Grundbegriffe der Informatik

Übung

Simon Wacker

Karlsruher Institut für Technologie

Wintersemester 2015/2016

Nerode-Relation

L formale Sprache über X

Nerode-Relation $\equiv_L$ auf X^*

$$\forall w, w' \in X^* : w \equiv_L w' \leftrightarrow (\forall u \in X^* : wu \in L \leftrightarrow w'u \in L)$$

$\equiv_L$ ist Äquivalenzrelation

Äquivalenzklasse von $w \in X^*$

$$[w]_{\equiv_L} = \{w' \in X^* \mid w \equiv_L w'\}$$

Faktormenge

$$X^*_{/\equiv_L} = \{[w]_{\equiv_L} \mid w \in X^*\}$$

Nerode-Akzeptor

L formale Sprache über X so, dass $|X^*_{/\equiv_L}| < \infty$

Nerode-Akzeptor $A_L = (Z, z_0, X, f, F)$

- $Z = X^*_{/\equiv_L}$
- $z_0 = [\varepsilon]_{\equiv_L}$
- $f : Z \times X \to Z, ([w]_{\equiv_L}, x) \mapsto [wx]_{\equiv_L}$
- $F = \{[w]_{\equiv_L} \mid w \in L\}$

A_L ist wohldefiniert

Theorem: $L(A_L) = L$

Schrittweiser Beweis von $L(A_L) = L$

$$L(A_L) = \{w \in X^* \mid f^*(z_0, w) \in F\}$$

Lemma 1: $\forall w \in X^* : f^*(z_0, w) = [w]_{\equiv_L}$

Lemma 2: $\forall w \in X^* : [w]_{\equiv_L} \in F \leftrightarrow w \in L$

Folgerung: $\forall w \in X^* : w \in L(A_L) \leftrightarrow f^*(z_0, w) \in F$

$$\leftrightarrow [w]_{\equiv_L} \in F$$

$$\leftrightarrow w \in L$$

Schrittweiser Beweis von $L(A_L) = L$

$$L(A_L) = \{w \in X^* \mid f^*(z_0, w) \in F\}$$

Lemma 1: $\forall w \in X^* : f^*(z_0, w) = [w]_{\equiv_L}$

Beweis durch strukturelle Induktion:

I.A. $f^*(z_0, \varepsilon) = z_0 = [\varepsilon]_{\equiv_L}$

I.S. Es sei $w \in X^*$ derart, dass $f^*(z_0, w) = [w]_{\equiv_L}$ (I.V.).
Dann gilt für jedes $x \in X$,

$$\begin{aligned} f^*(z_0, wx) &= f(f^*(z_0, w), x) \\ &= f([w]_{\equiv_L}, x) \\ &= [wx]_{\equiv_L}. \end{aligned}$$

Schrittweiser Beweis von $L(A_L) = L$

$$L(A_L) = \{w \in X^* \mid f^*(z_0, w) \in F\}$$

Lemma 1: $\forall w \in X^* : f^*(z_0, w) = [w]_{\equiv_L}$

Lemma 2: $\forall w \in X^* : [w]_{\equiv_L} \in F \leftrightarrow w \in L$

Beweis:

$\rightarrow$ Es gelte $[w]_{\equiv_L} \in F$.
Dann gibt es $w' \in L$ so, dass $[w']_{\equiv_L} = [w]_{\equiv_L}$.
Also $w' \in [w]_{\equiv_L}$.
Das heißt $w \equiv_L w'$.
Insbesondere $w \in L \leftrightarrow w' \in L$.
Folglich $w \in L$.

$\leftarrow$ Es gelte $w \in L$. Dann $[w]_{\equiv_L} \in F$.

Schrittweiser Beweis von $L(A_L) = L$

$$L(A_L) = \{w \in X^* \mid f^*(z_0, w) \in F\}$$

Lemma 1: $\forall w \in X^* : f^*(z_0, w) = [w]_{\equiv_L}$

Lemma 2: $\forall w \in X^* : [w]_{\equiv_L} \in F \leftrightarrow w \in L$

Folgerung: $\forall w \in X^* : w \in L(A_L) \leftrightarrow f^*(z_0, w) \in F$

$$\leftrightarrow [w]_{\equiv_L} \in F$$

$$\leftrightarrow w \in L$$

Akzeptor-Relation

$A = (Z, z_0, X, f, F)$ endlicher Akzeptor

Akzeptor-Relation $\equiv_A$ auf X^*

$$\forall w, w' \in X^* : w \equiv_A w' \leftrightarrow f^*(z_0, w) = f^*(z_0, w')$$

$\equiv_A$ ist Äquivalenzrelation

Lemma 3: $\forall w, w' \in X^* : (w \equiv_A w' \rightarrow w \equiv_{L(A)} w')$

Folgerungen:

- $\forall w \in X^* : [w]_{\equiv_A} \subseteq [w]_{\equiv_{L(A)}}$
- $|X^*_{/\equiv_{L(A)}}| \leq |X^*_{/\equiv_A}| \leq |Z| < \infty$
- $A_{L(A)}$ hat kleinste Anzahl von Zuständen

Akzeptor-Relation

$A = (Z, z_0, X, f, F)$ endlicher Akzeptor

Akzeptor-Relation $\equiv_A$ auf X^*

$$\forall w, w' \in X^* : w \equiv_A w' \leftrightarrow f^*(z_0, w) = f^*(z_0, w')$$

Lemma 3: $\forall w, w' \in X^* : (w \equiv_A w' \rightarrow w \equiv_{L(A)} w')$

Beweis: Es seien $w, w' \in X^*$ so, dass $w \equiv_A w'$.
Weiter sei $u \in X^*$.
Dann $f^*(z_0, wu) = f^*(f^*(z_0, w), u)$

$$= f^*(f^*(z_0, w'), u) = f^*(z_0, w'u)$$

Also $f^*(z_0, wu) \in F \leftrightarrow f^*(z_0, w'u) \in F$.
Das heißt $wu \in L(A) \leftrightarrow w'u \in L(A)$.
Folglich $w \equiv_{L(A)} w'$.

Charakterisierung regulärer Sprachen

L formale Sprache über X

Satz: L regulär $\leftrightarrow |X^*_{/\equiv_L}| < \infty$

Beweis:

- $\rightarrow$ L sei regulär.
  Dann gibt es Akzeptor A so, dass $L(A) = L$.
  Somit $|X^*_{/\equiv_L}| \leq |X^*_{/\equiv_A}| < \infty$.
- $\leftarrow$ Es gelte $|X^*_{/\equiv_L}| < \infty$.
  Dann ist A_L definiert und $L(A_L) = L$.
  Somit ist L regulär.

Halteproblem

$H = \{w \in \{\texttt{[}, \texttt{0}, \texttt{1}, \texttt{]}\}^* \mid w \text{ codiert TM und } T_w \text{ hält für Eingabe } w\}$

Theorem: $\nexists$TM $T : T$ entscheidet H

Indirekter Beweis:

Halteproblem

$H = \{w \in \{\texttt{[}, \texttt{0}, \texttt{1}, \texttt{]}\}^* \mid w \text{ codiert TM und } T_w \text{ hält für Eingabe } w\}$

Theorem: $\nexists$TM $T : T$ entscheidet H

Indirekter Beweis: Angenommen es gibt TM T, die H entscheidet.
Dann gibt es TM $T' = (Z', z_0', X', f', g', m')$, die H entscheidet so, dass

$$\forall w \in A^* : \Delta_*^{T'}(w) = \begin{cases} (e_{\text{nicht}}, c_0(\texttt{0}), 0), & \text{falls } w \notin H, \\ (e_{\text{hält}}, c_0(\texttt{1}), 0), & \text{falls } w \in H, \end{cases}$$

wobei e_{nicht} und $e_{\text{hält}}$ zwei ausgezeichnete Zustände sind.

Halteproblem

$H = \{w \in \{\texttt{[}, \texttt{0}, \texttt{1}, \texttt{]}\}^* \mid w \text{ codiert TM und } T_w \text{ hält für Eingabe } w\}$

Theorem: $\nexists$TM $T : T$ entscheidet H

Indirekter Beweis: ... Definiere TM $T'' = (Z', z_0', X', f'', g'', m'')$ durch

$$f''(z,x) = \begin{cases} f(z,x), & \text{falls } z \neq e_{\text{hält}}, \\ e_{\text{hält}}, & \text{sonst,} \end{cases}$$

$$g''(z,x) = \begin{cases} g(z,x), & \text{falls } z \neq e_{\text{hält}}, \\ x, & \text{sonst,} \end{cases}$$

$$m''(z,x) = \begin{cases} m(z,x), & \text{falls } z \neq e_{\text{hält}}, \\ \texttt{R}, & \text{sonst.} \end{cases}$$

Halteproblem

$H = \{w \in \{\texttt{[}, \texttt{0}, \texttt{1}, \texttt{]}\}^* \mid w \text{ codiert TM und } T_w \text{ hält für Eingabe } w\}$

Theorem: $\nexists$TM T : T entscheidet H

Indirekter Beweis: ... $\forall w \in A^*$: T'' hält für Eingabe $w \quad \leftrightarrow \quad w \notin H$
Codiert $w \in A^*$ eine TM, so gilt

$$T'' \text{ hält für Eingabe } w \quad \leftrightarrow \quad T_w \text{ hält } \textit{nicht} \text{ für Eingabe } w.$$

Nun sei w die Codierung von T'', das heißt, $T_w = T''$. Dann gilt

$$T'' \text{ hält für Eingabe } w \quad \leftrightarrow \quad T'' \text{ hält } \textit{nicht} \text{ für Eingabe } w.$$

Widerspruch!
Also war anfängliche Existenzannahme von T falsch.

Goldbachsche Vermutung

$$\forall n \in (2\mathbb{N}_+ + 2) : \exists p_1, p_2 \in \mathbb{P} : p_1 + p_2 = n.$$

Goldbachsche Vermutung

$$\forall n \in (2\mathbb{N}_+ + 2) : \exists p_1, p_2 \in \mathbb{P} : p_1 + p_2 = n.$$

$n \leftarrow 4$

$m \leftarrow 2$

while $m < n$ **do**

  if $m \in \mathbb{P} \wedge n - m \in \mathbb{P}$ **then**

    $n \leftarrow n + 2$

    $m \leftarrow 2$

  else

    $m \leftarrow m + 1$

  fi

od

Goldbachsche Vermutung

$$\forall n \in (2\mathbb{N}_+ + 2) : \exists p_1, p_2 \in \mathbb{P} : p_1 + p_2 = n.$$

$n \leftarrow 4$

$m \leftarrow 2$

while $m < n$ **do**

  if $m \in \mathbb{P} \wedge n - m \in \mathbb{P}$ **then**

    $n \leftarrow n + 2$

    $m \leftarrow 2$

  else

    $m \leftarrow m + 1$

  fi

od

Algorithmus hält
gdw. $\exists n \in (2\mathbb{N}_+ + 2)$:
$\forall p_1, p_2 \in \mathbb{P} : p_1 + p_2 \neq n$
gdw. Goldbachsche Vermutung falsch

Wenn Halteproblem entscheidbar,
dann Goldbachsche Vermutung
beantwortbar

Offenes Problem seit 1742

Berechnungsproblem vs. Entscheidungsproblem

Jedes Berechnungsproblem f als Entscheidungsproblem L_f formulierbar so, dass

- f berechenbar gdw. L_f entscheidbar

Bei Fragen über Grenzen der Berechenbarkeit kann man sich also auf Entscheidungsprobleme beschränken!

Bei Fragen über Komplexitätsklassen berechenbarer Probleme jedoch nicht.

Berechnungsproblem vs. Entscheidungsproblem

Beispiel

$$f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*,$$
$$(v, w) \mapsto \mathrm{Repr}_2(\mathrm{Num}_2(v) + \mathrm{Num}_2(w))$$

Formulierung als Entscheidungsproblem

$$L_f = \{v{+}w{=}f(v,w) \in \{0,1,+,=\}^* \mid v, w \in \{0,1\}^*\}$$

Berechnungsproblem vs. Entscheidungsproblem

Beispiel

$$f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*,$$
$$(v, w) \mapsto \mathrm{Repr}_2(\mathrm{Num}_2(v) + \mathrm{Num}_2(w))$$

Formulierung als Entscheidungsproblem

$$L_f = \{v{+}w{=}f(v,w) \in \{0,1,+,=\}^* \mid v, w \in \{0,1\}^*\}$$

Ist f berechenbar, so gibt es TM T, die f berechnet

- Konstruiere TM T', die L_f entscheidet
  - T' analysiert Syntax der Eingabe
  - geht in nicht-akzeptierende Endkonfiguration bei Syntaxfehler
  - extrahiert v, w und x sonst
  - ... simuliert T mit Eingabe (v, w)
  - ... vergleicht Ausgabe mit x

Berechnungsproblem vs. Entscheidungsproblem

Beispiel

$$f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*,$$
$$(v, w) \mapsto \mathrm{Repr}_2(\mathrm{Num}_2(v) + \mathrm{Num}_2(w))$$

Formulierung als Entscheidungsproblem

$$L_f = \{v{+}w{=}f(v,w) \in \{0,1,+,=\}^* \mid v, w \in \{0,1\}^*\}$$

Ist L_f entscheidbar, so gibt es TM T', die L_f entscheidet

- Konstruiere TM T, die f berechnet
  - Bei Eingabe (v, w)
  - ... simuliert T' für $k \in \mathbb{N}_+$ in aufsteigender Reihenfolge T'
  - ... mit Eingaben $v{+}w{=}x$, für $x \in \{0,1\}^k$,
  - ... bis T' für ein x die Eingabe akzeptiert (solches x gibt es immer),
  - ... gibt dieses x aus