Prof. Javier Esparza
Philipp Czerner, Kevin Kappelmann, Valentin Krasotin
Technische Universität München
Lehrstuhl für Theoretische Informatik

Einführung in die Theoretische Informatik

Sommersemester 2024 – Hausaufgabenblatt 11

- Die Aufgaben werden in folgender Reihenfolge korrigiert: H11.1, H11.2, H11.3
- Die Knobelaufgabe bitte separat auf Moodle abgeben. Sie wird korrigiert.
- $0 \in \mathbb{N}$, TMs sind deterministisch

Aufgabe H11.1. (*Downwards is the only way forwards.*) 7 Punkte

Wir betrachten folgende Probleme, für eine kontextfreie Grammatik $G = (V, \Sigma, P, S)$:

$\langle 1 \rangle$ Ist $L(G) = \Sigma^*$? $\langle 2 \rangle$ Ist $L(G) = L(G)^R$?

Von $\langle 1 \rangle$ wurde in der Vorlesung gezeigt, dass es unentscheidbar ist. Wir wollen nun die Unentscheidbarkeit von $\langle 2 \rangle$ beweisen. Reduzieren Sie also $\langle 1 \rangle$ auf $\langle 2 \rangle$. Beschreiben Sie dafür Ihre Reduktionsfunktion und beweisen, dass diese die notwendigen Eigenschaften erfüllt.

Hinweise: Zur Vereinfachung dürfen Sie $\Sigma = \{a, b\}$ für das zu reduzierenden Problem annehmen, ohne das Problem, auf das Sie reduzieren, einzuschränken.

Lösungsskizze. Wir nehmen eine Grammatik G (von $\langle 1 \rangle$) als Eingabe, und geben eine Grammatik $H = (V', \Sigma', P', S')$ (für $\langle 2 \rangle$) aus. Falls $\varepsilon \notin L(G)$ (dies ist entscheidbar), ist H eine Grammatik für die Sprache $\{ab\}$. Nun sei also $\varepsilon \in L(G)$.

Wir nehmen wie im Hinweis beschrieben an, dass G über den Alphabet $\Sigma = \{a, b\}$ definiert ist. Unsere Ausgabe H verwendet das Alphabet $\Sigma' = \{a, b, c\}$.

Weiterhin definieren wir $V' := \{S', W\} \cup V$ (fügen also Variablen S', W hinzu), und die Produktionen P' als

$$\begin{aligned} S' &\to cS \mid Wc \\ X &\to \alpha \qquad\qquad \text{für } (X \to \alpha) \in P \\ W &\to aW \mid bW \mid \varepsilon \end{aligned}$$

Es gilt also $L(H) = \{c\}L(G) \cup \Sigma^*\{c\}$.

Nun zeigen wir die Korrektheit der Reduktion. Wenn $L(G) = \Sigma^*$, folgt $L(H) = \{c\}\Sigma^* \cup \Sigma^*\{c\} = L(H)^R$. Falls $L(G) \neq \Sigma^*$, dann gibt es ein $w \in \Sigma^* \setminus L(G)$. Insbesondere erhalten wir $cw \notin \{c\}L(G)$. Nach unserer Annahme gilt nun $w \neq \varepsilon$, woraus $cw \notin \Sigma^*\{c\}$ und schließlich $cw \notin L(H)$ folgt. Aber $cw \in \{c\}\Sigma^* \subseteq L(H)^R$ gilt, und somit $L(H) \neq L(H)^R$.

Aufgabe H11.2. (*The line must be drawn here! This far, no further!*) 10 Punkte

Zum Geburtstag hat Theo eine k-Band-Turingmaschine geschenkt bekommen. Er ist sich aber nicht sicher, ob er sie laufen lassen soll – dies könnte ja sehr lange dauern, und eigentlich wollte er noch den Schnecken beim Kriechen zuschauen. Können Sie ihm helfen?

Wir nennen eine k-Band-TM $(+1)$-zeitbeschränkt, wenn sie für alle Eingaben mit Länge n innerhalb von $n + 1$ Schritten hält. (Beachten Sie, dass n variabel ist.) Zeigen Sie, dass die Sprache

$$L := \{w \in \{0, 1\}^* : M_w \text{ ist } (+1)\text{-zeitbeschränkt}\}$$

unentscheidbar ist.

Hinweise: Reduzieren sie von $\overline{\mathcal{H}_0}$ (dem Komplement des Halteproblems auf leerem Band). Beachten Sie, dass $\mathcal{H}_0$ nur 1-Band-TMs kodiert. Die Eingabe einer k-Band-TM steht auf dem ersten Band, die anderen Bänder sind am Anfang leer.

Lösungsskizze. Sei $\mathcal{H}_0$ das Halteproblem auf leerem Band und $\overline{\mathcal{H}_0}$ sein Komplement. Dann ist $\overline{\mathcal{H}_0}$ unentscheidbar, und wir zeigen nun $\overline{\mathcal{H}_0} \leq L$.

Sei M eine beliebige 1-Band-TM über dem Alphabet $\{0, 1\}$. Wir müssen nun also eine k-Band-TM M' konstruieren, die genau dann $(+1)$-zeitbeschränkt ist, wenn M auf dem leeren Band *nicht* hält.

Dafür konstruieren wir M' als die 2-Band-TM, die M auf dem zweiten Band ausführt. Bei jedem Schritt, den M macht, löscht M' dabei ein Zeichen der Eingabe. Falls M' so das letzte Zeichen der Eingabe löscht, hält M' (1). Falls M vorher terminiert, geht M' stattdessen in eine Endlosschleife (2).

Nun gibt es zwei Möglichkeiten. Wenn M auf dem leeren Band nicht hält, kann (2) nicht eintreten, und M' wird auf einer Eingabe der Länge n innerhalb von $n+1$ Schritten halten, ist also $(+1)$-zeitbeschränkt.

Falls doch, dann gibt es ein n, sodass M auf dem leeren Band in n Schritten hält. Nun können wir M' auf einer Eingabe mit Länge n ausführen, und nach (2) geht M' in eine Endlosschleife – somit ist M' nicht $(+1)$-zeitbeschränkt.

Quizaufgabe H11.3. (*Do or do not. There is no try.*) unkorrigiert (8 Punkte)

Dr. Evilsparza hat sich auf eine Stelle an der Technischen Hochschule Estlingen-Oberfeld beworben, und könnte bald Prof. Evilsparza sein. Um dies zu verhindern, versuchen Sie, ihn vor der Auswahlkommission bloßzustellen, indem Sie seine Ausführungen zur Unentscheidbarkeit als falsch entlarven.

Sei $\Sigma := \{0, 1\}$. Bestimmen Sie jeweils, ob folgende Aussagen wahr sind. Falls ja, geben Sie eine *kurze* Begründung an, ansonsten ein Gegenbeispiel.

(a) Sei $L \subseteq \Sigma^*$ unentscheidbar und $w \in L$. Dann ist $\{v : M_w[v]\downarrow\}$ unentscheidbar.

(b) Für zwei unentscheidbare Sprachen $L_1, L_2 \subseteq \Sigma^*$ ist $L_1 \cup L_2$ unentscheidbar.

(c) Sei $f : \mathbb{N} \to \mathbb{N}$ total, berechenbar und bijektiv. Dann ist f^{-1} berechenbar.

(d) Für beliebige TMs M_1, M_2 ist die Sprache $L(M_1) \setminus L(M_2)$ semi-entscheidbar.

(e) Sei $L \subseteq \Sigma^*$ unendlich. Dann gibt es eine unentscheidbare Sprache $L' \subseteq L$.

Hinweis: Bitte beachten Sie, dass nach Definition $L(M)$, für eine TM M, die Sprache der Wörter ist, auf denen M in einem Haltezustand terminiert. Insbesondere ist $L(M)$ semi-entscheidbar, aber nicht unbedingt entscheidbar.

Lösungsskizze.

(a) Falsch. Sei L eine beliebige unentscheidbare Sprache (z.B. $\mathcal{H}_0$) und w die Kodierung einer TM, die nie hält (also $L(M_w) = \emptyset$). Dann ist $L \cup \{w\}$ immer noch unentscheidbar, aber $\{v : M_w[v]\downarrow\} = \emptyset$ ist entscheidbar.

(b) Falsch. Sei L_1 eine beliebige unentscheidbare Sprache, zum Beispiel das Halteproblem auf leerem Band. Dann ist das Komplement $L_2 := \overline{L_1}$ ebenfalls unentscheidbar (Fakt 5.29). Es gilt $L_1 \cup L_2 = \Sigma^*$, aber Σ^* ist entscheidbar.

(c) Wahr. Um $f^{-1}(y)$ zu berechnen, gehen wir alle möglichen $x \in \mathbb{N}$ durch und überprüfen, ob $f(x) = y$ gilt. Da f berechenbar ist, können wir dies machen, und da f bijektiv ist, terminiert die Suche mit einem x, das wir ausgeben.

(d) Falsch. Wähle $L(M_1) = \Sigma^*$ und $L(M_2) = \mathcal{H}_0$, das Halteproblem auf leerem Band. Diese sind beide semi-entscheidbar, daher gibt es TMs für diese Sprachen. Nun ist $L(M_1) \setminus L(M_2)$ das Komplement des Halteproblems und damit nicht semi-entscheidbar. Denn sonst wären sowohl $\mathcal{H}_0$ als auch das Komplement semi-entscheidbar und damit $\mathcal{H}_0$ entscheidbar (Satz 5.42).

(e) Wahr. Da $L \subset \Sigma^*$ ist L abzählbar. Wähle also eine Bijektion $\mathbb{N} \to L$. Die Anzahl möglicher Wahlen von L' ist die Anzahl möglicher Funktionen $\mathbb{N} \to \{0, 1\}$ (wir können für jede Nummer eines Elements von L wählen ob das Element in L' ist). Dies ist überabzählbar. Da es aber nur abzählbar viele TMs gibt, muss eine unentscheidbare Sprache enthalten sein.

Knobelaufgabe H11.4. (*No one can be told what The Matrix is.*)

Doras Urgroßonkel, der Rektor der Technischen Hochschule Estlingen-Oberfeld, hat Geburtstag, und die ganze Familie ist eingeladen. Nach altem Estlinger Brauch gibt es statt Kerzen auf einer Geburtstagstorte einen Vektor mit dem Alter, und statt zu pusten wird dieser Vektor so lange mit Matrizen multipliziert, bis er verschwunden ist. (Die Matrizen werden von den Gästen mitgebracht.) Leider hat Doras Urgroßonkel es dieses Jahr nicht geschafft, seinen Altersvektor wegzumultiplizieren, obwohl er sich viel Mühe gegeben hat. Dora möchte ihn nun trösten, und ihm beweisen, dass das Problem nicht immer gelöst werden kann.

Wir untersuchen nun das Vektorvernichtungsproblem (VVP):

Eingabe: Matrizen $M_1, ..., M_k \in \mathbb{Z}^{3\times 3}$, Vektor $v \in \mathbb{Z}^3$
Ausgabe: Existieren $A_1, ..., A_l \in \{M_1, ..., M_k\}$ mit $A_1 A_2 \cdots A_l v = 0$?

Unser Ziel ist, zu zeigen, dass das VVP unentscheidbar ist.

(a) Sei $M := \begin{pmatrix} 0 & v & -v \end{pmatrix}$, mit $v \in \mathbb{Z}^3$, und $M_1, ..., M_k \in \mathbb{Z}^{3\times 3}$, wobei $M_1, ..., M_k$ invertierbar sind. Zeigen Sie, dass das VVP für $M, M_1, ..., M_k; v$ genau dann eine Lösung hat, wenn es $A_1, ..., A_l \in \{M_1, ..., M_k\}$ gibt, sodass $M A_1 A_2 \cdots A_l v = 0$.

(b) Zeigen Sie nun, dass das VVP unentscheidbar ist, indem sie 01-MPCP reduzieren.[1]

Lösungsskizze. **(a)** Wir zeigen beide Richtungen, wobei „⇐“ allerdings trivial ist. Für „⇒“ sei nun $B_0, ..., B_l \in \{M, M_1, ..., M_k\}$ eine Lösung des VVP für $M, M_1, ..., M_k; v$. Wir wählen eine kürzeste Lösung, also eine mit minimalem l. Es gibt nun folgende Fälle.

- $B_0 \in \{M_1, ..., M_k\}$: Sei $x := B_1 \cdots B_l v$. Wenn $x = 0$ wäre l nicht minimal, also gilt $x \neq 0$. Da B_0 invertierbar ist, muss aber $B_0 x \neq 0$ gelten, ein Widerspruch dazu, das $B_0, ..., B_l$ eine Lösung des VVP ist. Dieser Fall kann also gar nicht auftreten.
- $\exists i > 0 : B_i = M$: Sei $x := B_i \cdots B_l v$. Es muss wieder $x \neq 0$ gelten, da sonst $B_i, ..., B_l$ eine kürzere Lösung wäre. Da $B_i = M$, muss aber $x = \alpha v$ gelten, für ein $\alpha \in \mathbb{R}$, $\alpha \neq 0$. Dies folgt aus der Beobachtung, dass für jeden Vektor $y = (y_1, y_2, y_3)^\top \in \mathbb{R}^3$ gilt, dass $My = v(y_2 - y_3)$. Es gilt:

  $$B_0 \cdots B_l v = 0 \;\Rightarrow\; B_0 \cdots B_{i-1} x = 0 \;\Rightarrow\; B_0 \cdots B_{i-1}(\tfrac{1}{\alpha} x) = 0$$

  Aber $\frac{1}{\alpha} x = v$, also wäre $B_0, ..., B_{i-1}$ eine kürzere Lösung und dieser Fall kann ebenfalls nicht eintreten.

[1] Wir haben zwar nicht explizit in der Vorlesung gezeigt, dass 01-MPCP unentscheidbar ist, aber der Beweis von Korollar 5.59 funktioniert unverändert.

- $B_0 = M$ und $B_1, ..., B_l \in \{M_1, ..., M_k\}$: Dies ist genau die Aussage, die wir zeigen wollen, und wir sind fertig.

(b) Wir verwenden Zahlen, um Wörter darzustellen. Sei also $\Sigma := \{0, 1\}$ und $f : \Sigma^* \to \mathbb{N}$ definiert als $f(\varepsilon) := 0$ und $f(wc) := 3f(w) + c + 1$ für $w \in \Sigma^*$, $c \in \Sigma$. Insbesondere gilt somit $f(u) = f(v) \Leftrightarrow u = v$ für alle $u, v \in \Sigma^*$.

Nach Definition von f folgt $f(ux) = f(u) \cdot 3^{|x|} + f(x)$, da f Zeichen an die Basis-3 Darstellung der Zahl anhängt. Um sicher zu gehen, zeigen wir diese Aussage kurz per Induktion über $n := |x|$.

Die Basis $x = \varepsilon$ ist klar. Für den Induktionsschritt fixieren wir ein n und nehmen $f(ux) = f(u) \cdot 3^{|x|} + f(x)$ für alle $u, x \in \Sigma^*$ mit $|x| = n$ an. Für beliebige $u, x \in \Sigma^*$ mit $x = rc$ für ein $r \in \Sigma^*$ und $c \in \Sigma$ gilt nun

$$\begin{aligned} f(ux) = f(urc) &\overset{f}{=} 3f(ur) + c + 1 \overset{\text{IA}}{=} 3(f(u) \cdot 3^{|r|} + f(r)) + c + 1 \\ &= f(u) \cdot 3^{|r|+1} + 3f(r) + c + 1 \overset{f}{=} f(u) \cdot 3^{|rc|} + f(rc) = f(u) \cdot 3^{|x|} + f(x) \end{aligned}$$

Seien $x, y \in \Sigma^*$ beliebig. Wir konstruieren nun eine Matrix $M_{x,y} \in \mathbb{Z}^{3\times 3}$ mit

$$M_{x,y} \begin{pmatrix} 1 \\ f(u) \\ f(v) \end{pmatrix} = \begin{pmatrix} 1 \\ f(ux) \\ f(vy) \end{pmatrix} \qquad \text{für alle } u, v \in \Sigma^*.$$

Dazu wählen wir

$$M_{x,y} := \begin{pmatrix} 1 & 0 & 0 \\ f(x) & 3^{|x|} & 0 \\ f(y) & 0 & 3^{|y|} \end{pmatrix}$$

Wir reduzieren von 01-MPCP und erhalten somit Wörter $x_1, ..., x_k, y_1, ..., y_k \in \{0, 1\}^*$ als Eingabe. Unsere Reduktion konstruiert die Instanz $M, M_1, ..., M_k; v$ des VVPs, mit $M_i := M_{x_k,y_k}$ (wie in (b) definiert) und $v := (1, f(x_1), f(y_1))^\top$. Nun zeigen wir, dass die Reduktion korrekt ist, also „MPCP lösbar“ $\Leftrightarrow$ „VVP lösbar“.

„$\Rightarrow$“: Sei $i_1, ..., i_n \in \{1, ..., k\}$ eine Lösung des MPCP, es gilt somit $i_1 = 1$. Wir behaupten nun, dass $M, M_{i_n}, ..., M_{i_2}$ eine Lösung des VVPs ist. Es gilt

$$\begin{aligned} &MM_{i_n} \cdots M_{i_3} M_{i_2} v \\ &\quad = MM_{i_n} \cdots M_{i_3} M_{i_2} \begin{pmatrix} 1 \\ f(x_{i_1}) \\ f(y_{i_1}) \end{pmatrix} \overset{(b)}{=} MM_{i_n} \cdots M_{i_3} \begin{pmatrix} 1 \\ f(x_{i_1}x_{i_2}) \\ f(y_{i_1}y_{i_2}) \end{pmatrix} \\ &\quad = ... = M \begin{pmatrix} 1 \\ f(x_{i_1}...x_{i_n}) \\ f(y_{i_1}...y_{i_n}) \end{pmatrix} = (f(x_{i_1}...x_{i_n}) - f(y_{i_1}...y_{i_n}))v \overset{(*)}{=} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \end{aligned}$$

Für $(*)$ verwenden wir, dass $i_1, ..., i_n \in \{1, ..., k\}$ eine Lösung des MPCPs ist und somit $x_{i_1}...x_{i_n} = y_{i_1}...y_{i_n}$ gilt.

„$\Leftarrow$“: Da $\det(M_{x,y}) = 3^{|x|+|y|} \neq 0$ für $x, y \in \Sigma^*$, können wir die Aussage der (a) anwenden, und es existiert eine Lösung der Form $M, M_{i_n}, ..., M_{i_2}$ mit $i_2, ..., i_n \in \{1, ..., k\}$. Wie wir für den anderen Fall bereits argumentiert haben, gilt

$$MM_{i_n} \cdots M_{i_2} v = \begin{pmatrix} f(x_{i_1}...x_{i_n}) - f(y_{i_1}...y_{i_n}) \\ 0 \\ 0 \end{pmatrix}$$

wobei wir $i_1 := 1$ setzen. Da $M, M_{i_n}, ..., M_{i_2}$ eine Lösung des VVPs ist, muss die linke Seite 0 sein. Somit folgt direkt $f(x_{i_1}...x_{i_n}) = f(y_{i_1}...y_{i_n})$ und schließlich, wie nach der Definition von f angemerkt, $x_{i_1}...x_{i_n} = y_{i_1}...y_{i_n}$. Folglich ist $i_1, ..., i_n$ eine Lösung des MPCP, mit $i_1 = 1$.