Diskrete Mathematik

Martin Avanzini   Arne Dür   Kurt Girstmair   Georg Moser

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2010

Zusammenfassung der letzten LV

Ein ϵ-NEA ist gegeben durch

1. eine endliche Menge Q, deren Elemente Zustände heißen,
2. eine endliche Menge Σ, die Eingabealphabet heißt und deren Elemente Eingabezeichen genannt werden,
3. eine Abbildung
$$\delta\colon Q \times \Sigma \cup \{\epsilon\} \to \mathcal{P}(Q)$$
die Übergangsfunktion heißt und angibt, wie sich der Zustand des Automaten bei einer Eingabe ändern kann.
4. einen ausgezeichneten Zustand, der Startzustand genannt wird,
5. eine Teilmenge $F \subseteq Q$, deren Elemente akzeptierende Zustände genannt werden.

Epsilon-Hülle

Definition — Epsilon-Hülle von q

Betrachte den (gerichteten) Zustandsgraphen des Automaten, setze $S = \{q\}$ und betrachte nur die mit ϵ marktierten Kanten

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 — L(E)

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

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

Teilmengenkonstruktion für ϵ-NEAs

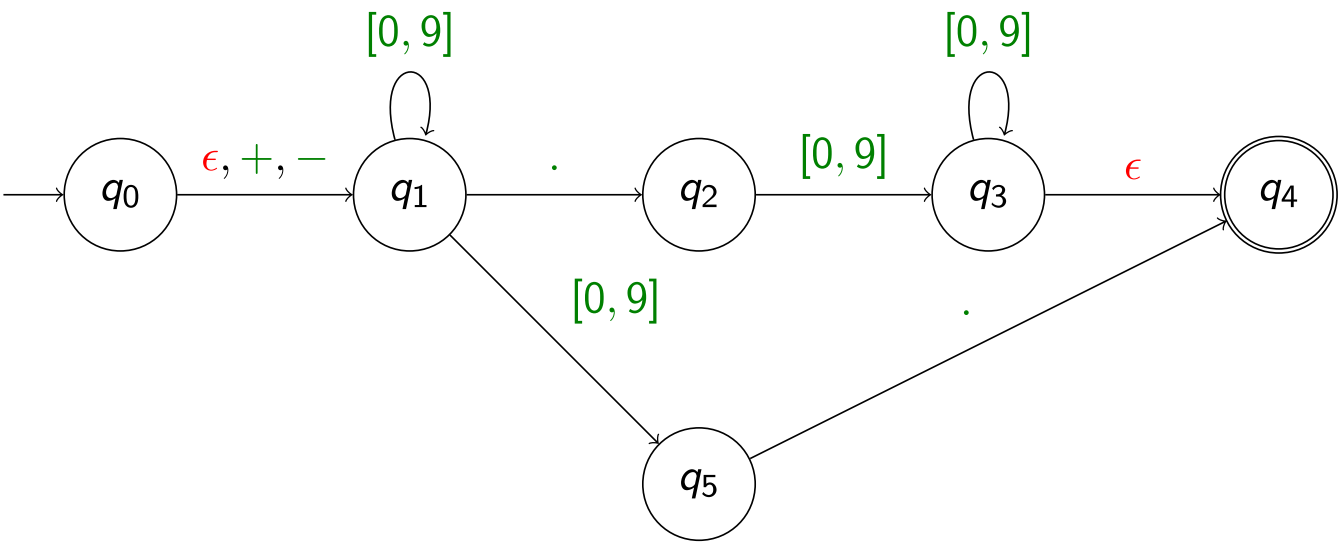
sei $E = (Q_E, \Sigma, \delta_E, q_E, F_E)$

konstruiere deterministischen Automaten $D = (Q_D, \Sigma, \delta_D, q_D, F_D)$

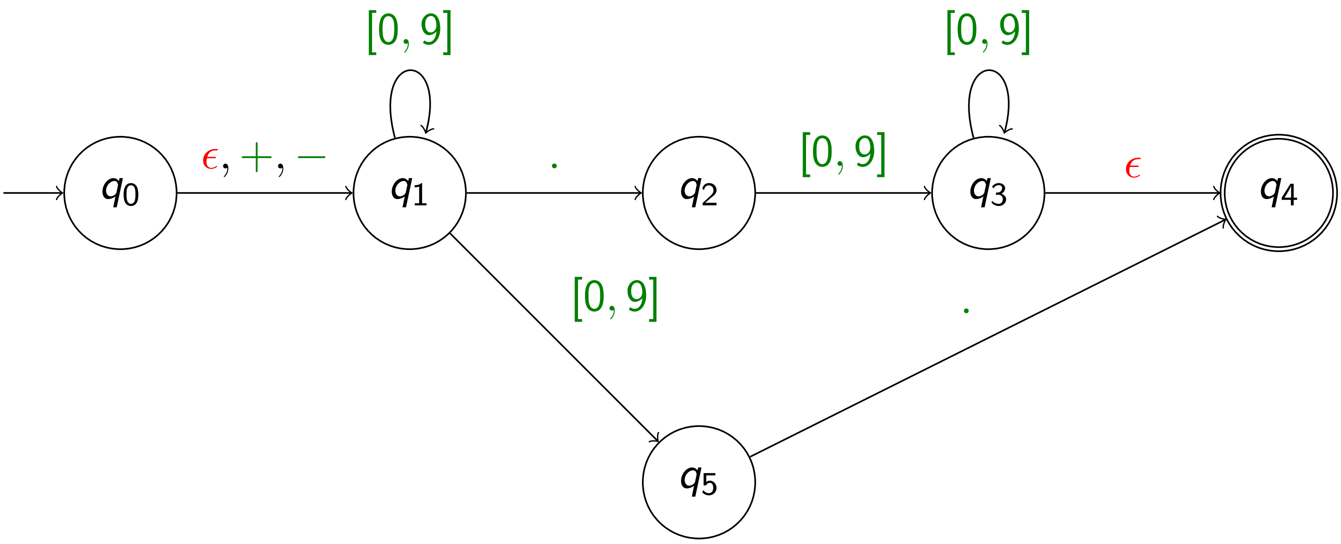
1. Q_D ist die Menge der Teilmengen von Q_E.
2. Zur Berechnung von δ_D betrachten wir jede Teilmenge $S \subseteq Q_E$ und jedes $a \in \Sigma$:
   - angenommen $S = \{p_1, \ldots, p_k\}$
   - berechne $\bigcup_{i=1}^{k} \delta_E(p_i, a) := \{r_1, \ldots, r_m\}$

   setze
$$\delta_D(S, a) = \bigcup_{j=1}^{m} \epsilon\text{-Hülle}(r_j)$$
3. $q_D = \epsilon\text{-Hülle}(q_E)$
4. $F_D = \{S \subseteq Q_E \mid S \cap F_E \neq \varnothing\}$

Beispiel (1)



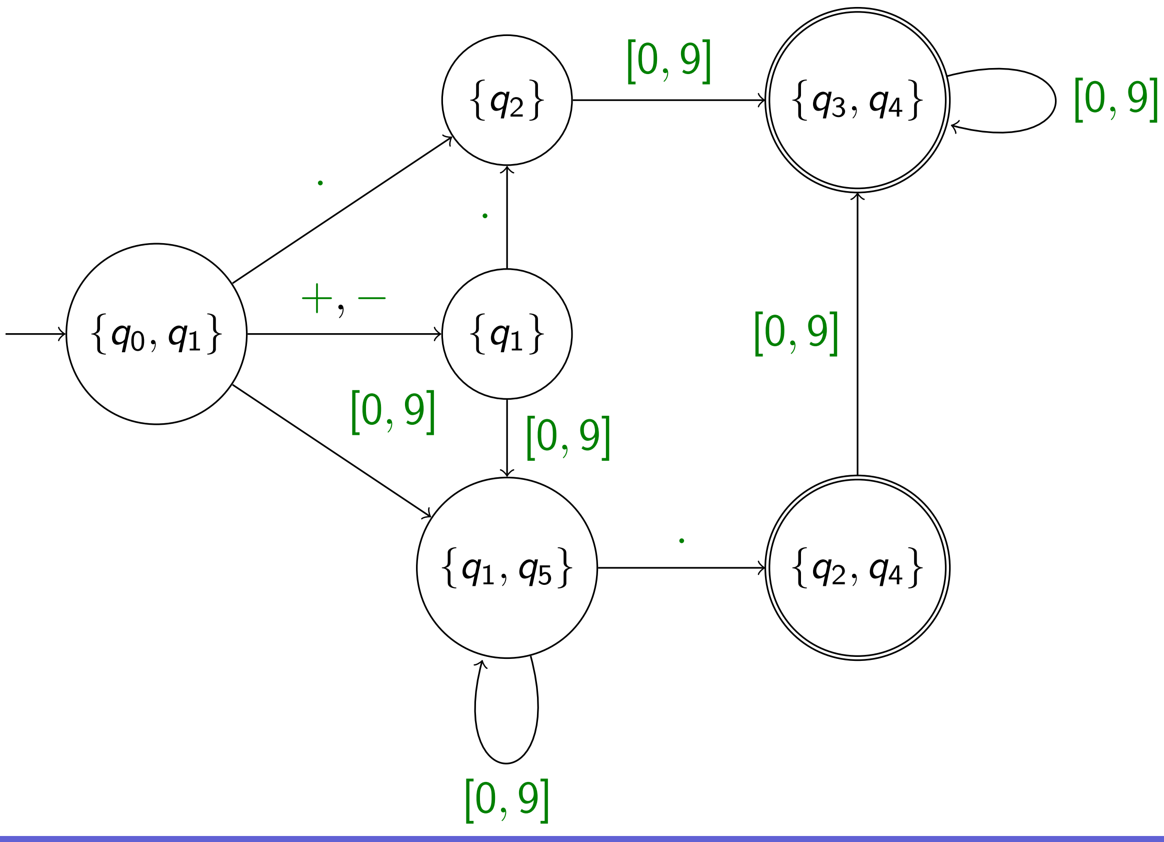
$$\begin{aligned}
\delta_D(\{q_0, q_1\}, +) &= \epsilon\text{-Hülle}(q_1) = \{q_1\} \\
\delta_D(\{q_0, q_1\}, -) &= \epsilon\text{-Hülle}(q_1) = \{q_1\} \\
\delta_D(\{q_0, q_1\}, \cdot) &= \epsilon\text{-Hülle}(q_2) = \{q_2\} \\
\delta_D(\{q_0, q_1\}, [0, 9]) &= \epsilon\text{-Hülle}(q_1) \cup \epsilon\text{-Hülle}(q_5) = \{q_1, q_5\}
\end{aligned}$$



	$+$	$-$	$\cdot$	$[0,9]$
$\rightarrow \{q_0, q_1\}$	$\{q_1\}$	$\{q_1\}$	$\{q_2\}$	$\{q_1, q_5\}$
$\{q_1\}$	$\emptyset$	$\emptyset$	$\{q_2\}$	$\{q_1, q_5\}$
$\{q_2\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{q_3, q_4\}$
$\{q_1, q_5\}$	$\emptyset$	$\emptyset$	$\{q_2, q_4\}$	$\{q_1, q_5\}$
$* \{q_3, q_4\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{q_3, q_4\}$
$* \{q_2, q_4\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{q_3, q_4\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

Beispiel (2)

In Summe erhalten wir den folgenden determinisierten Dezimalzahlautomaten, wobei wir den Fangzustand $\emptyset$ weglassen können



Äquivalenz von ϵ-NEAs und DEAs

Satz

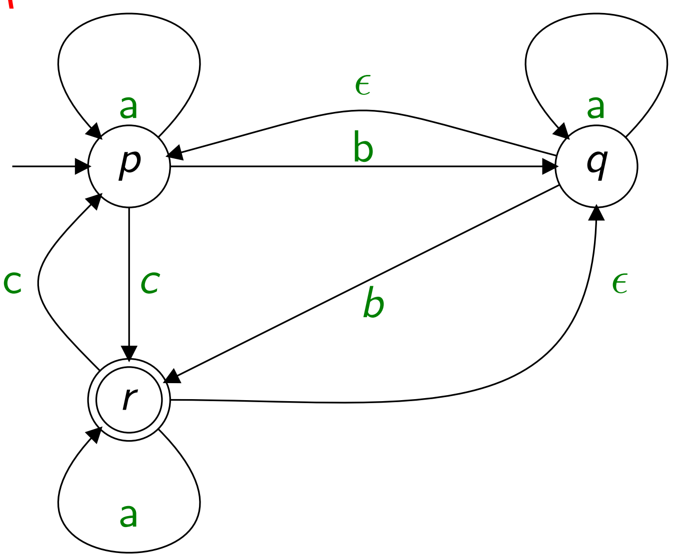
Eine Sprache L wird genau dann von einem ϵ-NEA akzeptiert, wenn L von einem DEA akzeptiert wird.

Beweis

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

Beispiel (1)

betrachte ϵ-NEA *A*



Sprache von *A*

Kombinationen von a, b und c sodass

- entweder zwei bs oder
- ein c auftreten

Beispiel (2)

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

1. Epsilon Hüllen

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

2. Übergangsfunktion δ_D

   δ_D für das erste Argument $\{p\}$:

$$\delta_D(\{p\}, \mathrm{a}) = \epsilon\text{-Hülle}(p) = \{p\}$$
$$\delta_D(\{p\}, \mathrm{b}) = \epsilon\text{-Hülle}(q) = \{p, q\}$$
$$\delta_D(\{p\}, \mathrm{c}) = \epsilon\text{-Hülle}(r) = \{p, q, r\}$$

Beispiel (3)

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

2. Übergangsfunktion δ_D

   δ_D für das erste Argument $\{p, q\}$:

$$\delta_D(\{p, q\}, \mathrm{a}) = \epsilon\text{-Hülle}(p) \cup \epsilon\text{-Hülle}(q) = \{p, q\}$$
$$\delta_D(\{p, q\}, \mathrm{b}) = \epsilon\text{-Hülle}(q) \cup \epsilon\text{-Hülle}(r) = \{p, q, r\}$$
$$\delta_D(\{p, q\}, \mathrm{c}) = \epsilon\text{-Hülle}(r) \cup \varnothing = \{p, q, r\}$$

   δ_D mit dem ersten Argument $\{p, q, r\}$:

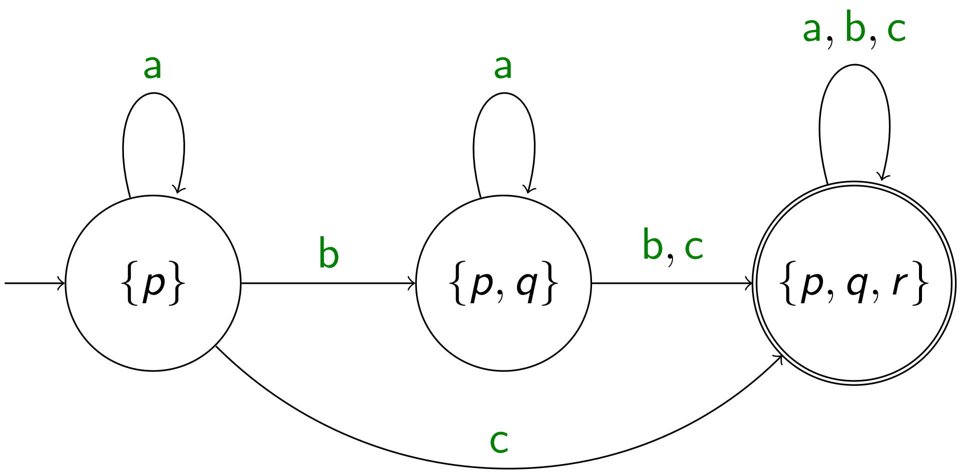
$$\delta_D(\{p, q, r\}, \mathrm{a}) = \epsilon\text{-Hülle}(p) \cup \epsilon\text{-Hülle}(q) \cup \epsilon\text{-Hülle}(r) = \{p, q, r\}$$
$$\delta_D(\{p, q, r\}, \mathrm{b}) = \epsilon\text{-Hülle}(q) \cup \epsilon\text{-Hülle}(r) = \{p, q, r\}$$
$$\delta_D(\{p, q, r\}, \mathrm{c}) = \epsilon\text{-Hülle}(r) \cup \epsilon\text{-Hülle}(p) = \{p, q, r\}$$

Beispiel (4)

3. akzeptierende Zustände

   Zustand $\{p, q, r\}$ von D enthält den akzeptierenden Zustand r von E; also ist $\{p, q, r\}$ akzeptierend

in Summe erhalten wir:



Operationen auf formalen Sprachen

seien L, M formale Sprachen

Definition $L \cup M$

Die Vereinigung von L und M, ist die Menge der Wörter, die entweder in L oder in M liegen

Definition $L \cdot M$

Die Konkatenation 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 L^*

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

Beispiel

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

Reguläre Ausdrücke

Definition RA

Sei Σ ein endliches Alphabet. Wir definieren reguläre Ausdrücke induktiv

Basis

1. $\varnothing$ ist ein RA $\qquad \mathsf{L}(\varnothing) = \varnothing$
2. ϵ ist ein RA $\qquad \mathsf{L}(\epsilon) = \{\epsilon\}$
3. Für jedes Symbol $a \in \Sigma$ ist $\mathbf{a}$ ein RA $\qquad \mathsf{L}(\mathbf{a}) = \{a\}$

Schritt

1. Für jeden RA E ist auch E^* ein RA $\qquad \mathsf{L}(E^*) = (\mathsf{L}(E))^*$
2. Für RAs E und F ist auch EF ein RA $\qquad \mathsf{L}(EF) = \mathsf{L}(E)\mathsf{L}(F)$
3. Für RAs E und F ist auch $E + F$ ein RA $\qquad \mathsf{L}(E+F) = \mathsf{L}(E) \cup \mathsf{L}(F)$
4. Wenn E ein RA ist, dann ist auch (E) ein RA $\qquad \mathsf{L}((E)) = \mathsf{L}(E)$

Beispiel: Reguläre Ausdrücke

Aufgabe

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

Lösung

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

$$0101010101\ldots$$

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

$$1010101010\ldots$$

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

Reguläre Ausdrücke und Endliche Automaten

Satz

die folgenden Mengen sind gleich:

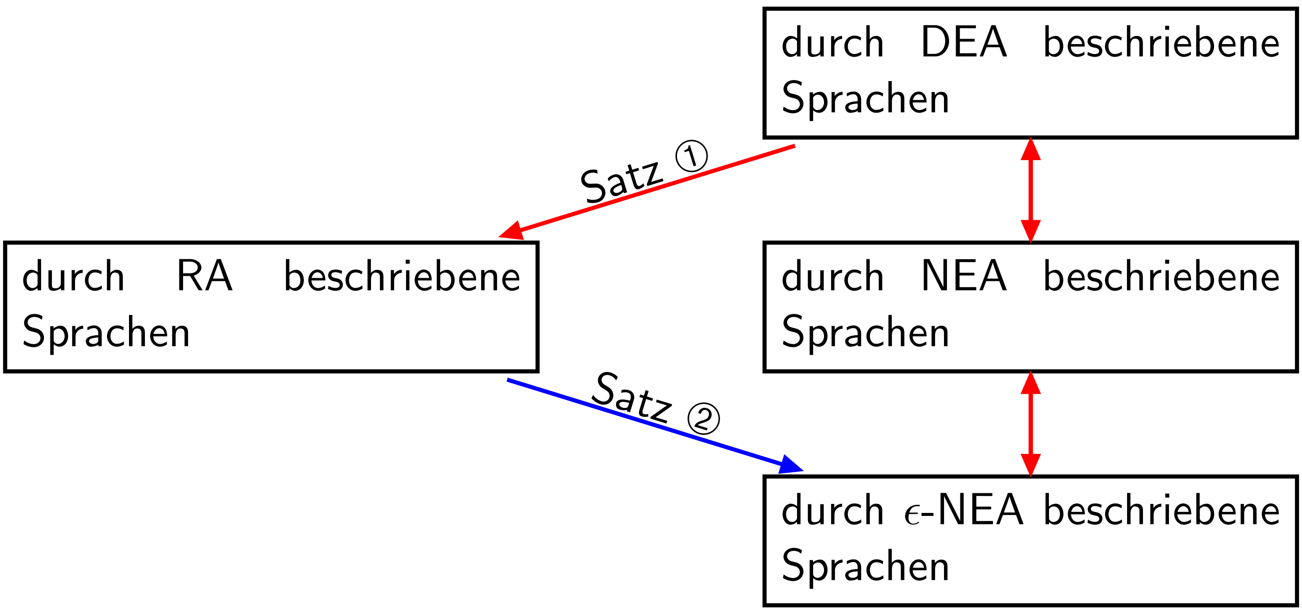
- die Menge der durch RA beschriebenen Sprachen
- die Menge der von DEA akzeptierten Sprachen
- die Menge der von NEA akzeptierten Sprachen
- die Menge der von ϵ-NEA akzeptierten Sprachen.

Definition

reguläre Sprachen

diese Sprachen nennt man reguläre Sprachen

Reguläre Sprachen



Satz ① DEA $\rightarrow$ RA

Wenn für einen beliebigen DEA A: $\mathsf{L} = \mathsf{L}(A)$, dann
$\exists$ regulären Ausdruck R, sodass $\mathsf{L} = \mathsf{L}(R)$

Satz ② RA $\rightarrow$ ϵ-NEA

Wenn für einen beliebigen RA R: $\mathsf{L} = \mathsf{L}(R)$, dann
$\exists$ ϵ-NEA E, sodass $\mathsf{L} = \mathsf{L}(E)$

EAs in reguläre Ausdrücke transformieren

Satz

DEA $\rightarrow$ RA

Wenn für einen beliebigen DEA A: $\mathsf{L} = \mathsf{L}(A)$, dann
$\exists$ regulären Ausdruck R, sodass $\mathsf{L} = \mathsf{L}(R)$

Beweis

- Zustände von A in natürliche Zahlen umbenennen
- sei n Anzahl der Zustände
- definiere regulären Ausdrücke:

$$R_{ij}^{(k)}$$

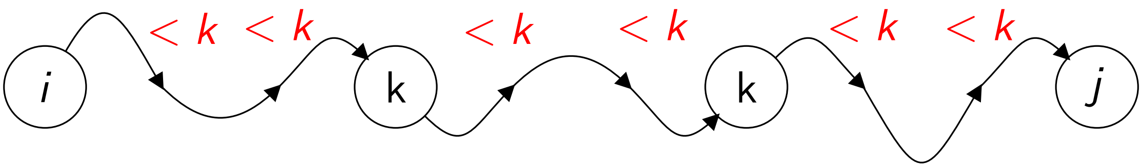
für alle $1 \leqslant i, j \leqslant n$, $0 \leqslant k \leqslant n$

$R_{ij}^{(k)}$ beschreibt die Wörter, die A von Zustand i bis Zustand j lesen kann
wobei nur Zustände $\leqslant k$ besucht werden

- angenommen $R_{ij}^{(k)}$ ist schon definiert, für alle k
- angenommen, der Startknoten des DEA A ist 1
- definiere RA E, sodass $\mathrm{L} = \mathrm{L}(E)$:

$$E := \bigcup \{ R_{1j}^{(n)} \mid j \text{ ist akzeptierend} \}$$

Beobachtung



$R_{ik}^{(k-1)}$ $(R_{kk}^{(k-1)})^*$ $R_{kj}^{(k-1)}$

Menge der gelesenen Zeichen $= R_{ik}^{(k-1)}(R_{kk}^{(k-1)})^* R_{kj}^{(k-1)}$

definiere $R_{ij}^{(k)}$ induktiv

Basis $k = 0$

1. Wir betrachten die Wege der Länge $\leqslant 1$
2. unterscheiden die Fälle ①: $i \neq j$ und ②: $i = j$

Fall ① $i \neq j$

betrachte die Kanten zwischen i und j

- wenn es keine solche Kante
  setze $R_{ij}^{(0)} = \varnothing$
- wenn es genau eine solche Kante (i, a, j) gibt
  setze $R_{ij}^{(0)} = \mathbf{a}$
- wenn es mehrere Kanten $(i, a_1, j), \dots, (i, a_l, j)$ gibt
  setze $R_{ij}^{(0)} = \mathbf{a_1} + \cdots + \mathbf{a_l}$

Fall ② $i = j$

- zusätzlich repräsentieren wir Wege der Länge 0 durch das Leerwort ϵ

Schritt $k > 0$

1. Angenommen $\exists$ Weg von i nach j der nur durch Zustände $\leqslant k$ führt
2. zwei Fälle: ① k liegt auf dem Weg oder nicht ②

Fall ① — k liegt auf dem Weg

- spalte den Pfad in Teilstücke, die k nicht passieren
- das Anfangsstück führt von i nach k
- das Endstück von k nach j
- die Mittelstücke führen von k nach k

Fall ② — k liegt nicht auf dem Pfad

- verwende $R_{ij}^{(k-1)}$

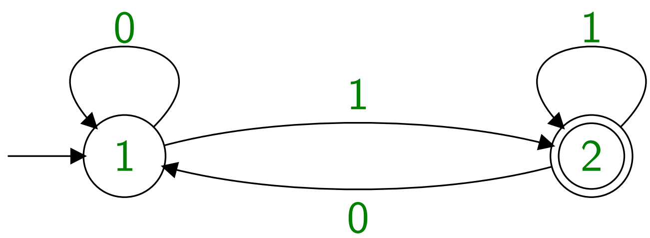
in Summe erhalten wir:

$$R_{ij}^{(k)} = R_{ij}^{(k-1)} + R_{ik}^{(k-1)}(R_{kk}^{(k-1)})^* R_{kj}^{(k-1)}$$

■

Beispiel

gegeben der folgende DEA A



mit Hilfe des Verfahrens folgt $R = (\mathbf{0}^*\mathbf{1})(\mathbf{0}^*\mathbf{1})^* = \mathrm{L}(A)$:

$$\begin{aligned}
R_{12}^{(2)} &= R_{12}^{(1)} + R_{12}^{(1)}(R_{22}^{(1)})^* R_{22}^{(1)} \\
R_{12}^{(1)} &= R_{12}^{(0)} + R_{11}^{(0)}(R_{11}^{(0)})^* R_{12}^{(0)} \\
&= \mathbf{1} + (\mathbf{0} + \epsilon)(\mathbf{0} + \epsilon)^*\mathbf{1} = \mathbf{0}^*\mathbf{1} \\
R_{22}^{(1)} &= R_{22}^{(0)} + R_{21}^{(0)}(R_{11}^{(0)})^* R_{12}^{(0)} \\
&= (\mathbf{1} + \epsilon) + \mathbf{0}(\mathbf{0} + \epsilon)^*\mathbf{1} = \mathbf{0}^*\mathbf{1} + \epsilon
\end{aligned}$$