Einführung in die Theoretische Informatik

Johannes Köbler

Institut für Informatik
Humboldt-Universität zu Berlin

WS 2016/17

Unentscheidbarkeit des Halteproblems

Definition

- Das Halteproblem ist die Sprache

$$H = \left\{ w\#x \;\middle|\; \begin{array}{l} w, x \in \{0,1\}^* \text{ und} \\ \text{die DTM } M_w \text{ hält} \\ \text{bei Eingabe } x \end{array} \right\}$$

- Das spezielle Halteproblem ist

$$K = \left\{ w \in \{0,1\}^* \;\middle|\; \begin{array}{l} \text{die DTM } M_w \\ \text{hält bei Eingabe } w \end{array} \right\}$$

χ_H	x_1	x_2	x_3	$\cdots$
w_1	0	1	0	$\cdots$
w_2	0	1	1	$\cdots$
w_3	1	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

χ_K				
w_1	**0**			
w_2		**1**		
w_3			**0**	
$\vdots$				$\ddots$

Satz

$K \in \mathrm{RE} \setminus \text{co-RE}$.

Semi-Entscheidbarkeit des speziellen Halteproblems

Beweis von $K \in \mathrm{RE}$

- Sei w_h die Kodierung einer DTM, die bei jeder Eingabe (sofort) hält und betrachte die Funktion

$$f(x) = \begin{cases} w, & x \text{ ist Kodierung einer haltenden Rechnung einer DTM } M_w \text{ bei Eingabe } w, \\ w_h, & \text{sonst.} \end{cases}$$

- Da f berechenbar und $img(f) = K$ ist, folgt $K \in \mathrm{RE}$. □

Bemerkung

Ganz ähnlich lässt sich $H \in \mathrm{RE}$ zeigen.

Unentscheidbarkeit des speziellen Halteproblems

Beweisidee

- Für eine DTM M sei $dom(M) = \{x \in \Sigma^* \mid M(x)\downarrow\}$ der Definitionsbereich der von M berechneten Funktion.
- Wir wissen bereits, dass RE $= \{dom(M) \mid M \text{ ist eine DTM}\}$ ist.
- Sei $A = (a_{w,x})_{w,x \in \{0,1\}^*}$ die durch $a_{w,x} = \chi_H(w\#x)$ def. Binärmatrix.
- Wegen

$$a_{w,x} = \chi_H(w\#x) = \chi_{dom(M_w)}(x)$$

  repräsentiert Zeile w von A die Sprache $dom(M_w)$, d.h. die Zeilen von A repräsentieren genau die semi-entscheidbaren Binärsprachen.
- Wegen $a_{w,w} = \chi_H(w\#w) = \chi_K(w)$ repräsentiert die Diagonale von A die Sprache K.
- Da aber die komplementierte Diagonale von A mit keiner Zeile von A übereinstimmen kann, folgt $\bar{K} \notin$ RE und somit $K \notin$ REC.

Beweis von $\bar{K} \notin \mathrm{RE}$

- Angenommen, die Sprache

$$\bar{K} = \{w \mid M_w(w)\uparrow\}$$

wäre semi-entscheidbar.

- Dann existiert eine DTM $M_{w'}$ mit $dom(M_{w'}) = \bar{K}$, d.h. es gilt

$$M_{w'}(w)\downarrow \Leftrightarrow w \in \bar{K} \qquad (*)$$

χ_H	x_1	x_2	x_3	$\cdots$
w_1	**0**	1	0	...
w_2	0	**1**	1	...
w_3	1	1	**0**	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

w'	**1**	**0**	**1**	$\cdots$

- Folglich gilt

$$w' \in \bar{K} \;\Leftrightarrow\; M_{w'}(w')\uparrow \underset{(*)}{\Leftrightarrow} w' \notin \bar{K} \qquad \lightning \text{ (Widerspruch!)}$$

$\square$

Unentscheidbarkeit des speziellen Halteproblems

Korollar

REC $\subsetneq$ RE.

Beweis

Klar, da $K \in \mathrm{RE} - \mathrm{REC}$. $\square$

Der Reduktionsbegriff

Definition

Eine Sprache $A \subseteq \Sigma^*$ heißt auf $B \subseteq \Gamma^*$ reduzierbar (kurz: $A \leq B$), falls eine berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ ex., so dass gilt:

$$\forall x \in \Sigma^* : x \in A \Leftrightarrow f(x) \in B.$$

Beispiel

- Es gilt $K \leq H$ mittels $f : w \mapsto w\#w$, da für alle $w \in \{0,1\}^*$ gilt:

$$w \in K \quad \Leftrightarrow \quad M_w(w)\downarrow \quad \Leftrightarrow \quad w\#w \in H$$

- Es gilt sogar $A \leq H$ für jede Binärsprache $A \in \mathrm{RE}$ mittels $f : x \mapsto w\#x$, wobei w die Kodierung einer DTM M_w mit $dom(M_w) = A$ ist:

$$x \in A \quad \Leftrightarrow \quad M_w(x)\downarrow \quad \Leftrightarrow \quad w\#x \in H$$

◁

Der Vollständigkeitsbegriff

Definition

- Eine Sprache B heißt hart für eine Sprachklasse $\mathcal{C}$ (kurz: $\mathcal{C}$-hart oder $\mathcal{C}$-schwer), falls jede Sprache $A \in \mathcal{C}$ auf B reduzierbar ist:

$$\forall A \in \mathcal{C} : A \leq B.$$

- Eine $\mathcal{C}$-harte Sprache B, die zu $\mathcal{C}$ gehört, heißt $\mathcal{C}$-vollständig.

Beispiel

Das Halteproblem H ist RE-vollständig. Es gilt nämlich

- $H \in \mathrm{RE}$ und
- $\forall A \in \mathrm{RE} : A \leq H$

mittels der Reduktionsfunktion $x \mapsto w\#bin(x)$, wobei M_w eine DTM mit $dom(M_w) = \{bin(x) \mid x \in A\}$ ist. ◁

Bemerkung

Auch das spezielle Halteproblem K ist RE-vollständig (siehe Übungen).

Abschluss von REC unter $\leq$

Definition

Eine Sprachklasse $\mathcal{C}$ heißt unter $\leq$ abgeschlossen, wenn für beliebige Sprachen A, B gilt:

$$A \leq B \wedge B \in \mathcal{C} \Rightarrow A \in \mathcal{C}.$$

Satz

Die Klassen REC und RE sind unter $\leq$ abgeschlossen.

Beweis

- Gelte $A \leq B$ mittels f und sei $B \in \text{REC}$.
- Wegen $B \in \text{REC}$ ex. eine DTM M, die χ_B berechnet.
- Betrachte folgende DTM M':
  - M' berechnet bei Eingabe x zuerst den Wert $f(x)$ und
  - simuliert dann M bei Eingabe $f(x)$.

Abschluss von REC und RE unter $\le$

Satz

Die Klasse REC ist unter $\le$ abgeschlossen.

Beweis.

- Gelte $A \le B$ mittels f und sei $B \in \text{REC}$.
- Dann ex. eine DTM M, die χ_B berechnet.
- Betrachte folgende DTM M':
  - M' berechnet bei Eingabe x zuerst den Wert $f(x)$ und
  - simuliert dann M bei Eingabe $f(x)$.
- Wegen $x \in A \Leftrightarrow f(x) \in B$ ist $\chi_A(x) = \chi_B(f(x))$ und daher folgt

$$M'(x) = M(f(x)) = \chi_B(f(x)) = \chi_A(x).$$

- Also berechnet M' die Funktion χ_A, d.h. $A \in \text{REC}$. $\square$

Bemerkung

Der Abschluss von RE unter $\le$ folgt analog (siehe Übungen).

H ist nicht entscheidbar

Korollar

- $A \leq B \wedge A \notin \mathrm{REC} \Rightarrow B \notin \mathrm{REC}$,
- $A \leq B \wedge A \notin \mathrm{RE} \Rightarrow B \notin \mathrm{RE}$.

Beweis

Aus der Annahme, dass B entscheidbar (bzw. semi-entscheidbar) ist, folgt wegen $A \leq B$, dass dies auch auf A zutrifft (Widerspruch). $\square$

Bemerkung

Wegen $K \leq H$ überträgt sich somit die Unentscheidbarkeit von K auf H.

Korollar

$H \notin \mathrm{REC}$.

Das Halteproblem bei leerem Band

Definition

Das Halteproblem bei leerem Band ist die Sprache

$$H_0 = \left\{ w \in \{0,1\}^* \;\middle|\; \begin{array}{l}\text{die DTM } M_w \\ \text{hält bei Eingabe } \varepsilon\end{array} \right\}$$

Satz

H_0 ist RE-vollständig.

Beweis

- $H_0 \in \mathrm{RE}$ folgt wegen $H_0 \le H \in \mathrm{RE}$ mittels der Reduktionsfunktion $w \mapsto w\#\varepsilon$.

χ_H	x_1	x_2	x_3	$\cdots$
w_1	0	1	0	$\cdots$
w_2	0	1	1	$\cdots$
w_3	1	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

χ_{H_0}	x_1 $(=\varepsilon)$
w_1	0
w_2	0
w_3	1
$\vdots$	$\vdots$

H_0 ist RE-vollständig

Beweis

- $H_0 \in \mathrm{RE}$ folgt wegen $H_0 \leq H \in \mathrm{RE}$ mittels der Reduktionsfunktion $w \mapsto w\#\varepsilon$.
- Sei $A \in \mathrm{RE}$ und sei M eine DTM mit $dom(M) = A$.
- Um A auf H_0 zu reduzieren, transformieren wir x in die Kodierung w_x einer DTM M_{w_x}, die zunächst ihre Eingabe durch x ersetzt und dann $M(x)$ simuliert.
- Dann gilt

  $$x \in A \iff w_x \in H_0$$

  und somit $A \leq H_0$ mittels der Reduktionsfunktion $x \mapsto w_x$.

Korollar

$H_0 \notin \mathrm{REC}$.

Der Satz von Rice

Frage

- Kann man einer beliebig vorgegebenen DTM ansehen, ob die von ihr berechnete partielle Funktion eine gewisse Eigenschaft hat?
- Kann man beispielsweise entscheiden, ob eine gegebene DTM eine totale Funktion berechnet?

Antwort

Nein (es sei denn, die fragliche Eigenschaft ist trivial, d.h. keine oder jede DTM berechnet eine Funktion mit dieser Eigenschaft).

Der Satz von Rice

Definition

- Zu einer Klasse $\mathcal{F}$ von partiellen Funktionen definieren wir die Sprache
$$L_{\mathcal{F}} = \left\{ w \in \{0,1\}^* \;\middle|\; \text{die DTM } M_w \text{ ber. eine partielle Funktion in } \mathcal{F} \right\}$$
- Die Eigenschaft $\mathcal{F}$ heißt trivial, wenn $L_{\mathcal{F}} = \varnothing$ oder $L_{\mathcal{F}} = \{0,1\}^*$ ist.

Der Satz von Rice besagt, dass $L_{\mathcal{F}}$ nur für triviale Eigenschaften entscheidbar ist.

Satz (Satz von Rice)

Für jede nicht triviale Eigenschaft $\mathcal{F}$ ist $L_{\mathcal{F}}$ unentscheidbar.

Der Satz von Rice

Beispiel

- Die Sprache

  $$L = \{w \in \{0,1\}^* \mid M_w(0^n) = 0^{n+1} \text{ für alle } n \geq 0\}$$

  ist unentscheidbar.
- Dies folgt aus dem Satz von Rice, da die Eigenschaft

  $$\mathcal{F} = \{f \mid f(0^n) = 0^{n+1} \text{ für alle } n \geq 0\}$$

  nicht trivial und $L = L_{\mathcal{F}}$ ist.
- $\mathcal{F}$ ist nicht trivial, da z.B. die berechenbare partielle Funktion

  $$f(x) = \begin{cases} 0^{n+1}, & x = 0^n \text{ für ein } n \geq 0 \\ \uparrow, & \text{sonst} \end{cases}$$

  in $\mathcal{F}$ und die konstante Funktion $g(x) = 0$ nicht in $\mathcal{F}$ enthalten ist.
- Dagegen ist die Eigenschaft $\mathcal{F}' = \{\chi_H\}$ trivial, da $L_{\mathcal{F}'} = \varnothing$ ist.

Der Satz von Rice

Satz (Satz von Rice)

Für jede nicht triviale Eigenschaft $\mathcal{F}$ ist die Sprache $L_{\mathcal{F}}$ unentscheidbar.

Beweisidee

- Die Idee besteht darin, H_0 auf $L_{\mathcal{F}}$ (oder auf $\overline{L}_{\mathcal{F}}$) zu reduzieren, indem wir für eine gegebene DTM M_w eine DTM $M_{w'}$ konstruieren mit

  $$w \in H_0 \Leftrightarrow M_{w'} \text{ berechnet (k)eine partielle Funktion in } \mathcal{F}.$$

- Hierzu lassen wir $M_{w'}$ bei Eingabe x zunächst einmal die DTM M_w bei Eingabe ε simulieren.
- Falls $w \notin H_0$ ist, berechnet $M_{w'}$ also die überall undefinierte Funktion u mit $u(x)\uparrow$ für alle $x \in \{0, 1, \#\}^*$.
- Damit die Reduktion gelingt, müssen wir nur noch dafür sorgen, dass $M_{w'}$ im Fall $w \in H_0$ eine partielle Funktion f berechnet, die sich bzgl. der Eigenschaft $\mathcal{F}$ von u unterscheidet d.h. $f \in \mathcal{F} \Leftrightarrow u \notin \mathcal{F}$.
- Da $\mathcal{F}$ nicht trivial ist, ex. eine DTM M, die ein solches f berechnet.

Der Satz von Rice

Satz (Satz von Rice)

Für jede nicht triviale Eigenschaft $\mathcal{F}$ ist die Sprache $L_{\mathcal{F}}$ unentscheidbar.

Beweis

- Sei M eine DTM, die eine Funktion f mit $f \in \mathcal{F} \Leftrightarrow u \notin \mathcal{F}$ berechnet.
- Betrachte die Reduktionsfunktion

  $h(w) = w'$, wobei w' die Kodierung einer DTM ist, die bei Eingabe x zunächst die DTM $M_w(\varepsilon)$ simuliert und im Fall, dass $M_w(\varepsilon)$ hält, mit der Simulation von $M(x)$ fortfährt.

- Dann ist $h : w \mapsto w'$ eine totale berechenbare Funktion und es gilt

$$\begin{array}{lcl} w \in H_0 & \Rightarrow & M_{w'} \text{ berechnet } f \\ w \notin H_0 & \Rightarrow & M_{w'} \text{ berechnet } u. \end{array}$$

- Dies zeigt, dass h das Problem H_0 auf $L_{\mathcal{F}}$ (oder auf $\overline{L}_{\mathcal{F}}$) reduziert, und da H_0 unentscheidbar ist, muss auch $L_{\mathcal{F}}$ unentscheidbar sein. □

Der Satz von Rice für Akzeptoren

Der Satz von Rice gilt auch für Eigenschaften, die das Akzeptanzverhalten einer gegebenen Turingmaschine betreffen.

Satz (Satz von Rice für Spracheigenschaften)

Für eine beliebige Sprachklasse $\mathcal{S}$ sei

$$L_{\mathcal{S}} = \{w \in \{0,1\}^* \mid L(M_w) \in \mathcal{S}\}.$$

Dann ist $L_{\mathcal{S}}$ unentscheidbar, außer wenn $L_{\mathcal{S}} = \varnothing$ oder $L_{\mathcal{S}} = \{0,1\}^*$ ist.

Beweis

Siehe Übungen.

Weitere (Un-)entscheidbarkeitsresultate

Neben dem Wortproblem sind für eine Sprachklasse $\mathcal{C}$ auch folgende Entscheidungsprobleme interessant:

Das Schnittproblem

Gegeben: Zwei Sprachen L_1 und L_2 aus $\mathcal{C}$.
Gefragt: Ist $L_1 \cap L_2 = \emptyset$?

Das Äquivalenzproblem

Gegeben: Zwei Sprachen L_1 und L_2 aus $\mathcal{C}$.
Gefragt: Gilt $L_1 = L_2$?

Das Leerheitsproblem

Gegeben: Eine Sprache L aus $\mathcal{C}$.
Gefragt: Ist $L = \emptyset$?

Hierbei repräsentieren wir Sprachen in $\mathcal{C} = \mathrm{REG}, \mathrm{CFL}, \mathrm{CSL}, \mathrm{RE}$ durch entsprechende Grammatiken und Sprachen in $\mathcal{C} = \mathrm{DCFL}, \mathrm{DCSL}$ durch entsprechende Akzeptoren.

Das Postsche Korrespondenzproblem (PCP)

Definition

- Sei Σ ein beliebiges Alphabet mit $\# \notin \Sigma$.
- Das Postsche Korrespondenzproblem über Σ (kurz PCP_Σ) ist:
  - gegeben: k Paare $(x_1, y_1), \ldots, (x_k, y_k)$ von Wörtern in Σ^*.
  - gefragt: Gibt es eine Folge $\alpha = (i_1, \ldots, i_n)$, $n \geq 1$, von Indizes $i_j \in \{1, \ldots, k\}$ mit $x_{i_1} \ldots x_{i_n} = y_{i_1} \ldots y_{i_n}$?
- Das modifizierte PCP über Σ (kurz $MPCP_\Sigma$) fragt nach einer Lösung $\alpha = (i_1, \ldots, i_n)$ mit $i_1 = 1$.
- Wir notieren eine PCP-Instanz meist in Form einer Matrix $\binom{x_1 \ldots x_k}{y_1 \ldots y_k}$ und kodieren sie durch das Wort $x_1 \# y_1 \# \ldots \# x_k \# y_k$.

Beispiel

Die Instanz $I = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} = \begin{pmatrix} a & ab & caa \\ aca & bc & aa \end{pmatrix}$ besitzt wegen

$$x_1 x_3 x_2 x_3 = acaaabcaa$$
$$y_1 y_3 y_2 y_3 = acaaabcaa$$

die PCP-Lösung $\alpha = (1, 3, 2, 3)$, die auch eine MPCP-Lösung ist. ◁