Computational Logic

Diskrete Mathematik

Martin Avanzini Arne Dür Christoph Kollreider Georg Moser

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2010

Zusammenfassung der letzten LV

Definition Halteproblem

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

Definition PCP

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
3. ist eine beliebige Sprache regulär?

Turingmaschinen

Definition Turingmaschine

eine deterministische, einbändige Turingmaschine 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 $t \neq r$.

Zusatzbedingungen

- $\forall\ p \in Q$, $\exists\ q \in Q$ sodass:
$$\delta(p, \vdash) = (q, \vdash, \mathrm{R})$$
- $\forall\ b \in \Gamma\ \exists\ c, c' \in \Gamma$ und $d, d' \in \{\mathrm{L}, \mathrm{R}\}$:
$$\delta(t, b) = (t, c, d)$$
$$\delta(r, b) = (r, c', d')$$

Definition Konfiguration

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

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

Definition Sprache einer TM

$\mathrm{L}(M)$ bezeichnet die Menge aller von M akzeptierten Wörter

Übersicht

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, Automaten mit ϵ-Übergängen, Umwandlung endlicher Automaten in reguläre Ausdrücke, Algebraische Gesetze für reguläre Ausdrücke, Pumpinglemma, Minimierung

Einführung in die Berechenbarkeitstheorie, Turing Maschinen, Entscheidungsprobleme, Äquivalente Formulierungen, Universelle Maschinen und Diagonalisierung,

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

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

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

Satz

1. jede rekursive Menge ist rekursiv aufzählbar
2. aber nicht jede rekursiv aufzählbare Menge rekursiv

Satz

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

Beweis

- $\exists$ TM M, M' mit $A = \mathrm{L}(M)$ und $\sim(A) = \mathrm{L}(M')$
- definiere TM N, die bei Eingabe x die Maschinen M und M' simuliert
- dazu teile das Band in eine obere und untere Hälfte
- M wird auf der oberen und M' auf der unteren Hälfte simuliert
- das Band von N kann folgende Gestalt haben:

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

$\ldots$ ■

Definition

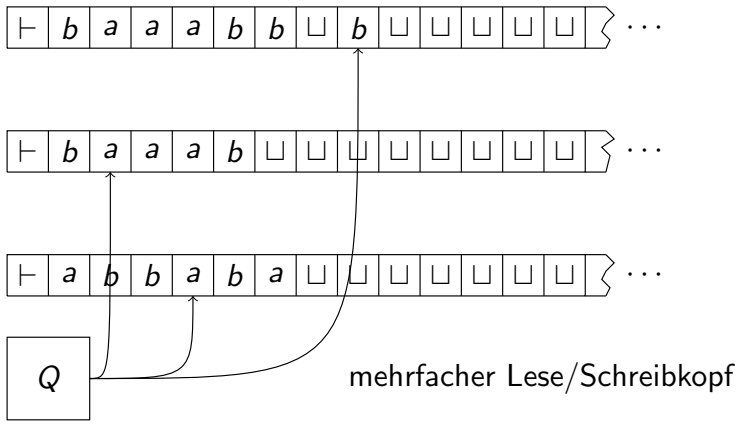
Eigenschaft P heißt

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

Äquivalente Formulierungen

Definition

Erweiterung um mehrere Bänder und Lese/Schreibköpfe:



formale Erweiterung

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

"Beispiel": Palindrome

$p \in Q$	$a_1 \in \Gamma$	$a_2 \in \Gamma$	$\delta(p, a_1, a_2)$	
s	0	$\sqcup$	$(s, 0, 0, \mathrm{R}, \mathrm{R})$	kopieren
s	1	$\sqcup$	$(s, 1, 1, \mathrm{R}, \mathrm{R})$	
s	$\vdash$	$\vdash$	$(s, \vdash, \vdash, \mathrm{R}, \mathrm{R})$	
s	$\sqcup$	$\sqcup$	$(q, \sqcup, \sqcup, \mathrm{L}, -)$	
q	0	$\sqcup$	$(q, 0, \sqcup, \mathrm{L}, -)$	Lesekopf zurücksetzen
q	1	$\sqcup$	$(q, 1, \sqcup, \mathrm{L}, -)$	
q	$\vdash$	$\sqcup$	$(p, \vdash, \sqcup, \mathrm{R}, \mathrm{L})$	
p	0	0	$(p, 1, \sqcup, \mathrm{R}, \mathrm{L})$	vergleichen
p	1	1	$(p, 1, \sqcup, \mathrm{R}, \mathrm{L})$	
p	0	1	$(r, 1, \sqcup, \mathrm{R}, \mathrm{R})$	
p	1	0	$(r, 1, \sqcup, \mathrm{R}, \mathrm{R})$	
p	$\sqcup$	$\vdash$	$(t, \sqcup, \vdash, \mathrm{R}, \mathrm{R})$	

Beispiel (2)

betrachte die Sprache

$$L = \{wcw^R \mid w \in \{0,1\}^*\}$$

Beobachtung

wenn $x \in L$, dann ist x ein Palindrom ungerader Länge

Korrektur der TM

- Anhalten des zweiten Lesekopfes

$p \in Q$	$a_1 \in \Gamma$	$a_2 \in \Gamma$	$\delta(p, a_1, a_2)$
s	$\sqcup$	$\sqcup$	$(u, \sqcup, \sqcup, \mathrm{L}, \mathrm{R})$
u	0	$\sqcup$	$(g, 0, \sqcup, \mathrm{L}, \mathrm{L})$
u	1	$\sqcup$	$(g, 1, \sqcup, \mathrm{L}, \mathrm{L})$
g	0	$\sqcup$	$(u, 0, \sqcup, \mathrm{L}, \mathrm{R})$
g	1	$\sqcup$	$(u, 1, \sqcup, \mathrm{L}, \mathrm{R})$
g	$\vdash$	$\sqcup$	$(p, \vdash, \sqcup, \mathrm{R}, \mathrm{L})$

- Buchstabenvergleich anpassen

Beispiel: Elementare Arithmetik

betrachte die Sprache

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

bei Eingabe w

1. lies die Eingabe und stelle fest, ob $w \in \mathrm{L}(a^*b^*c^*)$
   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

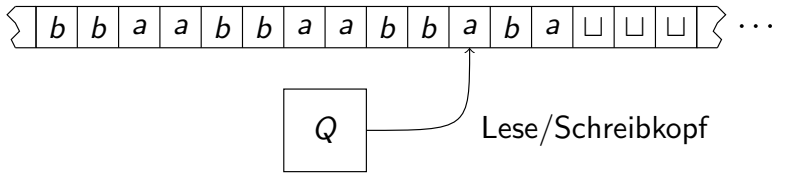
$\forall$ deterministische TM mit k Bändern $\exists$ einbändige, deterministische TM M', sodass $\mathrm{L}(M) = \mathrm{L}(M')$

Beweisskizze

- die k Bänder können nebeneinander
- oder übereinander simuliert werden ■

Definition

zweiseitig unbeschränktes Band



Satz

$\forall$ M eine einbändige, deterministische TM, dessen Band in beide Richtungen unbeschränkt ist $\exists$ einbändige, deterministische TM M', sodass $\mathrm{L}(M) = \mathrm{L}(M')$