Diskrete Mathematik

Martin Avanzini   Arne Dür   Christoph Kollreider   Georg Moser

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2010

Zusammenfassung der letzten LV

1. $L + (M + N) \equiv (L + M) + N$
2. $L + M \equiv M + L$
3. $L + \varnothing \equiv L$
4. $L + L \equiv L$
5. $L(MN) \equiv (LM)N$
6. $\epsilon L \equiv L\epsilon \equiv L$
7. $L(M + N) \equiv LM + LN$
8. $(L + M)N \equiv LN + MN$
9. $\varnothing L \equiv L\varnothing \equiv \varnothing$
10. $\epsilon + LL^* \equiv L^*$
11. $\epsilon + L^*L \equiv L^*$

Basierend auf diesen Gesetzen kann die Äquivalenz von regulären Ausdrücken vollständigkeit axiomatisiert werden, sodass die Äquivalenz rein algebraisch ableitbar wird

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, Abgeschlossenheit regulärer Sprachen, Pumpinglemma, Minimierung

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

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

Abgeschlossenheit regulärer Sprachen

Satz

reguläre Sprachen sind abgeschlossen

- unter Vereinigung
- unter Schnitt
- unter Komplement
- unter Mengendifferenz
- unter Abschluss (unter Kleene Stern)
- ...

Vereinigung

Satz

$\cup$

reguläre Sprachen sind abgeschlossen unter Vereinigung

Beweis

- seien A, B reguläre Sprachen
- und seien E, F RAs sodass $A = \mathrm{L}(E)$, $B = \mathrm{L}(F)$

$$A \cup B = \mathrm{L}(E + F)$$

■

$A = \{w \mid w \in \{0,1\}^* \text{ endet in } 01\}$ $B = \{w \mid w \in \{0,1\}^* \text{ endet mit } 10\}$

$E = (\mathbf{0} + \mathbf{1})^*\mathbf{01}$ $F = (\mathbf{0} + \mathbf{1})^*\mathbf{10}$

$$A \cup B = \mathrm{L}((\mathbf{0} + \mathbf{1})^*\mathbf{01} + (\mathbf{0} + \mathbf{1})^*\mathbf{10}) = \mathrm{L}(((\mathbf{0} + \mathbf{1})^*(\mathbf{01} + \mathbf{10}))$$

Komplement

Definition

$\sim(\cdot)$

sei L eine formale Sprache über dem Alphabet Σ

das Komplement $\sim L$ von L ist $\Sigma^* \setminus L$

Satz

$\sim(\cdot)$

reguläre Sprachen sind abgeschlossen unter Komplement

Beweis

- sei L regulär
- $\exists$ DEA $A = (Q, \Sigma, \delta, q_0, F)$, sodass $L = \mathrm{L}(A)$

$$\sim L = \mathrm{L}(B) \qquad B = (Q, \Sigma, \delta, q_0, Q \setminus F)$$

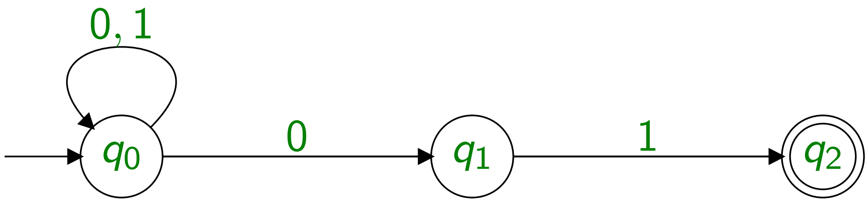
■

Beispiel: Abgeschlossenheit unter Komplement

$$L = \mathsf{L}((\mathbf{0}+\mathbf{1})^*\mathbf{01}) \qquad \sim L = ???$$

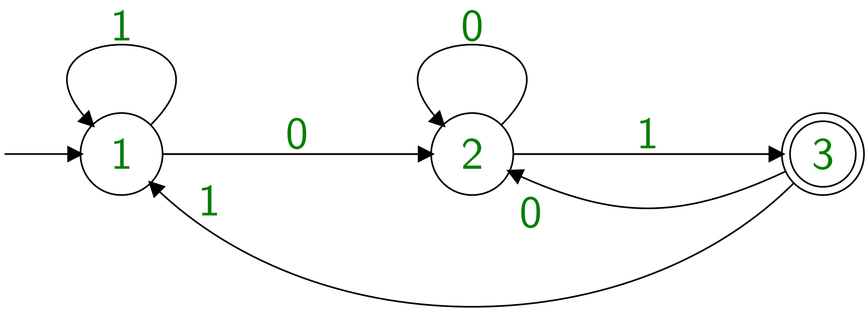
RA $\longrightarrow$ NEA

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

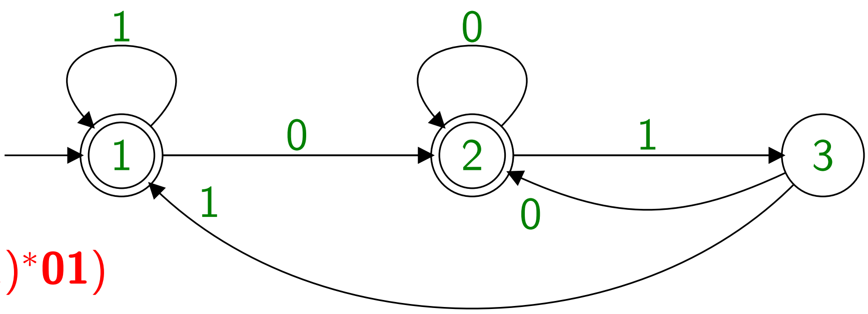


NEA $\longrightarrow$ DEA

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



Komplement des DEA



$\{0,1\}^* \setminus \mathsf{L}((\mathbf{0}+\mathbf{1})^*\mathbf{01})$

DEA $\longrightarrow$ RA

Berechne

$$\begin{aligned} R_{11}^{(3)} &= \mathbf{1}^* + (\mathbf{1}^*\mathbf{0}^+\mathbf{1})^+\mathbf{1}^+ \quad \text{und} \\ R_{12}^{(3)} &= (\mathbf{1}^*\mathbf{0}^+\mathbf{1})^*\mathbf{1}^*\mathbf{0}^+ \end{aligned}$$

Somit gilt

$$\sim L = \mathsf{L}(\mathbf{1}^* + (\mathbf{1}^*\mathbf{0}^+\mathbf{1})^+\mathbf{1}^+ + (\mathbf{1}^*\mathbf{0}^+\mathbf{1})^*\mathbf{1}^*\mathbf{0}^+)$$

Schnitt

Satz $\cap$

reguläre Sprachen sind unter Schnitt abgeschlossen

Beweis mit Logik

seien L, M reguläre Sprachen

- dann gilt $L \cup M$ ist regulär
- $\sim L$ ist regulär

wir wenden das Gesetz von de Morgan an:

$$L \cap M = \sim(\sim L \cup \sim M)$$

■

Schnitt: direkter Beweis

Beweis direkt

- seien L, M reguläre Sprachen
- $\exists$ DEA $A_L = (Q_L, \Sigma, \delta_L, q_L, F_L)$ sodass $L = \mathrm{L}(A_L)$
- $\exists$ DEA $A_M = (Q_M, \Sigma, \delta_M, q_M, F_M)$ sodass $M = \mathrm{L}(A_M)$

wir konstruieren den Produktautomaten $A = A_L \times A_M$:

$$A = (Q_L \times Q_M, \Sigma, \delta, (q_L, q_M), F_L \times F_M)$$

$$\text{mit} \quad \delta((p,q),a) = (\delta_L(p,a), \delta_M(q,a))$$

wir sehen: $\mathrm{L}(A) = \mathrm{L}(A_L) \cap \mathrm{L}(A_M)$

■

Mengendifferenz

Satz

$\setminus$

reguläre Sprachen sind unter Differenz abgeschlossen

Beweis

- seien L, M reguläre Sprachen
- $\sim L$ ist regulär
- dann gilt $L \cap M$ ist regulär

$$L \setminus M = L \cap \sim M$$

■

Anwendung von Endlichen Automaten

Anwendung

- Softwarebasiertes Entwickeln und Testen von Schaltkreisen
- Compilerbau: *Lexical analyzers*
- Textsuche; Pattern Matching
- Softwareverifikation von Protokollen
- Spielengine von Computerspiele

Problemstellung

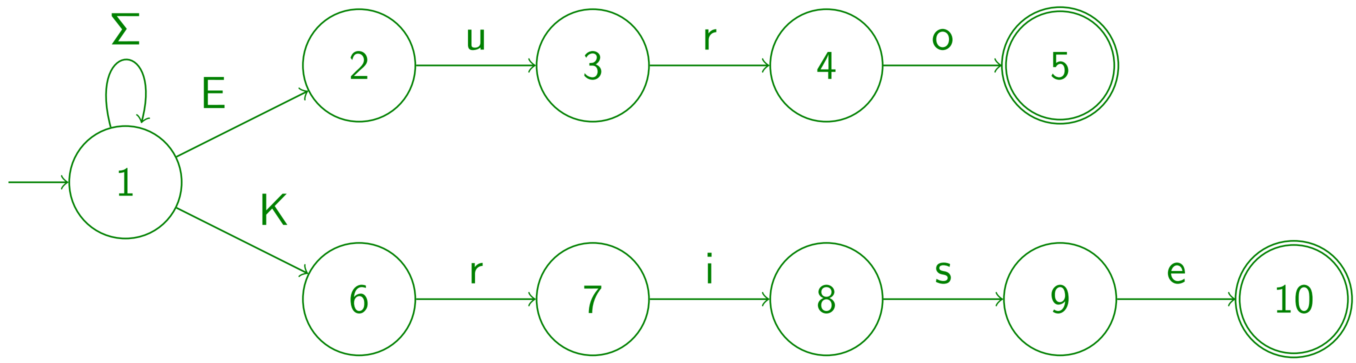
- gesucht sei eine Liste von Schlüsselwörter in einem Text oder HTML/XML Dokument
- Inhalt des Textes ändert sich täglich, sodass Indizierung zu teuer

Beispiel

suche die Worte Euro oder Krise in einer Online-Zeitung

Beispiel

suche die Worte Euro und Krise; wir definieren den folgenden NFA N



Implementierung

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

Beobachtung

der DEA hat maximal soviele Zustände wie der NEA

Direkte Konstruktion

1. sei p ein Zustand in N, erreichbar beim Lesen von $a_1 \dots a_m$; der korrespondierende Zustand in D besteht aus
   - 1
   - p
   - jeder Zustand aus N der durch einen Suffix von $a_1 \dots a_m$ erreichbar ist
2. Kanten in N von $\{1, p_1, \dots, p_n\}$ nach $\{1, q_1, \dots, q_m\}$, wenn
   - in N mit a markierte Kante von p_i nach q_j
   - in N mit a markierte Kante von 1 nach q_j und keine Kanten 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 $\Sigma \setminus \{\mathrm{E}, \mathrm{K}, \mathrm{u}\}$ markiert

Beispiel

durch die Teilmengenkonstruktion erhalten wir den folgenden DEA D