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

ein ϵ-NEA ist gegeben durch

1. eine endliche Menge Q, den Zuständen
2. eine endliche Menge Σ, dem Eingabealphabet
3. eine Abbildung
$$\delta\colon Q \times \Sigma \cup \{\epsilon\} \to \mathcal{P}(Q)$$
die Übergangsfunktion
4. einen ausgezeichneten Zustand, den Startzustand
5. eine Teilmenge $F \subseteq Q$, den akzeptierenden Zuständen

um Verwechslungen auszuschließen, fordern wir dass $\epsilon \notin \Sigma$

Epsilon-Hülle

Definition

betrachte den Zustandsgraphen des Automaten, setze $S = \{q\}$

der folgende Algorithmus markiert alle Zustände in ϵ-Hülle(q):

1. markiere die Zustände in S
2. solange $S \neq \varnothing$, wiederhole:
   - wähle einen Zustand p aus S und entferne p
   - bestimme alle unmarkierten Nachfolger von p die mit einer ϵ-Kante erreichbar sind
   - markiere diese und füge sie zu S hinzu

Definition

die Sprache von ϵ-NEA $E = (Q, \Sigma, \delta, q_0, F)$:

$$\mathrm{L}(E) := \{x \mid \widehat{\delta}(q_0, x) \cap F \neq \varnothing\}$$

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,

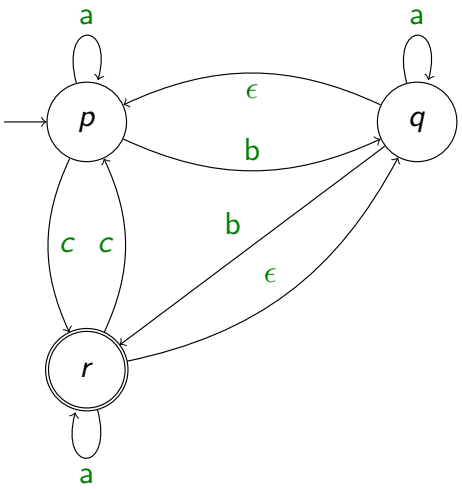
Komplexitätstheorie

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

Beispiel (1)

Beispiel

betrachte ϵ-NEA A



Frage

welche Sprache akzeptiert A?

Beispiel (2)

	ϵ	a	b	c
$\rightarrow p$	$\varnothing$	$\{p\}$	$\{q\}$	$\{r\}$
q	$\{p\}$	$\{q\}$	$\{r\}$	$\varnothing$
$*r$	$\{q\}$	$\{r\}$	$\varnothing$	$\{p\}$

Epsilon-Hüllen

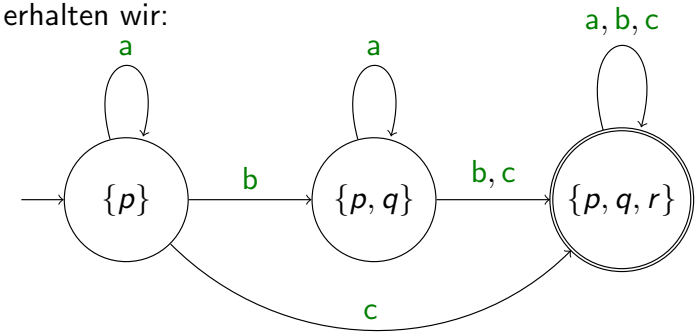
$$\epsilon\text{-Hülle}(p) = \{p\} \quad \epsilon\text{-Hülle}(q) = \{q, p\} \quad \epsilon\text{-Hülle}(r) = \{r, q, p\}$$

Zustandstabelle

	a	b	c
$\rightarrow \{p\}$	$\{p\}$	$\{p, q\}$	$\{p, q, r\}$
$\{p, q\}$	$\{p, q\}$	$\{p, q, r\}$	$\{p, q, r\}$
$*\{p, q, r\}$	$\{p, q, r\}$	$\{p, q, r\}$	$\{p, q, r\}$

Beispiel (3)

in Summe erhalten wir:



Antwort

A akzeptiert alle Wörter über $\{a, b, c\}$, sodass

1. entweder zwei bs oder
2. ein c auftreten

Äquivalenz von ϵ-NEAs und DEAs

Satz

sei $D = (Q_D, \Sigma, \delta_D, \{q_0\}, F_D)$ der DEA, der mit der Teilmengenkonstruktion aus ϵ-NEA $E = (Q_E, \Sigma, \delta_E, q_0, F_E)$ konstruiert ist, dann gilt $L(D) = L(N)$

Beweisansatz

wie für die Korrektheit der Teilmengenkonstruktion für NEAs ■

Satz

eine Sprache L *wird genau dann von einem ϵ-NEA akzeptiert, wenn* L *von einem DEA akzeptiert wird.*

Beweis.

der Satz folgt aus der Teilmengenkonstruktion und der einfachen Einsicht, dass jeder DEA in einen ϵ-NEA umgeschrieben werden kann ■

Anwendung von Endlichen Automaten

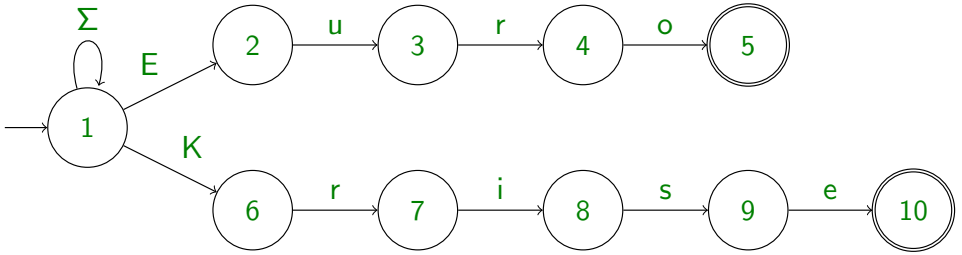
Anwendung

- Softwarebasiertes Entwickeln und Testen von Schaltkreisen
- Compilerbau: Lexikalische Analyse
- Textsuche; Pattern Matching
- Softwareverifikation von Protokollen
- Spielengine von Computerspiele

Beispiel

- gesucht sei eine Liste von Schlüsselwörter in einem Text oder HTML/XML Dokument
- Inhalt des Textes ändert sich täglich, sodass Indizierung zu teuer
- suche die Worte Euro oder Krise in einer Online-Zeitung

Beispiel



Implementierung

- wir können N direkt simulieren, indem wir alle Möglichkeiten aufzählen
- oder wir wanden N in einen DEA D um und implementieren D

Lemma

der so erhaltene DEA hat maximal soviele Zustände wie der NEA

Beweis.

Analyse der Teilmengenkonstruktion ergibt:

1. sei p ein Zustand in N, erreichbar beim Lesen von $a_1 \dots a_m$ korrespondierende Zustand in D besteht aus 1 und p, sowie jedem Zustand aus N der durch einen Suffix von $a_1 \dots a_m$ erreichbar
2. Kanten in D von $\{1, p_1, \dots, p_n\}$ nach $\{1, q_1, \dots, q_m\}$, wenn
   - entweder in N mit a markierte Kante von p_i nach q_j, oder
   - in N mit a markierte Kante von 1 nach q_j, wenn keine Kante von p_i nach q_j mit a markiert

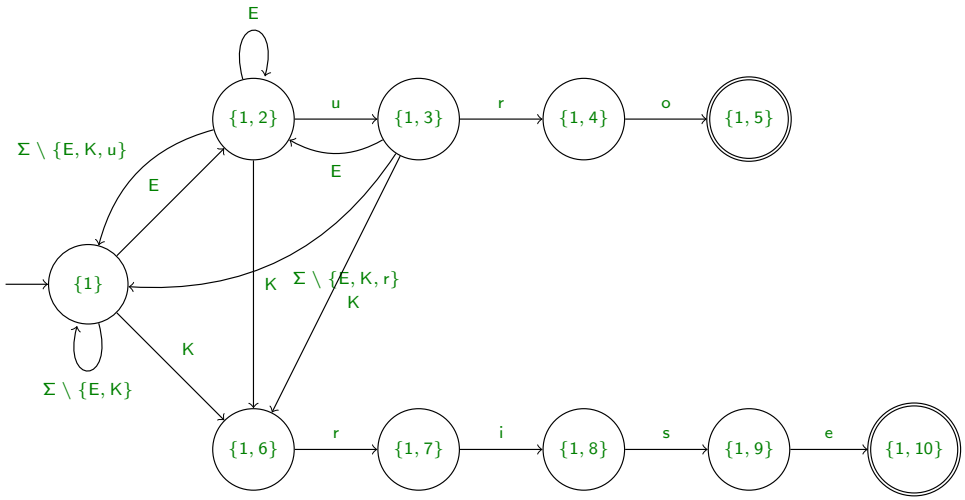
∎

Beispiel

- D enthält zB die Zustände: $\{1\}$, $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{1,5\}$
- Kante von $\{1\}$ nach $\{1,2\}$ mit E markiert; Kante von $\{1,2\}$ nach $\{1\}$ mit $\Sigma \setminus \{E, K, u\}$ markiert

Beispiel

durch die Teilmengenkonstruktion erhalten wir den folgenden DEA D (vereinfacht)



seien L, M formale Sprachen

Definition

die Vereinigung $L \cup M$ von L und M, ist die Menge der Wörter, die entweder in L oder in M liegen

Definition

die Konkatenation $L \cdot M$ von L und M, ist die Menge der Wörter, die gebildet werden können, indem wir ein Wort aus L mit einem Wort aus M verketten

Definition

der Abschluss L^* von L ist die Menge der Wörter, die gebildet werden können durch die Verkettung von beliebig vielen Elementen aus L

Beispiel

Algebra $(\Sigma^*, \cdot, \epsilon)$, sodass Σ^* die Menge aller Wörter über Σ, $\cdot$ die Verkettung und ϵ das neutrale Element, heißt Wortmonoid

Reguläre Ausdrücke

Erinnerung

sei Σ ein endliches Alphabet; wir definieren reguläre Ausdrücke induktiv

Basis — Sprache von $\varnothing$: $\overbrace{\mathrm{L}(\varnothing)}$

1. $\varnothing$ ist ein regulärer Ausdruck (kurz: RA) — $\mathrm{L}(\varnothing) := \varnothing$
2. ϵ ist ein RA — $\mathrm{L}(\epsilon) := \{\epsilon\}$
3. für jedes Symbol a ist $\mathbf{a}$ ein RA — $\mathrm{L}(\mathbf{a}) := \{a\}$

Schritt

1. für jeden RA E ist E^* ein RA — $\mathrm{L}(E^*) := \mathrm{L}(E)^*$
2. für RAs E und F ist EF ein RA — $\mathrm{L}(EF) := \mathrm{L}(E) \cdot \mathrm{L}(F)$
3. für RAs E und F ist $E + F$ ein RA — $\mathrm{L}(E + F) := \mathrm{L}(E) \cup \mathrm{L}(F)$
4. wenn E ein RA ist, dann ist (E) ein RA — $\mathrm{L}((E)) := \mathrm{L}(E)$

Aufgabe

wir wollen einen regulären Ausdruck formulieren,
dessen Sprache L alle Strings mit abwechselnden 0en und 1en enthält

Lösung

- regulärer Ausdruck $\mathbf{10}$ beschreibt den String 10
- also beschreibt $(\mathbf{01})^*$ alle Strings der Form

$$0101010101\ldots$$

- und $(\mathbf{10})^*$ beschreibt

$$1010101010\ldots$$

$$\begin{aligned} \mathrm{L} &= (\mathbf{01})^* + (\mathbf{10})^* + \mathbf{0}(\mathbf{10})^* + \mathbf{1}(\mathbf{01})^* \\ &= (\epsilon + \mathbf{1})(\mathbf{01})^*(\epsilon + \mathbf{0}) \end{aligned}$$

Algebraische Gesetze für reguläre Ausdrücke

Beispiel

$$\mathbf{0^*1} + (\mathbf{0^*1})(\mathbf{0^*1} + \epsilon)^*(\mathbf{0^*1}) \equiv (\mathbf{0^*1})^+$$

seien L, M, N beliebige reguläre Ausdrücke

Assoziativität und Kommutativität

1. $\mathrm{L}(L + M) = \mathrm{L}(M + L)$ — Kommutativität von $+$
2. $\mathrm{L}((L + M) + N) = \mathrm{L}(L + (M + N))$ — Assoziativität von $+$
3. $\mathrm{L}((LM)N) = \mathrm{L}(L(MN))$ — Assoziativität der Verkettung

Erinnerung

Kommutativität der Verkettung gilt nicht

Neutrales Element und Löscher

Erinnerung
ein neutrales Element für einen Operator ist ein Element das die Operation nicht beeinflusst

Lemma
1. $\mathrm{L}(\varnothing + L) = \mathrm{L}(L + \varnothing) = \mathrm{L}(L)$ — *$\varnothing$ ist das neutrale Element für $+$*
2. $\mathrm{L}(\epsilon L) = \mathrm{L}(L\epsilon) = \mathrm{L}(L)$ — *ϵ is das neutrale Element von $\cdot$*

Definition
ein Löscher (Annihilator) für einen Operator ist ein Element das die Operation zunichte macht

Lemma
1. $\mathrm{L}(\varnothing L) = \mathrm{L}(L\varnothing) = \varnothing$ — *$\varnothing$ ist ein Löscher der Verkettung*

Distributivgesetze und Idempotenzgesetz

Lemma
1. $\mathrm{L}(L(M + N)) = \mathrm{L}(LM + LN)$ — *Linksdistributivität*
2. $\mathrm{L}((M + N)L) = \mathrm{L}(ML + NL)$ — *Rechtsdistributivität*

$$\mathbf{0} + \mathbf{01}^* \equiv \mathbf{0}\epsilon + \mathbf{01}^* \equiv \mathbf{0}(\epsilon + \mathbf{1}^*) \equiv \mathbf{01}^*$$

Lemma
1. $\mathrm{L}(L + L) = \mathrm{L}(L)$ — *Idempotenzgesetz von $+$*

$$\mathbf{0}^* + \mathbf{0}^* \equiv \mathbf{0}^*$$

Gesetze für den Kleene-Stern

Lemma
1. $\mathrm{L}(L^*) = \mathrm{L}(\mathrm{L}^*\,\mathrm{L}^*) = \mathrm{L}((L^*)^*)$
2. $\mathrm{L}(\varnothing^*) = \mathrm{L}(\epsilon)$
3. $\mathrm{L}(L^+) = \mathrm{L}(L L^*) = \mathrm{L}(L^* L)$ — *Definition*
4. $\mathrm{L}(L^*) = \mathrm{L}(L^+ + \epsilon)$
5. $\mathrm{L}(L?) = \mathrm{L}(\epsilon + L)$ — *Definition*
6. $\mathrm{L}((E + F)^*) = \mathrm{L}((E^* + F^*)^*) =$
   $= \mathrm{L}((E^* F^*)^*) = \mathrm{L}((E^* F)^* E^*) = \mathrm{L}(E^*(FE^*)^*)$

$$(\mathbf{0}^* + \mathbf{1}?)^* \equiv ((\mathbf{0}^*)^*(\mathbf{1}?)^*)^* \equiv (\mathbf{0}^*(\epsilon + \mathbf{1})^*)^* \equiv (\mathbf{0}^*\mathbf{1}^*)^*$$

Gesetze für den Kleene-Stern (2)

Lemma
$\mathrm{L}(L^*) = \mathrm{L}(L^* L^*)$ $\quad (= \mathrm{L}(L^*)\,\mathrm{L}(L^*) = \mathrm{L}(L)^*\,\mathrm{L}(L)^*)$

Beweis.
zunächst $\mathrm{L}(L)^* \subseteq \mathrm{L}(L)^*\,\mathrm{L}(L)^*$:
- sei $x \in \mathrm{L}(L)^*$, dann $x = x\epsilon \in \mathrm{L}(L)^*\,\mathrm{L}(L)^*$
- also folgt die Behauptung

zunächst $\mathrm{L}(L)^* \supseteq \mathrm{L}(L)^*\,\mathrm{L}(L)^*$:
- sei $x \in \mathrm{L}(L)^*\,\mathrm{L}(L)^*$
- $\exists\ y, z$ aus $\mathrm{L}(L)^*$, sodass $x = yz$
- $\exists\ k, l$ sodass $y \in \mathrm{L}(L)^k$, $z \in \mathrm{L}(L)^l$ und $x \in \mathrm{L}(L)^{k+l}$
- somit $x \in \mathrm{L}(L)^*$ und die Behauptung folgt

■