

Diskrete Mathematik

Arne Dür Kurt Girstmair Simon Legner
 Georg Moser Harald Zankl

Fakultät für Mathematik, Informatik und Physik © UIBK
 Sommersemester 2011



Zusammenfassung der letzten LV

Definition

eine k -bändige NTM N ist ein 9-Tupel

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

sodass

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

Satz

wenn L und $\sim L$ rekursiv aufzählbar sind, dann ist L rekursiv

Definition

Eigenschaft P heißt

- **entscheidbar**, wenn $\{x \mid P(x)\}$ rekursiv
- **semi-entscheidbar**, wenn $\{x \mid P(x)\}$ rekursiv aufzählbar

Satz

\forall DTM mit k Bändern \exists einbändige DTM M' , sodass $L(M) = L(M')$

Übersicht

Endliche Automaten

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, ϵ -NEAs, Umwandlung endlicher Automaten in reguläre Ausdrücke, Pumpinglemma, Minimierung

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie, **Turingmaschinen**, Entscheidungsprobleme, **Universelle Maschinen** und Diagonalisierung

Komplexitätstheorie

Einführung in die Komplexitätstheorie, die Klassen P und NP, logarithmisch platzbeschränkte Reduktionen, Speicherplatzkomplexität

Beispiel

betrachte NTM $N = (\{s, p, t, r\}, \{0, 1\}, \{0, 1, \vdash, \sqcup\}, \vdash, \sqcup, \delta, s, t, r)$ mit δ :

$p \in Q$	$a \in \Gamma$	$\delta(p, a)$	$p \in Q$	$a \in \Gamma$	$\delta(p, a)$
s	0	$\{(s, 1, R)\}$	p	0	$\{(p, 0, R), (s, 0, L)\}$
s	1	$\{(p, 0, R)\}$	p	1	$\{(p, 1, R), (s, 1, L)\}$
s	\vdash	$\{(s, \vdash, R)\}$	p	\vdash	$\{(p, \vdash, R)\}$
s	\sqcup	\emptyset	p	\sqcup	$\{(t, \sqcup, R)\}$

Erinnerung

- (N)TM N **akzeptiert** $x \in \Sigma^*$, wenn $\exists y, n: (s, \vdash x \sqcup^\infty, 0) \xrightarrow[N]{*} (t, y, n)$
- **Sprache** einer (N)TM N : $L(N) := \{x \in \Sigma^* \mid N \text{ akzeptiert } x\}$

Beispiel

$$(s, \vdash 011 \sqcup^\infty, 0) \xrightarrow[N]{*} (p, \vdash 101 \sqcup^\infty, 3) \xrightarrow[N]{*} (t, \vdash 110 \sqcup^\infty, 5)$$

Satz

\forall einbändige NTM N , \exists dreibändige DTM M , sodass $L(M) = L(N)$

Definition

- 1 sei b der "Grad des Nichtdeterminismus"
beziehungsweise b ist der **Verzweigungsgrad** des Berechnungsbaums
- 2 String über dem Alphabet $\Sigma_b = \{1, 2, \dots, b\}$
nennen wir **Adresse**
- 3 Adresse ist ungültig, oder bezeichnet eine
eindeutige **Position im Berechnungsbaum**

Beweis des Satzes.

- 1 sei N 1-Band NTM; konstruiere 3-Band DTM M mit $L(M) = L(N)$
- 2 sei x das Eingabewort; Simulation ist **uniform** für jedes x
- 3 erstes Band von M wird immer nur Eingabe x enthalten
- 4 zweites Band simuliert Rechengänge von N
- 5 drittes Band adressiert den aktuellen Pfad
- 6 nach der Simulation eines Pfades, ersetze die Adresse auf Band 3 durch die nächstgrößere in der graduiert-lexikographischen Ordnung

Simulation eines Pfades

- 4 anfangs enthält Band 1 von M das Eingabewort x ; Bänder 2 und 3 sind leer
- 4 kopiere den Inhalt von Band 1 auf Band 2
- 4 verwende Band 2, um die Rechenschritte von N auf x zu simulieren; bei nichtdeterministischen Entscheidungen: siehe Band 3

Satz

- \forall DTM M mit k Bändern \exists einbändige DTM M' und $L(M) = L(M')$
- \forall einbändige NTM $N \exists$ dreibändige DTM M , sodass $L(M) = L(N)$

Folgerung

\forall k -bändige NTM $N \exists$ einbändige DTM M , sodass $L(M) = L(N)$

Satz

die folgenden Erweiterungen von Turingmaschinen verändern die Ausdrucksfähigkeit nicht:

- Nichtdeterminismus
- mehrere Bänder
- zweifach unendliches Band

die Klasse der rekursiven, rekursiv aufzählbaren Mengen wird nicht verändert

Universelle Turingmaschinen

Codierung

TMs können codiert werden indem alle notwendigen Informationen als Wörter über $\{0, 1\}$ dargestellt werden:

- 1 Anzahl der Zustände
- 2 Übergangsfunktion
- 3 Eingabe- und Bandalphabet
- 4 ...

Beispiel

sei $M = (Q, \Sigma, \Gamma, \vdash, \sqcup, \delta, s, t, r)$ eine TM; Codierung über $\{0, 1\}$

$$0^n 1 0^m 1 0^k 1 0^s 1 0^t 1 0^r 1 0^u 1 0^v 1 \dots$$

entspricht $Q = \{0, \dots, n-1\}$, $\Gamma = \{0, \dots, m-1\}$, $\Sigma = \{0, \dots, k-1\}$,
 ($k \leq m$), s Startzustand, t akzeptierend, r verwerfend, u linker
 Endmarker, v Blanksymbol

Codierung (Fortsetzung)

betrachte M und kodiere die Übergangsfunktion δ

$$\delta(p, a) = (q, b, d)$$

$$0^p 1 0^a 1 0^q 1 0^b 1 \underbrace{1}_d$$

Richtung d

Definition

eine TM U heißt **universell**, wenn bei Eingabe

- des Codes $\ulcorner M \urcorner$ einer TM M
- und des Codes $\ulcorner x \urcorner$ einer Eingabe x für M

die TM U , die TM M auf x **simuliert**, das heißt

$$L(U) = \{\ulcorner M \urcorner \# \ulcorner x \urcorner \mid x \in L(M)\}$$

Algorithmus einer UTM

Simulation

- 1 U kontrolliert Korrektheit der Codes; wenn inkorrekt, verwirft U
- 2 U simuliert M mit 3 Bändern auf der Eingabe x
 - Band 1 enthält die Beschreibung von M
 - Band 2 enthält das (dekodierte) Eingabewort x
 - Band 3 enthält (simulierten) Bandinhalt des Bandes von M
- 3 wenn M jemals auf der Eingabe x hält, hält U ebenfalls und akzeptiert; beziehungsweise verwirft entsprechend

Konvention

wir schreiben

$$L(U) = \{M\#x \mid x \in L(M)\}$$