Einführung in die Theoretische Informatik

Woche 11

Harald Zankl

Institut für Informatik @ UIBK

Wintersemester 2014/2015

Zusammenfassung der letzten LV

Satz

Es kann kein Testprogramm für „hello, world"-Programme geben.

Definition (informell)

Ist ein Problem nicht algorithmisch lösbar, nennen wir es unentscheidbar.

Satz

Die folgenden Probleme sind unentscheidbar:

1. *das Halteproblem*
2. *das Postsche Korrespondenzproblem*
3. *Eindeutigkeit einer beliebigen kontextfreien Grammatik*
4. *das Wortproblem in der Gleichungslogik* ($E \models s \approx t$)
5. ...

Zusammenfassung der letzten LV

Definition

eine deterministische, einbändige Turingmaschine (TM) M ist ein 9-Tupel

$$M = (Q, \Sigma, \Gamma, \vdash, \sqcup, \delta, s, t, r)$$

sodass

1. Q eine endliche Menge von Zuständen,
2. Σ eine endliche Menge von Eingabesymbolen,
3. Γ eine endliche Menge von Bandsymbolen, mit $\Sigma \subseteq \Gamma$,
4. $\vdash \in \Gamma \setminus \Sigma$, der linke Endmarker,
5. $\sqcup \in \Gamma \setminus \Sigma$, das Blanksymbol,
6. $\delta\colon Q \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}$ die Übergangsfunktion,
7. $s \in Q$, der Startzustand,
8. $t \in Q$, der akzeptierende Zustand und
9. $r \in Q$, der verwerfende Zustand mit $t \neq r$.

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare, Verschlüsselung und Sicherheit

Konfigurationen

Definition

eine Konfiguration einer TM M ist ein Tripel (p, z, n), sodass

1. $p \in Q$ Zustand,
2. $z = y\sqcup^{\infty}$ Bandinhalt $\qquad y \in \Gamma^*$
3. $n \in \mathbb{N}$ Position des Lese/Schreibkopfes

Konfigurationen

Definition

eine Konfiguration einer TM M ist ein Tripel (p, z, n), sodass

1. $p \in Q$ Zustand,
2. $z = y\sqcup^\infty$ Bandinhalt $\quad y \in \Gamma^*$
3. $n \in \mathbb{N}$ Position des Lese/Schreibkopfes

Definition

Startkonfiguration bei Eingabe $x \in \Sigma^*$:

$$(s, \vdash x\sqcup^\infty, 0)$$

Konfigurationen

Definition

eine Konfiguration einer TM M ist ein Tripel (p, z, n), sodass

1. $p \in Q$ Zustand,
2. $z = y\sqcup^\infty$ Bandinhalt $\quad y \in \Gamma^*$
3. $n \in \mathbb{N}$ Position des Lese/Schreibkopfes

Definition

Startkonfiguration bei Eingabe $x \in \Sigma^*$:

$$(s, \vdash x\sqcup^\infty, 0)$$

Beispiel

Die Startkonfiguration bei Eingabe 0011 ist $(s, \vdash 0011\sqcup^\infty, 0)$.

Schrittfunktion

Definition

Schrittfunktion $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

Hier ist z' das Wort, das wir aus z erhalten, wenn z_n durch b ersetzt wird.

Schrittfunktion

Definition

Schrittfunktion $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

Hier ist z' das Wort, das wir aus z erhalten, wenn z_n durch b ersetzt wird.

Definition

$\xrightarrow[M]{*}$ definieren wir induktiv:

Schrittfunktion

Definition

Schrittfunktion $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

Hier ist z' das Wort, das wir aus z erhalten, wenn z_n durch b ersetzt wird.

Definition

$\xrightarrow[M]{*}$ definieren wir induktiv:

1. $\alpha \xrightarrow[M]{0} \alpha$

Schrittfunktion

Definition

Schrittfunktion $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

Hier ist z' das Wort, das wir aus z erhalten, wenn z_n durch b ersetzt wird.

Definition

$\xrightarrow[M]{*}$ definieren wir induktiv:

1. $\alpha \xrightarrow[M]{0} \alpha$
2. $\alpha \xrightarrow[M]{k+1} \beta$, wenn $\alpha \xrightarrow[M]{k} \gamma$ und $\gamma \xrightarrow[M]{1} \beta$ für eine Konfiguration γ

Schrittfunktion

Definition

Schrittfunktion $\xrightarrow[M]{1}$ ist wie folgt definiert:

$$(p, z, n) \xrightarrow[M]{1} \begin{cases} (q, z', n-1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{L}) \\ (q, z', n+1) & \text{wenn } \delta(p, z_n) = (q, b, \mathrm{R}) \end{cases}$$

Hier ist z' das Wort, das wir aus z erhalten, wenn z_n durch b ersetzt wird.

Definition

$\xrightarrow[M]{*}$ definieren wir induktiv:

1. $\alpha \xrightarrow[M]{0} \alpha$
2. $\alpha \xrightarrow[M]{k+1} \beta$, wenn $\alpha \xrightarrow[M]{k} \gamma$ und $\gamma \xrightarrow[M]{1} \beta$ für eine Konfiguration γ
3. $\alpha \xrightarrow[M]{*} \beta$, wenn es ein $k \in \mathbb{N}$ gibt mit $\alpha \xrightarrow[M]{k} \beta$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$(s, \vdash 0011 \sqcup^{\infty}, 0)$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011 \sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011 \sqcup^\infty, 1)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011 \sqcup^{\infty}, 0) \xrightarrow[M]{1} (s, \vdash 0011 \sqcup^{\infty}, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011 \sqcup^{\infty}, 2)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011\sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 2)$$
$$\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 3)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011 \sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011 \sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011 \sqcup^\infty, 2)$$
$$\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011 \sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1 \sqcup^\infty, 2)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011\sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 2)$$
$$\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 2) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 1)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$(s, \vdash 0011\sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 2)$$
$$\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 2) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 1)$$
$$\xrightarrow[M]{1} (s, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 2)$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$
\begin{aligned}
&(s, \vdash 0011\sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 2)\\
&\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 2) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 1)\\
&\xrightarrow[M]{1} (s, \vdash \mathrm{X}0\mathrm{Y}1\sqcup^\infty, 2) \xrightarrow[M]{1} (q_1, \vdash \mathrm{XXY}1\sqcup^\infty, 3) \xrightarrow[M]{1} (q_1, \vdash \mathrm{XXY}1\sqcup^\infty, 4)\\
&\xrightarrow[M]{1} (q_2, \vdash \mathrm{XXYY}\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{XXYY}\sqcup^\infty, 2) \xrightarrow[M]{1} (s, \vdash \mathrm{XXYY}\sqcup^\infty, 3)\\
&\xrightarrow[M]{1} (q_3, \vdash \mathrm{XXYY}\sqcup^\infty, 4) \xrightarrow[M]{1} (q_3, \vdash \mathrm{XXYY}\sqcup^\infty, 5) \xrightarrow[M]{1} (t, \vdash \mathrm{XXYY}\sqcup\sqcup^\infty, 6)
\end{aligned}
$$

Sei $M = (\{s, t, r, q_1, q_2, q_3\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1, \mathrm{X}, \mathrm{Y}\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ:

	$\vdash$	$\sqcup$	0	1	X	Y
s	$(s, \vdash, R)$	$(r, \sqcup, R)$	(q_1, X, R)	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)
q_1	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_1, 0, R)$	(q_2, Y, L)	(r, X, R)	(q_1, Y, R)
q_2	$(r, \vdash, R)$	$(r, \sqcup, R)$	$(q_2, 0, L)$	$(r, 1, R)$	(s, X, R)	(q_2, Y, L)
q_3	$(r, \vdash, R)$	$(t, \sqcup, R)$	$(r, 0, R)$	$(r, 1, R)$	(r, X, R)	(q_3, Y, R)

Wir betrachten die Schrittfunktion für die Eingabe 0011:

$$
\begin{aligned}
&(s, \vdash 0011\sqcup^\infty, 0) \xrightarrow[M]{1} (s, \vdash 0011\sqcup^\infty, 1) \xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 2) \\
&\xrightarrow[M]{1} (q_1, \vdash \mathrm{X}011\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X0Y1}\sqcup^\infty, 2) \xrightarrow[M]{1} (q_2, \vdash \mathrm{X0Y1}\sqcup^\infty, 1) \\
&\xrightarrow[M]{1} (s, \vdash \mathrm{X0Y1}\sqcup^\infty, 2) \xrightarrow[M]{1} (q_1, \vdash \mathrm{XXY1}\sqcup^\infty, 3) \xrightarrow[M]{1} (q_1, \vdash \mathrm{XXY1}\sqcup^\infty, 4) \\
&\xrightarrow[M]{1} (q_2, \vdash \mathrm{XXYY}\sqcup^\infty, 3) \xrightarrow[M]{1} (q_2, \vdash \mathrm{XXYY}\sqcup^\infty, 2) \xrightarrow[M]{1} (s, \vdash \mathrm{XXYY}\sqcup^\infty, 3) \\
&\xrightarrow[M]{1} (q_3, \vdash \mathrm{XXYY}\sqcup^\infty, 4) \xrightarrow[M]{1} (q_3, \vdash \mathrm{XXYY}\sqcup^\infty, 5) \xrightarrow[M]{1} (t, \vdash \mathrm{XXYY}\sqcup\sqcup^\infty, 6)
\end{aligned}
$$

Definition

eine TM M

- akzeptiert Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:

$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y \sqcup^\infty, n)$$

Definition

eine TM M

- akzeptiert Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y \sqcup^\infty, n)$$
- verwirft Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (r, y \sqcup^\infty, n)$$

Definition

eine TM M

- akzeptiert Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:

$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y \sqcup^\infty, n)$$

- verwirft Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:

$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (r, y \sqcup^\infty, n)$$

- hält bei Eingabe x, wenn M Eingabe x akzeptiert oder verwirft

Definition

eine TM M

- akzeptiert Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y\sqcup^\infty, n)$$
- verwirft Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*,\ n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (r, y\sqcup^\infty, n)$$
- hält bei Eingabe x, wenn M Eingabe x akzeptiert oder verwirft
- ist total, wenn M auf allen Eingaben hält

Definition

eine TM M

- akzeptiert Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*$, $n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (t, y \sqcup^\infty, n)$$
- verwirft Eingabe $x \in \Sigma^*$, wenn $\exists\ y \in \Gamma^*$, $n \in \mathbb{N}$:
$$(s, \vdash x \sqcup^\infty, 0) \xrightarrow[M]{*} (r, y \sqcup^\infty, n)$$
- hält bei Eingabe x, wenn M Eingabe x akzeptiert oder verwirft
- ist total, wenn M auf allen Eingaben hält

Definition

die Sprache einer TM M ist wie folgt definiert:
$$\mathsf{L}(M) := \{x \in \Sigma^* \mid M \text{ akzeptiert } x\}$$

Satz

Sei M eine Turingmaschine. Dann ist $\mathsf{L}(M)$ *rekursiv aufzählbar.*
Umgekehrt gibt es zu jeder rekursiv aufzählbaren Sprache L eine Turingmaschine M mit $L = \mathsf{L}(M)$.

Satz

Sei M eine Turingmaschine. Dann ist $\mathsf{L}(M)$ rekursiv aufzählbar. Umgekehrt gibt es zu jeder rekursiv aufzählbaren Sprache L eine Turingmaschine M mit $L = \mathsf{L}(M)$.

Definition (Berechenbarkeit mit einer TM)

Satz

Sei M eine Turingmaschine. Dann ist $\mathsf{L}(M)$ rekursiv aufzählbar. Umgekehrt gibt es zu jeder rekursiv aufzählbaren Sprache L eine Turingmaschine M mit $L = \mathsf{L}(M)$.

Definition (Berechenbarkeit mit einer TM)

- Gegeben TM $M = (Q, \{\sqcap, \Box\}, \{\vdash, \sqcup, \sqcap, \Box\}, \vdash, \sqcup, \delta, s, t, r)$.
  Eine partielle Funktion $f \colon \mathbb{N}^k \to \mathbb{N}$ heißt M-berechenbar, wenn:

$$f(n_1, \ldots, n_k) = m \quad \text{gdw.} \quad (s, \vdash \sqcap^{n_1} \Box \cdots \Box \sqcap^{n_k} \sqcup^{\infty}, 0) \xrightarrow[M]{*} (t, \vdash \sqcap^{m} \sqcup^{\infty}, n)$$

  Das Zeichen $\sqcap$ kodiert Zahlen und $\Box$ dient als Trennsymbol.

Satz

Sei M eine Turingmaschine. Dann ist $\mathsf{L}(M)$ rekursiv aufzählbar. Umgekehrt gibt es zu jeder rekursiv aufzählbaren Sprache L eine Turingmaschine M mit $L = \mathsf{L}(M)$.

Definition (Berechenbarkeit mit einer TM)

- Gegeben TM $M = (Q, \{\sqcap, \square\}, \{\vdash, \sqcup, \sqcap, \square\}, \vdash, \sqcup, \delta, s, t, r)$.
  Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt M-berechenbar, wenn:

  $$f(n_1, \dots, n_k) = m \quad \text{gdw.} \quad (s, \vdash \sqcap^{n_1} \square \cdots \square \sqcap^{n_k} \sqcup^\infty, 0) \xrightarrow[M]{*} (t, \vdash \sqcap^m \sqcup^\infty, n)$$

  Das Zeichen $\sqcap$ kodiert Zahlen und $\square$ dient als Trennsymbol.
- Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt berechenbar mit einer TM, wenn eine TM M über dem Alphabet $\{\sqcap, \square\}$ existiert, sodass f M-berechenbar.

Satz

Sei M eine Turingmaschine. Dann ist $\mathrm{L}(M)$ rekursiv aufzählbar.
Umgekehrt gibt es zu jeder rekursiv aufzählbaren Sprache L eine Turingmaschine M mit $L = \mathrm{L}(M)$.

Definition (Berechenbarkeit mit einer TM)

- Gegeben TM $M = (Q, \{\sqcap, \square\}, \{\vdash, \sqcup, \sqcap, \square\}, \vdash, \sqcup, \delta, s, t, r)$.
  Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt M-berechenbar, wenn:

  $$f(n_1, \ldots, n_k) = m \quad \text{gdw.} \quad (s, \vdash \sqcap^{n_1} \square \cdots \square \sqcap^{n_k} \sqcup^\infty, 0) \xrightarrow[M]{*} (t, \vdash \sqcap^m \sqcup^\infty, n)$$

  Das Zeichen $\sqcap$ kodiert Zahlen und $\square$ dient als Trennsymbol.
- Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt berechenbar mit einer TM, wenn eine TM M über dem Alphabet $\{\sqcap, \square\}$ existiert, sodass f M-berechenbar.

Church-Turing These

Jedes algorithmisch lösbare Problem ist mit einer Turingmaschine lösbar.

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten
2. P ein Programm

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten
2. P ein Programm

Programme sind endliche Folgen von Befehlen und induktiv definiert:

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten
2. P ein Programm

Programme sind endliche Folgen von Befehlen und induktiv definiert:

1. Für jedes Register x_i sind die folgenden Instruktionen sowohl Befehle wie Programme: $x_i := x_i + 1$ und $x_i := x_i - 1$

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten
2. P ein Programm

Programme sind endliche Folgen von Befehlen und induktiv definiert:

1. Für jedes Register x_i sind die folgenden Instruktionen sowohl Befehle wie Programme: $x_i := x_i + 1$ und $x_i := x_i - 1$
2. Wenn P_1 und P_2 Programme sind, dann ist $P_1; P_2$ ein Programm.

Registermaschinen

Definition

Eine Registermaschine (RM) R ist ein Paar $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$ sodass

1. $(x_i)_{1 \leqslant i \leqslant n}$ eine Sequenz von n Registern x_i, die natürliche Zahlen beinhalten
2. P ein Programm

Programme sind endliche Folgen von Befehlen und induktiv definiert:

1. Für jedes Register x_i sind die folgenden Instruktionen sowohl Befehle wie Programme: $x_i := x_i + 1$ und $x_i := x_i - 1$
2. Wenn P_1 und P_2 Programme sind, dann ist $P_1; P_2$ ein Programm.
3. Wenn P_1 ein Programm und x_i ein Register, dann ist

$$\text{while } x_i \neq 0 \text{ do } P_1 \text{ end}$$

sowohl ein Befehl als auch ein Programm.

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.
2. Die Befehle
   - $x_i := x_i + 1$
   - $x_i := x_i - 1$

   bedeuten, dass der Inhalt des Register x_i um 1 erhöht bzw. erniedrigt wird .

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.
2. Die Befehle
   - $x_i := x_i + 1$
   - $x_i := x_i - 1$

   bedeuten, dass der Inhalt des Register x_i um 1 erhöht bzw. erniedrigt wird (falls möglich).

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.
2. Die Befehle
   - $x_i := x_i + 1$
   - $x_i := x_i - 1$

   bedeuten, dass der Inhalt des Register x_i um 1 erhöht bzw. erniedrigt wird (falls möglich).
3. $P_1; P_2$ bedeutet, dass zunächst das Programm P_1 und dann das Programm P_2 ausgeführt wird.

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.
2. Die Befehle
   - $x_i := x_i + 1$
   - $x_i := x_i - 1$

   bedeuten, dass der Inhalt des Register x_i um 1 erhöht bzw. erniedrigt wird (falls möglich).
3. $P_1; P_2$ bedeutet, dass zunächst das Programm P_1 und dann das Programm P_2 ausgeführt wird.
4. Der Befehl (und das Programm)

   $$\text{while } x_i \neq 0 \text{ do } P_1 \text{ end}$$

   bedeutet, der Schleifenrumpf P_1 wird ausgeführt, bis die Bedingung $x_i \neq 0$ falsch ist.

Semantik von Registermaschinen

1. Zu Beginn der Berechnung steht die Eingabe (in Form natürlicher Zahlen) in den Registern.
2. Die Befehle
   - $x_i := x_i + 1$
   - $x_i := x_i - 1$

   bedeuten, dass der Inhalt des Register x_i um 1 erhöht bzw. erniedrigt wird (falls möglich).
3. $P_1; P_2$ bedeutet, dass zunächst das Programm P_1 und dann das Programm P_2 ausgeführt wird.
4. Der Befehl (und das Programm)

   $$\text{while } x_i \neq 0 \text{ do } P_1 \text{ end}$$

   bedeutet, der Schleifenrumpf P_1 wird ausgeführt, bis die Bedingung $x_i \neq 0$ falsch ist.
5. RM R hält, wenn kein auszuführender Befehl mehr existiert.

Beispiel (Addition)

Sei $R = ((x_i)_{1 \leqslant i \leqslant 3}, \mathrm{P})$ eine RM mit folgendem Programm:

$$
\begin{array}{l}
\text{while } x_1 \neq 0 \text{ do} \\
\quad x_1 := x_1 - 1; \\
\quad x_3 := x_3 + 1 \\
\text{end;} \\
\text{while } x_2 \neq 0 \text{ do} \\
\quad x_2 := x_2 - 1; \\
\quad x_3 := x_3 + 1 \\
\text{end}
\end{array}
$$

Startet R mit $(m, n, 0)$, dann hält R mit $(0, 0, m + n)$.

Proseminar

Zuweisungen der Form $x_i := x_j$ können (mit einem Hilfsregister) als Programm einer Registermaschine formuliert werden.

Proseminar

Zuweisungen der Form $x_i := x_j$ können (mit einem Hilfsregister) als Programm einer Registermaschine formuliert werden.

Beispiel (Multiplikation)

Sei $R = ((x_i)_{1 \leqslant i \leqslant 5}, \mathrm{P})$ eine RM mit folgendem Programm:

$$
\begin{array}{l}
x_3 := 0; \\
\text{while } x_1 \neq 0 \text{ do} \\
\quad x_1 := x_1 - 1; \\
\quad x_4 := x_2; \\
\quad \text{while } x_4 \neq 0 \text{ do} \\
\quad\quad x_4 := x_4 - 1; \\
\quad\quad x_3 := x_3 + 1 \\
\quad \text{end} \\
\text{end}
\end{array}
$$

Proseminar

Zuweisungen der Form $x_i := x_j$ können (mit einem Hilfsregister) als Programm einer Registermaschine formuliert werden.

Beispiel (Multiplikation)

Sei $R = ((x_i)_{1 \leqslant i \leqslant 5}, \mathrm{P})$ eine RM mit folgendem Programm:

$$
\begin{array}{l}
x_3 := 0; \\
\text{while } x_1 \neq 0 \text{ do} \\
\quad x_1 := x_1 - 1; \\
\quad x_4 := x_2; \\
\quad \text{while } x_4 \neq 0 \text{ do} \\
\quad\quad x_4 := x_4 - 1; \\
\quad\quad x_3 := x_3 + 1 \\
\quad \text{end} \\
\text{end}
\end{array}
$$

Proseminar

Zuweisungen der Form $x_i := x_j$ können (mit einem Hilfsregister) als Programm einer Registermaschine formuliert werden.

Beispiel (Multiplikation)

Sei $R = ((x_i)_{1 \leqslant i \leqslant 5}, \mathrm{P})$ eine RM mit folgendem Programm:

$$
\begin{array}{l}
x_3 := 0; \\
\text{while } x_1 \neq 0 \text{ do} \\
\quad x_1 := x_1 - 1; \\
\quad x_4 := x_2; \\
\quad \text{while } x_4 \neq 0 \text{ do} \\
\quad\quad x_4 := x_4 - 1; \\
\quad\quad x_3 := x_3 + 1 \\
\quad \text{end} \\
\text{end}
\end{array}
$$

Startet R mit $(m, n, 0, 0, 0)$, dann hält R mit $(0, n, m \times n, 0, 0)$.

Definition (Berechenbarkeit mit einer RM)

Definition (Berechenbarkeit mit einer RM)

- Gegeben RM $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$.
  Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt *R-berechenbar*, wenn:

  $f(n_1, \ldots, n_k) = m$ gdw. R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ startet und R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ und m im Register x_{k+1} hält.

Definition (Berechenbarkeit mit einer RM)

- Gegeben RM $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$.
  Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt R-berechenbar, wenn:

  $f(n_1, \dots, n_k) = m$ gdw. R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ startet und R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ und m im Register x_{k+1} hält.
- Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt berechenbar auf einer RM, wenn eine RM R existiert, sodass f R-berechenbar.

Definition (Berechenbarkeit mit einer RM)

- Gegeben RM $R = ((x_i)_{1 \leqslant i \leqslant n}, \mathrm{P})$.
  Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt *R-berechenbar*, wenn:
  $f(n_1, \ldots, n_k) = m$ gdw. R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ startet und R mit n_i in den Registern x_i für $1 \leqslant i \leqslant k$ und m im Register x_{k+1} hält.
- Eine partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$ heißt *berechenbar auf einer RM*, wenn eine RM R existiert, sodass f R-berechenbar.

Satz

Jede partielle Funktion $f\colon \mathbb{N}^k \to \mathbb{N}$, die berechenbar auf einer RM ist, ist auf einer TM berechenbar und umgekehrt.

Evaluierung: LVA Nummer: 703007-0

Zusatzfragen

- Die Folien sind verständlich.
- Das Skriptum ist verständlich.
- Die Beispiele sind verständlich.
- Die VO und das PS sind gut abgestimmt.

Anregungen für Freitext

- Aufwand
- Vortrag
- Koordination VO – PS
- Probleme
- Resultat

Evaluierung: LVA Nummer: 703007-0

Zusatzfragen

- Die Folien sind verständlich.
- Das Skriptum ist verständlich.
- Die Beispiele sind verständlich.
- Die VO und das PS sind gut abgestimmt.

Anregungen für Freitext

- Aufwand (Modul hat 5 ECTS $\approx$ 8.5h @ 15 Wochen)
- Vortrag (Mikrofon, etc.)
- Koordination VO – PS (PS mit Wissen aus VO schaffbar)
- Probleme (welche Kapitel sind schwierig)
- Resultat (Ich habe durch den Besuch der VO etwas gelernt)