Theoretische Informatik HS24

Nicolas Wehrli

Übungsstunde 09

19. November 2024

ETH Zürich
nwehrl@ethz.ch

Heute

1. Feedback zur Serie
2. Reduktion continued
3. Satz von Rice - Beweis
4. EE Reduktion angewendet für $\mathcal{L}_{\mathrm{RE}}$
5. Worked example
6. Reduktionsaufgaben

Feedback zur Serie

Feedback zur Serie

- Recht gut.
- EE-Reduktion braucht nur das Eingabe zu Eingabe Mapping.
- Ihr müsst erwähnen, dass eure TM terminiert!

Reduktion continued

Aufgabe 5.22

Wir zeigen

$$L \in \mathcal{L}_{\mathrm{RE}} \wedge L^{\complement} \in \mathcal{L}_{\mathrm{RE}} \iff L \in \mathcal{L}_{\mathrm{R}}$$

$(\implies)$:

Nehmen wir $L \in \mathcal{L}_{\mathrm{RE}} \wedge L^{\complement} \in \mathcal{L}_{\mathrm{RE}}$ an.

Dann existiert eine TM M und M_C mit $L(M) = L$ und $L(M_C) = L^{\complement}$.

Wir konstruieren eine TM A, die für eine Eingabe w die beiden TM's M und M_C parallel auf w simuliert.

A akzeptiert w, falls M das Wort akzeptiert und verwirft, falls M_C das Wort akzeptiert.

Aufgabe 5.22

Bemerke, dass $L(M) \cap L(M_C) = \emptyset$ und $L(M) \cup L(M_C) = \Sigma^*$.

Da $w \in L(M)$ oder $w \in L(M_C)$, hält A immer.

Da A genau dann akzeptiert, falls $w \in L(M)$, folgt $L(A) = L(M) = L$.

Demnach gilt $L \in \mathcal{L}_\mathrm{R}$.

$(\Longleftarrow):$

Nehmen wir $L \in \mathcal{L}_\mathrm{R}$ an. Per Lemma 5.4 gilt $L^\complement \leq_\mathrm{R} L$ und daraus folgt auch $L^\complement \in \mathcal{L}_\mathrm{R}$.

Da $\mathcal{L}_\mathrm{R} \subset \mathcal{L}_\mathrm{RE}$, folgt $L \in \mathcal{L}_\mathrm{RE} \wedge L^\complement \in \mathcal{L}_\mathrm{RE}$.

$\blacksquare$

Satz von Rice - Beweis

Satz von Rice

Satz 5.9

Jedes semantisch nichttriviale Entscheidungsproblem über Turingmaschinen ist unentscheidbar.

Prerequisites

Zur Erinnerung:

Semantisch nichttriviales Entscheidungsproblem über TMs

Das Entscheidungsproblem (Σ, L), bzw. die Sprache L muss folgendes erfüllen.

I. $L \subseteq \textbf{KodTM}$
II. $\exists M_1$ so dass $\mathrm{Kod}(M_1) \in L$(i.e. $L \neq \emptyset$)
III. $\exists M_2$ so dass $\mathrm{Kod}(M_2) \notin L$(i.e. $L \neq \textbf{KodTM}$)
IV. Für zwei TM A und B mit $L(A) = L(B)$ gilt

$$\mathrm{Kod}(A) \in L \iff \mathrm{Kod}(B) \in L$$

$\textbf{KodTM} \subseteq (\Sigma_{\text{bool}})^*$ ist die Menge aller Kodierungen von Turingmaschinen.

Wir brauchen

Lemma 5.8

$$L_{H,\lambda} \notin \mathcal{L}_{\mathrm{R}}$$

Zur Erinnerung:

$$L_{H,\lambda} = \{\mathrm{Kod}(M) \mid M \text{ hält auf } \lambda\}$$

Idee

Wir zeigen für jedes **semantisch nichtriviale Entscheidungsproblem** (Σ, L)

$$L \in \mathcal{L}_{\mathrm{R}} \implies L_{H,\lambda} \in \mathcal{L}_{\mathrm{R}}$$

Aus dem folgt dann per Kontraposition

$$L_{H,\lambda} \notin \mathcal{L}_{\mathrm{R}} \implies L \notin \mathcal{L}_{\mathrm{R}}$$

Mit der Aussage $L_{H,\lambda} \notin \mathcal{L}_{\mathrm{R}}$ von **Lemma 5.8**, können wir dann

$$L \notin \mathcal{L}_{\mathrm{R}}$$

wie gewünscht folgern.

Idee

Wir müssen noch die Implikation

$$L \in \mathcal{L}_{\mathrm{R}} \implies L_{H,\lambda} \in \mathcal{L}_{\mathrm{R}}$$

beweisen.

Kernidee

Wir zeigen die **Existenz** einer Reduktion, aus der die Implikation folgt.

Idee

Konkret machen wir eine **Case Distinction** und zeigen jeweils

- Die **Existenz** einer EE-Reduktion von $L_{H,\lambda}$ auf L
  Daraus folgt $L_{H,\lambda} \leq_{\text{EE}} L$.
- oder die **Existenz** einer EE-Reduktion $L_{H,\lambda}$ auf $L^{\complement}$
  Daraus folgt $L_{H,\lambda} \leq_{\text{EE}} L^{\complement}$.

Zur Erinnerung:

Lemma 5.3

Seien $L_1 \subseteq \Sigma_1^*$ und $L_2 \subseteq \Sigma_2^*$ zwei Sprachen.

$$L_1 \leq_{\text{EE}} L_2 \implies L_1 \leq_{\text{R}} L_2$$

Idee

Weshalb reicht es $L_{H,\lambda} \leq_{\mathrm{EE}} L^{\complement}$ zu zeigen?

Lemma 5.4

Sei Σ ein Alphabet. Für jede Sprache $L \subseteq \Sigma^*$ gilt:

$$L \leq_{\mathrm{R}} L^{\complement} \text{ und } L^{\complement} \leq_{\mathrm{R}} L$$

In beiden Cases folgt mit **Lemma 5.3** und **Lemma 5.4**, die gewünschte Aussage $L_{H,\lambda} \leq_{\mathrm{R}} L$.

Idee

Explizit gilt nun

1. $$L_{H,\lambda} \leq_{\text{EE}} L^{\complement} \xRightarrow{\textbf{Lemma 5.3}} L_{H,\lambda} \leq_{\text{R}} L^{\complement} \xRightarrow{\textbf{Lemma 5.4}} L_{H,\lambda} \leq_{\text{R}} L$$

2. $$L_{H,\lambda} \leq_{\text{EE}} L \xRightarrow{\textbf{Lemma 5.3}} L_{H,\lambda} \leq_{\text{R}} L$$

Aus $L_{H,\lambda} \leq_{\text{R}} L$ folgt (in beiden Cases) die gewünschte Implikation

$$L \in \mathcal{L}_{\text{R}} \implies L_{H,\lambda} \in \mathcal{L}_{\text{R}}$$

Beweis

Sei $M_\emptyset$ eine TM s.d. $L(M_\emptyset) = \emptyset$.

Case Distinction

I. $\mathbf{Kod}(\mathbf{M}_\emptyset) \in \mathbf{L}$
   Wir zeigen $L_{H,\lambda} \leq_{\text{EE}} L^\complement$.
II. $\mathbf{Kod}(\mathbf{M}_\emptyset) \notin \mathbf{L}$
   Wir zeigen $L_{H,\lambda} \leq_{\text{EE}} L$.

Case I. $\mathbf{Kod}(\mathbf{M}_\emptyset) \in \mathbf{L}$

Es **existiert** eine TM $\overline{M}$, so dass $\text{Kod}(\overline{M}) \notin L$. (Nichttrivialität)

Wir beschreiben eine TM S, so dass für eine Eingabe $x \in (\Sigma_{\text{bool}})^*$

$$x \in L_{H,\lambda} \iff S(x) \in L^{\complement}$$

Daraus folgt dann die gewünschte EE-Reduktion.

Wir verwenden dabei $M_\emptyset$ und $\overline{M}$, da $\text{Kod}(M_\emptyset) \notin L^{\complement}$ und $\text{Kod}(\overline{M}) \in L^{\complement}$.

Case I. Kod($\mathbf{M}_\emptyset$) $\in$ L - Beschreibung von S

Eingabe $x \in (\Sigma_{\text{bool}})^*$

1. S überprüft ob $x = \text{Kod}(M)$ für eine TM M.
   Falls dies **nicht** der Fall ist, gilt $S(x) = \text{Kod}(M_\emptyset)$
2. Sonst $x = \text{Kod}(M)$. Dann $S(x) = \text{Kod}(A)$, wobei A wie folgt kodiert ist.
   i. Gleiches Eingabealphabet wie $\overline{M}$, i.e. $\Sigma_A = \Sigma_{\overline{M}}$.
   ii. Für eine beliebige Eingabe $y \in (\Sigma_{\overline{M}})^*$, simuliert A zuerst M auf λ **ohne die Eingabe** y **zu überschreiben**.
   iii. Danach simuliert A die TM $\overline{M}$ auf die gegebene Eingabe y.
   iv. Akzeptiert y genau dann, wenn $\overline{M}$ y akzeptiert.

Korrektheit

Wir zeigen

$$x \in L_{H,\lambda} \iff S(x) \in L^{\complement}$$

$(\implies)$:

Wir nehmen $x \in L_{H,\lambda}$ an und zeigen $S(x) \in L^{\complement}$.

Da M auf λ hält, wird A immer $\overline{M}$ auf der Eingabe y simulieren und wir haben $L(A) = L(\overline{M})$.

Da L (und somit auch $L^{\complement}$) ein **semantisches** Entscheidungsproblem ist, gilt

$$\mathrm{Kod}(\overline{M}) \in L^{\complement} \implies \mathrm{Kod}(A) \in L^{\complement}$$

Da die LHS der Implikation gegeben ist, folgt $S(x) = \mathrm{Kod}(A) \in L^{\complement}$

Korrektheit

$(\Longleftarrow):$

Wir nehmen $x \notin L_{H,\lambda}$ an und zeigen $S(x) \notin L^{\complement}$.

Aus Kontraposition folgt dann die gewünschte Rückimplikation.

Da M nicht auf λ hält, wird A bei jeder Eingabe nicht halten.

Somit folgt $L(A) = L(M_{\emptyset})$ und da $\mathrm{Kod}(M_{\emptyset}) \notin L^{\complement}$ per semantische Eigenschaft von L

$$S(x) = \mathrm{Kod}(A) \notin L^{\complement}$$

Case II.

Zweite Case funktioniert genau gleich.

Wir haben $\mathrm{Kod}(M_\emptyset) \notin L$.

Per Nichttrivialität existiert eine TM $\overline{M}$ mit $\mathrm{Kod}(\overline{M}) \in L$.

...

$\blacksquare$

EE Reduktion angewendet für $\mathcal{L}_{\mathrm{RE}}$

Lemma zu RE-Reduktion

EE-Reduktion impliziert RE-Reduktion (**nicht in der Vorlesung**)

$$L_1 \leq_{\mathrm{EE}} L_2 \implies (L_2 \in \mathcal{L}_{\mathrm{RE}} \implies L_1 \in \mathcal{L}_{\mathrm{RE}})$$

Beweis

Sei $L_1 \leq_{\mathrm{EE}} L_2$ und $L_2 \in \mathcal{L}_{\mathrm{RE}}$.

Wir zeigen nun $L_1 \in \mathcal{L}_{\mathrm{RE}}$.

Per Definition von $L_1 \leq_{\mathrm{EE}} L_2$ existiert ein Algorithmus F, der die Funktion $f : \Sigma_1^* \to \Sigma_2^*$ berechnet, so dass

$$\forall x \in \Sigma_1^*. x \in L_1 \iff f(x) \in L_2$$

Lemma zu RE-Reduktion

Da $L_2 \in \mathcal{L}_{\text{RE}}$ existiert eine TM M_2 (die nicht unbedingt immer terminiert) mit $L(M_2) = L_2$.

Wir beschreiben mit F und M_2 nun eine TM M_1 mit $L(M_1) = L_1$.

Eingabe: $x \in \Sigma_1^*$

1. F berechnet auf x und übergibt seine Ausgabe $f(x)$ zur TM M_2
2. M_2 berechnet auf $f(x)$ und die Ausgabe wird übernommen.

Lemma zu RE-Reduktion

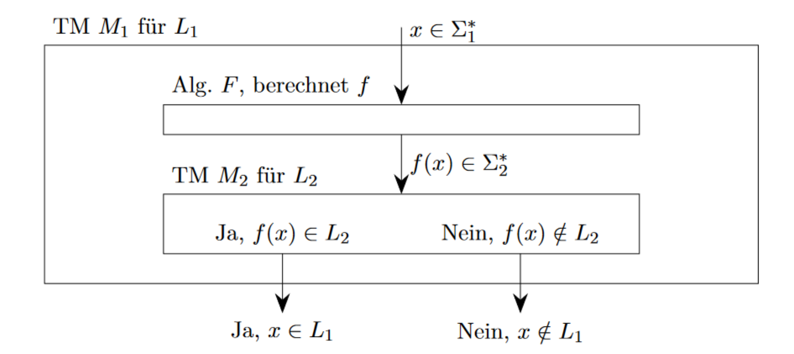

Abbildung 1: TM M_1, Zsf. Fabian Frei

Lemma zu RE-Reduktion

Korrektheit $(L_1 = L(M_1))$

Case Distinction

I. $\mathbf{x} \in \mathbf{L_1}$

$\implies f(x) \in L_2$ (Algorithmus F terminiert immer)

$L(M_2) = L_2 \implies f(x) \in L(M_2)$

da die Ausgabe von M_2 übernommen wird

$\implies x \in L(M_1)$

II. $\mathbf{x} \notin \mathbf{L_1}$

$\implies f(x) \notin L_2$

$\implies f(x) \notin L(M_2)$

$\implies x \notin L(M_1)$

$\blacksquare$

Worked example

Worked example

Aufgabe

Sei $L_{\text{all}} = \{\text{Kod}(M) \mid M \text{ akzeptiert jede Eingabe}\}$.

Zeigen Sie $L_{\text{H}}^{\complement} \leq_{\text{EE}} L_{\text{all}}$.

Kernidee

Für eine Eingabe $x = \text{Kod}(M)\#w$, generieren wir $\text{Kod}(A)$ einer TM A, die folgendes folgendes macht:

Worked example

A :

Eingabe y

1. Berechnet $|y|$ Schritte von M auf w.
2. Falls danach die Berechnung nach $|y|$ noch nicht terminiert hat, akzeptiert A die Eingabe y.
3. Sonst verwirft A die Eingabe.

$$A \text{ akzeptiert jede Eingabe} \iff M \text{ läuft unendlich auf } w$$
$$\text{Kod}(A) \in L_{\text{all}} \iff \text{Kod}\#w \in L_H^{\complement}$$

$L_1 \leq_{\mathbf{R}} L_2 \;\not\Longrightarrow\; (L_2 \in \mathcal{L}_{\mathbf{RE}} \implies L_1 \in \mathcal{L}_{\mathbf{RE}})$

Wir beweisen diese Aussage per Gegenbeispiel.

Sei $L_1 = L_{\text{diag}}$ und $L_2 = L_{\text{diag}}^{\complement}$.

Wir haben

- $L_1 = L_{\text{diag}} \notin \mathcal{L}_{\text{RE}}$ (Satz 5.5)
- $L_2 = L_{\text{diag}}^{\complement} \in \mathcal{L}_{\text{RE}} \setminus \mathcal{L}_{\text{R}}$ (Korollar 5.2, Lemma 5.5)

Per **Lemma 5.4** gilt $L_{\text{diag}} \leq_{\text{R}} L_{\text{diag}}^{\complement}$.

Die rechte Implikation gilt jedoch nicht.

■

$L_1 \leq_{\mathbf{R}} L_2 \;\not\Longleftarrow\; (L_2 \in \mathcal{L}_{\mathbf{RE}} \implies L_1 \in \mathcal{L}_{\mathbf{RE}})$

Sei $L_1 = L_{\mathrm{U}}$ und $L_2 = \{0^i \mid i \in \mathbb{N}\}$.

Wir haben

- $L_1 = L_{\mathrm{U}} \in \mathcal{L}_{\mathrm{RE}} \setminus \mathcal{L}_{\mathrm{R}}$ (Satz 5.6 und 5.7)
- $L_2 = \{0^i \mid i \in \mathbb{N}\} \in \mathcal{L}_{\mathrm{R}}$ (da $\mathcal{L}_{\mathrm{EA}} \subset \mathcal{L}_{\mathrm{R}}$)

Da $L_1 \in \mathcal{L}_{\mathrm{RE}}$, gilt die Implikation auf der rechten Seite für dieses L_1 und L_2.

Da per Definition

$$L_1 \leq_{\mathrm{R}} L_2 \iff (L_2 \in \mathcal{L}_{\mathrm{R}} \implies L_1 \in \mathcal{L}_{\mathrm{R}})$$

folgt aus $L_1 \notin \mathcal{L}_{\mathrm{R}}$ und $L_2 \in \mathcal{L}_{\mathrm{R}}$, dass diese Instanzierung von L_1 und L_2 ein Gegenbeispiel ist.

$\blacksquare$

Relation zu EE-Reduktion

Wir haben aber gezeigt, dass

$$L_1 \leq_{\mathrm{EE}} L_2 \implies L_1 \leq_{\mathrm{R}} L_2$$

und

$$L_1 \leq_{\mathrm{EE}} L_2 \implies (L_2 \in \mathcal{L}_{\mathrm{RE}} \implies L_1 \in \mathcal{L}_{\mathrm{RE}})$$

Die Rückrichtung gilt jeweils nicht.

Reduktionsaufgaben

Aufgabe 1

Zeige

$$L_{\text{diag}} \leq_{\text{EE}} L_{\text{H}}^{\complement}$$

Zur Erinnerung:

$$L_{\text{diag}} = \{w_i \in (\Sigma_{\text{bool}})^* \mid M_i \text{ akzeptiert } w_i \text{ nicht}\}$$

$$\begin{aligned} L_{\text{H}}^{\complement} = &\{\text{Kod}(M)\#w \in \{0,1,\#\}^* \mid M \text{ hält nicht auf } w\} \\ &\cup \{x \in \{0,1,\#\}^* \mid x \text{ nicht von der Form } \text{Kod}(M)\#w\} \end{aligned}$$

Lösung 1

Wir beschreiben einen Algorithmus A, so dass

$$x \in L_{\text{diag}} \iff A(x) \in L_{\text{H}}^{\complement}$$

Eingabe: $x \in (\Sigma_{\text{bool}})^*$

1. Findet i so dass $x = w_i$
2. Generiert Kod(M_i)
3. Generiert Kod$(\overline{M}_i)$ mit folgenden Modifikationen zu Kod(M_i)
   - Transitionen nach q_{reject} werden in eine Endlosschleife umgeleitet.
4. Gibt Kod$(\overline{M}_i)\#w_i$ aus.

Lösung 1

Case Distinction

I. $\mathbf{x} \in \mathbf{L}_{\text{diag}}$

$$\begin{aligned} &\implies M_i \text{ akzeptiert } x = w_i \text{ nicht} \\ &\implies \overline{M}_i \text{ hält nicht auf } w_i \\ &\implies A(x) = \text{Kod}(\overline{M}_i)\#w_i \in L_{\text{H}}^{\complement} \end{aligned}$$

II. $\mathbf{x} \notin \mathbf{L}_{\text{diag}}$

$$\begin{aligned} &\implies M_i \text{ akzeptiert } x = w_i \\ &\implies \overline{M}_i \text{ hält auf } w_i \\ &\implies A(x) = \text{Kod}(\overline{M}_i)\#w_i \notin L_{\text{H}}^{\complement} \end{aligned}$$

$\blacksquare$

Aufgabe 2

Zeige

$$L_{\mathrm{U}}^{\mathtt{C}} \leq_{\mathrm{EE}} L_{\mathrm{diag}}$$