kontextfrei.