Lösungsvorschlag Arbeitsheft 1

1 Der Rice Trick

a)

Zuerst baut man eine TM M' aus M und M_2, welche bei Eingabe $x \in \Sigma^*$ mithilfe der Universellen TM dann M bei Eingabe ε simuliert und darauf, falls dieser Vorgang terminiert, die TM M_2 bei Eingabe x simuliert und dessen Ausgabe übernimmt. Da hier $\langle M \rangle, \langle M_2 \rangle$ beim Bau von M' schon feststehen, kann man diese als Konstanten in $\langle M' \rangle$ speichern. Dann ist M' letztendlich nur die Universelle TM, mit einem Unterprogramm, welches nach der ersten Simulation alle Bänder löscht und die Simulation von M_2 auf x vorbereitet.

Die TM M'' sei nun als 2-Band-TM aufgefasst, wobei man auf Band 1 eben M_1 auf der Eingabe simuliert, und auf Band2 eben M' auf der Eingabe parallel simuliert. Diese Parallelität kann mit einer Art Produktkonstruktion der DFA's von M_1 und M' geschehen, welche dann auf dem Zustandsraum $Q_{M_1} \times Q_{M'}$ arbeitet und eine entsprechend angepasste Übergangsfunktion besitzt.

Schließlich können wir M^+ als Simulation von M'' ansehen, wobei wir zwischen jedem Simulationsschritt die Akzeptanz von M_1 und M' überprüfen.

b)

Durch $\langle M \rangle \in H_\varepsilon$ wird M' stets terminieren. Wenn also die Eingabe $x \in \Sigma^*$ nicht in L_1 ist, so wird trotzdem nach endlicher Zeit noch $x \in L_2$ geprüft. Es gilt also

$$\langle M \rangle \in H_\varepsilon \implies L(M^+) = L_1 \cup L_2$$

c)

Durch $\langle M \rangle \notin H_\varepsilon$ wird M' niemals dazu kommen, $x \in L_2$ für die Eingabe $x \in \Sigma^*$ zu überprüfen. Es folgt

$$\langle M \rangle \notin H_\varepsilon \implies L(M^+) = L_1$$

d) Aus den beiden obigen Fällen folgt mit $L_1 = \varnothing$ gut und L_2 schlecht sofort, dass

$$\langle M \rangle \in H_\varepsilon \implies L(M^+) = L_1 \cup L_2 = L_2 \implies \langle M^+ \rangle \notin L_{\mathcal{E}}$$

sowie dass

$$\langle M \rangle \notin H_\varepsilon \implies L(M^+) = L_1 = \varnothing \implies \langle M^+ \rangle \in L_{\mathcal{E}}$$

Folglich akzeptiert $T(\mathcal{E})$ die Gödelnummer $\langle M^+ \rangle$ **genau dann**, wenn $\langle M \rangle \notin H_\varepsilon$.

e)

Gäbe es eine solche TM $T(\mathcal{E})$, so könnte man mit dieser als Unterprogramm H_ε entscheiden, indem man zu den festen $\langle M_1 \rangle, \langle M_2 \rangle$ mit den beschriebenen Eigenschaften und gegebener Eingabe $\langle M \rangle$ die TM $\langle M^+ \rangle$ konstruiert und das Akzeptanzverhalten von $T(\mathcal{E})$ auf $\langle M^+ \rangle$ invertiert.

f)

Was wir von den Sprachen L_1, L_2 benötigen, damit die Argumentation so bestehen kann, ist, dass genau eine der Sprachen L_1 und $L_1 \cup L_2$ gut ist. Wenn also L_1 schlecht ist, so benötigen wir nur eine gute Sprache L_2. Wenn wir nun M^+ zu diesen so wie zuvor konstruieren haben wir analog zu d), dass

$$\langle M \rangle \in H_\varepsilon \iff \langle M^+ \rangle \in L_\mathcal{E}$$

also dass wir wie in e) beschrieben H_ε entscheiden können (nur diesmal ohne das Akzeptanzverhalten von $T(\mathcal{E})$ zu invertieren).

g)

Dies ist analog zu d), da wenn $\langle M \rangle \notin H_\varepsilon$, die TM M' aus der Konstruktion von M^+ (siehe a)) niemals halten wird, also M^+ genau L_1 entscheidet. Damit $\langle M^+ \rangle \in L_\mathcal{E}$, $T(\mathcal{E})$ akzeptiert $\langle M^+ \rangle$.

h)

Ebenfalls analog zu d) und g), da wenn $\langle M \rangle \in H_\varepsilon$ dann M^+ genau $L_1 \cup L_2 = L_2$ entscheidet, also $\langle M^+ \rangle \notin L_\mathcal{E}$ und $T(\mathcal{E})$ akzeptiert $\langle M^+ \rangle$ nicht.

i)

Aus g) und h) folgt, dass für eine feste TM A mit $\langle A \rangle \in L_\mathcal{E}$ nun

$$f : \Sigma^* \to \Sigma^*, w \mapsto \begin{cases} \langle M^+ \rangle & , w = \langle M \rangle \text{ für eine TM } M \\ \langle A \rangle & , w \text{ keine Gödelnummer} \end{cases}$$

eine (berechenbare!) Reduktion $\overline{H_\varepsilon} \leq L_\mathcal{E}$ darstellt. Denn wenn $w \in \Sigma^*$ keine Gödelnummer ist, so ist schonmal $w \in \overline{H_\varepsilon}$ und $f(w) = \langle A \rangle \in L_\mathcal{E}$. Ist $w = \langle M \rangle$ für eine TM M, so ist nach g) und h) nun

$$f(w) = \langle M^+ \rangle \in L_\mathcal{E} \iff w \in \overline{H_\varepsilon}$$

Damit haben wir also eine korrekte Reduktion $\overline{H_\varepsilon} \leq L_\mathcal{E}$. Der Widerspruch ergibt sich, durch die Annahme, dass $L(\mathcal{E})$ rekursiv aufzählbar ist. Denn dann wäre auch $\overline{H_\varepsilon}$ rekursiv aufzählbar, und da nach VL schon H_ε rekursiv aufzählbar ist, wäre dann H_ε entscheidbar.

j) Die 8 nicht-rekursiv-aufzählbaren Mengen, für die das Werkzeug benutzbar ist:

1. $\{\langle M\rangle \mid L(M) = \varnothing\}$ mit $\varnothing = L_1 \subseteq L_2 = \Sigma^*$
2. $\{\langle M\rangle \mid \varepsilon \notin L(M)\}$ mit $\varnothing = L_1 \subseteq L_2 = \Sigma^*$
3. $\{\langle M\rangle \mid L(M)$ regulär$\}$ mit $\varnothing = L_1 \subseteq L_2 = \{0^n 1^n \mid n \in \mathbb{N}\}$ kontextfrei also rek. aufzählbar
4. $\{\langle M\rangle \mid L(M)$ nicht regulär$\}$ mit $\{0^n 1^n \mid n \in \mathbb{N}\} = L_1 \subseteq L_2 = \Sigma^*$
5. $\{\langle M\rangle \mid L(M)$ rekursiv$\}$ mit $\varnothing = L_1 \subseteq L_2 = H_\varepsilon$
6. $\{\langle M\rangle \mid L(M)$ nicht rekursiv$\}$ mit $H_\varepsilon = L_1 \subseteq L_2 = \Sigma^*$
7. $\{\langle M\rangle \mid |L(M)| = 1\}$ mit $\{0\} = L_1 \subseteq L_2 = \{0, 1\}$
8. $\{\langle M\rangle \mid |L(M)| \leq 3\}$ mit $\varnothing = L_1 \subseteq L_2 = \{0, 1, 00, 11\}$

k)

Das ist analog zu d), f), g) und h). Mit $\langle M\rangle \in H_\varepsilon$ folgt $L(\langle M^+\rangle) = L_1 \cup L_2 = L_2$, also $\langle M^+\rangle \in L_\mathcal{E}$ da L_2 nun gut ist. Ebenso ist mit $\langle M\rangle \notin H_\varepsilon$ dann $L(\langle M^+\rangle) = L_1$, also $\langle M^+\rangle \notin L_\mathcal{E}$, da L_1 hier schlecht. Damit folgt die Behauptung.

l)

Mit analoger Argumentation zu i) erhält man eine Reduktion $H_\varepsilon \leq L_\mathcal{E}$. Da wir bereits aus der VL wissen, dass H_ε rekursiv aufzählbar ist, gibt es hier keinen Widerspruch.

m)

Wir zeigen die rekursive Aufzählbarkeit von $L := \{\langle M\rangle \mid L(M) \neq \varnothing\}$.

Wie im Beweis dass semi-entscheidbare Sprachen rekursiv aufzählbar sind (VL 6) können wir zu einer Eingabe nach einem Syntaxcheck in "Runden" arbeiten; Da die Eingabe nun in der Form $\langle M\rangle$ ist, können wir in der i-ten Runde M auf den ersten i Worten der kanonischen Aufzählung von $\{0, 1\}^*$ für jeweils i Schritte simulieren. Dies führen wir für jedes $i \in \mathbb{N}$ durch und akzeptieren sobald eines der Worte von M akzeptiert wird.

Wenn nun $L(M) \neq \varnothing$, so existieren $w \in \{0, 1\}^*$ und $j, k \in \mathbb{N}$ sodass $w = w_j$ und w von M in k Schritten akzeptiert wird. Damit wird w von M in der $i = \max(j, k)$-ten Runde akzeptiert und wir akzeptieren $\langle M\rangle$.

Andererseits wird es kein Wort geben welches von M akzeptiert wird, sodass wir Berechnung für ewig weiterläuft, also $\langle M\rangle$ auch nicht akzeptiert wird.

Damit ist also L rekursiv aufzählbar. Die gesuchten Sprachen sind bspw. $L_1 = \varnothing, L_2 = \{0\}$.

2 Ein weiterer Rice Trick

a)

Ähnlich wie in der a) vom letzten Kapitel baut man eine Art Produktkonstruktion welche auf 2 Bändern parallel arbeitet. Dabei wird auf Band 1 eine Universelle TM, welche M_4 auf der Eingabe x simuliert, ausgeführt und auf Band 2 eine modifizierte Universelle TM, welche M für $|x|$ Schritte auf ε simuliert, ausgeführt. Da wir nicht frühzeitig abbrechen müssen, können wir hier akzeptieren, sobald beide "Unterprogramme" akzeptiert haben (wobei die 2. Berechnung eben akzeptiert, wenn der Endzustand von M nicht erreicht wird).

b)

Im Fall $\langle M\rangle \notin H_\varepsilon$ wird die zweite Berechnung nie den Endzustand von M erreichen, sodass wir nur die Akzeptanz der ersten Berechnung, welche $x \in L_4$ überprüft, benötigen, um zu akzeptieren. Es gilt also

$$\langle M\rangle \notin H_\varepsilon \implies L(M^{++}) = L_4$$

c)

Im Fall $\langle M\rangle \in H_\varepsilon$ wird M auf ε in $k \in \mathbb{N}$ Schritten halten. Folglich haben wir für Eingaben $x \in \Sigma^*$ mit $|x| < k$ das Szenario b) erhalten, und für die restlichen Eingaben x mit $|x| \geq k$ wird M^{++} verwerfen. Es folgt

$$\langle M\rangle \in H_\varepsilon \implies L(M^{++}) = L_4 \cap \bigcup_{i=0}^{k-1} \Sigma^i = \{x \in L_4 : |x| < k\}$$

wobei $k = \min\{n \in \mathbb{N} \mid M \text{ hält auf } \varepsilon \text{ in } n \text{ Schritten}\}$. Da Σ stets endlich ist kann es nur endlich viele Wörter mit höchstens Länge k geben, sodass $L(M^{++})$ eine endliche Teilmenge von L_4 darstellt und damit nach dem gegebenen Szenario nicht gut ist.

d)

Dies folgt sofort aus b):

$$\langle M\rangle \notin H_\varepsilon \implies L(M^{++}) = L_4 \implies \langle M^{++}\rangle \in L_\mathcal{E}$$

Also akzeptiert $T(\mathcal{E})$ auch $\langle M^{++}\rangle$.

e)

Analog zu d) folgt dies aus c):

$$\langle M\rangle \in H_\varepsilon \implies L(M^{++}) \text{ endliche Teilmenge von } L_4 \implies \langle M^{++}\rangle \notin L_\mathcal{E}$$

Also wird $\langle M^{++}\rangle$ nicht von $T(\mathcal{E})$ akzeptiert.

f)

Wie in Aufgabe i) des letzten Kapitels bekommt man nun eine Reduktion $\overline{H_\varepsilon} \leq L_\mathcal{E}$, woraus mit der Annahme, dass $L_\mathcal{E}$ rekursiv aufzählbar ist, die Entscheidbarkeit von H_ε folgt. Widerspruch.

g)

Die nicht-rekursiv-aufzählbaren Mengen, für die das Werkzeug benutzbar ist:

- $\{\langle M \rangle \mid L(M) = \{0,1\}^*\}$
- $\{\langle M \rangle \mid L(M)$ enthält alle Worte in $\{0,1\}^*$ mit gerader Länge$\}$
- $\{\langle M \rangle \mid L(M)$ ist nicht regulär$\}$ da endliche Mengen stets regulär.
- $\{\langle M \rangle \mid L(M)$ ist nicht rekursiv$\}$ da endliche Mengen stets rekursiv.
- $\{\langle M \rangle \mid |L(M)| = \infty\}$

h)

Übrig auf der Liste sind

1. $\{\langle M \rangle \mid L(M) \neq \varnothing\}$
2. $\{\langle M \rangle \mid \varepsilon \in L(M)\}$
3. $\{\langle M \rangle \mid 11101 \in L(M)\}$
4. $\{\langle M \rangle \mid |L(M)| \geq 3\}$

Die erste Menge wurde im letzten Kapitel, Aufgabe m) als rekursiv aufzählbar bewiesen.

Mengen 2 und 3 Lassen sich trivialerweise semi-entscheiden, indem wir einfach nach einem Syntaxcheck die gegebene TM auf ε bzw. 11101 simulieren und die Ausgabe übernehmen.

Menge 4 lässt sich analog zu 1 entscheiden, nur dass wir erst akzeptieren, sobald mindestens 3 Wörter akzeptiert wurden.

Damit sind alle übrig-gebliebenen Mengen rekursiv-aufzählbar.

3 Unentscheidbarkeit für context-freie Grammatiken

a)

4 Das zehnte Hilbert'sche Problem

a)

Siehe HA 7.1. Man benutzt zu einer Instanz $p \in \mathbb{Z}[x_1, \cdots, x_k]$ dann

$$f(p(x_1, \cdots, x_k)) := p'(x_1, x_1', \cdots, x_k, x_k') := p(x_1 - x_1', \cdots, x_k - x_k')$$

Da $\forall z \in \mathbb{Z} : \exists n, m \in \mathbb{N} : z = n - m$ ist f eine funktionierende Reduktion.

d)

Sei also $f : \Sigma^* \to \Sigma^*$ eine Abbildung, welche Müll auf Müll abbildet. Zu einem korrekt-kodiertem Polynom $p \in \mathbb{Z}[x_1, \cdots, x_k]$ definieren wir

$$f(p(x_1, \cdots, x_k)) := p'(x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, \cdots, x_{k,1}, x_{k,2}, x_{k,3}, x_{k,4})$$

wobei

$$p'(x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, \cdots, x_{k,1}, x_{k,2}, x_{k,3}, x_{k,4}) := p(\sum_{i=1}^{4} x_{1,i}^2, \cdots, \sum_{i=1}^{4} x_{k,i}^2)$$

Offensichtlich ist p' ebenfalls ein Polynom und f ist berechenbar. Falls $(a_1, \cdots, a_k) \in \mathbb{N}^k$ eine Nullstelle von p ist, so gilt nach Lagrange, dass $\forall a_i : \exists b_{1,1}, b_{1,2}, b_{1,3}, b_{1,4} \in \mathbb{N} : \sum_{i=1}^{4} b_{1,i}^i = a_i$. Damit ist dann $(b_{1,1}, b_{1,2}, b_{1,3}, b_{1,4}, \cdots, b_{k,1}, b_{k,2}, b_{k,3}, b_{k,4}) \in \mathbb{Z}^{4k}$ eine Nullstelle von p'.

Für die Rückrichtung sei nun $(b_{1,1}, b_{1,2}, b_{1,3}, b_{1,4}, \cdots, b_{k,1}, b_{k,2}, b_{k,3}, b_{k,4}) \in \mathbb{Z}^{4k}$ eine Nullstelle von p'. Dann ist zu $a_i := \sum_{j=1}^{4} b_{i,j}^2 \in \mathbb{N}$ für $i \in [1, k]_\mathbb{N}$ nun $(a_1, \cdots, a_k) \in \mathbb{N}^k$ eine Nullstelle von p.

e)

Zu $q_1, \cdots, q_k \in \mathbb{Z}[x_1, \cdots, x_n]$ gilt

$$\forall i \in [1, k]_\mathbb{N} : q_i(x) = 0 \qquad \Longleftrightarrow \qquad \underbrace{\sum_{i=1}^{k} q_i(x)^2}_{\in \mathbb{Z}[x_1, \cdots, x_n]} = 0$$

f)

Wir gehen systematisch vor und starten mit dem gegebenen Gleichungssystem $p(x) = 0$.

1. Solange es Gleichungen $g(x) = a$ mit $g(x) = q(x) + r(x)$ mit $\deg(q) > 2, 0 \leq \deg(r) \leq 2$ gibt, ersetze die Gleichung $g(x) = a$ durch
$$q(x) = b \qquad r(x) = c \qquad b + c = a$$
2. Solange es Gleichungen $g(x) = a$ mit $g(x) = q(x) \cdot r(x)$ mit $\deg(q) \geq 2, \deg(r) = 1$ gibt, ersetze die Gleichung $g(x) = a$ durch
$$q(x) = b \qquad r(x) = c \qquad bc = a$$
3. Ersetze alle Gleichungen der Form $g(x) = a$ durch $g(x) - a = 0$.

Beispiel: $p \in \mathbb{Z}[x, y, z]$ mit $p(x, y, z) = 4x^2y - yz^2 + 1$. Wir formen $p(x, y, z) = 0$ um und erhalten

$$4x^2y - yz^2 + 1 = 0$$
$$4x^2y = a \qquad -yz^2 + 1 = b \qquad a + b = 0$$
$$4x^2y = a \qquad -yz^2 = c \qquad 1 = d \qquad c + d = b \qquad a + b = 0$$
$$4x^2 = e \qquad y = f \qquad ef = a \qquad -yz^2 = c \qquad 1 = d \qquad c + d = b \qquad a + b = 0$$
$$4x^2 = e \qquad y = f \qquad ef = a \qquad z^2 = g \qquad -y = h \qquad gh = c \qquad 1 = d \qquad c+d = b \qquad a+b = 0$$

Zu guter letzt haben wir dann das Gleichungssystem:

$4x^2 - e = 0$
$y - f = 0$
$ef - a = 0$
$z^2 - g = 0$
$-y - h = 0$
$gh - c = 0$
$1 - d = 0$
$c + d - b = 0$
$a + b = 0$

Da dies alles Äquivalenzumformungen waren, stimmen die Lösungsmengen der ursprünglichen Gleichung und des Gleichungssystems überein. Im Beispiel haben wir unter anderem:

$$x = 0 \qquad y = 1 \qquad z = 1$$

Bzw im Gleichungssystem

$$x = a = b = e = 0 \qquad y = z = d = f = g = 1 \qquad c = h = -1$$