Prof. Javier Esparza
Philipp Czerner, Martin Helfrich
Technische Universität München
Lehrstuhl für Theoretische Informatik

Einführung in die Theoretische Informatik

Sommersemester 2021 – Hausaufgabenblatt 11

- Sei $\Phi := \{\{1\}, \{2\}, \{3, 4\}\}$. Nach dem Abgabedatum werden wir für jede Menge $A \in \Phi$ eine zufällige Aufgabe $a \in A$ wählen und korrigieren.
- Wenn Sie einen Beweis aufstellen, von dem Sie wissen, das einzelne Schritte problematisch oder unvollständig sind, merken Sie dies bitte in Ihrer Lösung an, damit wir das bei der Korrektur positiv berücksichtigen können.
- $0 \in \mathbb{N}$, TMs sind deterministisch

Aufgabe H11.1. (*Do or do not. There is no try.*) 0.5+0.5+0.5+0.5+1 Punkte

Sei $\Sigma := \{0, 1\}$. Entscheiden 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 definiert als das universelle Halteproblem vom letzten Übungsblatt. Dann ist L unentscheidbar, aber $\{v : M_w[v]\downarrow\} = \Sigma^*$ ist entscheidbar, für jedes $w \in L$. (Ein einziges w würde bereits reichen, damit die Aussage falsch ist.)

(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.

Aufgabe H11.2. (*The line must be drawn here! This far, no further!*) 4 Punkte

Wir nennen eine TM $2n$-platzbeschränkt, wenn sie für alle Eingaben mit Länge n den Lesekopf nicht weiter als $2n$ Felder vom Ursprung entfernt. Zeigen Sie, dass L unentscheidbar ist, mit

$$L := \{w \in \{0,1\}^* : M_w \text{ ist } 2n\text{-platzbeschränkt}\}$$

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 TM über dem Alphabet $\{0,1\}$. Unsere Reduktion muss also M so ändern, dass die neue TM M' *nicht* $2n$-platzbeschränkt ist, gdw. M auf leerem Band hält. Unsere neue TM M' geht wie folgt vor:

1. Platziere Markierungen links und rechts von der Eingabe, lösche alles zwischen den Markierungen, und gehe in die Mitte der Eingabe.
2. Führe M aus. Falls der Kopf eine der Markierungen betritt, terminiere.
3. Falls M terminiert (ohne eine der Markierungen betreten zu haben), laufe in einer Schleife nach rechts.

Die Idee ist also, dass M' darauf achtet, immer platzbeschränkt zu sein. Die einzige Ausnahme ist, wenn M terminiert – dann bricht M' „absichtlich“ die Platzbeschränkung.

Wir argumentieren nun die Korrektheit der Reduktion, also $M \notin \mathcal{H}_0 \Leftrightarrow M' \in L$.

„⇒“: Wenn M auf der leeren Eingabe nicht terminiert, kann M' nie die Platzbeschränkung verletzten, und $M' \in L$ folgt.

„⇐“: Wir nehmen nun $M \in \mathcal{H}_0$ an. Insbesondere macht M auf der leeren Eingabe nur endlich viele Schritte, und es gibt ein $k \in \mathbb{N}$, sodass M sich hierbei nicht weiter als k Felder vom Ursprung entfernt. Wir führen nun M' auf Eingabe 1^{2k} aus. Da M sich nicht weiter als k Felder vom Ursprung entfernt, wird M' in Schritt 2. nie eine der Markierungen erreichen, und M terminiert. Damit ist M' aber auf dieser Eingabe nicht platzbeschränkt, und $M' \notin L$ folgt.

Aufgabe H11.3. (*Downwards is the only way forwards.*) 2+3 Punkte

In der Vorlesung haben wir folgende Probleme für kontextfreie Grammatiken G_1, G_2 über einem Alphabet Σ kennengelernt:

⟨1⟩ Ist $L(G_1) \cap L(G_2) = \emptyset$?

⟨2⟩ Ist $|L(G_1) \cap L(G_2)| < \infty$?

⟨3⟩ Ist $L(G_1) \cap L(G_2)$ kontextfrei?

⟨4⟩ Ist $L(G_1) \subseteq L(G_2)$?

⟨5⟩ Ist $L(G_1) = L(G_2)$?

Von ⟨1⟩ wurde in der Vorlesung gezeigt, dass es unentscheidbar ist, ⟨2⟩ und ⟨3⟩ werden in der Übung behandelt. Es verbleiben ⟨4⟩ und ⟨5⟩, zeigen Sie also:

(a) $\langle 4\rangle \leq \langle 5\rangle$

(b) $\langle 1\rangle \leq \langle 4\rangle$

Hinweise: Zur Vereinfachung dürfen Sie $\Sigma = \{a, b\}$ jeweils für das zu reduzierenden Problem annehmen (ohne das Problem, auf das Sie reduzieren, einzuschränken). Für die (b) mag es sinnvoll sein, die Sprache $L(G_1)\{\$\}L(G_2)^R$ zu betrachten.

Lösungsskizze. Wie im Hinweis nehmen wir $\Sigma = \{a, b\}$ entsprechend an. In beiden Fällen bildet unsere Reduktion die Eingabe G_1, G_2 auf G_1', G_2' ab, wobei letzteres die Eingabe für das Problem ist, auf das wir reduzieren.

(a) Hier konstruieren wir G_1' so, dass $L(G_1') = L(G_1) \cup L(G_2)$, und $G_2' := G_2$. Dann gilt

$$L(G_1') = L(G_2') \Leftrightarrow L(G_1) \cup L(G_2) = L(G_2) \Leftrightarrow L(G_1) \subseteq L(G_2)$$

(b) Unsere Reduktion konstruiert G_1' entsprechend dem Hinweis, also gilt $L(G_1') = L(G_1)\{\$\}L(G_2)^R$. Dies ist möglich, da wir CFGs sowohl konkatenieren als auch umdrehen können. Die Sprache $L := \{w\$w^R : w \in \Sigma^*\}$ ist deterministisch kontextfrei (siehe Beispiel 4.61), also ist auch ihr Komplement kontextfrei (Satz 4.66). Wir wählen also ein G_2' mit $L(G_2') = \overline{L}$.

Es gilt

$$L(G_1') \subseteq L(G_2') \Leftrightarrow L(G_1') \subseteq \overline{L} \Leftrightarrow L(G_1') \cap L = \emptyset$$

und

$$\begin{aligned} L(G_1') \cap L &= L(G_1)\{\$\}L(G_2)^R \cap \{w\$w^R : w \in \Sigma^*\} \\ &= \{w\$w^R : w \in L(G_1), w^R \in L(G_2)^R\} \\ &= \{w\$w^R : w \in L(G_1) \cap L(G_2)\} \end{aligned}$$

Offensichtlich gilt nun $L(G_1') \cap L = \emptyset$ genau dann, wenn $L(G_1) \cap L(G_2) = \emptyset$.

Anmerkung: Statt $\overline{L}$ kann man auch die Sprache $\{u\$v : u, v \in \Sigma^*, u \neq v^R\}$ verwenden. Die ist ebenfalls kontextfrei und wird z.B. von folgender Grammatik erzeugt:

$$\begin{aligned} &S \to aSa \mid bSb \mid aTb \mid bTa \mid CP \mid QC \\ &T \to CTC \mid \$ \\ &P \to CP \mid CPC \mid \$ \\ &Q \to QC \mid CQC \mid \$ \\ &C \to a \mid b \end{aligned}$$

Aufgabe H11.4. (*No one can be told what The Matrix is.*) 1+1+3 Punkte

Doras Urgroßonkel, der ehemalige Rektor der TH 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 (er ist $(100)_7$ geworden), 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 $M A_1 A_2 \cdots A_l v = 0$.

Wir verwenden wieder 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 $u, v \in \Sigma^*$.

(b) Seien $x, y \in \Sigma^*$ beliebig. Konstruieren Sie eine Matrix $M_{x,y} \in \mathbb{Z}^{3\times 3}$ mit

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

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

Erinnerung: Sei $M \in \mathbb{R}^{3\times 3}$. Folgende Aussagen sind äquivalent:

(1) M ist invertierbar

(2) $\det(M) \neq 0$

(3) $Mx \neq 0$ für alle $x \in \mathbb{R}^3 \setminus \{0\}$

Lösungsskizze. **(a)** Wir zeigen beide Richtungen, wobei „$\Leftarrow$“ allerdings trivial ist. Für „$\Rightarrow$“ 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.
- $B_0 = M$ und $B_1, ..., B_l \in \{M_1, ..., M_k\}$: Dies ist genau die Aussage, die wir zeigen wollen, und wir sind fertig.

(b) 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

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

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

Unsere Matrix ist nun folgende:

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

(c) 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

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

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 $i_1 = 1$.