Prof. Dr. M. Grohe E. Fluck, A. Riazsadri, J. Feith

Übungsblatt 3

Abgabetermin: Mittwoch, der 9. November 2022 um 14:30

Tutoriumsaufgabe 1 ((Un-)Entscheidbarkeit)

Formulieren Sie folgende Probleme als Sprache (z.B. $H = \{\langle M\rangle w \mid M \text{ hält auf } w\}$ für das Halteproblem). Zeigen oder widerlegen Sie, welche der folgende Probleme entscheidbar sind. Nutzen Sie die Unterprogrammtechnik für Beweise der Unentscheidbarkeit.

a) Eingabe: Eine TM M.

Frage: Stoppt M auf keiner Eingabe?

b) Eingabe: Eine TM M; ein Wort w.

Frage: Schreibt M auf der Eingabe w jemals ein Nicht-Blank-Symbol auf das Band?

c) Eingabe: Eine TM M.

Frage: Hält M auf der Eingabe 110 nicht?

Lösung:

a) $L_{\text{never}} = \{\langle M\rangle \mid M \text{ hält auf keiner Eingabe}\}$ ist unentscheidbar. Angenommen, L_{never} wäre entscheidbar, d.h. es existiert eine TM M_{never}, welche L_{never} entscheidet. Wir konstruieren per Unterprogrammtechnik eine TM M_H, welche Halteproblem H entscheidet.

Die TM M_H verhält sich wie folgt:

- Zunächst wird geprüft, ob die Eingabe das Format $\langle M\rangle w$ hat. Falls nein, so verwirft M_H sofort.
- Andernfalls konstruieren wir eine TM M^w mit den folgenden Eigenschaften:
  - Auf jeder Eingabe löscht M^w ihre Eingabe, schreibt w auf das Band und simuliert das Verhalten von M auf der Eingabe w. Falls M hält, so verwirft M^w.
- Nun prüft M_H mittels dem Unterprogramm M_{never}, ob $\langle M^w\rangle \in L_{\text{never}}$ gilt. Falls ja, so verwirft M_H, andernfalls akzeptiert M_H.

Offensichtlich verhält sich M_H auf Eingaben, welche nicht das Format $\langle M\rangle w$ haben, korrekt. Ansonsten hält M^w genau dann auf keiner Eingabe, wenn M auf w nicht hält (andernfalls hält M^w auf jeder Eingabe). Da M_{never} genau dann akzeptiert, wenn $\langle M^w\rangle \notin L_{\text{never}}$ gilt, folgern wir, dass M_H die Eingabe $\langle M\rangle w$ genau dann akzeptiert, wenn M auf w hält.

Somit entscheidet M_H das Halteproblem, was aber bekanntermaßen unentscheidbar ist. Es folgt, dass L_{never} nicht entscheidbar ist.

b) $L = \{\langle M \rangle w \mid M$ schreibt auf Eingabe w ein Nicht-Blank-Symbol auf das Band$\}$ ist entscheidbar.

Betrachten wir zunächst eine TM M, welche auf einer gegebenen Eingabe w stets Blanks schreibt. Somit ist der Bandinhalt (abgesehen von Blanks links und rechts der Eingabe) stets von der Form $B^k w'$ erreichen (da keine Nicht-Blanks geschrieben werden), wobei $k \in \mathbb{N}$ und w' ein Suffix von w ist, d.h. es gibt nur $|w|$ verschiedene Möglichkeiten für den Bandinhalt von M bei Eingabe w. Weiterhin kann M nur Konfigurationen der Form $qB^k w'$ erreichen.

Wir zeigen nun, dass dann die Anzahl der von M besuchten Bandpositionen durch eine Funktion in $|Q|$ und $|w|$ beschränkt ist, falls M auf w hält. Dazu stellen wir fest, dass M auf einem leeren Band nach maximal $|Q|+1$ Schritten eine Konfiguration wiederholt (und somit in einer Endlosschleife ist); M kann also (nach dem kompletten Überschreiben der Eingabe mit Blanks) höchstens $|Q|$ Positionen rechts des letzten Eingabesymbols besuchen, ohne eine Konfiguration zu wiederholen.

Nehmen wir nun an, dass M eine Konfiguration $qB^\ell w'$ (wobei w' wiederum ein Suffix von w ist) mit $\ell > |Q|$ erreicht hat. Dann hat M auch $|Q|+1$ Konfigurationen der Form $qB^i w'$ mit $i \in \{1, \ldots, |Q|+1\}$ erreicht (ggf. unterscheiden sich die Zustände in den Konfigurationen). Insbesondere hat M dabei aber einen Zustand mehrfach erreicht; es existiert also ein $q \in Q$ so, dass M die Konfigurationen $qB^x w'$ und $qB^y w'$ für zwei $x, y \in \{1, \ldots, |Q|+1\}$ erreicht hat. Gilt $x = y$, so hat M eine Konfiguration wiederholt und befindet sich in einer Endlosschleife, andernfalls muss M aber auch die Konfigurationen $qB^{c \cdot |x-y|} w'$ für alle $c \in \mathbb{N}$ erreichen und kann somit nie halten. Es folgt, dass M auf w entweder nicht hält, oder sich nie mehr als $|Q|$ Positionen von einem Nicht-Blank-Symbol auf dem Band entfernt. Da M keine Nicht-Blank-Symbole schreibt und initial $|w|$ Positionen des Bandes beschrieben sind, kann M also höchstens $|w| + 2 \cdot |Q|$ Bandpositionen besuchen, falls M hält. Genauer: M kann in diesem Fall maximal $|Q|$ Positionen links und $|Q|$ Symbole rechts des letzten Eingabesymbols erreichen.

Hält M also auf w, so kann M maximal $|Q| \cdot (|w| + 2 \cdot |Q|)$ verschiedene Konfigurationen erreichen (je eine pro möglicher Kopfposition und möglichem Zustand). Wir können L also mit folgendem Verfahren entscheiden:

- Zuerst prüfen wir die Eingabesyntax. Ist die Eingabe nicht von der Form $\langle M \rangle w$, so verwerfen wir die Eingabe.
- Andernfalls simulieren wir die TM M auf der Eingabe w für $|Q| \cdot (|w| + 2 \cdot |Q|)$ Schritte. Schreibt M während der Simulation ein Nicht-Blank-Symbol, so akzeptieren wir.
- Endet die Simulation ohne, dass M ein Nicht-Blank-Symbol geschrieben hat, so verwerfen wir.

Offensichtlich werden Eingaben, die nicht das Format $\langle M\rangle w$ haben, korrekt behandelt. Für Eingaben der Form $\langle M\rangle w$ hingegen unterscheiden wir 3 Fälle:

- M hält auf w und schreibt dabei ein Nicht-Blank-Symbol: Dann schreibt M das Nicht-Blank-Symbol nach höchstens $|Q| \cdot (|w| + 2 \cdot |Q|)$ Schritten, und unser Verfahren akzeptiert korrekterweise.
- M hält auf w und schreibt dabei kein Nicht-Blank-Symbol: Dann hält w während der Simulationsphase an, und unser Verfahren verwirft korrekterweise.
- M hält nicht auf w und schreibt dabei kein Nicht-Blank-Symbol: Dann gerät M auf w in eine Endlosschleife, und durchläuft diese bis zum Simulationsende mindestens ein mal, ohne dabei ein Nicht-Blank-Symbol zu schreiben. Folglich verwerfen wir die Eingabe korrekterweise.
- M hält nicht auf w und schreibt dabei mindestens ein Nicht-Blank-Symbol: Dann gerät M auf w in eine Endlosschleife, und durchläuft diese bis zum Simulationsende mindestens ein mal, d.h. M schreibt schon während der Simulation mindestens ein mal ein Nicht-Blank-Symbol und wir akzeptieren korrekterweise.

Somit ist unser Verfahren korrekt. Es folgt, dass L entscheidbar ist.

c) $L = \{\langle M\rangle \mid M \text{ hält nicht auf der Eingabe } 110\}$ ist unentscheidbar. Angenommen, die Sprache D wäre entscheidbar, d.h. es existiert eine TM M_L, welche L entscheidet. Wir konstruieren per Unterprogrammtechnik eine TM M_ε, welche das spezielle Halteproblem H_ε entscheidet.

Die TM M_ε verhält sich wie folgt:

- Zunächst wird geprüft, ob die Eingabe eine valide Gödelnummer ist. Falls nein, so verwirft M_ε sofort.
- Andernfalls hat die Eingabe die Form $\langle M\rangle$, und wir konstruieren eine TM M^* mit den folgenden Eigenschaften:
  - M^* prüft, ob die Eingabe 110 ist. Ist dies nicht der Fall, so verwirft M^*.
  - Auf der Eingabe 110 hingegen simuliert M^* das Verhalten von M auf der Eingabe ε. Falls M hält, so verwirft M^*.
- Nun prüft M_ε mittels dem Unterprogramm M_L, ob $\langle M^*\rangle \in L$ gilt. Falls ja, so akzeptiert M_ε, andernfalls verwirft M_ε.

Offensichtlich verhält sich M_ε auf Eingaben, welche keine validen Gödelnummern sind, korrekt. Ist die Eingabe hingegen eine Gödelnummer $\langle M\rangle$, so verwirft M^* genau dann die Eingabe 110, wenn M auf ε hält (andernfalls hält M^* nicht). Da M_ε genau dann akzeptiert, wenn $\langle M^*\rangle \in L$ gilt, folgern wir, dass M_ε die Eingabe $\langle M\rangle$ genau dann akzeptiert, wenn M auf ε hält.

Somit entscheidet M_ε das spezielle Halteproblem, was aber bekanntermaßen unentscheidbar ist. Es folgt, dass L nicht entscheidbar ist.

Prof. Dr. M. Grohe
E. Fluck, A. Riazsadri, J. Feith

Tutoriumsaufgabe 2 (Diagonalisierung)

Sei

$$L = \{1^k \mid k \in \mathbb{N}, M_k \text{ akzeptiert } 1^k \text{ nicht}\}.$$

Zeigen Sie durch Diagonalisierung, dass L nicht entscheidbar ist.

Lösung:

Angenommen, es gibt eine TM M_j, die L entscheidet. Wir unterscheiden, ob 1^j in L ist oder nicht.

- Fall 1:
$$1^j \in L \overset{\text{Def. } M_j}{\Rightarrow} M_j \text{ akz. } 1^j \overset{\text{Def. } L}{\Rightarrow} 1^j \notin L.$$

- Fall 2:
$$1^j \notin L \overset{\text{Def. } M_j}{\Rightarrow} M_j \text{ verw. } 1^j \Rightarrow M_j \text{ akz. } 1^j \text{ nicht } \overset{\text{Def. } L}{\Rightarrow} 1^j \in L.$$

Beide Fälle führen zu einem Widerspruch. Es gibt also keine solche TM M_j, und damit ist L nicht entscheidbar.

Tutoriumsaufgabe 3 (Mächtigkeiten von Mengen)

Was sind die Mächtigkeiten der nachfolgenden Mengen? Unterscheiden Sie insbesondere zwischen abzählbaren und überabzählbaren Mengen. Beweisen Sie die Korrektheit Ihrer Ergebnisse.

a) $M_1 = \{\langle M \rangle \mid M \text{ Turingmaschine}\}$

b) $M_2 = \{L \subseteq \{0,1\}^* \mid L \text{ ist unentscheidbar}\}$

c) $M_3 = \{L \subseteq \{0,1\}^* \mid L \text{ ist endlich}\}$

d) $M_4 = \{M \mid M \text{ Turingmaschine}\}$

Lösung:

a) Die Menge ist abzählbar unendlich.

Eine geeignete "Einschränkung" der Binärkodierung $\text{bin}\colon \mathbb{N} \to \{0,1\}^*$ ist eine Surjektion nach M_1, da jede Gödelnummer auch eine binärkodierte natürliche Zahl ist. Da aber nicht jede binärkodierte natürliche Zahl auch eine Gödelnummer ist, müssen wir unsere Abbildung dahingehend ändern, dass wir solche Zahlen etwa auf eine feste Gödelnummer w_1 abgebildet werden. Dies gibt uns die Surjektion $f\colon \mathbb{N} \to M_1$ mit

$$f(n) = \begin{cases} \text{bin}(n) & \text{falls } \text{bin}(n) \text{ eine Gödelnummer ist} \\ w_1 & \text{sonst.} \end{cases}$$

b) Die Menge ist überabzählbar.

Bekanntermaßen ist $2^{\{0,1\}^*}$, die Menge aller Sprachen (über $\{0,1\}$), gleichmächtig zum Kontinuum $\mathbb{R}$, womit wir eine obere Schranke erhalten. Weiterhin gilt $2^{\{0,1\}^*} = M_2 \uplus \{L \subseteq \{0,1\}^* \mid L \text{ entscheidbar}\}$, wobei die Menge der entscheidbaren Sprachen bekanntermaßen abzählbar ist.

Wäre M_2 also auch abzählbar, so wäre $2^{\{0,1\}^*}$ als Vereinigung zweier abzählbarer Mengen abzählbar: Angenommen, A und B sind abzählbare Mengen. Dann existieren Surjektionen $f\colon \mathbb{N} \to A$ und $g\colon \mathbb{N} \to B$ aus denen wir eine Surjektion $h\colon \mathbb{N} \to A \cup B$ konstruieren können, etwa

$$h(n) = \begin{cases} f(n/2) & \text{falls } n \text{ gerade} \\ g((n-1)/2) & \text{falls } n \text{ ungerade.} \end{cases}$$

Folglich muss M_2 überabzählbar sein.

c) Die Menge M_3 ist abzählbar unendlich.

Sei $v_1, v_2, \ldots$ die kanonische Aufzählung der Wörter über $\{0,1\}$. Jede Sprache L über $\{0,1\}$ lässt sich vollständig durch eine *charakteristische Folge* χ_L beschreiben, welche an Position k eine Eins hat, falls v_k in L liegt, und eine Null sonst.

Charakteristische Folgen endlicher Sprachen haben folglich nur endlich viele von Null verschiedene Einträge, und insbesondere existiert ein $k \in \mathbb{N}$ so, dass v_k das "letzte" Wort einer endlichen Sprache L in der kanonischen Aufzählung der Wörter über $\{0,1\}$ ist. Es folgt, dass zur vollständigen Beschreibung von L bereits die ersten k Einträge von χ_L ausreichen; alle nachfolgenden Einträge werden implizit als Null angenommen. Wir können jede endliche Sprache also als endliches Wort über $\{0,1\}$ kodieren, etwa via $f\colon \{0,1\}^* \to M_3$ mit

$$f(\chi) = \{v \in \{0,1\}^* \mid v \text{ ist das } i\text{-te Wort in der kanonischen Aufzählung und } \chi_i = 1\}.$$

Dann ist f eine Surjektion, und wir erhalten eine Surjektion $h\colon \mathbb{N} \to M_3$ durch die Komposition mit einer surjektiven Aufzählungsfunktion $g\colon \mathbb{N} \to \{0,1\}^*$ (etwa die kanonische Aufzählung) als $h = f \circ g$.

d) M_4 ist keine Menge, sondern eine echte Klasse wie die Klasse aller endlichen Graphen.

Dies folgt daraus, dass insbesondere jeder Zustand ein beliebiges mathematisches Objekt und somit eine beliebige Menge sein kann. Insbesondere gibt es also eine "Surjektion" der echten Klasse aller Mengen in M_4.