# Diskrete Mathematik

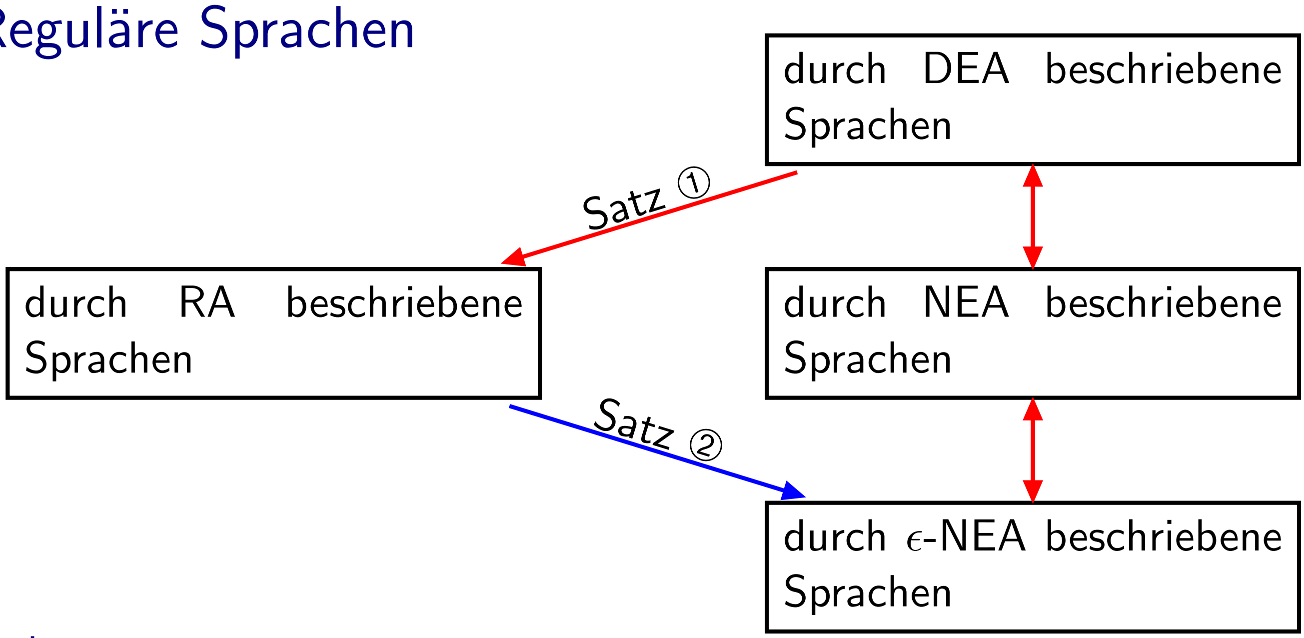
Martin Avanzini Arne Dür Christoph Kollreider Georg Moser

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2010





## Reguläre Sprachen




### 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 $\epsilon$-NEA akzeptierten Sprachen.

**Satz ①** DEA $\longrightarrow$ 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 $\longrightarrow$ $\epsilon$-NEA

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





# Übersicht

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

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

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

# Reguläre Ausdrücke in Endliche Automaten verwandeln

## Satz ②

RA $\rightarrow$ $\epsilon$-NEA

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

## Beweis

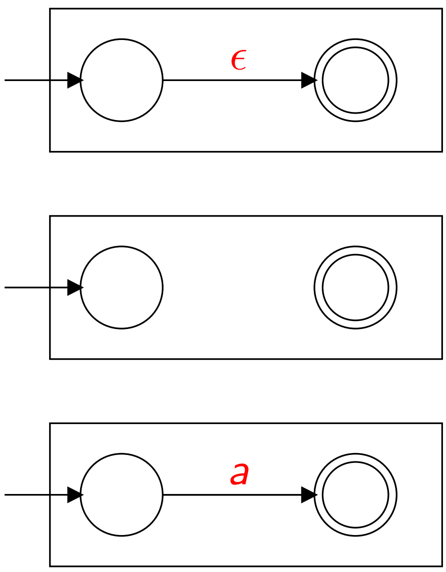
- angenommen $\mathsf{L} = \mathsf{L}(R)$, für einen RA $R$
- wir zeigen $\exists$ $\epsilon$-NEA $E$ mit
  1. genau einem akzeptierenden Zustand
  2. keinen Kanten zum Startzustand
  3. keinen Kanten vom akzeptierenden Zustand
- $\mathsf{L} = \mathsf{L}(E)$
- wir verwenden Induktion über reguläre Ausdrücke





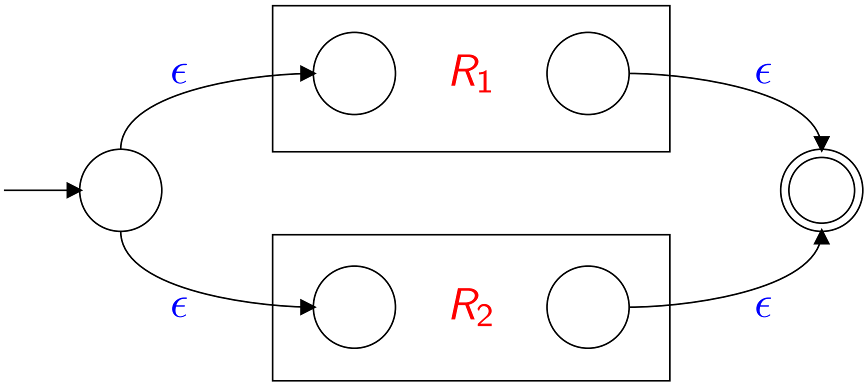
## Basis

für die RA $\epsilon$, $\varnothing$ und **a** betrachten wir die folgenden 3 Automaten.



## Induktionsschritt: $R \equiv R_1 + R_2$

- nach Induktionshypothese existieren Automaten für $R_1$ und $R_2$
- diese kombinieren wir:

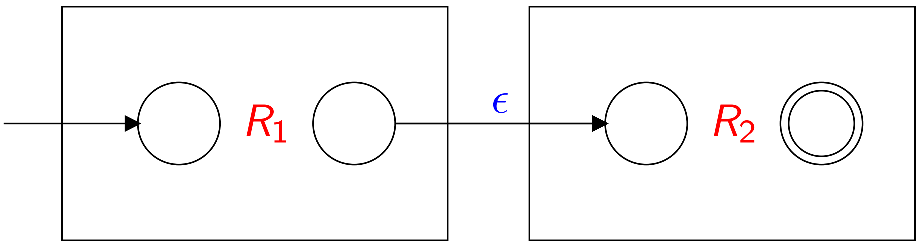






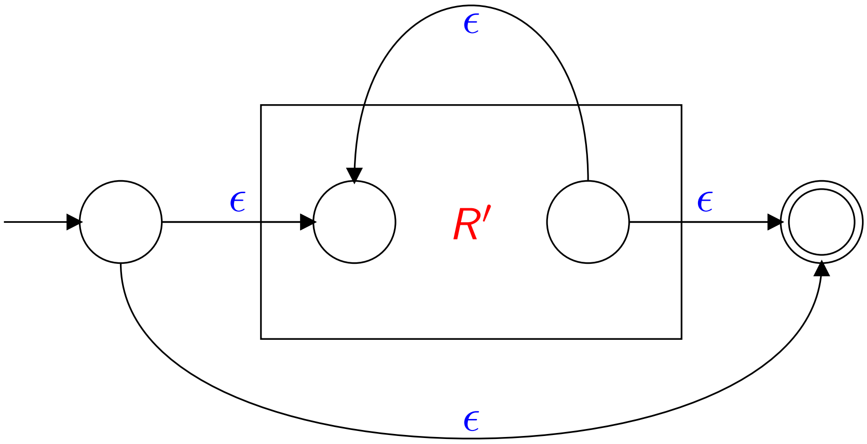

## Induktionsschritt: $R \equiv R_1 R_2$

- nach Induktionshypothese existieren Automaten für $R_1$ und $R_2$
- diese kombinieren wir:



## Induktionsschritt: $R \equiv (R')^*$

- nach Induktionshypothese existiert ein Automat für $R'$
- wir transformieren:




■





# Algebraische Gesetze für reguläre Ausdrücke

## Beispiel

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

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

### Definition

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

### Satz

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

$$\varnothing + \mathbf{0}^* \equiv \mathbf{0}^* \qquad \mathbf{0}^* \equiv \mathbf{0}^*\epsilon$$

### Definition

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

### Satz

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

$$\varnothing\mathbf{0}^* \equiv \varnothing \qquad \mathbf{0}^*\varnothing \equiv \varnothing$$





# Distributivgesetze und Idempotenzgesetz

### Satz

Distributivgesetze von $\cdot$ bezüglich $+$

1. $\mathsf{L}(L(M + N)) = \mathsf{L}(LM + LN)$
2. $\mathsf{L}((M + N)L) = \mathsf{L}(ML + NL)$

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

### Satz

1. $\mathsf{L}(L + L) = \mathsf{L}(L)$ — Idempotenzgesetz von $+$

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

# Gesetze für den Kleene-Stern

## Satz

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

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



Algebraische Gesetze für reguläre Ausdrücke

# Gesetze für den Kleene-Stern (2)

## Lemma

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

## Beweis

zunächst zeigen wir: $\mathrm{L}(L)^* \subseteq \mathrm{L}(L)^*\,\mathrm{L}(L)^*$:

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

zunächst zeigen wir: $\mathrm{L}(L)^* \supseteq \mathrm{L}(L)^*\,\mathrm{L}(L)^*$:

- 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

∎

# Ein Algorithmus für Algebraische Gesetze

seien $G$, $H$ seinen Schemata von regulären Ausdrücken

## Algorithmus

1. $\forall$ Variablen in $G$ und $H$: durch konkrete Symbole ersetzen
   verschiedene Variablen durch verschiedene Symbole ersetzen
2. Gleichung $\mathrm{L}(G) = \mathrm{L}(H)$ in eine Gleichung $\mathrm{L}(C) = \mathrm{L}(D)$ umwandeln
3. Teste $\mathrm{L}(C) = \mathrm{L}(D)$.
   - Wenn Ja, dann gilt auch $\mathrm{L}(G) = \mathrm{L}(H)$
   - Wenn Nein, dann ist $\mathrm{L}(G) \neq \mathrm{L}(H)$ falsch

## Satz

Der angegebene Test ist korrekt:
Für jedes so gefundene Gesetz gilt $\mathrm{L}(G) = \mathrm{L}(H)$ für alle beliebigen regulären Ausdrücke an der Stelle von $G$ bzw. $H$