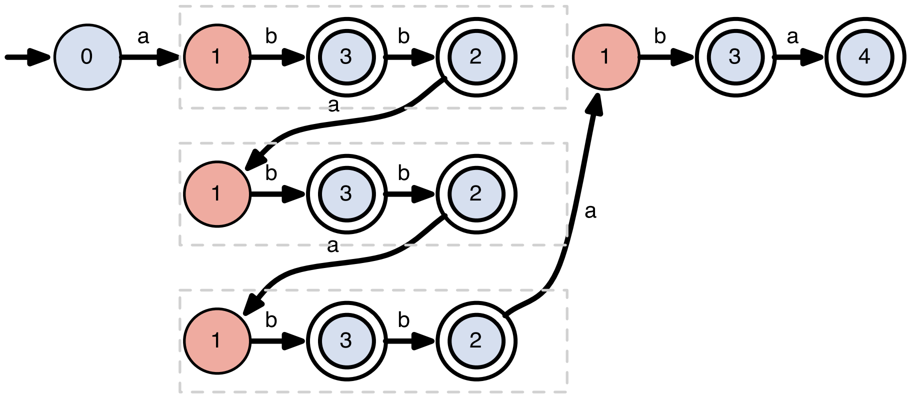
Berechenbarkeitstheorie

15. Vorlesung



Dr. Franziska Jahnke
Institut für Mathematische Logik und Grundlagenforschung
WWU Münster

Reduktionen

- wir haben bereits die Nichtentscheidbarkeit einer Sprache durch Diagonalisierung gezeigt
- Idee lässt sich abwandeln, z.B. für HALT $:= \{\langle M, w\rangle \mid M(w)\downarrow\}$

	1	2	3	4
T_1	$\uparrow$	$\downarrow$	$\downarrow$	$\downarrow$
T_2	$\downarrow$	$\downarrow$	$\downarrow$	$\uparrow$
T_3	$\downarrow$	$\uparrow$	$\downarrow$	$\downarrow$
T_4	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
D	$\downarrow$	$\uparrow$	$\uparrow$	$\uparrow$

Falls HALT $\in \mathbb{E}$ kann ich eine Diagonalisierungsmaschine D bauen

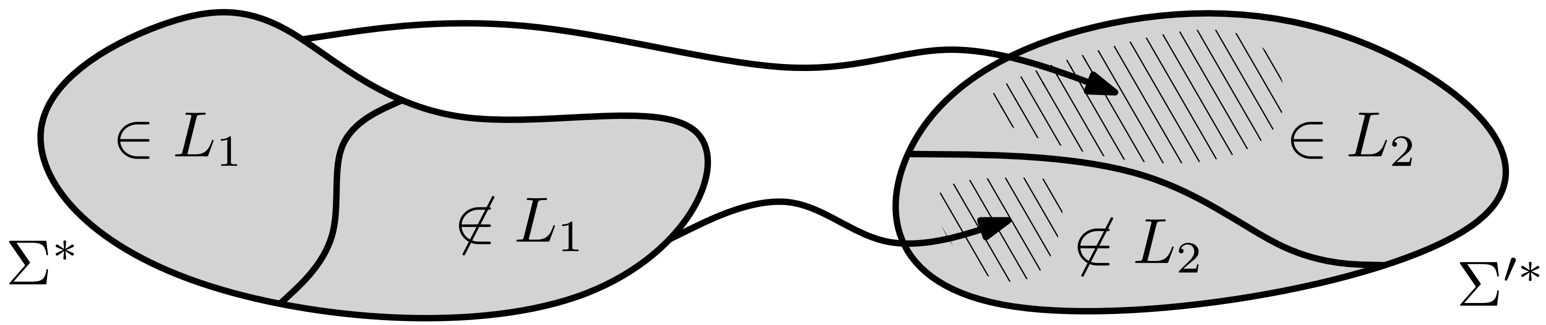
1. entscheide ob Eingabe $\langle M, \langle M\rangle\rangle$ aus HALT
2. Wenn ja, gehe in Endlosschleife, wenn nein stoppe

- D kann nicht existieren $\rightarrow$ HALT ist nicht entscheidbar
- gleiche Konstruktion zeigt, dass SHALT $= \{x \mid M_x(x)\downarrow\} \notin \mathbb{E}$
  (denn für die Diagonalisierung muss ich nur wissen ob $M_x(x)\uparrow$ oder $M_x(x)\downarrow$)
- **Gesucht:** Methode zum Transfer dieser Ergebnisse

Definition

Seien $L_1 \subseteq \Sigma^*$ und $L_2 \subseteq \Sigma'^*$ Sprachen. Die Funktion f heißt **many-one Reduktion von L_1 auf L_2**, gdw.

1. f ist berechenbar und total,
2. $\forall w \in \Sigma^* \colon w \in L_1 \iff f(w) \in L_2$.



f muss weder injektiv noch surjektiv sein (many-one)

Definition

Eine Sprache L_1 ist **many-one reduzierbar** auf L_2, gdw. es eine many-one Reduktion von L_1 auf L_2 gibt.
Schreibweise: $L_1 \leq_m L_2$

Satz 23

Sei $L_1 \leq_m L_2$, dann gilt

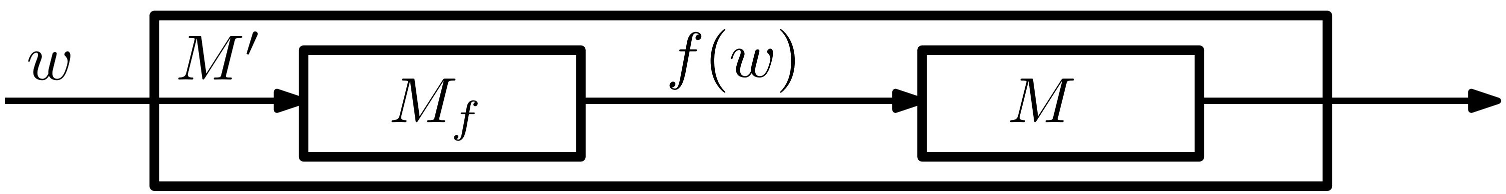
(a) $L_2 \in \mathbb{E} \Rightarrow L_1 \in \mathbb{E}$

(b) $L_2 \in \mathbb{A} \Rightarrow L_1 \in \mathbb{A}$

(c) $L_2 \in \mathbb{A}^{\text{co}} \Rightarrow L_1 \in \mathbb{A}^{\text{co}}$

Beweis (exemplarisch für (a))

- Sei M der Entscheider für L_2 und f eine many-one Reduktion von L_1 auf L_2.
- Sei M_f TM, die f berechnet.
- Konstuiere neue TM M', als Hintereinanderschaltung von M und M_f



$$M'(w) \text{ akz.} \iff M(f(w)) \text{ akz.} \iff f(w) \in L_2 \iff w \in L_1$$

- da M' Entscheider $\rightarrow L_1 \in \mathbb{E}$
- Teil (b) und (c) analog $\square$

Alternativer Beweis für HALT $\notin \mathbb{E}$

- Wir zeigen $A_{\text{TM}} \leq_m$ HALT,
  denn da $A_{\text{TM}} \notin \mathbb{E}$ folgt daraus HALT $\notin \mathbb{E}$.
- Gesucht: Reduktion $f\colon \Sigma^* \to \Sigma^*$

  $f(\langle M, w\rangle) := \langle M', w\rangle$, wobei:

> $M'(z)$
> 1. Simuliere $M(z)$
> 2. Wenn $M(z)$ verwirft, dann zykel
> 3. Ansonsten stoppe

$$\langle M, w\rangle \in A_{\text{TM}} \iff M \text{ akz. } w \iff M'(w)\downarrow \iff \langle M', w\rangle \in \text{HALT}$$

- also: $\langle M, w\rangle \in A_{\text{TM}} \iff f(\langle M, w\rangle) \in \text{HALT}$
- da f berechenbar und total: $A_{\text{TM}} \leq_m \text{HALT} \Rightarrow \text{HALT} \notin \mathbb{E}$

$\square$

Satz 24

$$\mathsf{REG}_{\mathsf{TM}} := \{\langle M\rangle \mid L(M) \in \mathsf{REG}\} \notin \mathbb{E}$$

Beweis

- Wir zeigen $\overline{\mathsf{HALT}} \leq_m \mathsf{REG}_{\mathsf{TM}}$, denn daraus folgt $\mathsf{REG}_{\mathsf{TM}} \notin \mathbb{E}$.
- Gesucht: Reduktion $f\colon \Sigma^* \to \Sigma^*$
  $f(\langle M, w\rangle) := \langle M'\rangle$, wobei:

> $M'(z)$
> 1. Simuliere $M(w)$
> 2. akzeptiere, wenn z die Form $\mathtt{a}^n\mathtt{b}^n$ hat

$$\langle M, w\rangle \in \overline{\mathsf{HALT}} \;\Rightarrow\; M(w)\uparrow \;\Rightarrow\; L(M') = \emptyset \;\Rightarrow\; L(M') \in \mathsf{REG}$$

$$\langle M, w\rangle \notin \overline{\mathsf{HALT}} \;\Rightarrow\; M(w)\downarrow \;\Rightarrow\; L(M') = \{\mathtt{a}^n\mathtt{b}^n \mid n \geq 0\}$$

$$\Rightarrow\; L(M') \notin \mathsf{REG}$$

- f ist berechenbar und total, deshalb $\overline{\mathsf{HALT}} \leq_m \mathsf{REG}_{\mathsf{TM}}$ $\square$

Variation vom Satz 24

Satz 24

E_{TM} $\cancel{\mathsf{REG}_{TM}} := \{\langle M\rangle \mid L(M) \overset{=\emptyset}{\cancel{\in \mathsf{REG}}}\} \notin \mathbb{E}$

Beweis

- Wir zeigen $\overline{\mathsf{HALT}} \leq_m \overset{E_{TM}}{\cancel{\mathsf{REG}_{TM}}}$

$f(\langle M, w\rangle) := \langle M'\rangle$, wobei:

> $M'(z)$
> 1. Simuliere $M(w)$
> 2. akzeptiere, wenn z die Form $\mathtt{a}^n\mathtt{b}^n$ hat

$$\langle M, w\rangle \in \overline{\mathsf{HALT}} \;\Rightarrow\; M(w)\uparrow \Rightarrow\; L(M') = \emptyset \;\Rightarrow\; \cancel{L(M') \in \mathsf{REG}}\ \langle M'\rangle \in E_{TM}$$

$$\langle M, w\rangle \notin \overline{\mathsf{HALT}} \;\Rightarrow\; M(w)\downarrow \Rightarrow\; L(M') = \{\mathtt{a}^n\mathtt{b}^n \mid n \geq 0\}$$

$$\Rightarrow\; \cancel{L(M') \notin \mathsf{REG}}\ \langle M'\rangle \notin E_{TM}$$

Kann ich diese Konstruktion verallgemeinern?

Folgende Sprachen sind alle nicht entscheidbar

$$
\begin{aligned}
L_1 &= \{\langle M\rangle \mid L(M) \in \mathsf{REG}\}\\
L_2 &= \{\langle M\rangle \mid |L(M)| = 14582643\}\\
L_3 &= \{\langle M\rangle \mid M \text{ berechnet totale Funktion}\}\\
L_4 &= \{\langle M\rangle \mid f_M \equiv 0\}
\end{aligned}
$$

- Beweise sehr ähnlich zum Satz 24

Formalisierung dieses Typs von Sprachen

- Sei $\mathcal{R} = \{f \subseteq \Sigma^* \times \Sigma^* \mid f \text{ rechtseindeutig und berechenbar}\}$ die Menge der partiell berechenbaren Funktionen
- Eine Teilmenge $\mathcal{U} \subseteq \mathcal{R}$ heißt **Eigenschaft** von $\mathcal{R}$

  Beispiel $\{f \in \mathcal{R} \mid f \text{ ist total}\}$ ist Eigenschaft

  Beispiel $\{f \in \mathcal{R} \mid f \equiv 0\}$ ist Eigenschaft
- Die Eigenschaften $\mathcal{U} = \emptyset$ und $\mathcal{U} = \mathcal{R}$ heißen **triviale Eigenschaften**.
- Struktur von $(L_1, L_2,)L_3, L_4$: Programme aller Funktionen mit Eigenschaft X.

Satz von Rice

Für eine nicht-triviale Eigenschaft $\mathcal{U} \subset \mathcal{R}$ gilt

$$L_{\mathcal{U}} := \{\langle M \rangle \mid f_M \in \mathcal{U}\} \notin \mathbb{E}.$$

Beweis

Wir zeigen: $\text{HALT} \leq_m L_{\mathcal{U}}$

$$f \colon \langle M, w \rangle \to \langle M' \rangle$$

Sei f_0 die überall undefinierte Funktion

1. Fall: $f_0 \notin \mathcal{U}$

wir wählen $f_u \in \mathcal{U}$ und TM M_u die f_u berechnet (existiert, da $\mathcal{U} \neq \emptyset$)

Die Reduktion arbeitet wie folgt: Zu einem gegebenen $\langle M, w \rangle$ konstruieren wir folgende Maschine M'

$M'(z)$

1. Simuliere $M(w)$
2. Simuliere $M_u(z)$

$M'(z)$
1. Simuliere $M(w)$ $(f_0 \notin \mathcal{U})$
2. Simuliere $M_u(z)$ $(f_u \in \mathcal{U})$

Reduktion! Fall 1

$\langle M, w\rangle \notin$ HALT $\Rightarrow$ M'stoppt bei keiner Eingabe
$\Rightarrow$ M' berechnet f_0
$\Rightarrow$ $\langle M'\rangle \notin L_{\mathcal{U}}$

$\langle M, w\rangle \in$ HALT $\Rightarrow$ M' rechnet wie M_u
$\Rightarrow$ $\langle M'\rangle \in L_{\mathcal{U}}$

Also: $L_{\mathcal{U}} \notin \mathbb{E}$

2. Fall: $f_0 \in \mathcal{U}$

betrachte $L_{\bar{\mathcal{U}}} = \{\langle M\rangle \mid M$ berechnet Fkt. aus $\bar{\mathcal{U}}\}$
$= \{\langle M\rangle \mid M$ berechnet nicht Fkt. aus $\mathcal{U}\} = \overline{L_{\mathcal{U}}}$

nach Fall 1 haben wir (da $f_0 \notin \overline{\mathcal{U}}$), dass $L_{\bar{\mathcal{U}}} \notin \mathbb{E} \Rightarrow \overline{L_{\mathcal{U}}} \notin \mathbb{E}$

Da die entscheidbaren Sprachen aber unter Komplement abgeschlossen sind (Tausch q_A/q_V), ist somit auch $L_{\mathcal{U}} \notin \mathbb{E}$

Satz von Rice – Anwendungen

Folgende Sprachen sind nach dem Satz von Rice nicht entscheidbar:

$$L_1 = \{\langle M\rangle \mid f_M \text{ Bijektion } \}$$
$$L_2 = \{\langle M\rangle \mid f_M \text{ monoton steigend}\}$$

Insbesondere gilt für $\mathcal{U} = \{g\}$:

$$L_3 = \{\langle M\rangle \mid f_M \equiv g\} \notin \mathbb{E}$$

Nach 1-1-Beziehung von $\{0,1\}^{\Sigma^*}$ und Sprachen über Σ erhält man:

Korollar
Sei $\mathcal{L} \subsetneq \{L \in \mathbb{A}\}$ mit $\mathcal{L} \neq \emptyset$ dann ist $\{\langle M\rangle \mid L(M) \in \mathcal{L}\} \notin \mathbb{E}$

Folgende Sprachen sind nach dem Korollar nicht entscheidbar:

$$L_4 = \{\langle M\rangle \mid |L(M)| = 100\}$$
$$L_5 = \{\langle M\rangle \mid L(M) \in \mathbb{E} \setminus \text{REG}\}$$

Hier trifft der Satz von Rice keine Aussage

$$L_6 = \{\langle M\rangle \mid M \text{ stoppt auf allen Eingaben nach 100 Schritten}\}$$
$$L_7 = \{\langle M\rangle \mid M \text{ besucht bei Eingabe } \varepsilon \text{ Zustand } q_0 \text{ mehrfach}\}$$

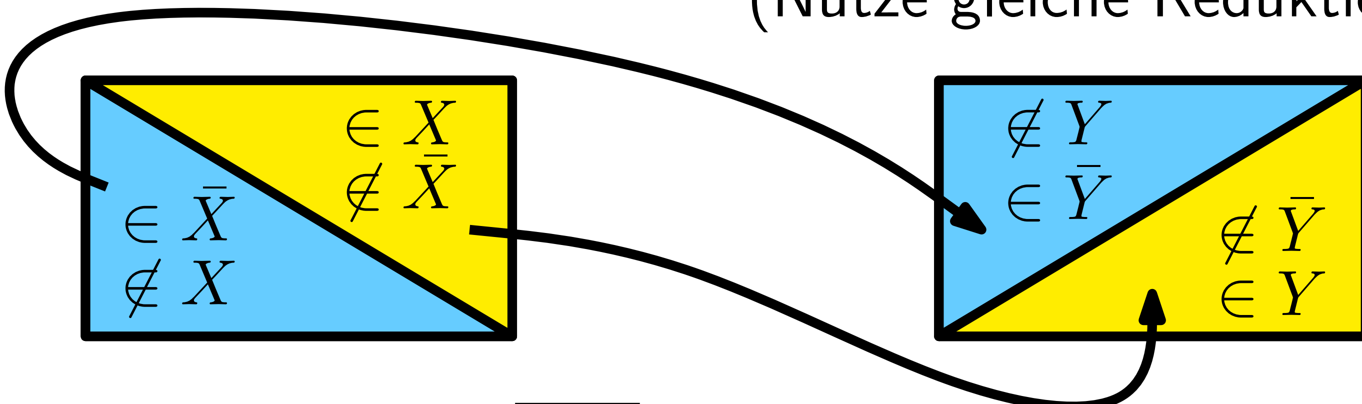
Satz 25

$\mathsf{EQ}_{\mathsf{TM}} := \{\langle M_1, M_2\rangle \mid L(M_1) = L(M_2)\} \notin \mathbb{A} \cup \mathbb{A}^{\mathsf{co}}$

Beweis

Vorüberlegung: $X \leq_m Y \iff \bar{X} \leq_m \bar{Y}$

(Nutze gleiche Reduktionsfunktion)



Wir zeigen: (a) $\overline{A_{\mathsf{TM}}} \leq_m \mathsf{EQ}_{\mathsf{TM}}$ $(\rightarrow \mathsf{EQ}_{\mathsf{TM}} \notin \mathbb{A})$

(b) $\overline{A_{\mathsf{TM}}} \leq_m \overline{\mathsf{EQ}_{\mathsf{TM}}}$ $(\rightarrow \overline{\mathsf{EQ}_{\mathsf{TM}}} \notin \mathbb{A}$

$\rightarrow \mathsf{EQ}_{\mathsf{TM}} \notin \mathbb{A}^{\mathsf{co}})$

Um die Reduktionen anzugeben nutzen wir die Reduktionen der Komplemente nach Vorüberlegung

Wir zeigen: (a') $A_{\mathsf{TM}} \leq_m \overline{\mathsf{EQ}_{\mathsf{TM}}}$

(b') $A_{\mathsf{TM}} \leq_m \mathsf{EQ}_{\mathsf{TM}}$

(a') $A_{\mathsf{TM}} \leq_m \overline{\mathsf{EQ}_{\mathsf{TM}}}$

- $\langle M, w\rangle$ Eingabe – Reduktion bildet ab auf $\langle M_1, M_2\rangle$

$$\begin{array}{lcl} M_1(z) & : & \text{verwirft immer} \\ M_2(z) & : & \text{1. Simuliere } M(w) \\ & & \text{2. akzeptiere, gdw. } M(w) \text{ akz.} \end{array}$$

$$\langle M, w\rangle \in A_{\mathsf{TM}} \Rightarrow M_2 \text{ akz. immer} \Rightarrow L(M_1) \neq L(M_2) \Rightarrow \langle M_1, M_2\rangle \in \overline{\mathsf{EQ}_{\mathsf{TM}}}$$

$$\langle M, w\rangle \notin A_{\mathsf{TM}} \Rightarrow M_2 \text{ akz. nie} \Rightarrow L(M_1) = L(M_2) \Rightarrow \langle M_1, M_2\rangle \notin \overline{\mathsf{EQ}_{\mathsf{TM}}}$$

(b') $A_{\mathsf{TM}} \leq_m \mathsf{EQ}_{\mathsf{TM}}$

- $\langle M, w\rangle$ Eingabe – Reduktion bildet ab auf $\langle M_1, M_2\rangle$

$$\begin{array}{lcl} M_1(z) & : & \text{akzeptiert immer} \\ M_2(z) & : & \text{1. Simuliere } M(w) \\ & & \text{2. akzeptiere, gdw. } M(w) \text{ akz.} \end{array}$$

$$\langle M, w\rangle \in A_{\mathsf{TM}} \Rightarrow M_2 \text{ akz. immer} \Rightarrow L(M_1) = L(M_2) \Rightarrow \langle M_1, M_2\rangle \in \mathsf{EQ}_{\mathsf{TM}}$$

$$\langle M, w\rangle \notin A_{\mathsf{TM}} \Rightarrow M_2 \text{ akz. nie} \Rightarrow L(M_1) \neq L(M_2) \Rightarrow \langle M_1, M_2\rangle \notin \mathsf{EQ}_{\mathsf{TM}} \qquad \square$$