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

als Halteproblem bezeichnen wir das Problem, ob ein beliebiges Programm auf seiner Eingabe hält

Definition

Postsches Korrespondenzproblem: Gegeben zwei Listen von Strings der gleichen Länge $w_1, w_2, \ldots, w_n$ und $x_1, x_2, \ldots, x_n$. Gesucht sind Indizes $i_1, i_2, \ldots, i_m$, sodass

$$w_{i_1} w_{i_2} \ldots w_{i_m} = x_{i_1} x_{i_2} \ldots x_{i_m}$$

Satz

die folgenden Probleme sind unentscheidbar:

1. *das Halteproblem*
2. *das Postsche Korrespondenzproblem*

Turingmaschinen

Definition

eine einbändige, deterministische Turingmaschine (DTM) 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, sodass $\Sigma \subseteq \Gamma$,
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 $t \neq r$.

Beispiel

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

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

Konfiguration einer TM

Definition

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

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

Definition

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

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

Step Function of TMs

Definition

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

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

z' ist String, den wir aus z erhalten, wenn z_n durch b ersetzt

Definition

reflexive, transitive Hülle $\xrightarrow[M]{*}$:

1. $\alpha\xrightarrow[M]{*}\alpha$
2. $\alpha\xrightarrow[M]{n+1}\beta$, wenn $\alpha\xrightarrow[M]{n}\gamma\xrightarrow[M]{1}\beta$ für Konfiguration γ
3. $\alpha\xrightarrow[M]{*}\beta$, wenn $\exists\ n\ \alpha\xrightarrow[M]{n}\beta$

Beispiel

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

$$(s,\vdash 0010\sqcup^\infty,0)\xrightarrow[M]{*}$$
$$(s,\vdash 0010\sqcup^\infty,5)\xrightarrow[M]{1}$$
$$(p,\vdash 0010\sqcup^\infty,4)\xrightarrow[M]{1}$$
$$(t,\vdash 0011\sqcup^\infty,3)$$

Definition

eine TM M

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

Definition

die Sprache einer TM M is wie folgt definiert:

$$\mathrm{L}(M) := \{x \in \Sigma^* \mid M \text{ akzeptiert } x\}$$

Beispiel

betrachte $M = (\{s, t, r, q_0, q_1, q_0', q_1'\}, \{0, 1\}, \{\vdash, \sqcup, 0, 1\}, \delta, s, t, r)$ mit δ:

$p \in Q$	$a \in \Gamma$	$\delta(p, a)$	$p \in Q$	$a \in \Gamma$	$\delta(p, a)$
s	0	$(q_0, \vdash, \mathrm{R})$	q_0'	0	$(q, \sqcup, \mathrm{L})$
s	1	$(q_1, \vdash, \mathrm{R})$	q_0'	1	$(r, 1, \mathrm{L})$
s	$\vdash$	$(s, \vdash, \mathrm{R})$	q_0'	$\vdash$	$(r, \vdash, \mathrm{R})$
s	$\sqcup$	$(t, \sqcup, \mathrm{L})$	q_1'	0	$(r, 1, \mathrm{L})$
q_0	0	$(q_0, 0, \mathrm{R})$	q_1'	1	$(q, \sqcup, \mathrm{L})$
q_0	1	$(q_0, 1, \mathrm{R})$	q_1'	$\vdash$	$(r, \vdash, \mathrm{R})$
q_0	$\sqcup$	$(q_0', \sqcup, \mathrm{L})$	q	0	$(q, 0, \mathrm{L})$
q_1	0	$(q_1, 0, \mathrm{R})$	q	1	$(q, 1, \mathrm{L})$
q_1	1	$(q_1, 1, \mathrm{R})$	q	$\vdash$	$(s, \vdash, \mathrm{R})$
q_1	$\sqcup$	$(q_1', \sqcup, \mathrm{L})$			

es gilt; $\mathrm{L}(M) = \{ww^R \mid w \in \{0, 1\}^*\}$

Definition

eine Sprache L (oder allgemeine eine Menge) heißt

- rekursiv aufzählbar (r.e.), wenn $\exists$ Turingmaschine M mit $L = \mathrm{L}(M)$
- co-r.e. wenn L das Komplement einer r.e. Sprache
- rekursiv, wenn $L = \mathrm{L}(M)$ und M totale TM

Satz

rekursive Mengen sind unter Komplementbildung abgeschlossen

Beweis.

1. angenommen $L = \mathrm{L}(M)$, wobei die TM M total
2. definiere M' indem der akzeptierende und der verwerfende Zustand von M vertauscht wird
3. offensichtlich $\sim L = \mathrm{L}(M')$ und M' total

Satz

jede rekursive Menge ist rekursiv aufzählbar, aber nicht jede rekursiv aufzählbare Menge ist rekursiv

Satz

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

Beweis.

1. $\exists$ TM M_1, M_2 mit $A = \mathrm{L}(M_1)$ und $\sim(A) = \mathrm{L}(M_2)$
2. definiere TM M', sodass das Band zwei Hälften hat

b	$\hat{b}$	a	b	a	a	a	a	b	a	a	a	$\cdots$
c	c	c	d	d	d	c	$\hat{c}$	d	c	d	c	

3. M_1 wird auf der oberen und M_2 auf der unteren Hälfte simuliert
4. wenn M_1 x akzeptiert, M' akzeptiert x
5. wenn M_2 x akzeptiert, M' verwirft x

Erinnerung

eine Sprache L (oder allgemeine eine Menge) heißt

- rekursiv, wenn $L = \mathrm{L}(M)$ und M totale TM
- rekursiv aufzählbar (r.e.), wenn $\exists$ Turingmaschine M mit $L = \mathrm{L}(M)$

Definition

Eigenschaft P heißt

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

Beispiele

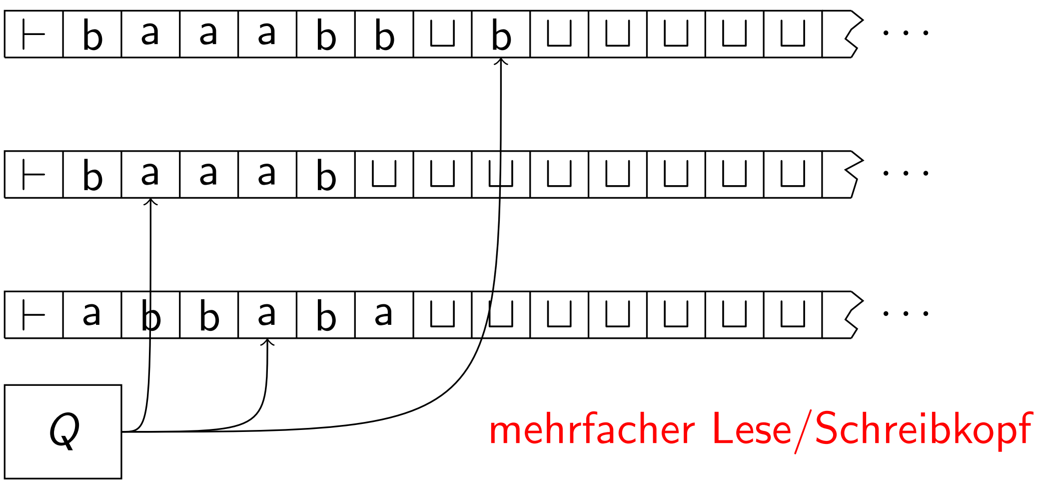
- $\{ww^R \mid w \in \{0,1\}^*\}$ ist rekursiv, also ist Wortumkehr entscheidbar
- das Postsche Korrespondenzproblem (PCP) ist unentscheidbar, also ist die folgende Sprache nicht rekursiv:

$$\{(w_1, x_1) \cdots (w_n, x_n) \mid \exists i_1 \cdots i_m \; w_{i_1} w_{i_2} \ldots w_{i_m} = x_{i_1} x_{i_2} \ldots x_{i_m}\}$$

Äquivalente Formulierungen

Definition (informell)

Erweiterung um mehrere Bänder und Lese/Schreibköpfe:



Erweiterung der Definition

$$\delta\colon Q \times \Gamma^3 \to Q \times \Gamma^3 \times \{\mathrm{L}, \mathrm{R}\}^3$$

Beispiel

betrachte die Sprache

$$L = \{a^i b^j c^k \mid i \times j = k \text{ und } i, j, k \geqslant 1\}$$

Lösung (informell)

bei Eingabe w

1. lies die Eingabe und stelle fest, ob $w \in L(a^*b^*c^*)$
   wenn nicht: verwerfe
2. setze den Lesekopf des ersten Bandes auf den Bandanfang
3. markiere das erste unmarkierte a
   markiere gleich viel b's wie c's
4. lösche die Markierung der b's
   wiederhole 3 solange wie möglich
5. wenn alle c markiert sind, dann akzeptiere, sonst verwerfe

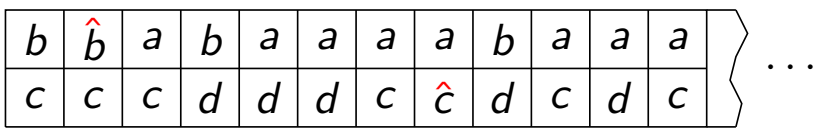
Satz

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

Beweis.

1. Bänder können nebeneinander oder übereinander simulieren
2. wir simulieren die Bänder übereinander, oBdA sei $k = 2$
3. wir erweitern das Alphabet von M'

4. Band von M' kann folgende Gestalt haben:



5. alle Bänder von M sind nun repräsentiert und die Leseköpfe werden durch die Zusatzmarkierung $\hat{}$ ausgedrückt

Nichtdeterministische Turingmaschine

Definition

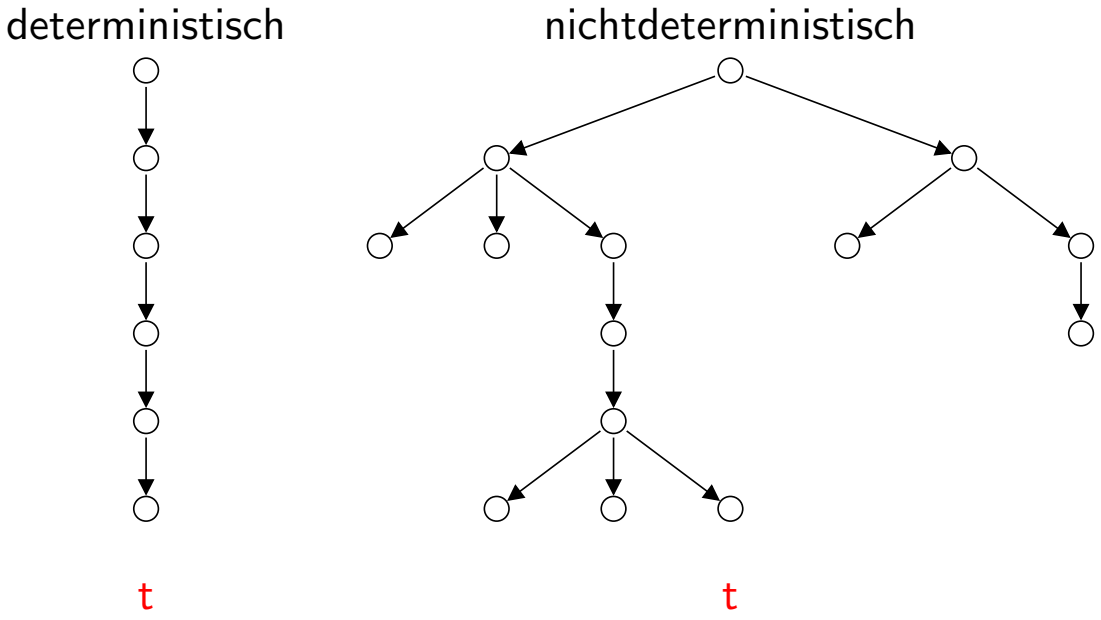
eine k-bändige, nichtdeterministische TM (NTM) N ist ein 9-Tupel

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

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. $\delta\colon Q \times \Gamma^k \to \mathcal{P}(Q \times \Gamma^k \times \{\mathrm{L}, \mathrm{R}\}^k)$ die Übergangsfunktion,
7. $s \in Q$, der Startzustand,
8. $t \in Q$, der akzeptierende Zustand und
9. $r \in Q$, der verwerfende Zustand mit $t \neq r$.

Nichtdeterministischer Berechnungsbaum



Beobachtung

damit NTM N akzeptiert, genügt ein Pfad, sodass N in den akzeptierenden Zustand gelangt

Nichtdeterminismus vs. Determinisums

Satz

- $\forall$ *N einbändige NTM,* $\exists$ *dreibändige DTM M, sodass* $\mathsf{L}(M) = \mathsf{L}(N)$
- *jede DTM ist auch eine NTM*