Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik
Vorlesung am 13. November 2014

INSTITUT FÜR THEORETISCHE INFORMATIK

Definition

Zu $w \in \{0,1\}^*$ sei T_w

- die Turing-Maschine mit der Gödelnummer (GN) w, bzw.
- die Turing-Maschine, die $\emptyset$ akzeptiert.

Es sei $L(T_w)$ die Sprache, die von T_w akzeptiert wird.

Die Diagonalsprache

Wir konstruieren die sogenannte **Diagonalsprache** L_d , wie folgt:

- Betrachte die Wörter aus $\{0,1\}^*$ in *kanonischer* Reihenfolge, d.h. w_i steht vor w_j $(i < j)$, falls
  - $|w_i| < |w_j|$, oder
  - $|w_i| = |w_j|$ und w_i lexikographisch vor w_j steht.
- $\mathcal{M}_j$ sei die TM, die durch die Gödelnummer w_j kodiert ist.
- Wir konstruieren eine unendliche Tabelle,
  - an deren Position (i,j) für $1 \leq i,j < \infty$ eine Null oder eine Eins steht, und
  - welche beinhaltet, ob w_i in $L(\mathcal{M}_j)$ ist.
- Damit gilt für die Einträge

$$(i,j) = \begin{cases} 1 & \text{falls } \mathcal{M}_j \; w_i \text{ akzeptiert} \\ 0 & \text{sonst} \end{cases}$$

Die Diagonalsprache

- Damit gilt für die Einträge

$$(i, j) = \begin{cases} 1 & \text{falls } \mathcal{M}_j \; w_i \text{ akzeptiert} \\ 0 & \text{sonst} \end{cases}$$

- Definiere dazu

$$L_d := \{w_i \mid \mathcal{M}_i \text{ akzeptiert } w_i \text{ nicht}\}\,.$$

- L_d enthält also alle w_i, für die auf der Diagonalen an der Stelle (i, i) eine Null steht.
- Dies führt später zu einem Diagonalbeweis (Cantor).

Die Diagonalsprache - Veranschaulichung

$w \in \{0,1\}^*$	Gödelnummer							
		w_i	w_j	w_k				
$\vdots$	$\vdots$							
w_i	1	**0**	1	0	1	0	0	$w_i \in L_d$
w_j	0	0	**1**	0	0	1	1	$w_j \notin L_d$
w_k	1	0	0	**1**	1	0	1	$w_k \notin L_d$
$\vdots$	$\vdots$							

Unentscheidbarkeit der Diagonalsprache

Satz (Unentscheidbarkeit der Diagonalsprache):
Die Sprache L_d ist nicht entscheidbar.

Unentscheidbarkeit der Diagonalsprache

Satz (Unentscheidbarkeit der Diagonalsprache):
Die Sprache L_d ist nicht entscheidbar.

Beweis:

Falls L_d entscheidbar ist, gibt es eine Turing-Maschine $\mathcal{M}_i$, die

- (1) stets hält,
- (2) genau die $w \in L_d$ akzeptiert.

Wende nun $\mathcal{M}_i$ auf w_i an:

- Falls $w_i \in L_d$, dann wird w_i, wegen (2) von $\mathcal{M}_i$ akzeptiert.
- Falls $w_i \notin L_d$, dann akzeptiert $\mathcal{M}_i$ das Wort w_i wegen (2) nicht.

Beides ist ein Widerspruch zur Definition von L_d.

Korollar

Korollar
Die Sprache $L_d^c := \{0,1\}^* \backslash L_d$ ist nicht entscheidbar.

Korollar

Korollar
Die Sprache $L_d^c := \{0,1\}^* \backslash L_d$ ist nicht entscheidbar.

Beweis:

- Falls L_d^c entscheidbar ist, gibt es eine Turing-Maschine, die L_d^c entscheidet.
- Diese kann aber leicht zu einer Turing-Maschine modifiziert werden, die L_d entscheidet.
- Dies ist ein Widerspruch zur Unentscheidbarkeit der Diagonalsprache.

Korollar

Korollar
Die Sprache $L_d^c := \{0,1\}^* \backslash L_d$ ist nicht entscheidbar.

Beweis:

- Falls L_d^c entscheidbar ist, gibt es eine Turing-Maschine, die L_d^c entscheidet.
- Diese kann aber leicht zu einer Turing-Maschine modifiziert werden, die L_d entscheidet.
- Dies ist ein Widerspruch zur Unentscheidbarkeit der Diagonalsprache.

Interpretation:

- Das Problem, ob eine Turing-Maschine auf einer Eingabe w stoppt, ist nicht entscheidbar.

Das Halteproblem

Das **Halteproblem** definiert folgende Sprache

$$\mathcal{H} := \{wv \mid T_w \text{ hält auf der Eingabe } v\} .$$

Satz (Unentscheidbarkeit des Halteproblems):
$\mathcal{H}$ ist nicht entscheidbar.

Das Halteproblem

Satz (Unentscheidbarkeit des Halteproblems):
$\mathcal{H} = \{wv \mid T_w$ hält auf der Eingabe $v\}$ ist nicht entscheidbar.

Beweis:

- Angenommen es existiert eine stets haltende Turing-Maschine, die $\mathcal{H}$ entscheidet.
- Wir konstruieren daraus eine stets haltende Turing-Maschine, die L_d^c entscheidet, mit Widerspruch zum letzten Korollar.

Sei w eine Eingabe, für die wir entscheiden wollen, ob $w \in L_d^c$.
Wir können wie folgt vorgehen:

- Berechne das i, so dass $w = w_i$ ist.
- Betrachte die durch w_i kodierte Turing-Maschine $\mathcal{M}_i$.
- Wende die Turing-Maschine für $\mathcal{H}$ auf $\langle \mathcal{M}_i \rangle \cdot w_i$ an.

Das Halteproblem

Satz (Unentscheidbarkeit des Halteproblems):
$\mathcal{H} = \{wv \mid T_w$ hält auf der Eingabe $v\}$ ist nicht entscheidbar.

Sei w eine Eingabe, für die wir entscheiden wollen, ob $w \in L_d^c$.
Wir können wie folgt vorgehen:

- Berechne das i, so dass $w = w_i$ ist.
- Betrachte die durch w_i kodierte Turing-Maschine $\mathcal{M}_i$.
- Wende die Turing-Maschine für $\mathcal{H}$ auf $\langle \mathcal{M}_i \rangle \cdot w_i$ an.

Wir machen folgende Fallunterscheidung:

- Falls $\langle \mathcal{M}_i \rangle \cdot w_i$ nicht akzeptiert wird, dann hält $\mathcal{M}_i$ nicht auf w_i.
- Nach Definition von $\mathcal{H}$ ist also $w_i \in L_d$ und damit $w_i \notin L_d^c$.
- Falls $\langle \mathcal{M}_i \rangle \cdot w_i$ akzeptiert wird, dann hält $\mathcal{M}_i$ auf w_i.
- Dann können wir auf der universellen Turing-Maschine die Berechnung von $\mathcal{M}_i$ auf w_i simulieren.

Die Universelle Sprache

Die **universelle Sprache** L_u über $\{0, 1\}$ ist definiert durch

$$L_u := \{wv \mid v \in L(T_w)\}.$$

L_u ist also die Menge aller Wörter wv für die T_w bei der Eingabe v hält und v akzeptiert.

Satz (Unentscheidbarkeit der Universellen Sprache):
Die Sprache L_u ist nicht entscheidbar.

Die Universelle Sprache

Satz (Unentscheidbarkeit der Universellen Sprache):
Die Sprache $L_u := \{wv \mid v \in L(T_w)\}$ ist nicht entscheidbar.

Beweis:

- Wir zeigen, dass L_u eine Verallgemeinerung von L_d^c ist.
- Wir nehmen an, dass es eine TM gibt, die L_u entscheidet.
- Dann zeigen wir, dass wir damit auch L_d^c entscheiden können.

Wir gehen wie folgt vor:

- Berechne das i, für das $w = w_i$.
- Betrachte die durch w_i codierte Turing-Maschine $\mathcal{M}_i$.
- Wende die Turing-Maschine für L_u auf $\langle \mathcal{M}_i \rangle\, w_i$ an.

Wäre L_u entscheidbar, so auch L_d^c im Widerspruch zum letzten Korollar.

Die Universelle Sprache

Satz (Semi-Entscheidbarkeit der Universellen Sprache):
Die Sprache $L_u := \{wv \mid v \in L(T_w)\}$ ist semi-entscheidbar.

Die Universelle Sprache

Satz (Semi-Entscheidbarkeit der Universellen Sprache):
Die Sprache $L_u := \{wv \mid v \in L(T_w)\}$ ist semi-entscheidbar.

Beweis:
Wir benutzen die universelle Turing-Maschine, mit der Eingabe wv:

- Falls T_w die Eingabe v akzeptiert, geschieht dies nach endlich vielen Schritten und die universelle Turing-Maschine akzeptiert wv.
- Falls T_w die Eingabe v nicht akzeptiert, wird wv von der universellen Turing-Maschine ebenfalls nicht akzeptiert. Dies ist unabhängig davon, ob die Simulation stoppt oder nicht.

Die Universelle Sprache

Satz (Semi-Entscheidbarkeit der Universellen Sprache):
Die Sprache $L_u := \{wv \mid v \in L(T_w)\}$ ist semi-entscheidbar.

Beweis:
Wir benutzen die universelle Turing-Maschine, mit der Eingabe wv:

- Falls T_w die Eingabe v akzeptiert, geschieht dies nach endlich vielen Schritten und die universelle Turing-Maschine akzeptiert wv.
- Falls T_w die Eingabe v nicht akzeptiert, wird wv von der universellen Turing-Maschine ebenfalls nicht akzeptiert. Dies ist unabhängig davon, ob die Simulation stoppt oder nicht.

Bemerkung:
Die Begriffe entscheidbar und semi-entscheidbar unterscheiden sich tatsächlich.

Satz von Rice - Motivation

- Wir haben bisher gezeigt, dass wir kein Programm schreiben können, das für ein Turing-Maschinen-Programm $\langle \mathcal{M} \rangle$ und eine Eingabe w entscheidet, ob $\mathcal{M}$ auf der Eingabe w hält.
- Wir werden im Folgenden sehen, dass wir aus einem Programm im Allgemeinen keine nicht-trivialen Eigenschaften der von dem Programm realisierten Funktion ableiten können.

Satz von Rice

Satz (Satz von Rice):
Sei R die Menge der von Turing-Maschinen berechenbaren Funktionen und S eine nicht-triviale Teilmenge von R ($\emptyset \neq S \neq R$). Dann ist die Sprache

$$L(S) := \{\langle \mathcal{M} \rangle \mid \mathcal{M} \text{ berechnet eine Funktion aus } S\}$$

nicht entscheidbar.

Satz von Rice

Satz (Satz von Rice):
Sei R die Menge der von Turing-Maschinen berechenbaren Funktionen und S eine nicht-triviale Teilmenge von R ($\emptyset \neq S \neq R$). Dann ist die Sprache

$$L(S) := \{\langle \mathcal{M} \rangle \mid \mathcal{M} \text{ berechnet eine Funktion aus } S\}$$

nicht entscheidbar.

Beweisskizze:

- Zeige: $\mathcal{H}_\varepsilon := \{\langle \mathcal{M} \rangle \mid \mathcal{M} \text{ hält auf der Eingabe } \varepsilon\}$ ist unentscheidbar
- Zeige: $\mathcal{H}_\varepsilon^c$ ist unentscheidbar
- Führe den Widerspruchsbeweis für die Unentscheidbarkeit von $L(S)$:
- Konstruiere TM für $\mathcal{H}_\varepsilon^c$ unter Benutzung von TM $\mathcal{M}'$ für $L(S)$

Bemerkungen zum Satz von Rice

Der Satz von Rice hat weitreichende Konsequenzen:

Es ist für Programme nicht entscheidbar, ob die durch sie definierte Sprache endlich, leer, unendlich oder ganz Σ^* ist.

Wir haben hier nur die Unentscheidbarkeit von L_d direkt bewiesen.
Die anderen Beweise folgten dem folgenden Schema:

Um zu zeigen, dass ein Problem A unentscheidbar ist, zeigen wir, wie man mit einem Entscheidungsverfahren für A ein bekanntermaßen unentscheidbares Problem B entscheiden kann. Dies liefert den gewünschten Widerspruch.

Das Post'sche Korrespondenzproblem

Post'sches Korrespondenzproblems
Gegeben ist endliche Folge von Wortpaaren

$$K = ((x_1, y_1), \dots, (x_n, y_n))$$

über einem endlichen Alphabet Σ. Es gilt $x_i \neq \varepsilon$ und $y_i \neq \varepsilon$. Gefragt ist, ob es eine endliche Folge von Indizes $i_1, \dots, i_k \in \{1, \dots, n\}$ gibt, so dass $x_{i_1} \dots x_{i_k} = y_{i_1} \dots y_{i_k}$ gilt.

Beispiele

- $K = ((1, 111), (10111, 10), (10, 0))$ hat die Lösung $(2, 1, 1, 3)$, denn es gilt:
$$x_2 x_1 x_1 x_3 = 101111110 = y_2 y_1 y_1 y_3$$
- $K = ((10, 101), (011, 11), (101, 011))$ hat keine Lösung
- $K = ((001, 0), (01, 011), (01, 101), (10, 001))$ hat eine Lösung der Länge 66.

Das Post'sche Korrespondenzproblem

Satz (Unentscheidbarkeit des PKP):
Das Post'sche Korrespondezproblem ist nicht entscheidbar

Beweis:
Beweis über Nicht-Entscheidbarkeit des Halteproblems.

Eigenschaften von (semi-)entscheibaren Sprachen

- Die entscheidbaren Sprachen sind abgeschlossen unter Komplementbildung, Schnitt und Vereinigung.
- Die semi-entscheidbaren Sprachen sind abgeschlossen unter Schnitt und Vereinigung, aber nicht unter Komplementbildung.

Satz:

Sei $L \subseteq \Sigma^*$ und $L^c = \Sigma^* \setminus L$. Dann gilt

- L entscheidbar gdw. L^c entscheidbar.
- L und L^c semi-entscheidbar gdw. L entscheidbar.

Beweis: Übung und Tutorien.