

# Theoretische Informatik – Schreibomat

Florian

December 4, 2012

## Tools

- Finite State Machine Designer: <http://madebyevan.com/fsm/>

## 1 Was ist Informatik?

- Konkrete<sup>1</sup> Konzepte: Algorithmus, Berechnung, Komplexität
- Was will die theoretische Informatik? Formale Bestimmung der Begriffe, unabhängig von Hard- und Software
- Ziel: Grundlegende Eigenschaften von Algorithmen, Berechnungen erkennen. Methoden entwickeln zum Entwurf beweisbar korrekter Hard- und Software (nicht Schwerpunkt dieser Vorlesung)
- Grenzen der automatischen Berechnung aufzeigen
- Typische Fragestellungen: Ist es möglich, ein Programm zu schreiben, das ein anderes Programm als Eingabe erhält und feststellen kann, ob dieses in eine Endlosschleife gerät oder nicht?  $\Rightarrow$  Halteproblem. Nein, es ist natürlich nicht möglich. Eine andere typische Fragestellung ist die Folgende: Wir haben einen Rucksack, und der hat 30 Liter Fassungsvermögen. Und wir haben noch 50 Gegenstände, und jetzt wollen wir wissen: wie lange dauert es, herauszufinden, wieviele Gegenstände in den Rucksack passen? Rucksackproblem, nicht in polynomialer Zeit lösbar  $\Rightarrow$  Es dauert exponentiell lange.
- Leider ist es in der Praxis so, dass die Antwort auf ähnliche Fragestellungen nicht immer so offensichtlich ist, und deshalb müssen wir es uns ein bisschen genauer betrachten.

**Übung.** Gegeben sei das folgende Strassennetz:  
(Wildes Gekritzelt)

---

<sup>1</sup>4. September 2012

- (a) Gibt es eine Möglichkeit, alle Strassen genau 1x zu durchlaufen und dann wieder am Ausgangspunkt anzulangen,
- (b) Gibt es eine Möglichkeit, alle Kreuzungen genau 1x zu passieren und dann wieder am Ausgangspunkt anzulangen?

Die Antworten sind imfall:

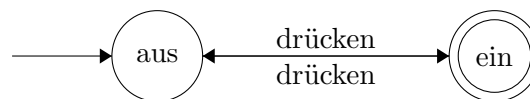
- (a) Einfache Aufgabe: Geht immer, wenn die Anzahl der Abzweigungen an jeder Kreuzung gerade ist.
- (b) Traveling salesman (TSP). Schwierig! Es ist keine wesentlich bessere Methode bekannt, als einfach alles durchzuprobieren.

Ziel für die Vorlesung: Um solche Fragestellungen systematisch beantworten zu können, brauchen wir ein exaktes mathematisches Modell eines Computers.

## 2 Automatentheorie

Endliche Automaten, Kontextfreie Grammatiken und Keller-Automaten. Zusätzliche Motivation: Das sind Konzepte, denen man auch häufig in der Praxis begegnet (Compilerbau, Textsuche, Textverarbeitung)

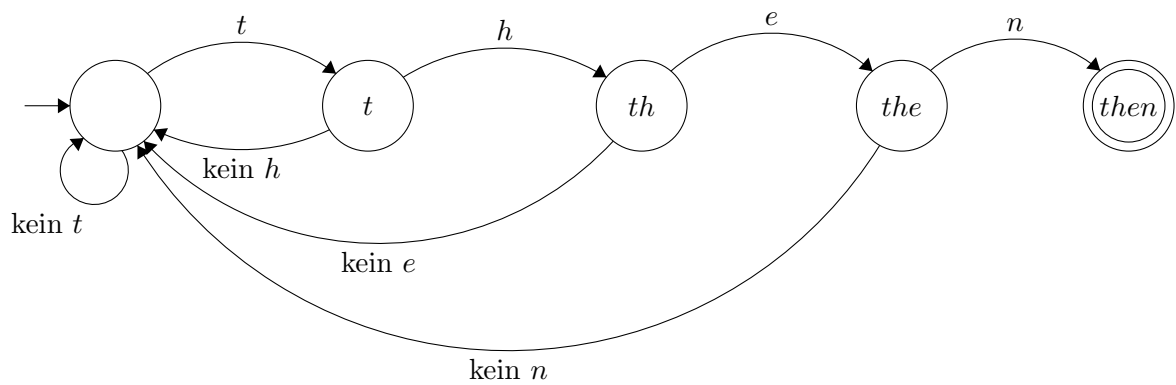
Noch nicht ganz so formal, bisschen intuitiv. Modellierung eines Kippschalters.



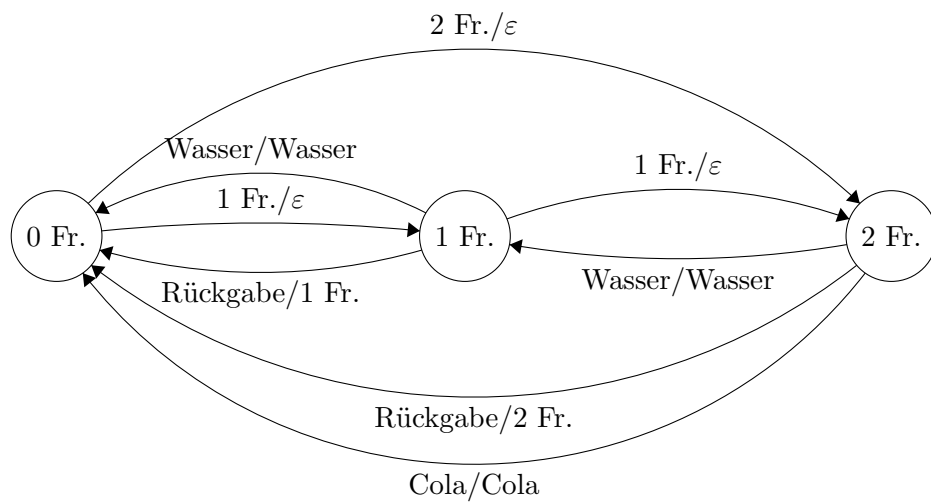
**Definition 1** (Endlicher Automat). Wir haben:

- Zwei Zustände, davon ein Startzustand
- und ein akzeptierender Zustand
- Transitionen (Zustandsübergänge): führen den Automaten anhand einer Eingabe von einem Zustand in den nächsten.

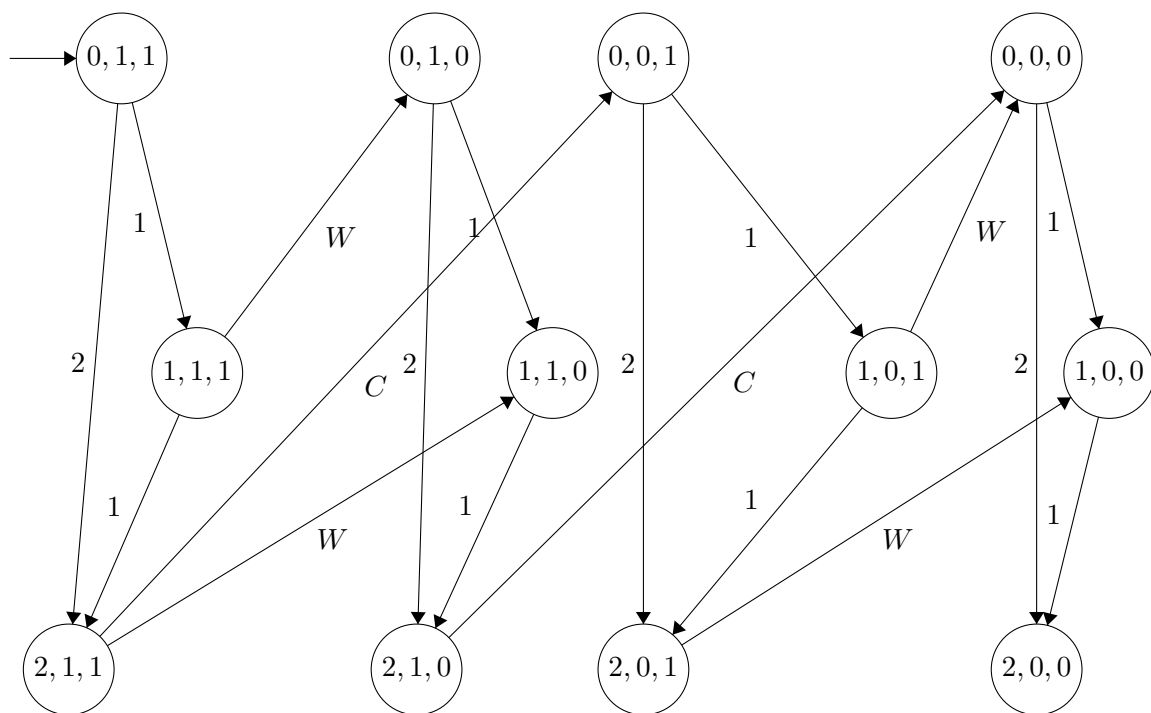
Beispiel: Mustererkennung in Texten: z.B. Suche das Wort "then"



Getränkeautomat (Beispiel für Automat mit Ausgabe): Cola für CHF 2, Wasser für CHF 1. Münzannahme: Münzen zu 1, 2 CHF.



Wenn der Automat nur eine Flasche Cola und eine Flasche Wasser enthält:



### 3 Formale Sprachen

Ziel: Genaue Beschreibung der Ein- und Ausgaben eines Automaten.

**Definition 2** (Alphabet). (endliche, nichtleere Menge von Symbolen). Bsp: Binäres Alphabet  $\Sigma_{\text{bin}} = \{0, 1\}$ , Tastaturalphabet  $\Sigma_{\text{tast}} = \{a, \dots, z, A, \dots, Z, 0, \dots, 9, \dots\}$

**Definition 3** (Wort (= Zeichenkette, String)). Endliche Folge von Symbolen eines gegebenen Alphabets. Beispiel: 01110 ist ein Wort über  $\Sigma_{\text{bin}}$ .

**Bemerkung** (Eigenschaften von Wörtern). Die da wären:

- Leeres Wort:  $\varepsilon$  (manchmal  $\lambda$ ) = leere Folge von Symbolen (über einem beliebigen Alphabet)
- Länge eines Wortes:  $|w|$  bezeichnet die Anzahl der Symbole im Wort  $w$ .  $|\varepsilon| = 0$ .

**Bemerkung** (Konventionen für Darstellung von Wörtern). Wir sagen:

- $a, b, c, \dots$  für Buchstaben, Symbole
- $v, w, x, \dots$  für Wörter

**Definition 4** (Potenzen von Wörtern). Es gibt im Angebot:

- Menge aller Wörter einer bestimmten Länge:

Sei  $\Sigma$  Alphabet, so:

$$\Sigma^0 = \{\varepsilon\}$$

$$\Sigma^1 = \Sigma$$

$$\Sigma^2 = \{ab \mid a, b \in \Sigma\}$$

$$\Sigma^i = \{a_1 \dots a_i \mid a_1 \dots a_i \in \Sigma\}$$

- Menge aller Wörter über  $\Sigma$ :

$$\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma^i, \varepsilon \in \Sigma^*$$

- Menge aller nichtleeren Wörter über  $\Sigma$ :

$$\Sigma^+ = \bigcup_{i=1}^{\infty} \Sigma^i, \varepsilon \notin \Sigma^+$$

**Beispiel.**

Beispiel:

$$\Sigma = \{0, 1\}$$

$$\Sigma^2 = \{00, 01, 10, 11\}$$

$$\Sigma^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots\}$$

**Definition 5** (Konkatenation (Verkettung) von Wörtern).

$$v = a_1 \dots a_k, w = b_1 \dots b_k \text{ über } \Sigma \Rightarrow v \cdot w = a_1 \dots a_k b_1 \dots b_k = vw$$

**Bemerkung** (Rechenregeln für Konkatenation von Wörtern).

$$v \cdot (v \cdot w) = (u \cdot v) \cdot w$$

$$|x \cdot y| = |x| + |y|$$

$$x \cdot \varepsilon = \varepsilon \cdot x = x$$

**Bemerkung** (Infixe, Präfixe, Suffixe). Seien  $v, w \in \Sigma^*$  für ein Alphabet  $\Sigma$ , dann ist  $v$  ein Teilwort (Infix) von  $w$ , falls es  $x, y \in \Sigma^*$  gibt, so dass  $w = x \cdot v \cdot y$ ;  $v$  ist ein Präfix von  $w$ , falls es  $y \in \Sigma^*$  gibt, so dass  $w = v \cdot y$ . Suffix funktioniert analog.

Beispiel:  $abc$  ist Teilwort von  $aabcc$ ,  $aa$  ist Präfix und Suffix von  $aabcaa$ .  $\varepsilon$  ist Teilwort von jedem Wort.

**Definition 6** (Sprache).  $L$  über Alphabet  $\Sigma$  ist eine Teilmenge von  $\Sigma^*$ ,  $L \subseteq \Sigma^*$ . Sprache ist Menge von Wörtern, kann unendlich gross sein. Leere Sprache:  $\emptyset$  enthält keine Wörter, ist über jedem Alphabet definiert. Spezielle Sprache:  $L_\varepsilon$  ist die Sprache, die nur das leere Wort enthält.  $L_\varepsilon \neq \emptyset$ .

**Definition 7** (Konkatenation von Sprachen).  $L_1, L_2 \subseteq \Sigma^* \Rightarrow L_1 \cdot L_2 = L_1 L_2 = \{v \cdot w | v \in L_1, w \in L_2\}$

**Definition 8** (Potenzen von Sprachen).

$$\begin{aligned} L^0 &= L_\varepsilon = \{\varepsilon\} \\ L^{i+1} &= L^i \cdot L \text{ für } i \in \mathbb{N} \end{aligned}$$

**Definition 9** (Kleene-Stern).

$$\begin{aligned} L^* &= \bigcup_{i \in \mathbb{N}} L^i \\ L^+ &= \bigcup_{i \in \mathbb{N}} L^i - L_\varepsilon \end{aligned}$$

**Beispiel.** Sei  $\Sigma = \{a, b\}, L_1 = \{a^i | i \geq 0\} = \{\varepsilon, a, aa, aaa, \dots\}, L_2 = \{b^i | i \geq 0\} = \{\varepsilon, b, bb, bbb, \dots\}$ :

$L_1 \cdot L_2 = \{\varepsilon, a, b, ab, aab, abb, aaab, \dots\} = \{a^i b^j | i \geq 0, j \geq 0\}$  ist die Menge aller Wörter über  $\{a, b\}$ , in dem alle  $a$ s vor allen  $b$ s vorkommen.

**Übung.** Seien  $L_1, L_2, L_3 \subseteq \Sigma^*$ .

- (a) Gilt  $(L_1 \cdot L_2) \cdot L_3 = L_1 \cdot (L_2 \cdot L_3)$ ? Ja.
- (b) Gilt  $(L_1 \cup L_2) \cdot L_3 = L_1 \cdot L_3 \cup L_2 \cdot L_3$ ? Ja.
- (c) Gilt  $(L_1 \cdot L_2) \cup L_3 = (L_1 \cup L_3) \cdot (L_2 \cup L_3)$ ? Quatsch.
- (d) Gilt  $L_1 \cdot L_2 = L_2 \cdot L_1$ ? Quatsch.

*Beweis.* (a)

$$\begin{aligned} (L_1 \cdot L_2) \cdot L_3 &= \{vw | v \in L_1 \cdot L_2, w \in L_3\} \\ &= \{xyz | x \in L_1, y \in L_2, z \in L_3\} \\ &= \{xz | x \in L_1, z \in L_2 L_3\} \\ &= L_1 \cdot (L_2 \cdot L_3) \end{aligned}$$

(b)

$$\begin{aligned} (L_1 \cup L_2) \cdot L_3 &= \{vw | v \in L_1 \cup L_2, w \in L_3\} \\ &= \{vw | v \in L_1, w \in L_3\} \cup \{vw | v \in L_2, w \in L_3\} \\ &= (L_1 \cdot L_3) \cup (L_2 \cdot L_3) \end{aligned}$$

(c) Gegenbeispiel:  $L_1 = L_2 = \{a\}, L_3 = \{b\}$ . Daraus folgt:

$$\begin{aligned} L_1 L_2 = \{aa\} &\Rightarrow (L_1 L_2) \cup L_3 = \{aa, b\} \\ L_1 \cup L_2 = \{a, b\} = L_2 \cup L_3 &\Rightarrow \dots \end{aligned}$$

□

**Bemerkung.** (d) gilt aber für  $|\Sigma| = 1$ .

**Definition 10** (Entscheidungsproblem). Die Eingabe ist eine Sprache  $L$  über einem Alphabet  $\Sigma$  sowie ein Wort  $w \in \Sigma^*$ . Die Ausgabe soll lauten: JA falls  $w \in L$  oder NEIN falls  $w \notin L$ .

Die Modellierung von vielen alltäglichen Berechnungsproblemen im Formalismus der formalen Sprachen.

**Beispiel** (Primzahltest). Das Alphabet  $\Sigma = \{0, 1\}$ . Die Sprache

$$L = \{w \in \Sigma^* \mid w \text{ ist Binärdarstellung einer Primzahl}\}$$

Eine Zahl  $p \in \mathbb{N}$  ist Primzahl genau dann, wenn  $\text{Bin}(p) \in L$ .

Identifizierung von Sprachen als Probleme.

## 4 Kurze Einführung in formale Beweise

Behauptungen<sup>2</sup> mit Unanfechtbarkeitsanspruch wollen bewiesen werden. Insbesondere negative Aussagen der Form "Dieses Rechenmodell kann diese Aufgabe nicht lösen" brauchen eine präzise Formulierung und Begründung, um glaubwürdig zu sein<sup>3</sup>.

Als Beweismethoden haben wir im Angebot:

Unkontrollierte  
Hausauf-  
gabe

**Deduktion (zum Beweis einer Implikation)** Zum Beweis von Wenn-Dann-Aussagen, z.B.

$$\text{Wenn } \underbrace{x \geq 4}_{\text{Hypothese}}, \text{ dann } \underbrace{x^2 \geq 16}_{\text{Konklusion}}$$

Vorgehen: Hypothese als wahr annehmen, dann Folgerungen darauf anwenden, bis die Konklusion folgt.

**Beispiel.** Sei  $x \geq 4$ . Es gilt  $4^2 = 16$  und die Quadratfunktion ist steigend. Daraus folgt:  $x^2 \geq 4^2 = 16$

Hierfür ist es oft hilfreich, Definitionen von Begriffen einzusetzen.

**Beispiel.** Wenn  $L = \{w \in \{a, b\}^* \mid |w| \text{ gerade}\}$ , dann gilt für alle  $x \in L^2$ , dass  $|x|$  gerade ist.

*Beweis.* Sei  $x \in L^2$ .

Definition von  $L^2$  einsetzen. Es existieren  $u, v \in L$ , so dass  $x = uv$ .

Definition von  $L$  einsetzen.  $|u|$  ist gerade,  $|v|$  ist gerade.

$\Rightarrow |x| = |u| + |v| \Rightarrow |x|$  ist gerade.

□

---

<sup>2</sup>11. September 2012

<sup>3</sup>Hopcraft et al., Abschnitt 1.2–1.4

**Doppelte Deduktion (zum Beweis einer Äquivalenz)** Zerlegung in zwei Wenn-Dann-Aussagen, wird getrennt bewiesen.

**Beispiel** (Gleichheit von Mengen).

$$A = B \Rightarrow A \subseteq B \wedge B \subseteq A \Rightarrow A = B$$

**Beispiel.** Sprachen sind ja auch Mengen. Also: seien  $L_1, L_2 \in \Sigma^*$ . Dann gilt:

$$L_1 \cdot (L_1 \cup L_2) = L_1^2 \cup L_1 \cdot L_2$$

*Beweis.* Zweimal:

” $\subseteq$ ”:

Sei  $x \in L_1 \cdot (L_1 \cup L_2) \Rightarrow \exists x = uv, u \in L_1, v \in L_1 \cup L_2$ .

Fallunterscheidung: (a)  $v \in L_1 \Rightarrow x = uv, u \in L_1, v \in L_1 \Rightarrow x \in L_1^2$ .

(b)  $v \in L_2 \Rightarrow x = uv, u \in L_1, v \in L_2 \Rightarrow x \in L_1 \cdot L_2$ .

• ” $\supseteq$ ”:

Sei  $x \in L_1^2 \cup L_1 \cdot L_2$ .

Fallunterscheidung: (a)  $x \in L_1^2 \Rightarrow x = uv, u, v \in L_1$

$\Rightarrow v \in L_1 \cup L_2$

$\Rightarrow x \in L_1 \cdot (L_1 \cup L_2)$ .

(b)  $x \in L_1 \cdot L_2 \Rightarrow x = uv, u \in L_1, v \in L_2$

$\Rightarrow v \in (L_1 \cup L_2)$

$\Rightarrow x \in L_1 \cdot (L_1 \cup L_2)$

□

**Widerspruchsbeweis** Es wird eine Annahme getroffen und dann solange gefolgert, bis Quatsch herauskommt. Daraus folgt, dass die Annahme auch falsch sein muss.

**Beispiel.** Seien  $a, b \in \mathbb{N}$  und  $a, b \geq 2$ . Dann gilt:  $a$  teilt nicht  $ab + 1$ .

*Beweis.* Seien  $a, b \in \mathbb{N}$ . Angenommen,  $a$  teilt  $ab + 1$ .

Ziel: Annahme zum Widerspruch führen, dann folgt daraus Negation, also die gewünschte Konklusion.

$a$  teilt  $ab \Rightarrow a$  teilt  $ab$  und  $ab + 1$ .

$\Rightarrow a$  teilt  $(ab + 1) - (ab) = 1$

$\Rightarrow a = 1$ . Bonk! Widerspruch zu  $a \geq 2$ .

□

**Beispiel.** Es gibt unendlich viele Primzahl (äquivalente Formulierung: Es gibt keine grösste Primzahl).



*Beweis.* Angenommen, es gäbe eine grösste Primzahl. Wir nennen die Anzahl der Primzahlen  $k$ .

Seien  $p_1 < p_2 < \dots < p_k$  die Primzahlen. Betrachten wir  $x = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ . Da  $p_k$  die grösste Primzahl ist und  $x > p_k$ , kann  $x$  keine Primzahl sein.

Also gibt es eine Primfaktorzerlegung von  $x$ , und  $p_l$  sei die kleinste Primzahl in dieser Zerlegung.

Dann gilt:  $p_l$  teilt  $p_1 \cdot p_2 \cdot \dots \cdot p_k$  und  $p_l$  teilt darum auch  $x$ .

Daraus folgt:  $p_l$  teilt  $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ . Aus dem vorhergehenden Beweis ( $a$  teilt  $ab + 1$ ) folgt, dass das ein Widerspruch ist.  $\square$

**Induktion** Vor allem verwendet für Beweise über natürliche Zahlen. Ziel: Zeige, dass die Aussage  $S(n)$  für alle  $n \geq n_0$  gilt.

Methode:

1. Induktionsanfang (Anker). Zeige  $S(n_0)$ .
2. Induktionsschritt. Zeige  $S(i) \Rightarrow S(i + 1)$ .

Idee: Wenn  $S(n_0)$  gilt und  $S(i) \Rightarrow S(i + 1)$  für alle  $i \geq n_0$ , dann folgt aus  $S(n_0)$  und  $S(n_0) \Rightarrow S(n_0 + 1)$ , dann gilt  $S(n_0 + 1)$ . Undsoweiter, undsofort.

**Beispiel** (Der kleine Gauss). . Für alle  $n \geq 1$  gilt:  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$

*Beweis.* Anker:  $\sum_{i=1}^1 = \frac{1+(1+1)}{2}$

Schritt: es gelte  $\sum_{i=1}^k i = \frac{k(k+1)}{2}$  (Induktionsvoraussetzung).

Zeige:  $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$  (Induktionsbehauptung).

$$\begin{aligned}
 \sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) \\
 &= \frac{k(k+1)}{2} + (k+1) \\
 &= \frac{k(k+1) + 2(k+1)}{2} \\
 &= \frac{(k+2)(k+1)}{2} \\
 &= \frac{(k+1+1)(k+1)}{2}
 \end{aligned}$$

$\square$

## Rekursive Definitionen und strukturelle Induktion

**Beispiel** (Rekursive Definition von arithmetischen Ausdrücken). Basis: Jede Zahl und jede Variable ist ein arithmetischer Ausdruck:  $(a + 3) \cdot 5$  ist ein arithmetischer Ausdruck,  $(a + 3 \cdot 5$  [sic] ist keiner (Klammerfehler).

Rekursion: Wenn  $E$  und  $F$  Ausdrücke sind, dann definieren wir, dass dann auch  $E + F$ ,  $E \cdot F$ ,  $(E)$  arithmetische Ausdrücke sind.

Behauptung: Jeder Ausdruck enthält gleichviele linke wie rechte Klammern.

*Beweis.* Mit struktureller Induktion:

1. I.A.: Basisausdrücke haben keine Klammern. Daraus folgt: gleichviele linke wie rechte Klammern (0).
2. Sei  $G$  ein arithmetischer Ausdruck ( $G = E + F, E \cdot F, (G)$ ). Fallunterscheidung:
  - (a)  $G = E + F$ : Induktionsvoraussetzung:  $E$  und  $F$  haben gleich viele linke wie rechte Klammern. Gilt also auch für  $G$ , da keine Klammern hinzukommen.
  - (b)  $G = E \cdot F$ : analog.
  - (c)  $(G)$ : Induktionsvoraussetzung:  $E$  hat gleich viele linke wie rechte Klammern. Gilt also auch für  $G$ , da 1 linke und 1 rechte Klammer hinzukommt.

□

## 5 Unendlichkeit

*Beweis für 3.7.* Behauptung:  $|A| < |B| \Leftrightarrow |A| = |C| \wedge C \subset B$

$A = B = \mathbb{N} = \{0, 1, 2, 3, \dots\}$   $C = \{1, 2, 3, 4, \dots\}$   $(0, 1), (1, 2), \dots, (k, k + 1)$  □

Aufgaben: 3.7, 3.8, 3.11, 3.17, 3.18, 3.19

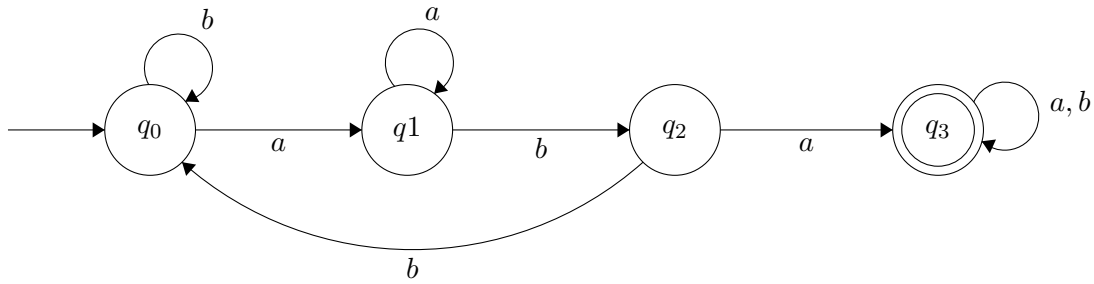
## 6 Endliche Automaten

Unterscheidung:

**Deterministisch** Automat kann zu einem Zeitpunkt nur einen Zustand annehmen.

**Nichtdeterministisch** Automat kann gleichzeitig mehrere Zustände besitzen.

**Beispiel.** DEA zum Erkennen des Musters aba:



Zustände speichern das bereits gelesene Teilmuster:

- $q_0$ : noch nichts vom Teilwort aba gelesen.
- $q_1$ : zumindest schon das Wort a gelesen.
- $q_2$ : schon ab gelesen.
- $q_3$ : das ganze Muster gelesen, es kann also akzeptiert werden.

Transitionen (Zustandsübergänge) beschreiben die Änderung beim Lesen eines Zeichens des Wortes.

**Definition 11** (Formale Definition (nochmal)). Ein DEA  $A$  wird beschrieben durch  $A = (Q, \Sigma, \delta, q_0, F)$ , wobei:

- $Q$  ist eine endliche Menge von Zuständen,
- $\Sigma$  ist das Alphabet für die Eingabe,
- $q_0$  ist der Startzustand,  $q_0 \in Q$ ,
- $F$  ist die Menge der akzeptierenden Zustände (Endzustände),  $F \subseteq Q$ ,
- $\delta : Q \times \Sigma \mapsto Q$  ist die Übergangsfunktion (Transitionsfunktion), die für jeden Zustand und jedes Eingabesymbol einen eindeutigen Folgezustand definiert.

**Beispiel** (von vorher).

$$A = (\{q_0, q_1, q_2, q_3\}, \{a, b\}, \delta, q_0, \{q_3\}),$$

wobei  $\delta$  gegeben ist durch:

$$\begin{aligned}
\delta(q_0, a) &= q_1, \\
\delta(q_0, b) &= q_0, \\
\delta(q_1, a) &= q_1, \\
\delta(q_1, b) &= q_2, \\
\delta(q_2, a) &= q_3, \\
\delta(q_2, b) &= q_0, \\
\delta(q_3, a) &= q_3, \\
\delta(q_3, b) &= q_3
\end{aligned}$$

(oder als Transitionstabelle aufgeschrieben):

	$a$	$b$
$\mapsto q_0$	$q_1$	$q_0$
$q_1$	$q_1$	$q_2$
$q_2$	$q_3$	$q_0$
$*q_3$	$q_3$	$q_3$

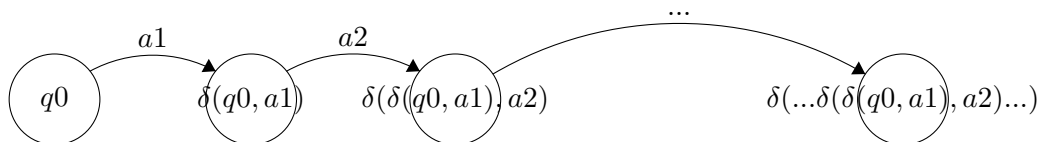
Die Transitionstabelle enthält alle Informationen über einen DEA, meistens ist aber die graphische Darstellung übersichtlicher.

Ziel: Automaten zur Beschreibung von Sprachen verwenden.

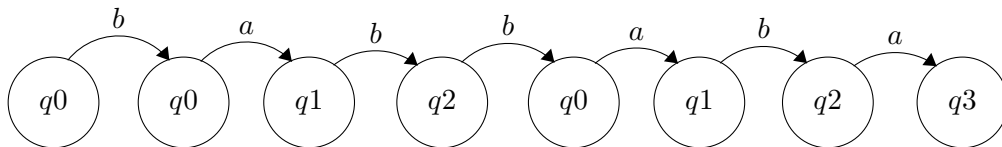
**Definition 12** (Berechnung). Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein DEA,  $w \in \Sigma^*$  ein Wort.

Die Berechnung von  $A$  auf  $w$  ist die Folge von Zuständen, die  $A$  beim Lesen von  $w$  durchläuft, also, gilt für  $w = a_1 a_2 \dots a_k$ :

$$q_0 \xrightarrow{a_1} \delta(q_0, a_1) \xrightarrow{a_2} \delta(\delta(q_0, a_1), a_2) \xrightarrow{\dots} \delta(\dots \delta(\delta(q_0, a_1), a_2) \dots)$$



**Beispiel.** Berechnung von  $A$  auf  $w = babbaba$ :



Sinnvollerweise: Erweiterung von  $\delta$  auf Wörter (erweiterte Übergangsfunktion).

**Definition 13** (Erweiterte Übergangsfunktion).  $\hat{\delta} : Q \times \Sigma^* \mapsto Q$  ist rekursiv definiert wie folgt:

- $\hat{\delta}(q, a) = \delta(q, a)$  für alle  $q \in Q, a \in \Sigma$
- $\hat{\delta}(q, xa) = \delta(\hat{\delta}(q, x), a)$  für alle  $q \in Q, x \in \Sigma^*, a \in \Sigma$ .

**Bemerkung.** Anschaulich:  $\hat{\delta}(q, w)$  bestimmt, in welchem Zustand  $A$  endet, wenn er vom Zustand  $q$  aus das Wort  $w$  liest.

**Beispiel.**  $\hat{\delta}(q_0, babbaba)$

**Definition 14.** Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein DEA. Die von  $A$  akzeptierte Sprache  $L(A) \subseteq \Sigma^*$  ist die Menge aller  $w \in \Sigma^*$ , so dass  $\hat{\delta}(q_0, w) \in F$ .

**Bemerkung.** Anschaulich: Die Menge aller Wörter, die den DEA vom Anfangszustand aus in einen Endzustand führen.

**Beispiel.**  $\hat{\delta}(q_0, babbaba) = q_3 \in F \Rightarrow w \in L(A)$  ( $w$  wird von  $A$  akzeptiert.)

**Definition 15** (Reguläre Sprachen).  $\mathcal{L}(\text{DEA}) = \{L(A) | A \text{ ist ein DEA}\}$  ist die Klasse der Sprachen, die von DEAs akzeptiert werden. Man nennt sie die Klasse der regulären Sprachen und  $L \in \mathcal{L}(\text{DEA})$  wird regulär genannt.

**Beispiel.** DEA  $A$  entwerfen, der die Sprache

$$L = \{w \in \{0, 1\}^* | w \text{ enthält eine gerade Anzahl Nullen und eine gerade Anzahl Einsen}\}$$

akzeptiert.

Idee: 4 Zustände, die speichern, wieviele Nullen und Einseln modulo 2 bereits gelesen wurden.

- $q_{00}$ : gerade Anzahl Nullen, gerade Anzahl Einsen
- $q_{01}$ : gerade Anzahl Nullen, ungerade Anzahl Einsen
- $q_{10}$ : ungerade Anzahl Nullen, gerade Anzahl Einsen
- $q_{11}$ : ungerade Anzahl Nullen, ungerade Anzahl Einsen

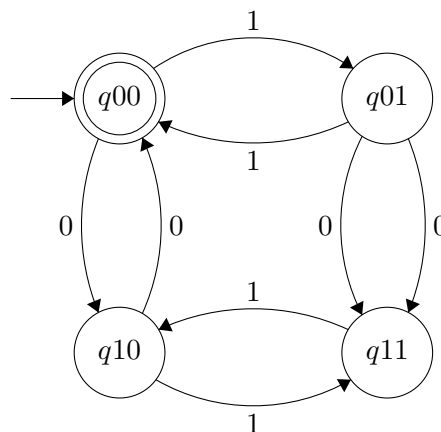
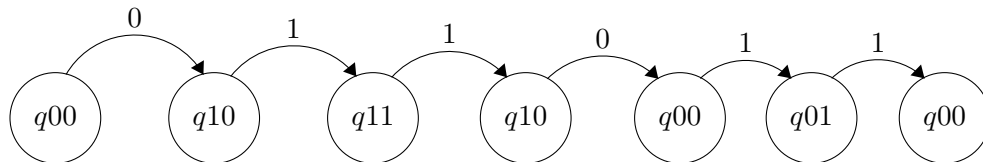


Tabelle:

	0	1
$\mapsto *q_{00}$	$q_{10}$	$q_{01}$
$q_{01}$	$q_{11}$	$q_{00}$
$q_{10}$	$q_{00}$	$q_{11}$
$q_{11}$	$q_{01}$	$q_{10}$

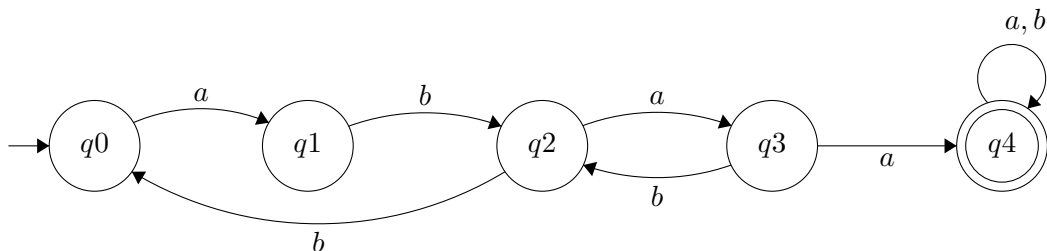
Berechnung von  $A$  auf  $w = 011011$ :



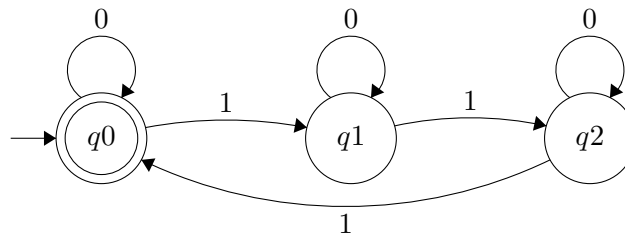
$\Rightarrow w \in L(A), \hat{\delta}(q_{00}, 011011) = q_0$

Lösung der Aufgaben

1a:



1b:

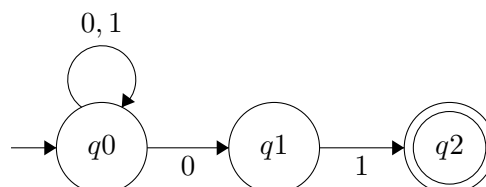


## 7 Nichtdeterministische erstaunliche Endliche Automaten (NEA)

Idee: Ein NEA kann sich nach dem Lesen eines Wortes in mehreren Zuständen befinden.

Vorteil: Sie sind einfacher zu entwerfen.

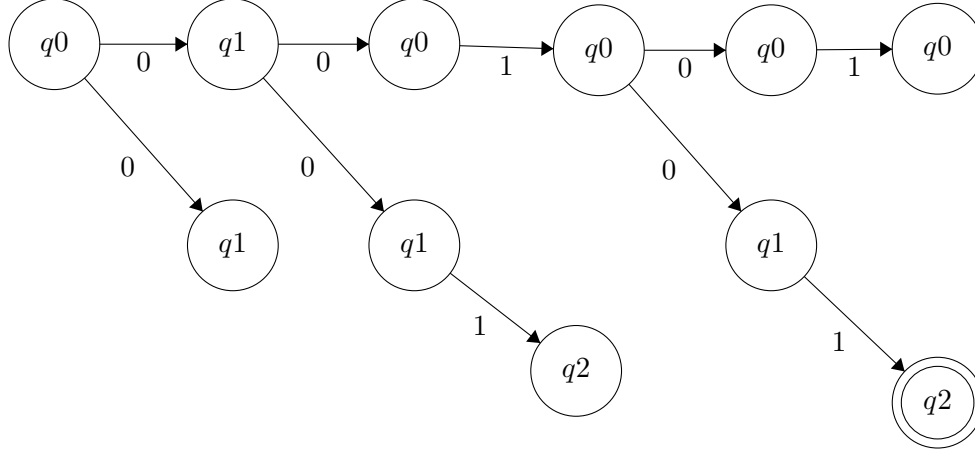
**Beispiel.** Akzeptiere alle Wörter, die mit 01 enden.



Transitionstabelle:

	0	1
$\mapsto q_0$	$\{q_0, q_1\}$	$\{q_0\}$
$q_1$	$\emptyset$	$\{q_2\}$
$*q_2$	$\emptyset$	$\emptyset$

Mögliche Berechnungen auf dem Wort 00101:



**Definition 16** (NEA). Ein NEA  $A$  wird beschrieben durch  $A = (Q, \Sigma, \delta, q_0, F)$ , wobei

$$\delta : Q \times \Sigma \mapsto 2^Q = \mathcal{P}(Q)$$

Die Transitionsfunktion definiert für jeden Zustand und jedes Eingabesymbol eine Menge von Folgezuständen.

**Definition 17** (Erweiterte NEA-Transitionsfunktion). Sei  $w \in \Sigma^*, q \in Q$ . Dann definieren wir

$$\hat{\delta} : Q \times \Sigma^* \mapsto 2^Q$$

rekursiv wie folgt:

- $\hat{\delta}(q, \varepsilon) = \{q\}$
- Sei  $w = xa$  und  $\hat{\delta}(q, x) = \{p_1, \dots, p_k\}$  für  $k \in \mathbb{N}$ , dann ist

$$\hat{\delta}(q, w) = \bigcup_{i=1}^k \delta(p_i, a)$$

**Beispiel.**

$$\begin{aligned}
 \hat{\delta}(q_0, \varepsilon) &= \{q_0\} \text{ (Grundregel)} \\
 \hat{\delta}(q_0, 0) &= \delta(q_0, 0) = \{q_0, q_1\} \\
 \hat{\delta}(q_0, 00) &= \delta(q_0, 0) \cup \delta(q_1, 0) = \{q_0, q_1\} \cup \emptyset = \{q_0, q_1\} \\
 \hat{\delta}(q_0, 001) &= \delta(q_0, 1) \cup \delta(q_1, 1) = \{q_0\} \cup \{q_2\} = \{q_0, q_2\} \\
 \hat{\delta}(q_0, 0010) &= \delta(q_0, 0) \cup \delta(q_0, 1) \cup \delta(q_1, 1) = \{q_1\} \cup \{q_2\} = \{q_0, q_2\} \text{ falsch} \\
 \hat{\delta}(q_0, 00101) &= \delta(q_0, 0) \cup \delta(q_0, 1) \cup \delta(q_1, 1) = \{q_1\} \cup \{q_2\} = \{q_0, q_2\} \text{ falsch}
 \end{aligned}$$

**Definition 18.** Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein NEA. Die von  $A$  akzeptierte Sprache  $L(A)$  ist  $L(A) = \{w \in \Sigma^* \mid \hat{\delta}(q_0, w) \cap F \neq \emptyset\}$ , also die Menge aller Wörter, mit denen vom Startzustand aus ein Endzustand erreichbar ist.

Fragen/Probleme:

1. Wie kann man möglichst effizient entscheiden, ob ein gegebenes Wort in der Sprache eines gegebenen NEA enthalten ist?
2. Sind NEAs mächtiger als DEAs?

Antwort: DEAs und NEAs sind äquivalent.

Ziel: Automatische Umwandlung von NEAs in DEAs.

**Bemerkung** (Teilmengenkonstruktion (Potenzmengenkonstruktion)). Idee: Zustände des DEA sind Mengen erreichbarer Zustände des NEA.

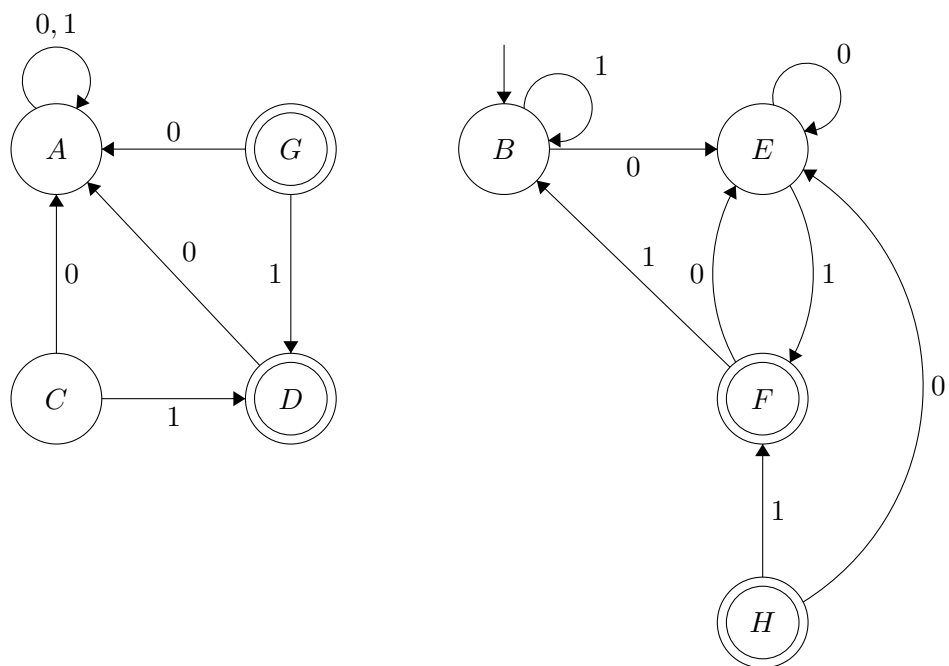
Formal: Sei  $N = (Q_N, \Sigma, \delta_N, q_0, F_N)$  ein NEA. Konstruiere einen äquivalenten DEA  $D = (Q_D, \Sigma, \delta_D, \{q_0\}, F_D)$  mit

- $Q_D = 2^{Q_N}$
- $F = \{S \subseteq Q_D \mid S \cap F \neq \emptyset\}$
- $\delta_D(S, a) = \bigcup_{p \in S} \delta_N(p, a)$  für  $S \in Q_D, a \in \Sigma$

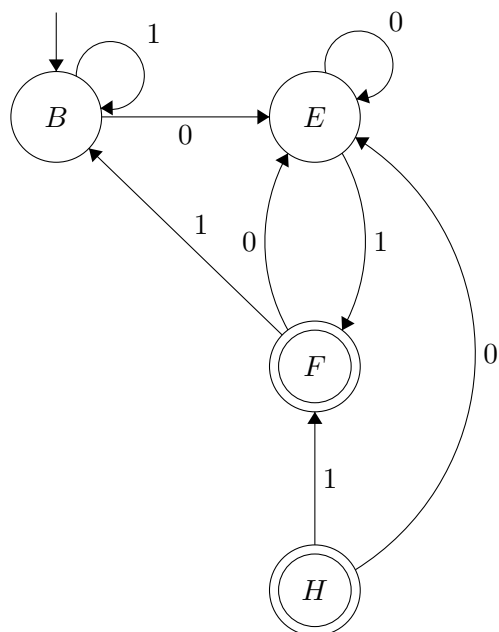
**Beispiel** (von vorher). Konstruktion des äquivalenten DEAs als Übergangstabelle.

	0	1
A $\emptyset$	$\emptyset = A$	$\emptyset = A$
B $\mapsto \{q_0\}$	$\{q_0, q_1\} = E$	$\{q_0\} = B$
C $\{q_1\}$	$\emptyset = A$	$\{q_2\} = D$
D $*\{q_2\}$	$\emptyset$	$\emptyset$
E $\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$
F $*\{q_0, q_2\}$	$\{q_0, q_1\}$	$\{q_0\}$
G $*\{q_1, q_2\}$	$\emptyset$	$\{q_2\}$
H $*\{q_1, q_2, q_3\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$

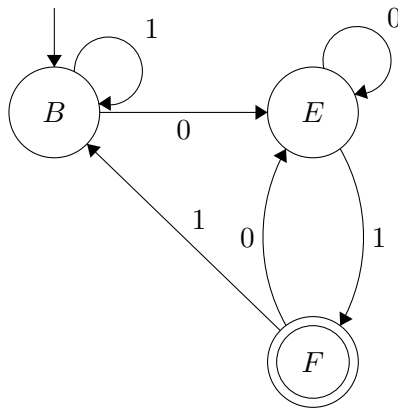




Der linke Teil ist nicht erreichbar:



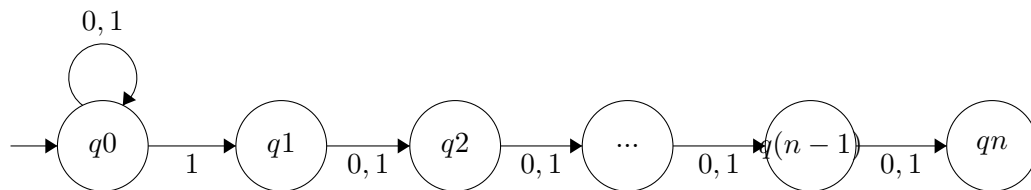
$H$  ist ebenfalls nicht erreichbar:



**Beispiel** (Ein ungünstiger Fall für die Teilmengenkonstruktion).

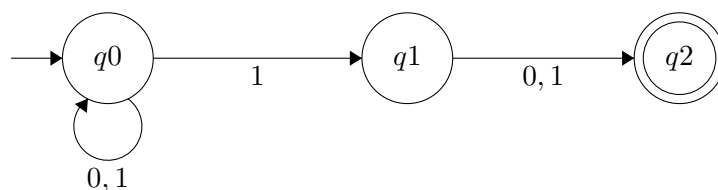
$$\begin{aligned} L_n &= \{w \in \{0,1\}^* \mid \text{Das } n\text{-t-letzte Zeichen von } w \text{ ist eine } 1\} \\ &= \{w \in \{0,1\}^* \mid w = x1y \text{ mit } x \in \{0,1\}^*, y \in \{0,1\}^{n-1}\} \end{aligned}$$

NEA für  $L_n$  mit  $n + 1$  Zuständen:



Aber jeder DEA für  $L_n$  braucht mindestens  $2^n$  Zustände, weil der DEA sich an die letzten  $n$  gelesenen Symbole erinnern muss, da er nicht weiss, wann das Wortende kommt. D.h.  $2^n$  verschiedene Teilworte müssen unterscheiden werden. D.h.  $2^n$  Zustände nötig.

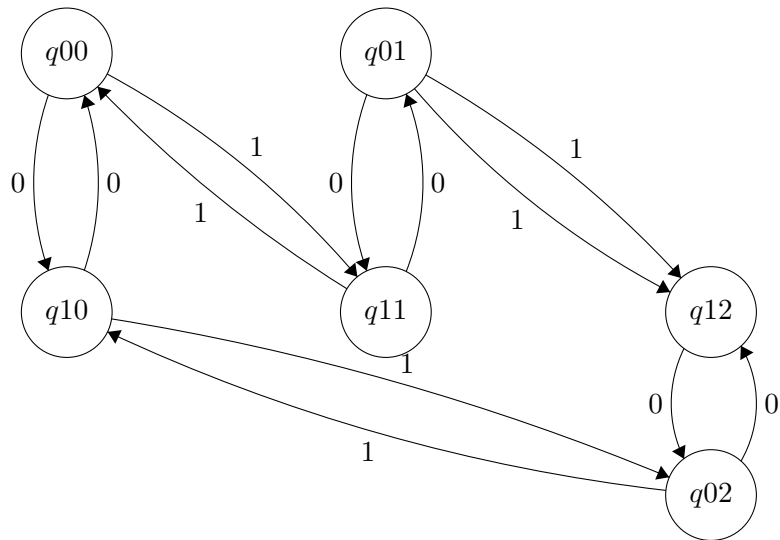
Beispiel mit  $n = 2$ :



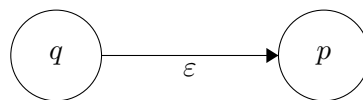
**Beispiel** (Lösung der Knobelaufgabe). Wir machen uns zunutze:

$$2^k \mod 3 = \begin{cases} 1 & \text{falls } k \text{ gerade} \\ 2 & \text{falls } k \text{ ungerade} \end{cases}$$

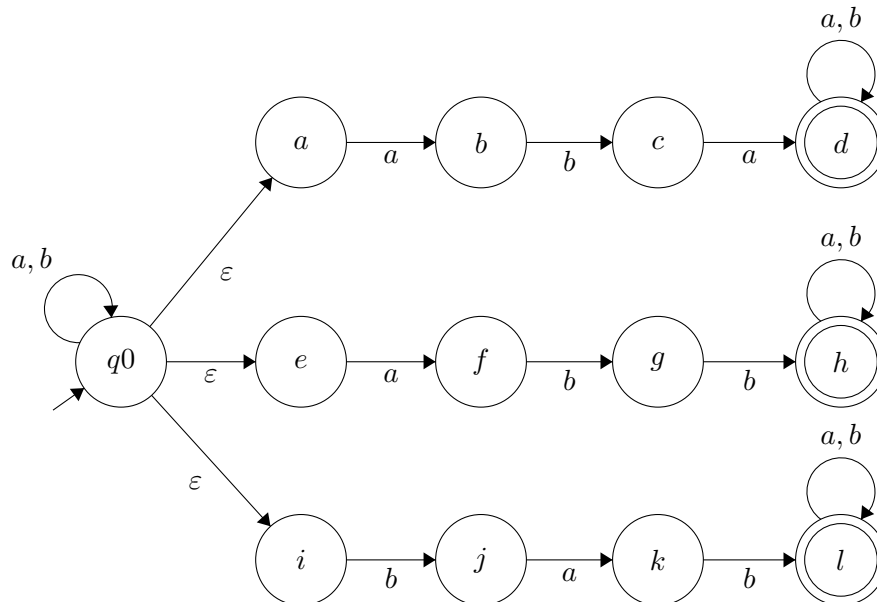
Wir haben Zustände  $q_{ij}$ .  $i$  ist der Exponent der nächsten 2er-Potenz modulo 2,  $j$  ist die Teilsumme.



## 8 NEAs mit $\varepsilon$ -Übergängen



**Beispiel.** Suche nach mehreren Mustern.  $L = \{w \in \{a, b\}^* \mid \text{enthält eines der Teilwörter aba, abb, bab} \}$   
 Der NEA  $N$  mit  $L(N) = L$  mit  $\varepsilon$ -Übergängen sieht aus:

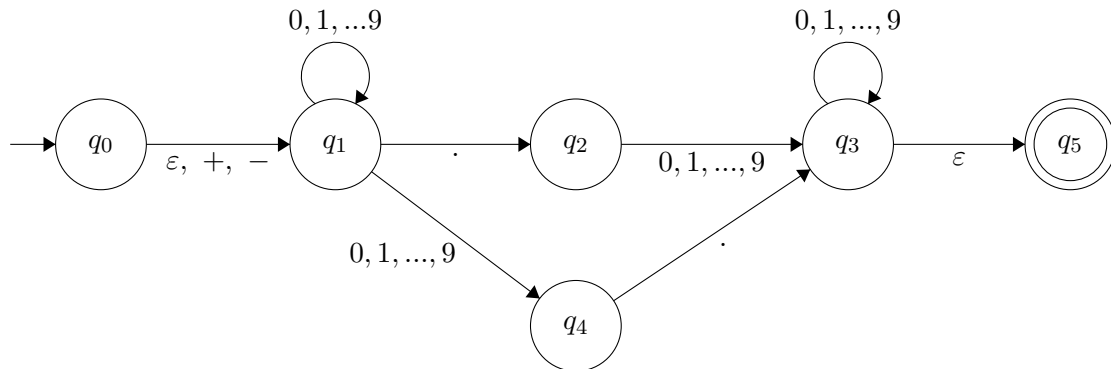


**Beispiel.** Ein  $\varepsilon$ -NEA, der Dezimalzahlen akzeptiert, die sich zusammensetzen aus:

- optionales  $+$  oder  $-$
- Zeichenreihe von Ziffern
- Dezimalpunkt
- Zeichenreihe von Ziffern

Eine der beiden Zeichenreihen von Ziffern darf leer sein.

Der Automat  $E$  sieht dann so aus:



**Definition 19** (NEA mit  $\varepsilon$ -Übergängen). Ein NEA mit  $\varepsilon$ -Übergängen  $A$  wird beschrieben durch  $A = (Q, \Sigma, \delta, q_0, F)$ , wobei  $Q, \Sigma, q_0, F$  wie beim DEA definiert sind, und

$$\delta : Q \times (\Sigma \cup \{\varepsilon\}) \mapsto 2^Q$$

die Transitionsfunktion ist.

**Bemerkung.** Annahme:  $\varepsilon \notin \Sigma$

**Beispiel** (von vorher).

$$E = (\{q_0, q_1, \dots, q_5\}, \{., +, -, 0, 1, \dots, 9\}, \delta, q_0, \{q_5\})$$

Übergangstabelle:

	$\varepsilon$	$+, -$	$.$	$0, 1, \dots, 9$
$q_0$	$\{q_1\}$	$\{q_1\}$	$\emptyset$	$\emptyset$
$q_1$	$\emptyset$	$\emptyset$	$\{q_2\}$	$\{q_1, q_4\}$
$q_2$	$\emptyset$	$\emptyset$	$\emptyset$	$\{q_3\}$
$q_3$	$\emptyset$	$\emptyset$	$\{q_3\}$	$\emptyset$
$q_4$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$q_5$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

## 9 $\varepsilon$ -Hüllen

Ziel: Zeigen, dass es zu jedem  $\varepsilon$ -NEA einen äquivalenten DEA gibt.

Idee: Finde für jeden Zustand die Menge aller Zustände, die von dort aus nur mit  $\varepsilon$ -Übergängen erreichbar sind.

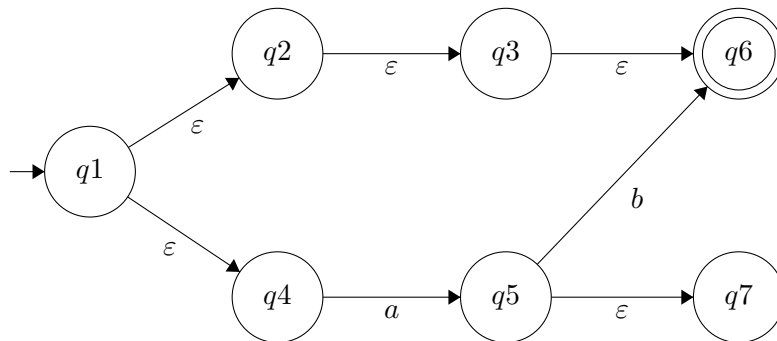
**Definition 20** (Rekursive Definition). Die  $\varepsilon$ -Hülle eines Zustands  $q \in Q$  wird bezeichnet mit  $\varepsilon\text{-Hülle}(q)$  und ist definiert durch:

- $q \in \varepsilon\text{-Hülle}(q)$
- Falls  $p \in \varepsilon\text{-Hülle}(q)$ , dann auch jeder Zustand  $r$ , so dass  $r \in \delta(p, \varepsilon)$

**Beispiel** (Von vorher).

$$\begin{aligned}\varepsilon\text{-Hülle}(q_0) &= \{q_0, q_1\} \\ \varepsilon\text{-Hülle}(q_1) &= \{q_1\} \\ \varepsilon\text{-Hülle}(q_2) &= \{q_2\} \\ \varepsilon\text{-Hülle}(q_3) &= \{q_3, q_5\} \\ \varepsilon\text{-Hülle}(q_4) &= \{q_4\} \\ \varepsilon\text{-Hülle}(q_5) &= \{q_5\}\end{aligned}$$

**Beispiel** (Noch eines). . Noch eines:



Bestimme  $\varepsilon\text{-Hülle}(q_1)$ :

1.  $q_1 \in \varepsilon\text{-Hülle}(q_1)$
2. Finde alle Zustände aus  $\delta(q_1, \varepsilon) = \{q_2, q_4\} \Rightarrow \{q_2, q_4\} \subseteq \varepsilon\text{-Hülle}(q_1)$

**Definition 21** ( $\varepsilon$ -Hülle einer Menge  $S$  von Zuständen).

$$\varepsilon\text{-Hülle}(S) = \bigcup_{q \in S} \varepsilon\text{-Hülle}(q)$$

## 10 Erweiterung der Übergangsfunktion auf Wörter

Finde alle Pfade im Graphen, die mit dem Wort  $w$  beschriftet sind (mit beliebig vielen  $\varepsilon$  dazwischen).

**Definition 22** (Rekursive Definition). Nun denn:

- $\hat{\delta}(q, \varepsilon) = \varepsilon\text{-Hülle}(q)$
- $\hat{\delta}(q, xa)$  wird für  $x \in \Sigma^*$  und  $a \in \Sigma$  definiert durch:
  1. Sei  $\hat{\delta}(a, x) = \{p_1, \dots, p_k\}$
  2. Sei  $\bigcup_{i=1}^k \delta(p_i, a) = \{r_1, \dots, r_m\}$
  3. Dann gilt  $\hat{\delta}(q, xa) = \varepsilon\text{-Hülle}(\{r_1, \dots, r_m\}) = \bigcup_{i=1}^m \varepsilon\text{-Hülle}(r_i)$

**Beispiel** ( $\hat{\delta}(q_0, 5,6)$ ). hmm...

1.  $\hat{\delta}(q_0, \varepsilon) = \varepsilon\text{-Hülle}(q_0) = \{q_0, q_1\}$
2.  $\hat{\delta}(q_0, 5)$ :  $\delta(q_0, 5) \cup \delta(q_1, 5) = \emptyset \cup \{q_1, q_4\}$   
 $\hat{\delta}(q_0, 5) = \varepsilon\text{-Hülle}(q_1) \cup \varepsilon\text{-Hülle}(q_4) = \{q_1, q_4\}$
3.  $\hat{\delta}(q_0, 5.)$ :  $\delta(q_1, .) \cup \delta(q_4, .) = \{q_2\} \cup \{q_3\} = \{q_2, q_3\}$   
 $\hat{\delta}(q_0, 5.) = \varepsilon\text{-Hülle}(q_2) \cup \varepsilon\text{-Hülle}(q_3) = \{q_2, q_3, q_5\}$
4.  $\hat{\delta}(q_0, 5.6)$ :  $\delta(q_2, 6) \cup \delta(q_3, 6) \cup \delta(q_5, 6) = \{q_2\} \cup \{q_3\} = \{q_2, q_3\}$   
 $\hat{\delta}(q_0, 5.) = \varepsilon\text{-Hülle}(q_2) \cup \varepsilon\text{-Hülle}(q_3) = \{q_2, q_3, q_5\} \dots$

**Definition 23.** Für einen  $\varepsilon$ -NEA  $E = (Q, \Sigma, \delta, q_0, F)$  ist  $L(E) = \{w | \hat{\delta}(q_0, w) \cap F \neq \emptyset\}$ .

## 11 Umwandlung von $\varepsilon$ -NEAs in DEAs

Schritt 1:  $\varepsilon$ -Übergänge eliminieren

Sei  $E = (Q_E, \Sigma, \delta_E, q_0, F_E)$  ein  $\varepsilon$ -NEA. Konstruiere einen äquivalenten DEA  $D = (Q_D, \Sigma, \delta_D, q_{0,D}, F_D)$ .

- $Q_0 = 2^{Q_E}$ . Alle erreichbaren Zustände sind  $\varepsilon$ -abgeschlossene Teilmengen, das heisst Mengen  $S \subseteq Q_E$ , so dass  $S = \varepsilon\text{-Hülle}(S)$ . D.h. jeder  $\varepsilon$ -Übergang von einem Zustand  $q \in S$  führt zu einem Zustand, der auch in  $S$  liegt.
- $q_{0,D} = \varepsilon\text{-Hülle}(q_0)$
- $F_D = \{S \in Q_D | S \cap F_E \neq \emptyset\}$
- $\delta_D(S, a)$  wird für alle  $S \in Q_D$  und  $a \in \Sigma$  wie folgt berechnet:

1. Sei  $S = \{p_1, \dots, p_k\}$
2. Berechne  $\bigcup_{i=1}^k \delta(p_i, a) = \{r_1, \dots, r_m\}$
3. Dann ist  $\delta_D(S, a) = \bigcup_{j=1}^n \varepsilon\text{-Hüllen}(r_j)$

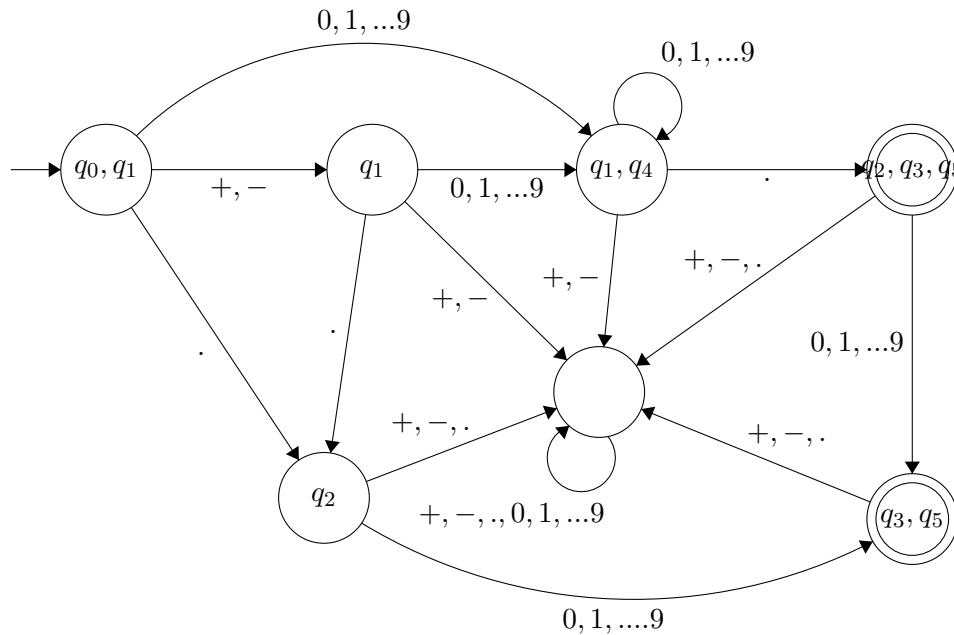
**Beispiel** (Von vorher). Äquivalenter DEA  $D$ : Startzustand ist  $\varepsilon\text{-Hülle}(q_0) = \{q_0, q_1\}$   
 Finde die Folgezustände von  $\{q_0, q_1\}$  für alle Symbole des Alphabets:

$+, -$  Kein Übergang von  $q_1$  aus, aber von  $q_0$  nach  $q_1$ . Daraus folgt  $\varepsilon\text{-Hülle}(q_1) = \{q_1\}$ .

$.$  Kein Übergang von  $q_0$ , aber von  $q_0$  nach  $q_2$ . Daraus folgt  $\varepsilon\text{-Hülle}(q_2) = \{q_2\}$ .

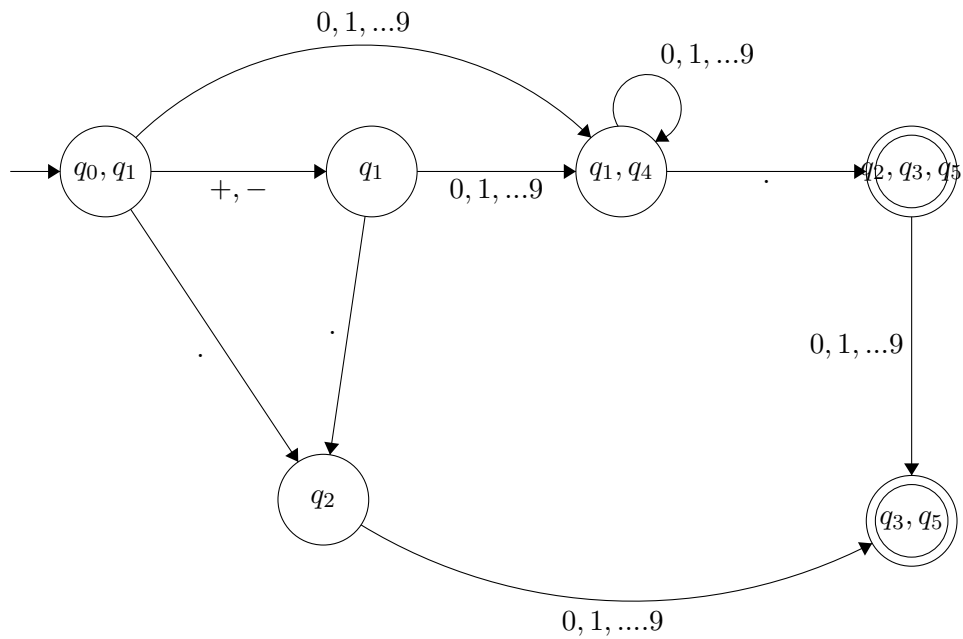
$0, 1, \dots, 9$  Kein Übergang von  $q_0$ , aber von  $q_1$  nach  $q_1$  oder  $q_4$ . Daraus folgt  $\varepsilon\text{-Hülle}(q_1, q_4) = \{q_1, q_4\}$

Transitionstabelle (siehe Excel => transferieren)!

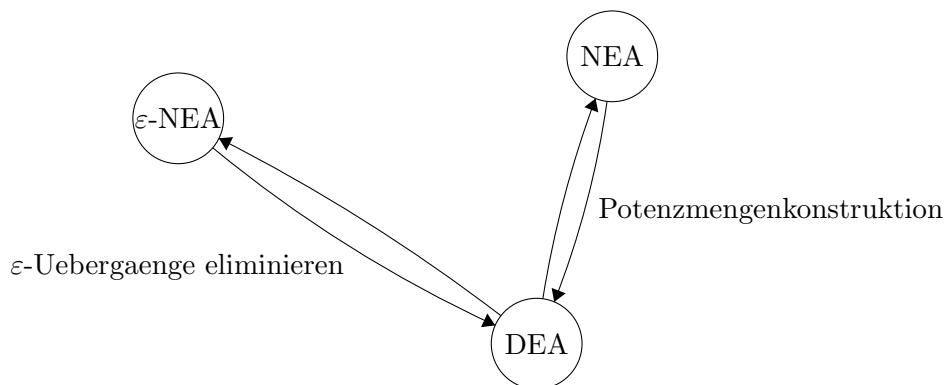


**Bemerkung** (Konvention). Die da wären:

- Der Zustand  $\emptyset$  wird Senkezustand (Abfallzustand) genannt und darf weggelassen werden.
- Darstellung eines DEA mit fehlenden Transitionen sind immer so zu verstehen, dass die fehlenden Transitionen in einen solchen Senkezustand führen:



Zusammenfassung: DEAs und  $\varepsilon$ -NEAs sind äquivalent.



## 12 Reguläre Ausdrücke

Besonders geeignet für die Mustersuche, anderer Formalismus zur Beschreibung von regulären Sprachen.

## 13 Operatoren für reguläre Ausdrücken

- Die Vereinigung von Sprachen  $L$  und  $M$ ,  $L \cup M$ , ist die Menge aller Zeichenreihen, die entweder in  $L$  oder in  $M$  oder in beiden enthalten sind.



- Die Verkettung (Konkatenation) von  $L$  und  $M$ ,  $L \cdot M$  oder  $LM$ , ist die Menge aller Zeichenreihe, gebildet aus einer Verkettung einer Zeichenreihe aus  $L$  umit einer beliebigen aus  $M$ .

Formal:

$$LM = \{w \in \Sigma^* | w = uv \text{ mit } u \in L \text{ und } v \in M\}$$

- Die Kleensche Hülle (Stern) von  $L$ ,  $L^*$ , ist die Menge aller Zeichenreihen, die durch die Verkettung einer beliebigen Anzahl von Zeichenreihen aus  $L$  gebildet wird.

Formal:

$$\begin{aligned} L^0 &= \{\varepsilon\} \\ L^1 &= L \\ L^n &= L \cdot L^{n-1} \\ L^* &= \bigcup_{i=0}^{\infty} L^i \end{aligned}$$

Anschaulich:  $w \in L^*$ , wenn sich  $w$  zerlegen lässt in endlich viele Wörter  $w = w_1 w_2 \dots w_k$  für ein  $k \in \mathbb{N}$ , so dass  $w_1 \in L, w_2 \in L \dots w_i \in L_i$  gilt.

Spezialfälle:

- $\emptyset^* = \{\varepsilon\}$ , da  $\emptyset^0 = \{\varepsilon\}$
- $\{\varepsilon\}^* = \{\varepsilon\}$

Aber:  $\emptyset^i = \emptyset$  für  $i > 1$ .

**Definition 24** (Reguläre Ausdrücke). Reguläre Ausdrücke lassen sich wie folgt definieren:

1.  $\varepsilon$  und  $\emptyset$  sind reguläre Ausdrücke.
2. Jedes Symbol  $a \in \Sigma$  ist ein regulärer Ausdruck.
3. Wenn  $\alpha$  und  $\beta$  reguläre Ausdrücke sind, dann sind:
  - $(\alpha \cdot \beta)$  (Konkatenation)
  - $(\alpha + \beta)$  (Vereinigung)

reguläre Ausdrücke.

4. Wenn  $\alpha$  ein regulärer Ausdruck ist, dann ist auch  $(\alpha)^*$  ein regulärer Ausdruck. (Kleenscher Stern)

**Bemerkung** (Konvention). Man tut:

- Überflüssige Klammern weglassen
- Stern bindet stärker als Verkettung
- Verkettung bindet stärker als Vereinigung

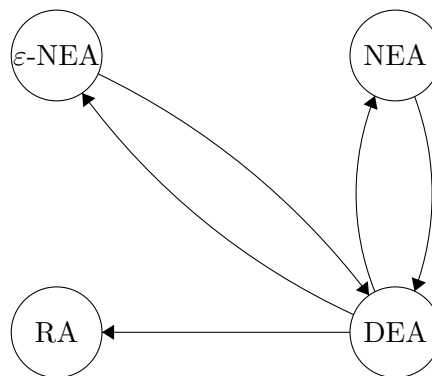
## 14 Bedeutung regulärer Ausdrücke

$L(\alpha)$  bezeichnet die durch den regulären Ausdruck beschriebene Sprache. Dabei gilt:

- $L(\varepsilon) = \{\varepsilon\}$
- $L(\emptyset) = \emptyset$
- $L(a) = \{a\}$
- $L(\alpha \cdot \beta) = L(\alpha) \cdot L(\beta)$
- $L(\alpha + \beta) = L(\alpha) \cup L(\beta)$
- $L(\alpha^*) = (L(\alpha))^*$

**Beispiel** (Beschreibung von Sprachen durch reguläre Ausdrücke). Nun:

1.  $L_1 = \{w \in \{0,1\}^* \mid w \text{ beginnt mit } 011 \text{ und enthält das Teilwort } 00\}$ . RA für  $L_1$ :  
 $011 \cdot (0+1)^* \cdot 00 \cdot (0+1)^*$
2.  $L_2 = \{w \in \{a,b,c\}^* \mid |w|_a \text{ ist gerade}\}$ .  
 RA für  $L_2$ :  $((b+c)^* a (b+c)^* a (b+c)^*)^*$
3.  $L_3 = \{w \in \{0,1\}^* \mid \text{In } w \text{ kommen die Nullen und Einsen immer abwechselnd vor}\}$   
 RA für  $L_3$ :  $(01)^* + (10)^* + 1(01)^* + 0(10)^* = (\varepsilon + 1)(01)^*(\varepsilon + 0)$



Lösung der Aufgabe 6 (Aufgabenblatt 2):

- a)  $(a+b)^* : \{a,b\}^*$ .  
 $(a^*b^*) : \varepsilon \in \mathcal{L}(a^*) \text{ und } \varepsilon \in \mathcal{L}(b^*) \Rightarrow a \in \mathcal{L}(a^*b^*) \text{ und } b \in \mathcal{L}(a^*b^*)$

## 15 Anwendungsbeispiel für RA

Spezifikation einer Eingabemaske für Kontostände. Bedingungen:

- Währungseingabe: CHF, EUR, USD
- optionales Vorzeichen vor dem Betrag:  $\oplus, \ominus$
- Betrag ganzzahlig oder mit Dezimalpunkt und zwei Nachkommastellen
- keine führende Nullen

$$\Sigma = \{C, D, E, F, H, R, S, U, \oplus, \ominus, ., 0, 1, \dots, 9\}$$

Idee: Setze den RA aus Teilen zusammen:

zahlung = waehrung vorzeichen betrag

waehrung =  $(CHF + EUR + USD)$

vorzeichen =  $(\varepsilon + \oplus + \ominus)$

betrag = ganzzahl  $(\varepsilon + .\text{nachkomma})$

ganzzahl =  $(0 + (1 + 2 + \dots + 9)(0 + 1 + \dots + 9)^*$

nachkomma =  $(0, 1, \dots, 9) + (0, 1, \dots, 9)$

$\Rightarrow \text{zahlung} = (CHF + EUR + USD) (\varepsilon + \oplus + \ominus) (0 + (1 + 2 + \dots + 9)(0 + 1 + \dots + 9)^* (\varepsilon + .(0, 1, \dots, 9) + (0, 1, \dots, 9))$

## 16 Eine ganz neue Idee

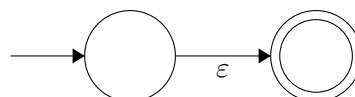
**Theorem 1.** Reguläre Ausdrücke und endliche Automaten sind äquivalent:

1. für jeden RA  $\alpha$  existiert ein DEA  $A_\alpha$  mit  $\mathcal{L}(\alpha) = \mathcal{L}(A_\alpha)$
2. für jeden DEA  $A$  existiert ein RA  $\alpha_A$  mit  $\mathcal{L}(A) = \mathcal{L}(\alpha_A)$

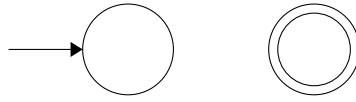
*Beweis für 1.* Nun. Umwandlung von RA in DEA. Vorgehensweise:  $\text{RA} \mapsto \varepsilon\text{-NEA} \mapsto \text{DEA}$ . Für einen gegebenen RA konstruiere einen  $\varepsilon$ -NEA induktiv entsprechend des regulären Ausdrucks des RA mit folgenden zusätzlichen Eigenschaften:

1. genau ein akzeptierender Zustand
2. keine Transitionen zum Startzustand
3. keine Transitionen vom akzeptierenden Zustand wegführende Transitionen

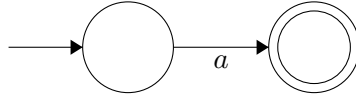
Induktionsanfang:  $\varepsilon$ -NEA für  $\varepsilon$ :



$\varepsilon$ -NEA für  $\emptyset$ :



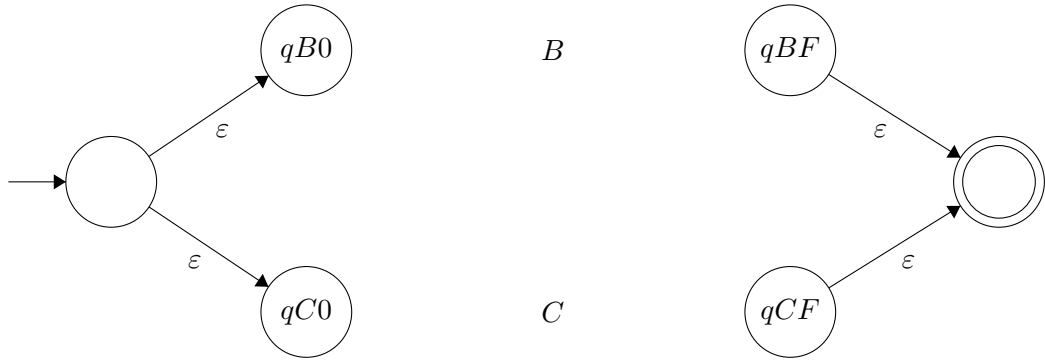
$\varepsilon$ -NEA für  $a \in \Sigma$ :



Induktionsschritt:

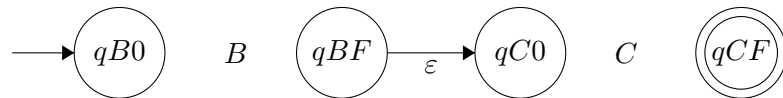
- Sei  $\alpha = \beta + \gamma$  ein RA, seien  $B$  und  $C$   $\varepsilon$ -NEAs für  $\beta$  und  $\gamma$  wie oben und mit Startzuständen  $q_{B0}$  und  $q_{C0}$  und akzeptierenden Zuständen  $q_{BF}$  und  $q_{CF}$ .

Konstruiere hieraus einen  $\varepsilon$ -NEA für  $\alpha$  wie folgt:



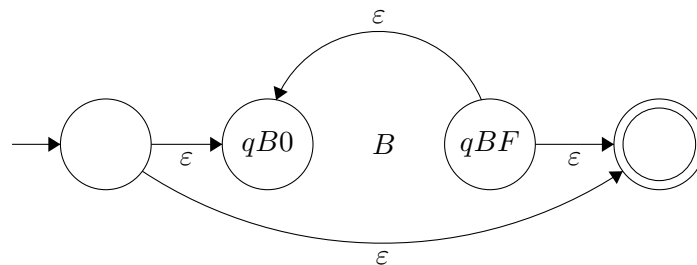
erfüllt alle Bedingungen.

- Seien  $\alpha = \beta \cdot \gamma$  und  $B, C$   $\varepsilon$ -NEAs für  $\beta, \gamma$ .  $\varepsilon$ -NEA für  $\alpha$ :



erfüllt alle Bedingungen.

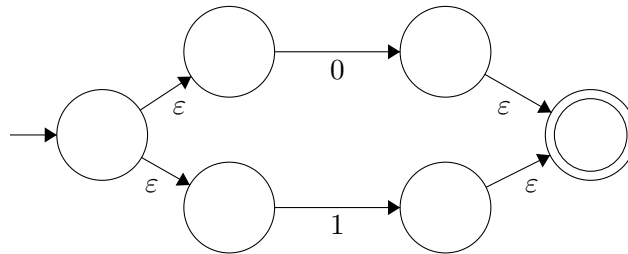
- Sei  $\alpha = \beta^*$ ,  $B$  ein  $\varepsilon$ -NEA für  $\beta$ .  $\varepsilon$ -NEA für  $\alpha$ :



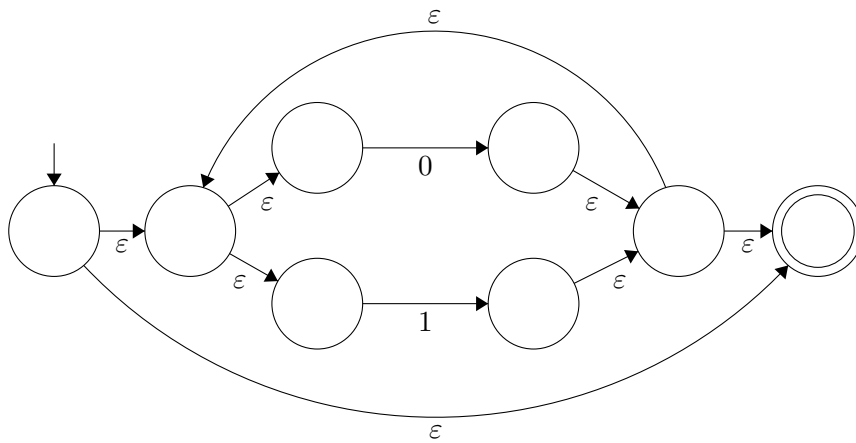
erfüllt alle Bedingungen.

□

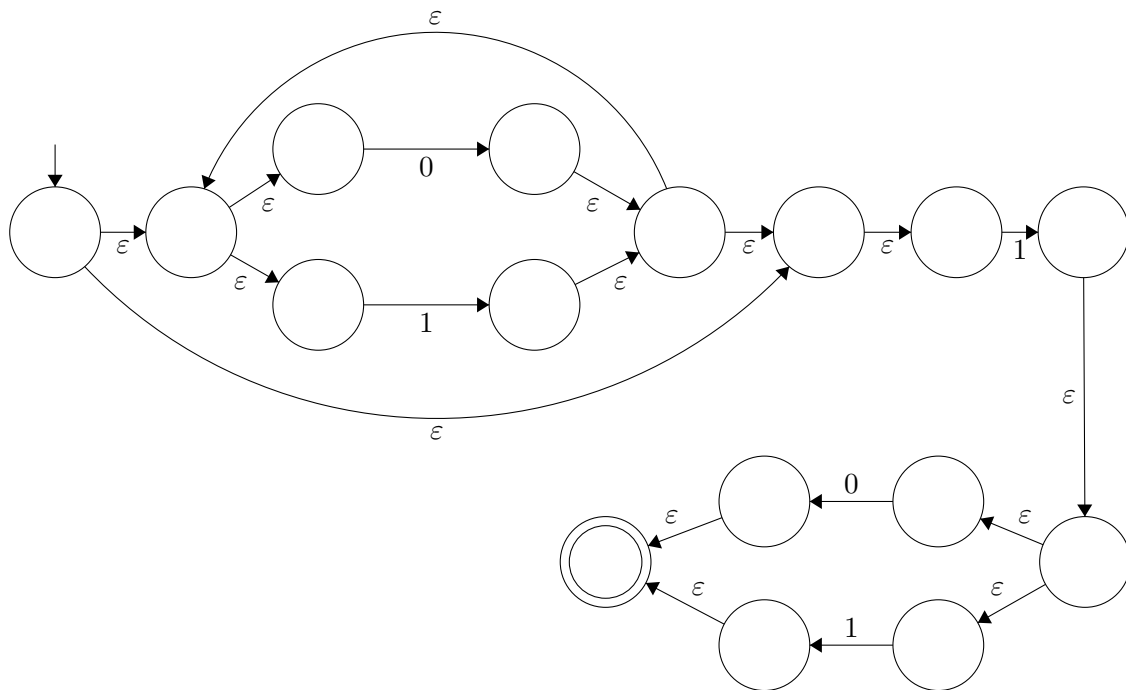
**Beispiel.** Beispiel:  $\varepsilon$ -NEAA für  $\alpha = (0 + 1)^*1(0 + 1)$ :  
 $\varepsilon$ -NEA für  $(0 + 1)$ :



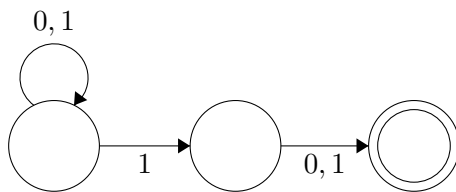
$\varepsilon$ -NEA für  $(0 + 1)^*$ :



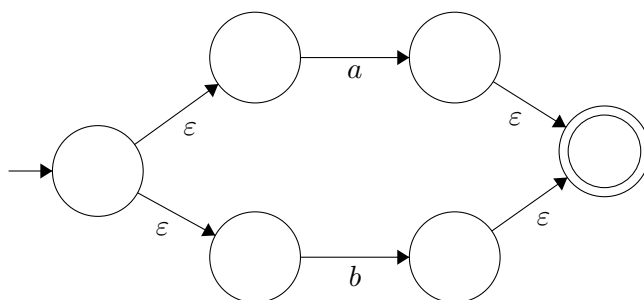
$\varepsilon$ -NEA für  $(0 + 1)^*1(0 + 1)$ :



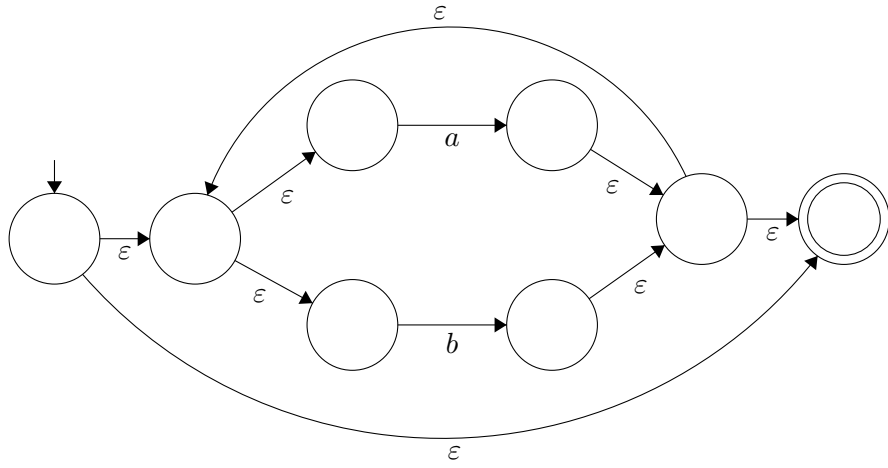
Vereinfachung:



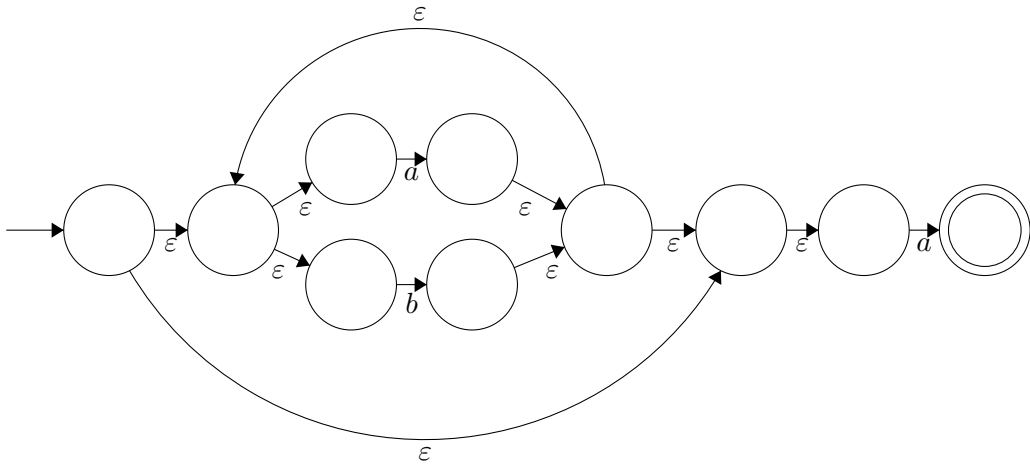
Übung (Aufgabe 1). a)  $a + b$ :



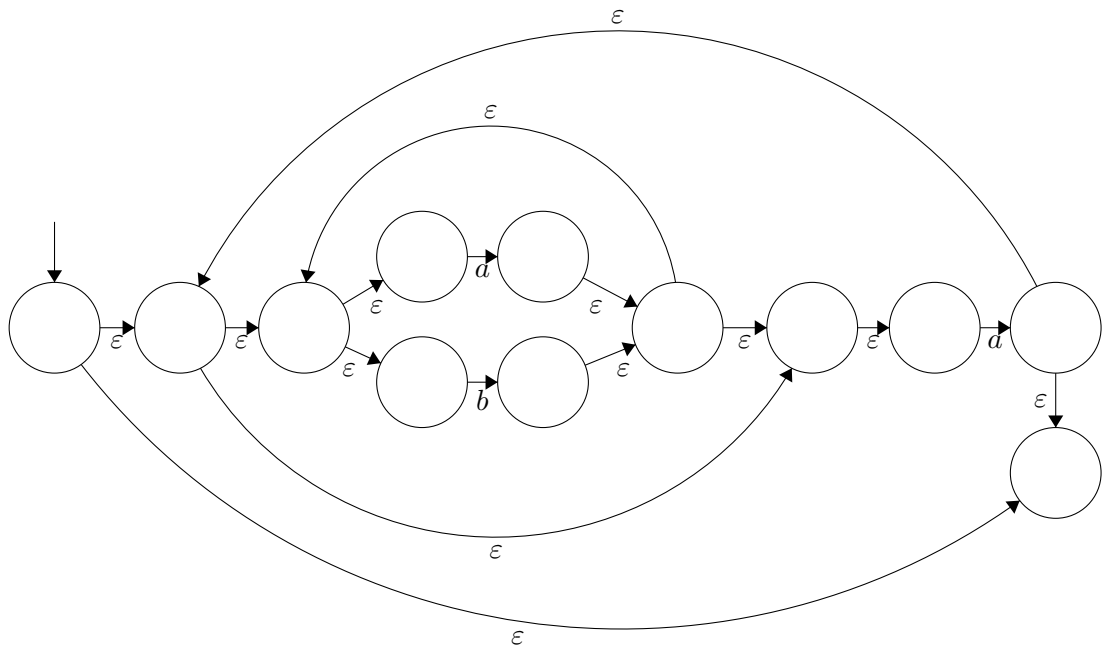
$(a + b)^*$ :



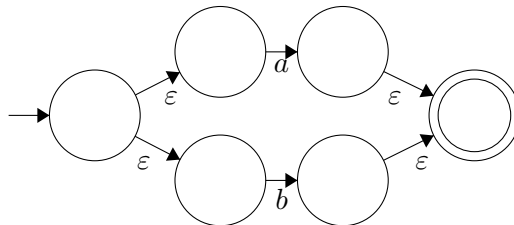
$(a+b)^*a$



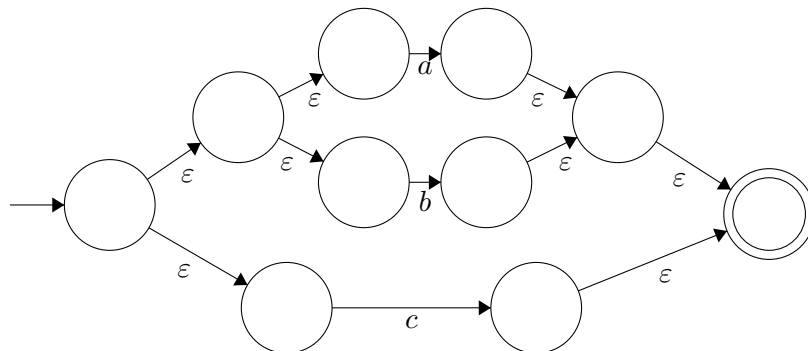
$((a+b)^*a)^*$



b)  $a + b$

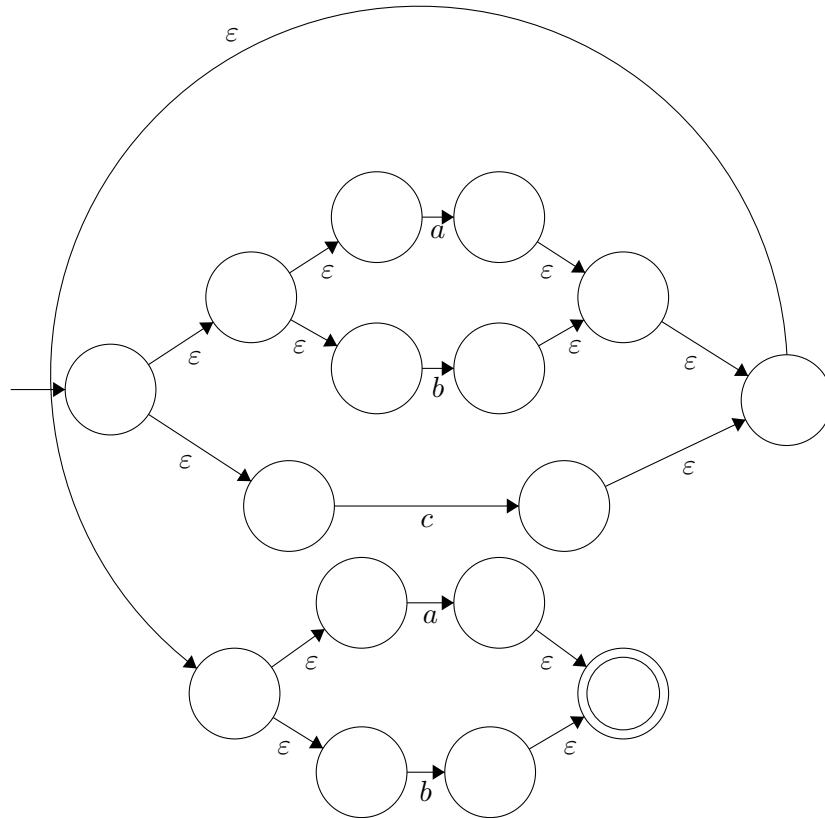


$a + b + c$

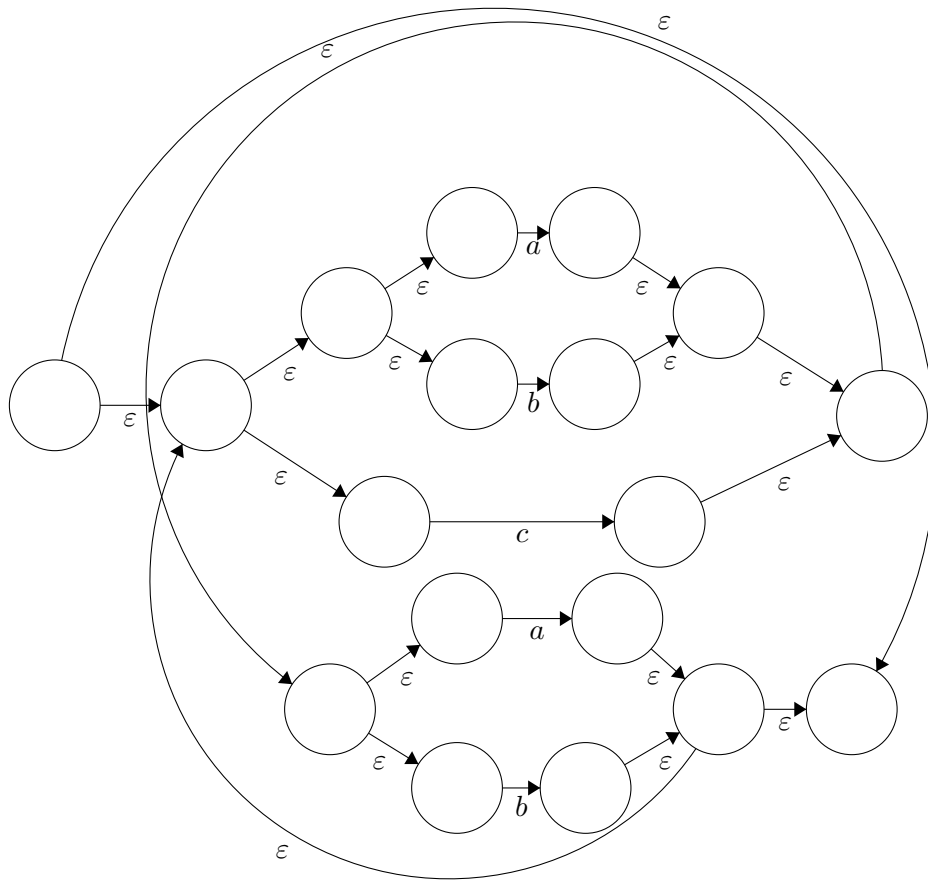




$$(a + b + c) \cdot (a + b)$$



Letzter Schritt:



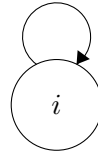
*Beweis für 2.* Idee: Dynamische Programmierung. Die Teilprobleme hier sind: Für jedes Paar  $(p, q)$  von Zuständen finde einen regulären Ausdruck, der alle Wörter beschreibt, die von  $p$  nach  $q$  führen.

Genauer: Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein DEA, seien die Zustände durchnummeriert, d.h.  $Q = \{1, 2, \dots, n\}$ ,  $q_0 = 1$ .

1. Berechne für alle  $i, j \in \{1, 2, \dots, n\}$  reguläre Ausdrücke  $\alpha_{i,j}^{(0)}$ , die die direkten Verbindungen von Zustand  $i$  zu Zustand  $j$  beschreiben:

a)  $i = j$ :

$a_1, a_2, \dots$



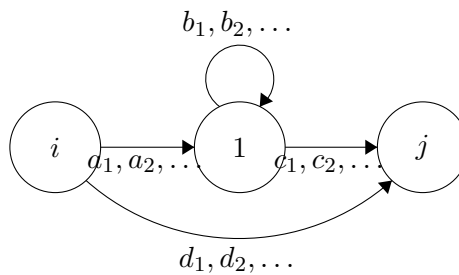
$$\alpha_{i,i}^{(0)} = \varepsilon + a_1 + a_2 + \dots \text{ oder } \alpha_{i,i}^{(0)} = \varepsilon$$

b)  $i \neq j$

$$\alpha_{i,i}^{(0)} = a_1 + a_2 + \dots \text{ oder } \alpha_{i,j}^{(0)} = \emptyset$$

2. Nun werden nacheinander alle anderen Zustände als mögliche Zwischenstation auf dem Weg von  $i$  nach  $j$  hinzugenommen – zunächst den Zustand 1:

$\alpha_{i,j}^{(1)}$  beschreibt die Wörter, mit denen man von  $i$  nach  $j$  kommt und zwischendurch nur den Zustand 1 besucht.



$$\alpha_{i,j}^{(1)} = \alpha_{i,j}^{(0)} + \alpha_{i,1}^{(0)} (\alpha_{1,1}^{(0)})^* \alpha_{1,j}^{(0)}$$

Induktion: Wir nehmen an, dass wir  $\alpha_{i,j}^{(k-1)}$  für alle  $i, j$  schon berechnet haben. Dann

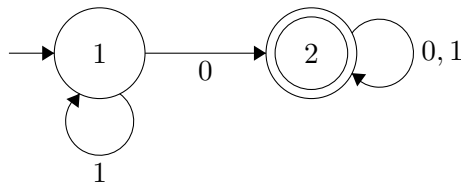
gilt:  $\alpha_{i,1}^{(k)} = \alpha_{i,j}^{(k-1)} + \alpha_{i,k}^{(k-1)} (\alpha_{k,k}^{(k-1)})^* \alpha_{k,j}^{(k-1)}$

Daraus folgt der Reguläre Ausdruck für den DEA  $A$  mit  $q_0 = 1$  und  $F = \{f_1, f_2, \dots, f_m\}$ :

$$\alpha_{1,f_1}^{(n)} + \alpha_{1,f_2}^{(n)} + \dots + \alpha_{1,f_m}^{(n)}$$

□

**Beispiel.** DEA  $A$ :



1.  $\alpha_{1,1}^{(0)} = 1 + \varepsilon$   
 $\alpha_{1,2}^{(0)} = 1$   
 $\alpha_{2,1}^{(0)} = \emptyset$   
 $\alpha_{2,2}^{(0)} = \varepsilon + 0 + 1$
2.  $\alpha_{1,1}^{(1)} = \alpha_{1,1}^{(0)} + \alpha_{1,1}^{(0)}(\alpha_{1,1}^{(0)})^* \alpha_{1,1}^{(0)} = 1 + \varepsilon + (1 + \varepsilon)(\alpha_{1,1}^{(0)})^* \alpha_{1,1}^{(0)} = (1 + \varepsilon)^* = 1^*$   
 $\alpha_{1,2}^{(1)} = \alpha_{1,2}^{(0)} + \alpha_{1,1}^{(0)}(\alpha_{1,1}^{(0)})^* \alpha_{1,2}^{(0)} = 0 + (1 + \varepsilon)(1 + \varepsilon)^* 0 = 1^* 0$   
 $\alpha_{2,1}^{(1)} = \alpha_{2,1}^{(0)} + \alpha_{2,1}^{(0)}(\alpha_{1,1}^{(0)})^* \alpha_{1,1}^{(0)} = \emptyset + \emptyset(1 + \varepsilon)^*(1 + \varepsilon) = \emptyset$   
 $\alpha_{2,2}^{(1)} = \alpha_{2,2}^{(0)} + \alpha_{2,1}^{(0)}(\alpha_{1,1}^{(0)})^* \alpha_{1,2}^{(0)} = (\varepsilon + 0 + 1) + \emptyset \cdots = \varepsilon + 0 + 1$
3.  $\alpha_{1,1}^{(1)} + \alpha_{1,2}^{(1)}(\alpha_{2,2}^{(1)})^* \alpha_{2,1}^{(1)} = 1^* + 1^* 0(\varepsilon + 0 + 1) \emptyset = 1^*$   
 $\alpha_{1,2}^{(2)} = \alpha_{1,2}^{(1)} + \alpha_{1,1}^{(1)}(\alpha_{2,2}^{(1)})^* \alpha_{2,2}^{(1)} = 1^* 0 + 1^* 0(\varepsilon + 0 + 1)^*(\varepsilon + 0 + 1) = 1^* 0(0 + 1)^* = \mathcal{L}(A)$

## 17 Reguläre Sprachen und ihre Eigenschaften

**Definition 25** (Reguläre Sprache). Eine Sprache heisst regulär, wenn sie von einem DEA akzeptiert wird.

$$\mathcal{L}_{\text{reg}} = \mathcal{L}(\text{DEA}) = \{L \mid L \text{ regulär}\}$$

Ziel: Charakterisierung von regulären Sprachen.

### 17.1 Abschlusseigenschaften regulärer Sprachen

**Vereinigung** Wenn  $L$  und  $M$  reguläre Sprachen sind, dann ist auch  $L$  vereinigt mit  $M$  regulär.

*Beweis.* Wenn  $L$  und  $M$  regulär sind, dann existieren reguläre Ausdrücke  $\alpha$  und  $\beta$  für  $L$  und  $M$ , d.h.  $L(\alpha) = L$  und  $L(\beta) = M$ .

Daraus folgt, dass  $\alpha + \beta$  ebenfalls ein RA ist, daraus folgt  $L(\alpha + \beta) = L \cup M$  (gemäss Definition der Vereinigung von RA).  $\square$

**Verkettung** Wenn  $L$  und  $M$  reguläre Sprachen sind, dann ist auch  $L$  verkettet mit  $M$  regulär.

*Beweis.* Analog der Vereinigung.  $\square$

**Kleene'scher Stern** Wenn  $L$  eine reguläre Sprache ist, dann ist auch  $L^*$  eine reguläre Sprache.

*Beweis.* Analog der Vereinigung. □

**Komplement** Wenn  $L$  eine reguläre Sprache ist, dann ist auch  $\bar{L} = \Sigma^* - L$  regulär.

*Beweis.* Sei  $A$  ein DEA für  $L$ . Dann gibt es für jedes Wort  $w$  aus  $\Sigma^*$  einen eindeutigen Zustand, in dem der DEA endet, wenn er  $w$  liest. Alle Wörter aus  $L(A) = L$  führen in Endzustände, alle Wörter aus  $\Sigma^* - L = \bar{L}$  in nichtakzeptierende Zustände. Vertauschen von End- und Nicht-Endzuständen ergibt einen DEA für  $\bar{L}$ . □

**Durchschnitt** Wenn  $L$  und  $M$  reguläre Sprachen sind, dann ist auch  $L \cap M$  regulär.

*Beweis 1 mit De Morgan'schen Gesetzen.* Es gelten ja:

$$\overline{A \cap B} = \bar{A} \cup \bar{B} \quad (1)$$

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \quad (2)$$

Da  $L, M$  regulär sind, sind auch  $\bar{L}, \bar{M}$  regulär.  $\bar{L} \cup \bar{M}$  ist ebenfalls regulär.  $\overline{\bar{L} \cup \bar{M}}$  ist ebenfalls regulär. Durch De Morgan No. 1 ist  $\bar{L} \cap \bar{M} = L \cap M$  schnurstracks auch regulär. □

*Beweis 2 durch Konstruktion des Produktautomaten.*

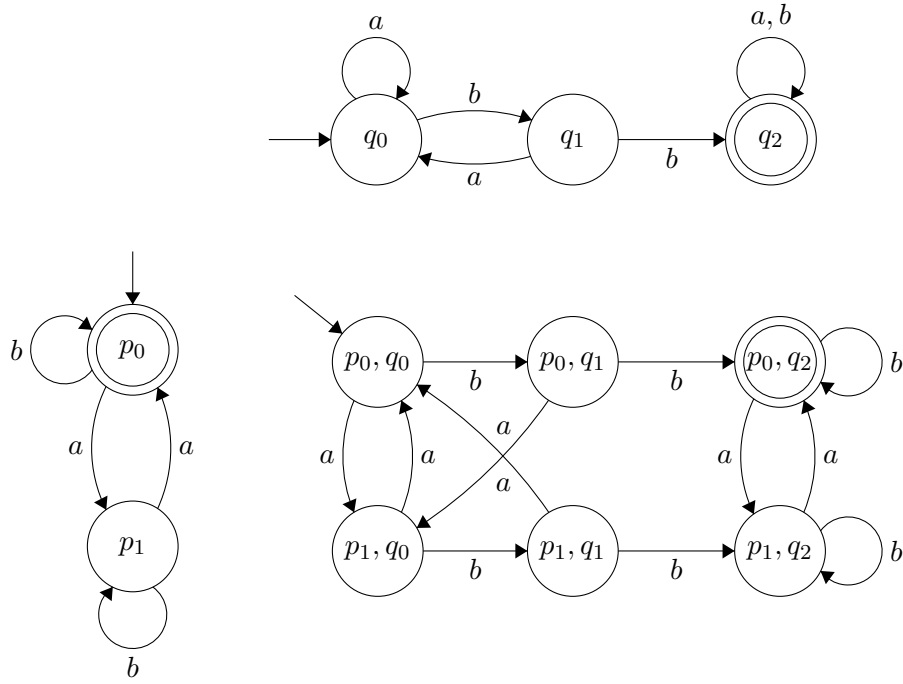
**Definition 26** (Produktautomat). Sei  $A = (Q_A, \Sigma, \delta_A, q_{0A}, F_A)$  ein DEA für  $L$ ,  $B = (Q_B, \Sigma, \delta_B, q_{0B}, F_B)$ . Dann ist der Produktautomat für  $A$  und  $B$  der DEA  $C = (Q_C, \Sigma, \delta_C, q_{0C}, F_C)$  mit

- $Q_C = Q_A \times Q_B$
- $\delta_C(p, q) = (\delta_A(p), \delta_B(q))$  für alle  $(p, q) \in Q_C$
- $q_{0C} = (q_{0A}, q_{0B})$
- $F_C = \{(p, q) \in Q_C \mid p \in F_A \text{ und } q \in F_B\}$

Anschaulich kann man sagen, dass  $C$  einfach die Arbeit von  $A$  und  $B$  simuliert und genau dann akzeptiert, wenn auch  $A$  und  $B$  akzeptieren.

Es gilt darum:  $L(C) = L(A) \cap L(B) = L \cap M$  □

**Beispiel.** Sei  $L = \{w \in \{a, b\}^* \mid |w|_a \text{ ist gerade}\}$ . Sei  $M = \{w \in \{a, b\}^* \mid w \text{ enthält das Teilwort } ab.\}$ .



**Bemerkung.** Mit  $F_C = \{(p, q) \in Q_C \mid p \in F_A \text{ oder } q \in F_B\}$  funktioniert auch für die Vereinigung.

**Mengendifferenz** Wenn  $L$  und  $M$  regulär sind, ist auch  $L - M$  regulär.

*Beweis.* Es gilt  $L - M = L \cap \overline{M}$ . Das Komplement ist regulär, der Schnitt ist regulär, ergo ist  $L \cap \overline{M}$  regulär.  $\square$

## Spiegelung

**Definition 27.** Sei  $w = a_1 \dots a_k$  ein Wort. Dann ist  $w^R = a_k \dots a_1$  die Spiegelung von  $w$ .

Sei  $L \subseteq \Sigma^*$  eine Sprache. Dann ist  $L^R = \{w \in \Sigma^* \mid w^R \in L\}$  die Spiegelung von  $L$ .

**Bemerkung.** Einige coole Sachen:

- $\varepsilon^R = \varepsilon$
- $(w^R)^R = w$
- Wenn  $L$  regulär ist, dann ist auch  $L^R$  regulär.

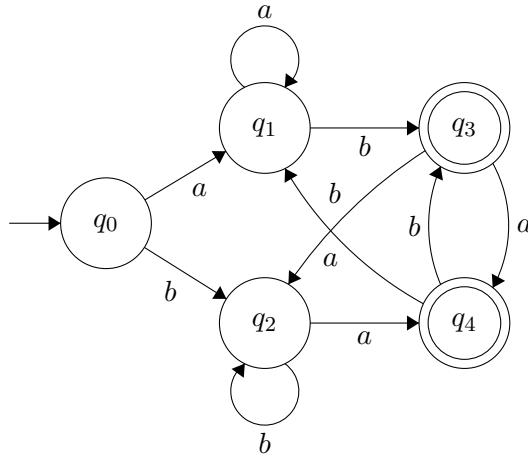
*Beweis.* Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein DEA für  $L$ . Wir konstruieren einen  $\varepsilon$ -NEAB für  $L^R$  wie folgt:

$B = (Q \cup \{q_S\}, \Sigma, \delta_B, q_S, F_B)$  mit

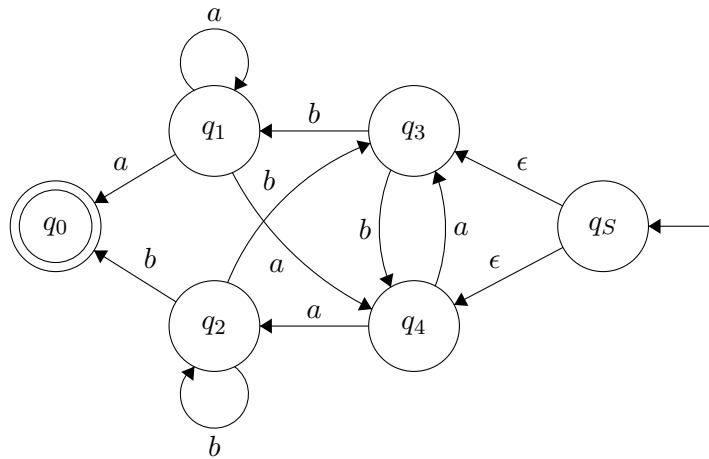
1.  $F_B = \{q_0\}$
2.  $\delta_B(q, a) = \{p\}$  für  $\delta(p, a) = q$
3.  $\delta_B(q_S, \varepsilon) = \{p\}$  für alle  $p \in F$

$B$  simuliert  $A$  in umgekehrter Richtung  $\Rightarrow B$  akzeptiert  $L^R$ . □

**Beispiel.**  $L = \{w \in \{a, b\}^* \mid w \text{ endet auf } ba \text{ oder } ab\}$ .



$L^R = \{w \in \{a, b\}^* \mid w \text{ beginnt mit } ba \text{ oder } ab\}$ .



*Beweis über Reguläre Ausdrücke.* Sei  $\alpha$  ein regulärer Ausdruck mit  $L(\alpha) = L$ .

Zu zeigen: Es gibt einen RA  $\beta$  mit  $L(\beta) = (L(\alpha))^R = L^R$ .

Strukturelle Induktion über den Aufbau von  $\alpha$ . Induktionsanfang:

- $\varepsilon^R = \varepsilon$

- $\emptyset^R = \emptyset$
- $a^R = a$  für ein  $a \in \Sigma$

Induktionsschritt:

- Vereinigung  $\alpha = \alpha_1 + \alpha_2$ :

$$L(\alpha_1 + \alpha_2)^R = (L(\alpha_1) \cup L(\alpha_2))^R = L(\alpha_1)^R \cup L(\alpha_2)^R \Rightarrow \alpha^R = \alpha_1^R + \alpha_2^R$$

- Konkatenation  $\alpha = \alpha_1 \alpha_2$ :

$$L(\alpha_1 \alpha_2)^R = (L(\alpha_1) L(\alpha_2))^R = L(\alpha_1)^R L(\alpha_2)^R \Rightarrow \alpha^R \stackrel{(w_1 w_2)^R = w_2^R w_1^R}{=} \alpha_1^R \alpha_2^R$$

- Kleene'scher Stern  $\alpha = \alpha_1^*$ :

$$L(\alpha_1^*)^R = (L(\alpha_1)^R)^* \rightarrow \alpha^R = (\alpha_1^R)^*$$

□

## Homomorphismus

**Definition 28.** Ein (Wort-)Homomorphismus ist eine Abbildung

$$h : \Sigma_1 \mapsto \Sigma_2^*$$

die die Symbole eines Alphabets auf Wörter abbildet.

**Beispiel.**  $\Sigma_1 = \{0, 1\}, \Sigma_2 = \{a, b\}, h(0) = ab, h(1) = \varepsilon$

Erweiterung auf Wörter: Sei  $w = a_1 \dots a_k$ . Dann ist  $h(w) = h(a_1) \cdot h(a_2) \cdot \dots \cdot h(a_k)$ .

**Beispiel.**  $h(0101) = ab \cdot \varepsilon \cdot ab \cdot \varepsilon = abab$

**Definition 29.** Sei  $h : \Sigma_1 \mapsto \Sigma_2^*$  ein Homomorphismus, sei  $L \subseteq \Sigma_1^*$  eine Sprache. Dann ist

$$h(L) = \{w \in \Sigma_2^* \mid w = h(x) \text{ für ein } x \in L\}$$

Satz: Sei  $h : \Sigma_1 \mapsto \Sigma_2^*$  ein Homomorphismus. Wenn  $L \subseteq \Sigma_1^*$  regulär ist, dann ist auch  $h(L)$  regulär.

*Beweis über rock-the-bottom strukturelle Induktion.* Für einen regulären Ausdruck  $\alpha$  über  $\Sigma_1$  ist  $h(\alpha)$  der reguläre Ausdruck über  $\Sigma_2$ , der entsteht, wenn jedes Vorkommen von  $a \in \Sigma_1$  durch  $h(a)$  ersetzt wird. □

**Beispiel.**  $\Sigma_1 = \{0, 1\}, \Sigma_2 = \{a, b\}, h(0) = ab, h(1) = \varepsilon$ .

$$\alpha = ((0 + 1)0)^* 1 \Rightarrow h(\alpha) = ((ab + \varepsilon) \cdot ab)^* \varepsilon = (ab)^*$$

Und latürnich gilt:  $L(h(\alpha)) = h(L)$

**Beispiel** (Übungsaufgaben 9. Oktober – Aufgabe 3). Deifniere die Menge der  $a$ -Vorgänger eines Zustands  $q$  als  $V_a(q) = \{p \in Q \mid \delta(p, a) = q\}$ . Dann ist  $B = (Q, \Sigma, \delta, q_0, V_a(F))$  ein DEA für  $L/a$ .

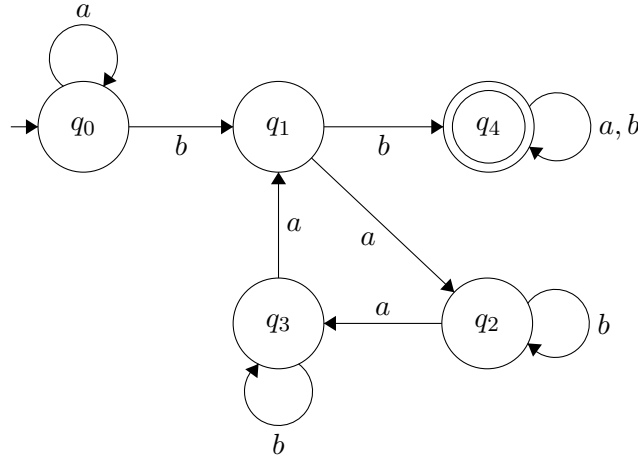


## 17.2 Nichtregularität

Ziel: Zeige, dass es Sprachen gibt, die nicht regulär sind.

Idee: DEAs analysieren: DEAs können nicht beliebig weit zählen.

**Beispiel.** Betrachte den folgenden DEA:



Arbeit von  $A$  auf dem Wort  $w = abaaab$ :

$$q_0 \xrightarrow{a} q_0 \xrightarrow{b} q_1 \xrightarrow{a} q_2 \xrightarrow{a} q_3 \xrightarrow{a} q_1 \xrightarrow{b} q_4$$

Enthält einen Zykel  $q_1 \xrightarrow{a} q_2 \xrightarrow{a} q_3 \xrightarrow{a} q_1$ .

Wiederholung des Zyklus:  $w' = abaaaaaab$

$$q_0 \xrightarrow{a} q_0 \xrightarrow{b} q_1 \xrightarrow{a} q_2 \xrightarrow{a} q_3 \xrightarrow{a} q_1 \xrightarrow{a} q_2 \xrightarrow{a} q_3 \xrightarrow{a} q_1 \xrightarrow{b} q_4$$

Da  $q_4 \in F$ , gilt  $w' \in L(A)$

Allgemein: Sei  $A$  ein DEA. Sei  $w = u \cdot x \cdot v$  ein Wort in  $L(A)$ ,  $u, v, x \in \Sigma^*$ ,  $x \neq \varepsilon$ . Falls der Automat auf dem Teilwort  $x$  in einer Schleife läuft, dann ist auch das Wort  $w' = uxxv \in L(A)$ .

Formal: Falls  $\hat{\delta}(q_0, u) = q$  und  $\hat{\delta}(q, x) = q$  und  $\hat{\delta}(q, v) \in F$ , dann ist  $w' = uxxv \in L(A)$ .

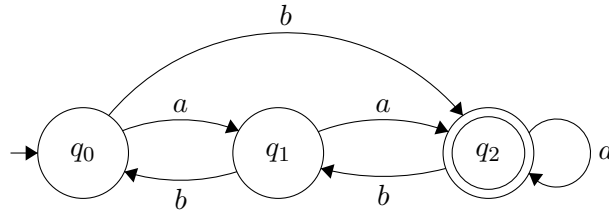
Im Beispiel oben:

$$w = \underbrace{u}_{ab} \underbrace{x}_{aaa} \underbrace{v}_b \in L(A)$$

$$, w' = \underbrace{u}_{ab} \underbrace{x}_{aaa} \underbrace{x}_{aaa} \underbrace{v}_b \in L(A)$$

**Bemerkung.** Ein DEA ist vollständig, d.h. für jedes  $q \in Q$  und jedes  $a \in \Sigma$  existiert genau ein Folgezustand  $\delta(q, a)$ . Daraus folgt direkt, dass man mit jedem Wort aus  $\Sigma^*$  kann man durch den Automaten laufen, ohne stecken zu bleiben. Daraus wiederum folgt, dass bei der Arbeit des DEA  $A$  mit  $n$  Zuständen auf einem Wort der Länge  $\geq n$  wird mindestens ein Zustand doppelt besucht.

**Beispiel.** Sei



$|Q| = 3$ .

z.B.  $w_1 = abb$ :  $q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_0 \xrightarrow{b} q_2$

$\Rightarrow q_0$  doppelt besucht.

Beobachtung: Sei  $A = (Q, \Sigma, \delta, q_0, F)$  ein DEA mit  $|Q| = n$ . Sei  $w \in L(A)$  mit  $|w| \geq n$ . Dann wiederholt sich in der Berechnung von  $A$  auf  $w$  mindestens einmal ein Zustand. Wir nennen einen dieser wiederholt besuchten Zustände  $q_x$ . Dann lässt sich  $w$  zerlegen in drei Teile

$$w = \underbrace{u}_{\text{bis zum ersten } q_x} \cdot \underbrace{x}_{\text{von } q_x \text{ nach } q_x} \cdot \underbrace{v}_{\text{nach } q_x}$$

Berechnung von  $A$  auf  $w$  hat die Form

$$q_0 \xrightarrow{u} q_x \xrightarrow{x} q_x \xrightarrow{v} q_F \in F$$

Damit gibt es auch eine Berechnung von  $A$  auf  $w' = uxxv$ :

$$q_0 \xrightarrow{u} q_x \xrightarrow{x} q_x q_x \xrightarrow{x} q_x \xrightarrow{v} q_F \in F$$

**Beispiel.** Diese Beobachtung können wir nutzen, um zu zeigen, dass  $L = \{a^k b^k \mid k \geq 0\}$  nicht regulär ist.

*Beweis durch Widerspruch.* Für  $L$  kann es keinen DEA mit 7 Zuständen geben.

Annahme: Es gibt einen DEA  $A = (Q, \Sigma, \delta, q_0, F)$  mit  $|Q| = 7$  und  $\Sigma = \{a, b\}$ , so dass  $L(A) = L$ .

Es gibt zwei Möglichkeiten zur Widerlegung:

1. alle möglichen DEA mit 7 Zuständen ausprobieren. Klappt nicht, weil zu viele.
2. Beobachtung über Zykel ausnutzen.

Betrachte das Wort  $w = aaaabbbb \in L$ . Es gilt  $|w| = 8 > 7 = |Q|$ . Also muss sich in der Berechnung von  $A$  auf  $w$  mindestens ein Zustand wiederholen.

Zerteilen wir  $w$  in  $w = u \cdot x \cdot v$  mit der Berechnung

$$q_0 \xrightarrow{u} q_x \xrightarrow{x} q_x \xrightarrow{v} q_F \in F$$

Daraus folgt  $w' = uxxv \in L(A)$ . Wie kann das Wort  $x$  aussehen? Fallunterscheidung:

- (a)  $x$  besteht nur aus  $as$ . z.B.  $w = \underbrace{aa}_u \underbrace{aa}_x \underbrace{bbbb}_v$ . Daraus folgt  $w' = \underbrace{aa}_u \underbrace{aa}_x \underbrace{aa}_x \underbrace{bbbb}_v = a^6b^4 \notin L$ . Widerspruch!
- (b)  $x$  besteht nur aus  $bs$ . z.B.  $w = \underbrace{aaaa}_u \underbrace{ab}_x \underbrace{bb}_v$ . Daraus folgt  $w' = \underbrace{aaaa}_u \underbrace{ab}_x \underbrace{b}_x \underbrace{bb}_v = a^4b^5 \notin L$ . Widerspruch!
- (c)  $x$  besteht aus  $as$  und  $bs$ . z.B.  $w = \underbrace{aa}_u \underbrace{aab}_x \underbrace{bbb}_v$ . Daraus folgt  $w' = \underbrace{aa}_u \underbrace{aab}_x \underbrace{aab}_x \underbrace{bbb}_v \notin L$ . Widerspruch!

Daraus folgt, dass es keinen DEA mit 7 Zuständen für  $L$  gibt.

Denselben Beweis hätten wir auch für jede andere Anzahl von Zuständen führen können. Daraus kann gefolgert werden, dass es überhaupt keinen DEA für  $L$  gibt. Daraus folgt, dass  $L$  nicht regulär ist.

□

**Beispiel.** Argumentieren wir, warum ein DEA mit 5 Zuständen die Sprache

$$L = \{a^k b^{2k} \mid k \geq 0\}$$

nicht akzeptieren kann.

*Beweis.* Annahme: Es gibt einen DEA mit  $|Q| = 5$ . Betrachten wir uns das Wort  $w = aabbbb \in L$ . Es gilt  $|w| = 6$ , das heisst es wird mindestens 1 Zustand mehrfach durchlaufen.  $w$  lässt sich also zerlegen in  $w = uv$ :

$$q_0 \xrightarrow{u} q_x \xrightarrow{x} q_F \in F.$$

Dann gilt  $w' = uxxv \in L(A)$ .

Fallunterscheidung über die Form von  $x$ :

1.  $x$  besteht nur aus  $as$ . D.h.  $w'$  enthält mehr  $as$  als  $w$ , aber nicht mehr  $bs \Rightarrow w' \notin L$ . Widerspruch!
2.  $x$  besteht nur aus  $bs$ . Analoger Widerspruch.
3.  $x$  besteht aus  $as$  und  $bs$ .  $\Rightarrow$  in  $w'$  kommt ein  $b$  vor einem  $a \Rightarrow w' \notin L$ . Darum gibt es keinen DEA mit 5 Zuständen, der  $L$  akzeptieren könnte.

□

### 17.3 Verallgemeinerung der Methode

Ziel: Zeige, dass es gar keinen DEA für  $L$  gibt.

**Definition 30** (Pumping-Lemma für reguläre Sprachen). Sei  $L$  eine reguläre Sprache. Dann gibt es eine Konstante  $n_0$  (die von  $L$  abhängt), so dass für jedes Wort  $w \in L$  mit  $|w| \geq n_0$  gilt:

$w$  kann zerlegt werden in  $w = uv$  mit den folgenden Eigenschaften:

- (a)  $|w| \geq 1$ , d.h.  $x \neq \varepsilon$
- (b)  $|ux| \leq n_0$
- (c) Für alle  $k \geq 0$  ist auch  $ux^k v \in L$ .

*Begründung der Korrektheit.* Falls  $L$  regulär ist, existiert ein DEA  $A$  für  $L$ . Setzen wir  $n_0 = |Q|$ .  $x$  ist dann die Beschriftung eines Zyklus in  $A$ , der in den ersten  $|Q|$  Berechnungsschritten auftritt ( $|ux| \leq n_0$ ). Eine Wiederholung des Zyklus ändert nichts an der Akzeptanz des Wortes.  $\square$

**Beispiel.** Zeigen wir, dass  $L = \{a^k b^k \mid k \in \mathbb{N}\}$ .

*Beweis.* Annahme:  $L$  ist regulär. Das Pumping-Lemma gibt uns die Existenz einer Konstanten  $n_0$ , sodass für alle Wörter  $w \in L$  mit  $|w| \geq n_0$  alle Bedingungen gelten. Um einen Widerspruch herzuleiten, können wir uns ein Wort  $w \in L$  auswählen, sei also  $w = a^{n_0} b^{n_0}$ . Nach dem Pumping-Lemma gibt es eine Zerlegung  $w = uxv$  mit  $|ux| \leq n_0$  und  $|x| \geq 1$ .

Daraus folgt, dass:

$$u = a^j \text{ für ein } 0 \leq j \leq n_0 \leq n_0$$

und

$$x = a^i \text{ für ein } 1 \leq i \leq n_0.$$

Weiter gilt nach dem Pumping-Lemma:  $ux^k v \in L$  für alle  $k$ . Um den Widerspruch herzuleiten, wählen wir  $k = 2$ . Nach dem Pumping-Lemma muss gelten, dass

$$ux^2 v = a^{n_0+i} b^{n_0} \in L.$$

Das ist ein Widerspruch weil  $n_0 + i \neq n_0$ . Also kann  $L$  nicht regulär sein.  $\square$

**Bemerkung.** So nützlich es auch ist, aber:

- Das Pumping-Lemma gibt nur notwendige Eigenschaften für reguläre Sprachen an, aber keine hinreichenden. Die Regularität einer Sprache kann also damit nicht gezeigt werden.
- Es gibt Sprachen, die nicht regulär sind und trotzdem das Pumping-Lemma erfüllen. Dumm gelaufen.

## 17.4 Anwendung des Pumping-Lemmas gegen einen Gegner

Wir spielen gegen Darth Vader, die Lemmings und die Achse der bösen Allquantoren.

1. Wir wählen die Sprache, deren Nichtregularität wir nachweisen wollen.
2. Darth Vader wählt  $n_0$ .
3. Wir wählen das Wort  $w$  mit  $|w| \geq n_0$ .

4. Darth Vader lässt sich davon nicht beeindrucken und zerlegt  $w = uv$  gemäss dem Pumping-Lemma.

5. Wir wählen  $k$  und gewinnen, falls wir einen Widerspruch herleiten können.

**Beispiel.** Viele viele Aufgaben:

(a) Nicht regulär:  $L = \{0^m 10^m\}, m \geq 1$

Annahme:  $L$  ist regulär. Darum gibt es  $n_0$ , sodass alle Pumping-Lemma-Bedingungen gelten.  $w = 0^{n_0} 10^{n_0}$ .

Zerlegung:  $w = uv$ .  $u = 0^j, x = 1$ .  $ux^k v \in L$  für alle  $k$ .  $k = 2$ . Daraus folgt:  $ux^2 v = 0^{n_0} 1^2 0^{n_0}$ . Foul.

(b) Nicht regulär:  $L = \{yy^R | y \in \{a, b^*\}\}$

Annahme:  $L$  ist regulär. Darum gibt es  $n_0$ , sodass alle Pumping-Lemma-Bedingungen gelten.  $w = a^{n_0} b b a^{n_0}$ . Zerlegung.  $\Rightarrow |ux| \leq n_0, |x| \geq 1$ , also

$$u = a^j, x = a^i$$

Gem. Pumping-Lemma ist  $ux^0 v = uv = a^{n_0-i} b b a^{n_0}$ . Widerspruch.

**Beispiel.** 6a. Differenz: Offenbar  $0^* 1^*$  regulär. Annahme:  $L_1$  ist regulär.

$$\{0^m 1^m\} = 0^* 1^* - \{0^i 1^j | i \neq j\}.$$

6b. Homomorphismus:  $h : \{a, b, c\} \mapsto \{0, 1\}$ .  $h(a) = 0, h(b) = 0, h(c) = 1$ .  
 $h(L_2) = \{0^m 0^l 1^{m+l} | l, m \geq 0\}$

## 18 Reguläre Grammatiken

Idee: Mechanismus zur Erzeugung aller Wörter aus einer Sprache.

**Beispiel.** Reguläre Sprache:

$$L = \{1w | w \in 0^*\} \subseteq \{0, 1\}^* = \{1, 10, 100, 1000, \dots\}$$

Vorgehen bei der Konstruktion solcher Wörter:

- 1 an den Anfang setzen
- beliebig viele 0 auffüllen.

Regeln:

(1)  $\text{start} \rightarrow 1N$

(2)  $N \rightarrow 0N$

(3)  $N \rightarrow \varepsilon$

Konstruktion von 1000:

$$\text{start} \xRightarrow{(1)} 1N \xRightarrow{(2)} 10N \xRightarrow{(2)} 100N \xRightarrow{(2)} 1000N \xRightarrow{(3)} 1000$$

**Definition 31.** Eine Rechtslineare Grammatik  $G$  erzeugt alle Wörter einer Sprache buchstabenweise von links nach rechts. Sie wird beschrieben durch

$$G = (N, T, P, S),$$

wobei

- $T$  das Terminalalphabet (Alphabet der Sprache)
- $N$  das Nichtterminalalphabet (Menge von Hilfssymbolen)
- $P \subseteq N \times (TN \cup T \cup \{\varepsilon\})$  die Menge von Produktionen (Regeln). Für  $p = (l, r)$  heisst  $l$  die linke Seite von  $P$  und  $r$  die rechte Seite von  $P$ . Wir schreiben statt  $p = (l, r)$  auch  $l \rightarrow r$
- $S \in N$  ist das Startsymbol

Anschauung: Produktion  $p = l \rightarrow r$  ist eine Ersetzungsregel. In einem Wort über  $T \cup N$  wird durch Anwendung von  $p$  ein Vorkommen von  $l$  durch  $r$  ersetzt.

**Definition 32** (Ableitungsschritt). Sei  $G = (N, T, P, S)$  eine rechtslineare Grammatik. Ein Ableitungsschritt in  $G$  ist eine Relation

$$\Rightarrow \subseteq T^*N \times T^*(N \cup \varepsilon)$$

definiert durch  $uA \Rightarrow uw$  genau dann, wenn  $A \rightarrow w \in P$ , wobei  $u \in T^*, A \in N, w \in TN \cup T \cup \{\varepsilon\}$ .

**Definition 33** (Ableitung). Eine Ableitung ist eine endliche Folge von Ableitungsschritten. Formal ist  $\xRightarrow{*}$  die reflexive, transitive Hülle von  $\Rightarrow$ .

Die von  $G$  erzeugte Sprache ist definiert als

$$L(G) = \{w \in \Sigma^* | S \xRightarrow{*} w\},$$

also die Menge aller Wörter, die aus  $S$  in endlich vielen Ableitungsschritten erzeugt werden können.

**Definition 34** (Äquivalenz von Grammatiken). Zwei Grammatiken sind  $G_1, G_2$  heissen äquivalent, falls

$$L(G_1) = L(G_2).$$

**Beispiel.** Ein Beispiel:

$$G = (\{S, A, B\}, \{0, 1\}, P, S),$$

wobei

$$P = \{S \xrightarrow{(1)} 0S, S \xrightarrow{(2)} 1S, S \xrightarrow{(3)} 0A, A \xrightarrow{(4)} 0B, A \xrightarrow{(5)} 1B, B \xrightarrow{(6)} 0, B \xrightarrow{(7)} 1\}$$

Ableitung von 011010:

$$S \xRightarrow{(1)} 0S \xRightarrow{(2)} 01S \xRightarrow{(2)} 011S \xRightarrow{(3)} 0110A \xRightarrow{(5)} 01101B \xRightarrow{(6)} 011010$$

Ableitung von 0111:

Zwei Regeln für  $S$ :

$$S \xRightarrow{(1)} 0S \xRightarrow{(2)} 01S \xRightarrow{(2)} 011S \xRightarrow{(2)} 0111S \dots$$

Klappt nicht.

$$S \xRightarrow{(3)} 0A \xRightarrow{(5)} 01B \xRightarrow{(7)} 011$$

Klappt ebenfalls nicht.

**Definition 35.**

$$\mathcal{L}_{\text{rlin}} = \{L \mid \text{es existiert eine rechtslineare Grammatik } G \text{ mit } L = L(G)\}$$

Vereinfachung rechtslinearer Grammatiken. 3 Typen von Regeln:

$$(1) A \rightarrow aB$$

$$(2) A \rightarrow a$$

$$(3) A \rightarrow \varepsilon$$

Zeige: Die Regel (2) kann vermieden werden: Ersetze  $A \rightarrow a$  durch  $A \rightarrow aC$  und  $C \rightarrow \varepsilon$ .

Weitere Vereinfachung: Es reicht, eine Regel vom Typ (3), zusätzlich wird gegebenfalls  $S \rightarrow \varepsilon$ , falls  $\varepsilon \in L(G)$ . Wie funktioniert das? Ersetze die Regeln  $A_1 \rightarrow a_1B_1, \dots, A_k \rightarrow a_kB_k$  und  $B_1 \rightarrow \varepsilon, \dots, B_k \rightarrow \varepsilon$  durch  $A_1 \rightarrow a_1T, \dots, A_k \rightarrow a_kT$  und  $T \rightarrow \varepsilon$ .

**Theorem 2** (Äquivalenz von rechtslinearen Grammatiken und Endlichen Automaten). Zu jeder rechtslinearen Grammatik über  $T = \Sigma$  existiert ein NEA  $A$  über  $\Sigma$  mit  $L(A) = L(G)$ .

*Beweis.*  $G = (N, \Sigma, P, S)$  ohne Typ (2).

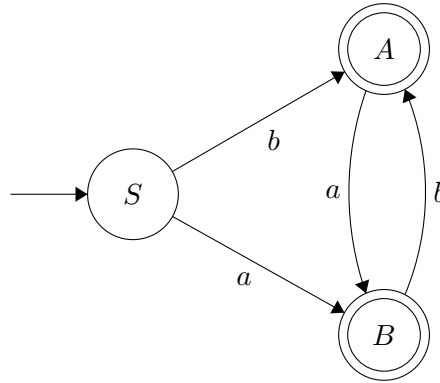
Daraus folgt: NEA  $A = (Q, \Sigma, \delta, q_0, F)$  mit

- $Q = N$

- $q_0 = S$
- $F = \{X \in N \mid X \rightarrow \varepsilon \in P\}$
- $\delta$  definiert durch:  $X \in \delta(Y, a) \Leftrightarrow Y \rightarrow aX \in P$

□

**Beispiel.**  $G = (\{S, A, B\}, \{a, b\}, P, S)$  mit  
 $P = \{S \rightarrow aB, S \rightarrow bA, A \rightarrow aB, B \rightarrow bA, A \rightarrow \varepsilon, B \rightarrow \varepsilon\}$ .  
 NEA für  $L(G)$ :

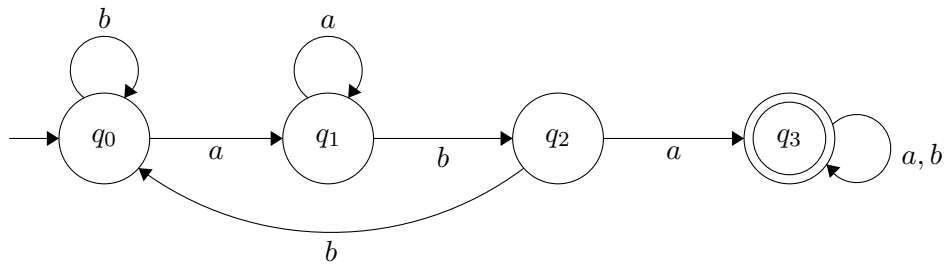


**Theorem 3.** Zu jedem DEA  $A$  über  $\Sigma$  existiert eine rechtslineare Grammatik  $G$  über  $\Sigma = T$  mit  $L(G) = L(A)$ .

*Proof.*  $A = (Q, \Sigma, \delta, q_0, F)$   
 $\Rightarrow G = (N, \Sigma, P, S)$  mit

- $N = Q$
- $S = q_0$
- $P$  definiert durch  $p \rightarrow aq \in P \Leftrightarrow \delta(p, a) = q$  und  $q \rightarrow \varepsilon \in P \Leftrightarrow q \in F$ .

□



**Beispiel.**



## 19 Kontextfreie Grammatiken

**Definition 36** (Kontextfreie Grammatik). Eine kontextfreie Grammatik  $G$  wird beschrieben durch

$$G = (\Sigma, N, P, S),$$

wobei:

- $\Sigma$  das Terminalalphabet;
- $N$  das Nichtterminalalphabet;
- $P \subseteq N \times (T \cup N)^*$  die Menge der Produktionen (Regeln). (Statt  $(X, abY)$  nutzen wir  $X \rightarrow abY$ ;
- $S$  das Startsymbol

ist.

**Beispiel.** Kontextfreie Grammatik für die folgende Sprache:  $L = \{a^n b^n \mid n \geq 0\}$ :

$$G = (\{a, b\}, \{S\}, P, S),$$

wobei

$$P = \{S \rightarrow aSb, S \rightarrow \varepsilon\}$$

.

Beispielableitung für  $aabb \in L$ :

$$S \Rightarrow aSb \Rightarrow aaSbb \Rightarrow aa\varepsilon bb = aabb$$

**Definition 37** (Kontextfreie Sprache). Eine Sprache  $L$  ist kontextfrei, wenn es eine Kontextfreie Grammatik  $G$  gibt mit

$$L = L(G).$$

Die Familie

$$\mathcal{L}_{\text{CF}}$$

ist die Menge aller kontextfreien Sprachen. Es gilt:

$$\mathcal{L}_{\text{REG}} \subseteq \mathcal{L}_{\text{CF}}$$

*Beweis.* Jede reguläre Grammatik ist auch eine kontextfreie Grammatik.  $\square$

**Beispiel.** Kontextfreie Grammatik zur Erzeugung aller arithmetischer Ausdrücke.

Induktion:

- $a$  ist ein arithmetischer Ausdruck.
- Für arithmetische Ausdrücke  $\alpha, \beta$  sind

- $(\alpha + \beta)$ ,
- $(\alpha - \beta)$ ,
- $\alpha \cdot \beta$ ,
- $\alpha / \beta$

ebenso arithmetische Ausdrücke.

Zum Beispiel  $(a + a), (a \cdot (a + a \cdot a) + a)$ .

Beschreibung durch eine kontextfreie Grammatik  $G = (\Sigma, N, P, S)$  mit

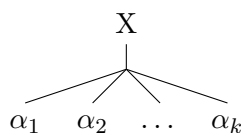
- $\Sigma = \{ (, ), a, +, -, \cdot, / \}$
- $N = \{ S, A, B, C \}$  ( $A$  für einen ganzen Ausdruck,  $B$  für Addition/Division,  $C$  für Multiplikation/Division),
- $P = \{ S \rightarrow A, A \rightarrow a, A \rightarrow (ABA), A \rightarrow ACA, B \rightarrow +, B \rightarrow -, C \rightarrow \cdot, C \rightarrow / \}$

Beispielableitung von  $(a \cdot (a - a) + a)$ :

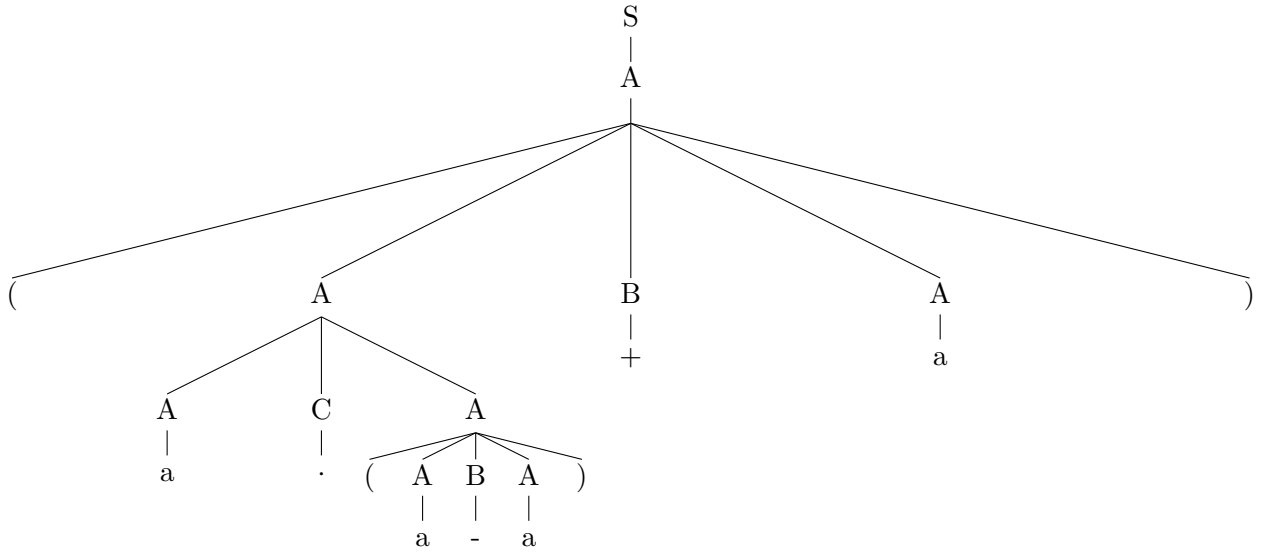
$$\begin{aligned}
 S &\Rightarrow A \Rightarrow (ABA) \Rightarrow (A + A) \Rightarrow (ACA + A) \Rightarrow (A \cdot A + A) \\
 &\Rightarrow (A \cdot (ABA) + A) \Rightarrow (A \cdot (A - A) + A) \Rightarrow (a \cdot (A - A) + A) \\
 &\Rightarrow (a \cdot (a - A) + A) \Rightarrow (a \cdot (a - a) + A) \Rightarrow (a \cdot (a - a) + a)
 \end{aligned}$$

Bessere Notation mit einem Parsebaum:

- Startsymbol als Wurzel
- Terminale als Blätter
- Nichtterminale als innere Knoten
- Regelanwendung:  $X \rightarrow \alpha_1 \alpha_2 \dots \alpha_k \mapsto$ :



Ableitungsbaum für  $(a \cdot (a - a) + a)$  in  $G$ :



## 20 Vereinfachung von kontextfreien Grammatiken

- (1) Elimination der  $\varepsilon$ -Regeln (Regeln der Form  $X \rightarrow \varepsilon$ ).

**Definition 38.** Eine kontextfreie Grammatik  $G$  heisst  $\varepsilon$ -frei, wenn sie keine Regeln der Form  $X \rightarrow \varepsilon$  hat.

**Theorem 4.** Sei  $G$  eine kontextfreie Grammatik. Dann gibt es eine  $\varepsilon$ -freie kontextfreie Grammatik  $G'$  mit

$$L(G') = L(G) - \{\varepsilon\}.$$

*Beweis.* Transformation von  $G$  in  $G'$ :

- (a) Sei  $N_1$  die Menge aller linken Seiten von  $\varepsilon$ -Regeln:

$$N_1 = \{A \in N \mid A \rightarrow \varepsilon\}$$

- (b) Bestimme alle in  $\varepsilon$  ableitbaren Nichtterminale. Dann gilt

$$N_1 = \{A \in N \mid A \xRightarrow{*} \varepsilon\}$$

Berechnung:  $N_1 \leftarrow N_1 \cup \{A \in N \mid A \rightarrow \alpha, \alpha \in N_1^*\}$

- (c) Für jede Regel  $A \rightarrow \alpha_1 B \alpha_2$  mit  $B \in N_1$ ,  $\alpha_1, \alpha_2 \in (\Sigma \cup N)^*$  füge die Regel  $A \rightarrow \alpha_1 \alpha_2$  zu  $P$  hinzu und erhalte  $P_1$ . Iteriere so lange bis sich  $P_1$  nicht mehr ändert.

- (d) Eliminiere alle  $\varepsilon$ -Regeln aus  $P_1$ :

$$P_2 \leftarrow P_1 - \{r \in P_1 \mid r = A \rightarrow \varepsilon\}.$$

Daraus ergibt sich die Sprache  $G' = (\Sigma, N, P_2, S)$ .

□

**Beispiel.** Betrachte  $G = (\{a, b, c\}, \{S, A, B, C\}, P, S)$  mit  $P = \{S \rightarrow AB, S \rightarrow C, A \rightarrow aB, a \rightarrow \varepsilon, B \rightarrow bA, B \rightarrow \varepsilon, C = c\}$ .

- (a)  $N_1 = \{A, B\}$
- (b) Wegen  $S \rightarrow AB$  und  $A, B \in N_1$  folgt  $N_1 \leftarrow N_1 \cup \{S\}$ .  $\Rightarrow N_1 = \{A, B, S\}$ .
- (c)  $P_1 \leftarrow P \cup \{S \rightarrow B, S \rightarrow A, A \rightarrow a, B \rightarrow b\}$ .
- (d)  $P_2 \leftarrow P_1 - \{A \rightarrow \varepsilon, B \rightarrow \varepsilon\}$

## (2) Elimination nutzloser Symbole

- (a) Ein Symbol  $x$  heisst erreichbar, falls es eine Ableitung  $S \xRightarrow{*} \alpha$  gibt, sodass  $X$  in  $\alpha$  vorkommt.

Bestimmung der Menge erreichbarer Symbole: Sei  $G = (\Sigma, N, P, S)$  eine kontextfreie Grammatik.

- i.  $E_N = \{S\}$  (erreichbare Nichtterminale),  $E_\Sigma = \emptyset$  (erreichbare Terminale)
- ii. Für alle  $A \rightarrow \alpha$  in  $P$  mit  $A \in E_N$ : Füge die Symbole von  $\alpha$  zu  $E_N$  bzw.  $E_\Sigma$  hinzu. Wiederhole solange, bis sich  $E_N$  und  $E_\Sigma$  nicht mehr ändern.
- iii. Reduziere die Grammatik zu  $G' = (E_\Sigma, E_N, P', S)$  mit

$$P' = \{A \rightarrow \alpha \in P \mid A \in E_N\}$$

- (b) Ein Nichtterminal  $x$  heisst produktiv (oder erzeugend), falls es eine Ableitung  $x \xRightarrow{*} w$  gibt für ein  $w \in \Sigma^*$ .

Bestimmung der Menge der produktiven Nichtterminale: Sei  $G = (\Sigma, N, P, S)$  eine kontextfreie Grammatik.

- i.  $\text{Prod} := \{A \in N \mid A \rightarrow w \in P, w \in \Sigma^*\}$ .
- ii. Für alle  $A \in N$ : Falls  $A \rightarrow \alpha \in P$  mit  $\alpha \in (\Sigma \cup \text{Prod})^*$ , füge  $A$  zu  $\text{Prod}$  hinzu. Wiederhole solange, bis sich  $\text{Prod}$  nicht mehr ändert.
- iii. Reduziere die Grammatik zu  $G' = (\Sigma, \text{Prod}, P', S)$  mit

$$P' = \{A \rightarrow \alpha \in P \mid A \in \text{Prod} \text{ und } \alpha \in (\text{Prod} \cup \Sigma)^*\}$$

**Beispiel.** Betrachte die kontextfreie Grammatik

$$G = (\{a, b, c\}, \{S, A, B, C\}, P, S)$$

mit

$$P = \{S \rightarrow A, S \rightarrow AB, A \rightarrow Aa, B \rightarrow bB, B \rightarrow Bb, C \rightarrow c\}$$

Erreichbare Symbole:  $\{S, A, B, a, b\}$

Also erhalten wir die Grammatik  $G' = (\{a, b\}, \{S, A, B\}, P', S)$  mit

$$P' = \{S \rightarrow A, S \rightarrow AB, A \rightarrow Aa, A \rightarrow a, B \rightarrow bB, B \rightarrow Bb\}.$$

Produktive Nichtterminale in  $G'$ :  $\{S, A\}$ .

Reduzierte Grammatik  $G'' = (\{a, b\}, \{S, A\}, P'', S)$  mit

$$P'' = \{S \rightarrow A, A \rightarrow Aa, A \rightarrow a\}$$

**Definition 39.** Eine kontextfreie Grammatik  $G$  heisst reduziert, falls sie keine unproduktiven und keine nichterreichbaren Symbole enthält.

(3) Elimination von Kettenregeln (Regeln der Form  $X \rightarrow Y$  mit  $X, Y \in N$ )

(a) Bestimme für jedes Nichtterminal  $A$  die Menge:

$$K(A) = \{D \in N \mid A \xRightarrow{*} D\}$$

aller Nichtterminale, die in  $G$  aus  $A$  (nur mit Kettenregeln) abgeleitet werden können. Iterativ berechnen wir:

$$K(A) := \{A\}$$

$$K(A) := K(A) \cup \{X \in N \mid \text{es existiert } C \in K(A) \text{ mit } C \rightarrow X \in P\}$$

(b) Für jedes  $X \in K(A)$  und jede Regel  $X \rightarrow \alpha$ , die keine Kettenregel ist, füge die Regel  $A \rightarrow \alpha$  zu  $P'$  hinzu.

**Beispiel.**  $G = (\{a, b, c, d\}, \{F, S\}, P, S)$  wobei

$$P = \{S \rightarrow F, F \rightarrow a, F \rightarrow bF, F \rightarrow d, F \rightarrow c\}$$

(a)  $K(S) = \{S, F\}, K(F) = \{F\}$

(b)  $P' = \{S \rightarrow a, S \rightarrow bF, S \rightarrow d, S \rightarrow c, F \rightarrow a, F \rightarrow bF, F \rightarrow d, F \rightarrow c\}$

## 21 Chomsky-Normalform

**Definition 40.** Zu jeder kontextfreien Grammatik  $G$  mit  $\varepsilon \notin L(G)$  existiert eine äquivalente Grammatik  $G'$  in Chomsky-Normalform.

Ziel: Umwandlung einer beliebigen kontextfreien Grammatik in Chomsky-Normalform.

**Theorem 5.** Sei  $G = (\Sigma, N, P, S)$  eine  $\varepsilon$ -freie, reduzierte Grammatik ohne Kettenregeln mit  $\varepsilon \notin L(G)$ .

*Beweis.* Sei  $G$  gemäss der Annahme. Forme alle Regeln, die nicht die gewünschte Form haben, um: Regeln der Form  $A \rightarrow X_1 X_2 \dots X_m, m \geq 2, X_i \in \Sigma \cup N$ .

1. Falls  $X_i \in \Sigma$ , dann ersetze  $X_i$  durch neues Nichtterminal  $C_{X_i}$  und füge die Regel  $C_{X_i} \rightarrow X_i$  hinzu.
2. Nach Schritt 1 haben alle nicht passenden Regeln die Form

$$A \rightarrow B_1 B_2 \dots B_m$$

für ein  $m \geq 3$  und  $B_i \in N$ .

Zur Umformung dieser Regeln definiere neue Nichtterminale  $D_1, \dots, D_{m-2}$  und ersetze die Regel durch folgende Regeln:

$$\begin{aligned} A &\rightarrow B_1 D_1 \\ D_1 &\rightarrow B_2 D_2 \\ &\vdots \\ D_{m-3} &\rightarrow B_{m-2} D_{m-2} \\ D_{m-2} &\rightarrow B_{m-1} B_m \end{aligned}$$

□

**Beispiel.**  $G = (\{a, b\}, \{S, A, B\}, P, S)$  mit  $P = \{S \rightarrow bA, S \rightarrow aB, A \rightarrow bAA, A \rightarrow aS, A \rightarrow a, B \rightarrow aBB, B \rightarrow bS, B \rightarrow b\}$ .

Transformation in Chomsky-Normalform:

1. Ersetzen:

Alte Regel	Neue Regel	
$S \rightarrow bA$	$S \rightarrow C_b A$	$C_b \rightarrow b$
$S \rightarrow aB$	$S \rightarrow C_a B$	$C_a \rightarrow a$
$A \rightarrow bAA$	$A \rightarrow C_b AA$	
$A \rightarrow aS$	$A \rightarrow C_a S$	
$B \rightarrow aBB$	$B \rightarrow C_a BB$	
$B \rightarrow bS$	$B \rightarrow C_b S$	

2. Noch nicht in Chomsky-Normalform:  $A \rightarrow C_b AA$  und  $B \rightarrow C_a BB$ . Also:

Alte Regel	Neue Regel	
$A \rightarrow C_b AA$	$A \rightarrow C_b D_1$	$D_1 \rightarrow AA$
$B \rightarrow C_a BB$	$B \rightarrow C_a E_1$	$E_1 \rightarrow BB$

Daraus folgt eine äquivalente kontextfreie Grammatik  $G'$  in Chomsky-Normalform:

$$G' = (\{a, b\}, \{S, A, B, C_a, C_b, D_1, E_1\}, P', S)$$

mit

$$P' = \dots$$

## 22 Anwendung der Chomsky-Normalform

Überprüfung, ob ein gegebenes Wort in der Sprache der Grammatik enthalten ist (sogenanntes Wortproblem). Motivation: Ist gegebenes Programm syntaktisch korrekt?

## 23 CYK (Cocke, Younger, Kasami)-Algorithmus

Algorithmus basiert auf dynamischer Programmierung, d.h. Zusammensetzen der Lösung aus Teillösungen.

Sei  $G$  eine kontextfreie Grammatik in Chomsky-Normalform. Sei ferner  $w = a_1 a_2 \dots a_n \in \Sigma^n$ . Idee: Bestimme für alle Teilwörter  $a_i \dots a_j$  von  $w$  die Menge  $V(i, j)$  aller Nichtterminale  $X \in N$ , sodass

$$X \xRightarrow{*} a_i \dots a_j.$$

Dann ist  $w \in L(G)$  genau dann, wenn  $S \in V(1, n)$ .

**Beispiel.**  $G = (\{a, b\}, \{S, A, B, C\}, P, S)$  mit  $P = \{S \rightarrow AB, S \rightarrow BC, A \rightarrow BA, A \rightarrow a, B \rightarrow CC, B \rightarrow b, C \rightarrow AB, C \rightarrow a\}$  und  $w = bbab$ .

1. Initialisierung der  $V$ -Mengen für Teilwörter der Länge 1.

Für alle  $i \in \{1, \dots, n\}$  gilt:  $V(i, i) = \{X \in N \mid X \rightarrow a_i \in P\}$ . Also:

- $V(1, 1) = \{B\}$ , da  $B \rightarrow b \in P$
- $V(2, 2) = \{B\}$
- $V(3, 3) = \{A, C\}$
- $V(4, 4) = \{B\}$

Darstellung als Tabelle:

					4
					3
					2
				1	$B \quad B \quad A, C \quad B$
			Länge	$b \quad b \quad a \quad a$	

2. Bestimmung der  $V$ -Mengen für Teilwörter der Länge 2:  $a_i a_{i+1}$ .

•

$$\begin{aligned}
 V(1, 2) &= \{X \in N \mid X \rightarrow YZ \in P \text{ mit } Y \in V(1, 1) \wedge Z \in V(2, 2)\} \\
 &= \{X \in N \mid X \rightarrow YZ \in P \text{ mit } Y \in \{B\} \wedge Z \in \{B\}\} \\
 &= \emptyset
 \end{aligned}$$

•

$$\begin{aligned}
V(2, 3) &= \{X \in N \mid X \rightarrow YZ \in P \text{ mit } Y \in V(2, 2) \wedge Z \in V(3, 3)\} \\
&= \{X \in N \mid X \rightarrow YZ \in P \text{ mit } Y \in \{B\} \wedge Z \in \{A, C\}\} \\
&= \{S, A\},
\end{aligned}$$

da  $S \rightarrow BC$  und  $A \rightarrow BA$ .

4				
3				
2	$\emptyset$	$S, A$	$C, S$	
1	$B$	$B$	$A, C$	$B$
Länge	$b$	$b$	$a$	$a$

**Bemerkung** (Allgemeine Regel für längere Teilwörter). Für alle  $i, j \in \{1, \dots, n\}$  mit  $i < j$  ist

$$\begin{aligned}
V(i, j) &= \{X \in N \mid \text{es existiert ein } k \text{ mit } i \leq k < j, \\
&\quad \text{so dass } X \rightarrow YZ \in P \text{ mit } Y \in V(i, j) \text{ und } Z \in V(k, j)\}
\end{aligned}$$

Beispielsweise lässt sich  $bba$  aufteilen als  $b|ba$  ( $k = 1$ ) oder  $bb|a$  ( $k = 2$ ).

3. Wörter der Länge 3:

4				
3	$A$	$C, S$		
2	$\emptyset$	$S, A$	$C, S$	
1	$B$	$B$	$A, C$	$B$
Länge	$b$	$b$	$a$	$a$

4. Wörter der Länge 4:

4	$C, S$			
3	$A$	$C, S$		
2	$\emptyset$	$S, A$	$C, S$	
1	$B$	$B$	$A, C$	$B$
Länge	$b$	$b$	$a$	$a$



## 24 Kellerautomaten (Pushdown Automata, PDA)

Ziel: Automatenmodell für kontextfreie Sprachen.

Idee: Nichtdeterministischer EA mit Zusatzspeicher in Form eines Stacks.

Arbeitsschritte (Übergänge):

Abhängig von Zustand, gelesenen Eingabesymbol und oberstem Symbol auf dem Stack:

- Bestimme neuen Zustand
- Entferne oberstes Symbol des Stacks und werfe beliebig viele Symbole auf den Stack.

**Definition 41** (Kellerautomat). Ein Kellerautomat wird beschrieben durch

$$A = (Q, \Sigma, \Gamma, \delta, q_0, \perp, F),$$

wobei:

- $Q$ : Menge der Zustände,
- $\Sigma$ : Eingabealphabet (wer hätte das gedacht),
- $\Gamma$ : Kelleralphabet,
- $\delta$ : Übergangsfunktion,
- $q_0 \in Q$ : Startsymbol,
- $\perp$ : Kellerbodensymbol ( $\perp \in \Gamma, \perp \notin \Sigma$ ),
- $F$ : Menge der akzeptierenden Zustände.

Die Übergangsfunktion ist definiert als

$$\delta : Q \times \Sigma \cup \{\varepsilon\} \times \Gamma \mapsto \mathcal{P}(Q \times \Gamma^*)$$

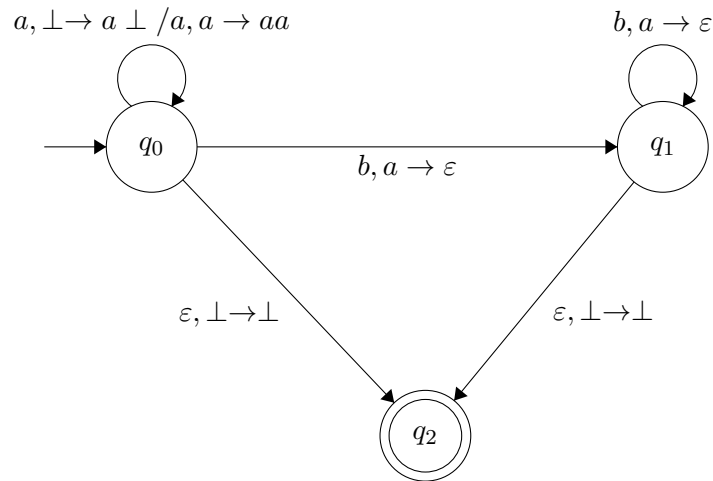
Ein Kellerautomat akzeptiert ein Wort  $w$ , falls es eine Berechnung auf  $w$  gibt, die die gesamte Eingabe liest und in einem akzeptierenden Zustand endet.

**Beispiel.** Kellerautomat für die Sprache  $L = \{a^k b^k \mid k \geq 0\}$ . Idee der Arbeitsweise: Der PDA liest alle  $a$ s und speichert sie auf dem Keller, dann entfernt er für jedes gelesene  $b$  ein  $a$  aus dem Keller. Bei gleicher Anzahl  $a$ s und  $b$ s akzeptiert er, sonst hat er keine Möglichkeit zum Weiterarbeiten, also verwirft er.

$$A = (\{q_0, q_1, q_2\}, \{a, b\}, \{A, \perp\}, \delta, q_0, \perp, \{q_2\})$$

mit

$$\begin{aligned}
\delta(q_0, \varepsilon, \perp) &= \{(q_2, \perp)\} \\
\delta(q_0, a, \perp) &= \{(q_0, a)\} \\
\delta(q_0, a, a) &= \{(q_0, aa)\} \\
\delta(q_0, b, a) &= \{(q_1, \varepsilon)\} \\
\delta(q_1, b, a) &= \{(q_1, \varepsilon)\} \\
\delta(q_1, \varepsilon, \perp) &= \{(q_2, \perp)\}
\end{aligned}$$



Berechnung von  $A$  auf dem Wort  $aaabbb$ :

$$\begin{aligned}
&(q_0, aaabbb, \perp) \rightarrow (q_0, aabbb, a \perp) \rightarrow (q_0, abbb, aa \perp) \rightarrow \\
&(q_0, bbb, aaa \perp) \rightarrow (q_1, bb, aa \perp) \rightarrow (q_1, b, a \perp) \rightarrow \\
&(q_1, \varepsilon, \perp) \rightarrow (q_2, \varepsilon, \perp)
\end{aligned}$$

## 25 Äquivalenz von kontextfreier Grammatik und PDA

**Theorem 6.** Sei  $G$  eine kontextfreie Grammatik. Dann gibt es einen PDA  $A$ , so dass  $L(A) = L(G)$ .

Idee des Beweises: Simuliere die Schritte einer Ableitung von  $G$  auf dem Keller  $A$ .  
 Beobachtung: Sei  $G$  eine kontextfreie Grammatik, sei  $w \in L(G)$ . Dann gibt es eine Ableitung von  $w$  in  $G$ , in der in jedem Ableitungsschritt das jeweils am weitesten links stehende Nichtterminal abgeleitet wird (sogenannte Linksableitung).

*Beweis.* Der zu  $G$  äquivalente PDA  $A$  arbeitet wie folgt:

- Falls das oberste Symbol auf dem Stack gleich dem nächsten Eingabesymbol ist, werden beide Symbole weggelesen.

- Falls das oberste Symbol auf dem Stack ein Nichtterminal ist, wird es durch die rechte Seite einer passenden Regel ersetzt. Dabei wird nichts von der Eingabe gelesen ( $\varepsilon$ -Übergang).

□

## 26 Turingmaschine

Motivation:

**Berechenbarkeit** Zeigen, dass es Probleme gibt, die nicht lösbar (entscheidbar) sind.

**Komplexität** Zeigen, dass es Probleme gibt, die nicht handhabbar sind.

Ziel: Berechnungsmodell, das so allgemein wie möglich, aber trotzdem einfach aufgebaut ist.

**Definition 42** (Turingmaschine). Eine Turingmaschine (TM) ist ein 6-Tupel

$$M = (Q, \Sigma, \Gamma, \delta, q_0, F),$$

wobei

- $Q$ : Zustandsmenge
- $\Sigma$ : Eingabealphabet,  $\sqcup \notin \Sigma$
- $\Gamma$ : Arbeitsalphabet,  $\sqcup \in \Gamma$ ,  $\Sigma \subset \Gamma$
- $q_0$ : Anfangszustand
- $F$ : Akzeptierende Zustände
- $\delta$ : Transitionsfunktion mit

$$\delta : Q \times \Gamma \mapsto Q \times \Gamma \times \{L, R, N\}$$

## 27 Berechnung eine TM auf der Eingabe $x$

Folge von Konfigurationen  $K_1, \dots, K_n$ , so dass

- $K_1$  ist Anfangskonfiguration  $(q_0, x)$  mit Kopf auf dem ersten Symbol der Eingabe
- $K_{i+1}$  entsteht aus  $K_i$  durch die Anwendung einer Transition von  $M$

Die TM  $M$  akzeptiert das Wort  $x$ , falls die Berechnung von  $M$  auf  $x$  in einem akzeptierenden Zustand hält.

$$L(M) = \{w \in \Sigma^* | M \text{ akzeptiert } w\}$$

**Definition 43.** Eine Sprache  $L$  heisst rekursiv aufzählbar (semi-entscheidbar), falls es eine TM  $M$  gibt, so dass

$$L = L(M).$$

$\mathcal{L}_{RE} = \{L(M) | M \text{ ist eine TM}\}$  ist die Menge aller rekursiv aufzählbaren Sprachen.

**Bemerkung.** Beobachtung: Eine Berechnung einer TM kann unendlich sein. Wenn das Wort nicht in der Sprache ist, kann  $M$  entweder verwerfen oder unendlich lange rechnen.

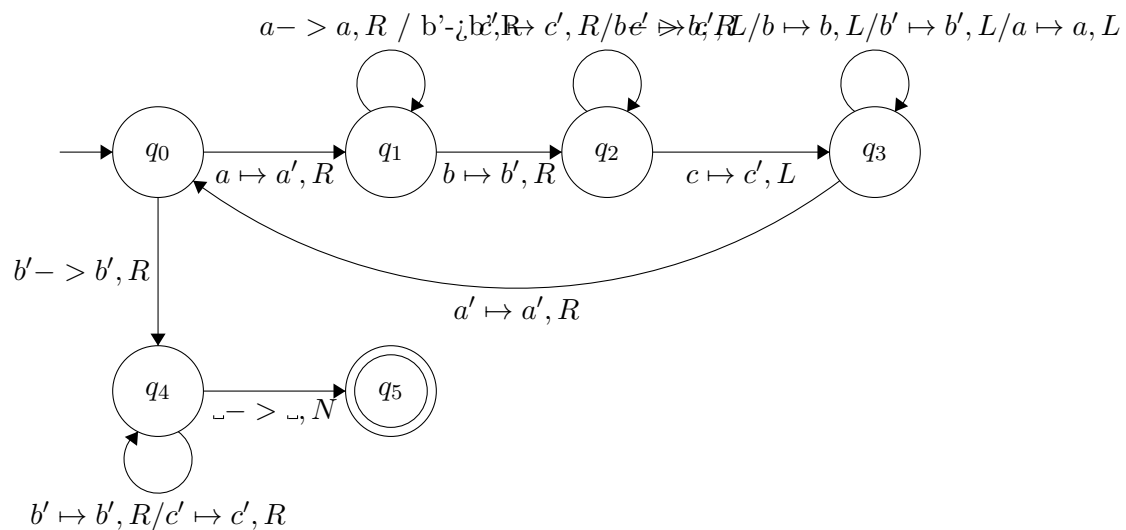
**Definition 44.** Eine Sprache heisst rekursiv (entscheidbar), wenn es eine TM  $M$  gibt mit  $L = L(M)$ , die auf jeder Eingabe  $w$  hält, und zwar in einem akzeptierenden Zustand für alle  $w \in L$  und in einem nichtakzeptierenden Zustand für alle  $w \notin L$ .

$\mathcal{L}_R$  = Menge aller rekursiven Sprachen.  $\mathcal{L}_R \subseteq \mathcal{L}_{RE}$

**Beispiel.** TM für  $L = \{a^k b^k c^k | k \geq 0\}$ . Idee: Wiederhole solange es unmarkierte  $a$ s gibt: markiere das  $a$ , gehe nach rechts bis zum ersten nichtmarkierten  $b$  und markiere es, gehe nach rechts bis zum ersten  $c$  und markiere es, gehe links bis zum linksten unmarkierten  $a$ .

Überprüfe von links nach rechts ob alle Eingaben markiert sind.

Graphische Darstellung:



**Theorem 7.** Eine TM mit mehreren Bändern kann simuliert werden durch eine TM mit einem Band.

**Beweis.** Idee: Grösseres Alphabet, das alle Bänder und Kopfpositionen beschreibt.

## 28 Universelle Turingmaschine

Ziel: Konstruktion einer TM, die alle anderen Turingmaschinen simulieren kann.

Sei  $M$  eine beliebige TM mit einem Band.  $M$  kann vollständig beschrieben werden durch die Transitionstabelle:

Jede Transition ist darstellbar als ein Wort

$$\underbrace{p}_{\text{aktueller Zustand}} \underbrace{A}_{\text{Arbeitssymbol}} \underbrace{q}_{\text{neuer Zustand}} \underbrace{B}_{\text{neues Bandsymbol}} \underbrace{S}_{\text{Kopfbewegung}}$$

Die Turingmaschine  $M$  ist darstellbar als Wort:

$$\text{Kod}(M) = q_0 \# q_{\text{accept}} \# q_{\text{reject}} \# t_1 \# t_2 \# \dots \# t_n$$

über dem Alphabet  $Q \cup \Gamma \cup \{L, R, N\} \cup \{\#\}$ , wobei  $t_i$  die wie oben codierte Transitionen von  $M$  sind.

**Bemerkung.** Im Prinzip ist auch eine Binärcodierung möglich.

Konstruktion einer universellen Turingmaschine  $U$ :

Eingabe:  $\text{Kod}(M) \# \# w$  für eine TM  $M$ , die auf dem Wort  $w$  simuliert werden soll.

Arbeitsweise von  $U$ :

1.  $U$  überprüft, ob  $\text{Kod}(M)$  eine gültige Codierung einer TM ist. Falls nicht, verwirft sie die Eingabe.
2.  $U$  schreibt die Anfangskonfiguration von  $M$  auf  $w$  auf das Band.
3.  $M$  simuliert die Berechnung von  $M$  auf  $w$  wie folgt: Solange der Zustand in der aktuellen Konfiguration von  $M$  nicht  $q_{\text{accept}}$  oder  $q_{\text{reject}}$  ist, generiere die Nachfolgekonfiguration von  $M$  auf  $w$  auf dem Band (suche passende Transition in der Eingabe und führe diese Änderung durch).
4. Wenn der Zustand von  $M$   $q_{\text{accept}}$  ist, dann akzeptiere die Eingabe, sonst verwerfe.

**Bemerkung.** Falls  $M$  auf  $w$  unendlich lange läuft, dann auch  $U$ .

Behauptung: Turingmaschinen sind ein geeignetes formales Modell zur Beschreibung der Rechenstärke realer Computer.

Hierfür: Zeige, wie man ein Programm einer beliebigen Programmiersprache durch eine äquivalente TM darstellt.

Beobachtung: Es reicht, eine solche Transformation für Assembler-Programme anzugeben.

Idee der Transformation:

- Eingabeband mit Programmzeile 1#Programmzeile 2#...#letzte Programmzeile
- Arbeitsband mit Register 1#Register 2#...
- Hauptspeicherband

- Arbeitsband zum Rechnen (Adressberechnungen etc)

Beobachtung: Alle bisher entwickelten Modelle zur Beschreibung der algorithmischen Lösbarkeit sind äquivalent zum Modell der Turingmaschine.

**Definition 45** (Church'sche These). Das Modell der TM, die immer hält, ist eine geeignete Formalisierung des intuitiven Begriffs "Algorithmus", d.h. die Klasse der rekursiven (entscheidbaren) Sprachen stimmt mit der Klasse der algorithmisch erkennbaren Sprachen überein.

## 29 Aufzählung von Wörtern

**Definition 46** (Kanonische Reihenfolge). Sei  $\Sigma = \{a_1, a_2, \dots, a_n\}$  ein Alphabet. Es sei  $a_1 < a_2 < \dots < a_n$ . Dann ist die kanonische Reihenfolge auf  $\Sigma^*$  definiert durch

$$w <_{\text{kan}} u$$

genau dann, wenn

- $|w| < |u|$
- $|w| = |u| = k, w = a_1 \dots a_k, u = b_1 \dots b_k$ : Es gibt ein  $i$  mit  $1 \leq i \leq k$ , so dass  $a_j = b_j$  für  $j < i$  und  $a_i < b_i$ .

**Beispiel.**  $ba <_{\text{kan}} aba$  und  $abb <_{\text{kan}} aca$

## 30 Aufzählung von Turingmaschinen

Sei  $\mathcal{M}$  die Menge aller TM. Dann ist die kanonische Reihenfolge auf  $\mathcal{M}$  definiert durch  $M_1 <_{\text{kan}} M_2$  genau dann, wenn  $\text{Kod}(M_1) <_{\text{kan}} \text{Kod}(M_2)$ .

## 31 Berechenbarkeit

Ziel: Zeigen, dass es keine TM  $U$  gibt, die hält, die für eine gegebene TM  $M$  und ein gegebenes Wort  $w$  entscheidet, ob  $w \in L(M)$  gilt.

Motivation: Gemäss der Church'schen These bedeutet dies, dass es nicht möglich ist, ein Programm zu schreiben, das beliebige andere Programme verifiziert.

## 32 Die Diagonalisierungssprache

Idee: Wir zeigen, dass es mehr Sprachen als TMs gibt. Das heisst, es gibt (unendlich viele) Sprachen, für die es keine TM gibt.

### 32.1 Methode der Diagonalisierung

Wir haben gesehen, dass wir alle Wörter und TMs aufzählen können.

Sei  $w_i$  das  $i$ -te Wort in kanonischer Reihenfolge, sei  $M_i$  die  $i$ -te Turingmaschine in kanonischer Reihenfolge. Wir konstruieren eine (unendlich grosse) Tabelle  $D$  mit Einträgen  $\{0, 1\}$ , so dass

$$D(i, j) = 1$$

genau dann, wenn  $M_i$  das Wort  $w_j$  akzeptiert. Beispielsweise:

$D$	$w_1$	$w_2$	$w_3$	$\dots$	$w_i$	$\dots$
$M_1$	0	1	0	$\dots$	0	$\vdots$
$M_2$	1	1	0	$\dots$	1	$\vdots$
$M_3$	0	0	1	$\dots$	1	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$M_i$	0	0	0	$\dots$	0	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\ddots$

Wir betrachten die Diagonaleinträge  $D(i, i)$ :

$D(i, i)$  beschreibt, ob die TM  $M_i$  das Wort  $w_i$  mit gleichem Index der Aufzählung akzeptiert.

Wir definieren nun die Sprache:

$$\begin{aligned} L_d &= \{w \in \{0, 1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w_i \text{ nicht}\} \\ &= \{w \in \{0, 1\}^* \mid w = w_i \text{ und } D(i, i) = 0\} \end{aligned}$$

In der Tabelle: Alle Spalten mit einer 0 in der Diagonalen.

**Theorem 8.** Es gibt keine TM, die  $L_d$  akzeptiert.

*Beweis.* Angenommen, es gibt eine TM  $M$ , die  $L_d$  akzeptiert. Da wir in der Tabelle  $D$  alle TMs aufgezählt haben, gibt es einen Index  $j$ , so dass  $M = M_j$ , also gilt, dass

$$L_d = L(M_j)$$

Für den gewünschten Widerspruch betrachten wir das entsprechende Wort  $w_j$ . Es gilt:

$$w_j \in L(M_j) \Leftrightarrow D(j, j) = 1$$

nach Definition von  $D$ . Aber ebenfalls gilt:

$$w_j \in L_d \Leftrightarrow D(j, j) = 0$$

nach Definition von  $L_d$ .

Es kann also nicht  $L_d = L(M_j)$  gelten, also war die Annahme falsch, somit gibt es keine TM, die  $L_d$  akzeptiert. □

Wiederholung:

- Eine Sprache  $L$  heisst rekursiv aufzählbar, wenn es eine TM  $M$  gibt, die  $L$  akzeptiert. (Wenn  $w \notin L$ , darf  $M$  unendlich lange laufen.)
- Eine Sprache  $L$  heisst rekursiv (entscheidbar), wenn es eine TM  $M$  gibt, die  $L$  entscheidet:
  - für alle  $w \in L$ : akzeptiert
  - für alle  $w \notin L$ : verworfen.

$M$  darf nicht unendlich lange laufen.

### 33 Reduktion

Wir wollen die Unlösbarkeit von Sprachen auf andere Sprachen ausweiten. Die Idee ist: eine Reduktion "leichter oder gleich schwer" bezüglich der algorithmischen Lösbarkeit einführen.

**Definition 47.** Seien  $L_1$  und  $L_2$  zwei Sprachen.  $L_1$  ist auf  $L_2$  rekursiv reduzierbar, geschrieben:

$$L_1 \leq_R L_2,$$

falls es eine immer-haltende Turingmaschine  $A$  gibt, die  $L_2$  entscheidet und man daraus eine TM  $B$  bauen kann, die  $L_1$  entscheidet.

Existiert eine Reduktion  $L_1 \leq_R L_2$ , dann gilt

- Ist  $L_1$  unentscheidbar, dann ist  $L_2$  unentscheidbar.
- Ist  $L_1$  nicht rekursiv aufzählbar, dann ist  $L_2$  ebenfalls nicht rekursiv aufzählbar.

### 34 Komplemente rekursiver Sprachen

Sei  $\bar{L} = \Sigma^* - L$  das Komplement von  $L$ .

**Theorem 9.**  $L$  ist rekursiv. Daraus folgt, dass  $\bar{L}$  rekursiv ist.

*Beweis.* Wir zeigen, dass  $\bar{L} \leq_R L$ .

Sei  $A$  eine TM, die  $L$  entscheidet. Eine TM  $B$ , die  $\bar{L}$  entscheidet, lässt sich nach folgendem Schema bauen:

(Biltli)

□

**Theorem 10.**  $\bar{L}_d$  ist rekursiv aufzählbar.

$$\bar{L}_d = \{w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w_i\}$$

Eine TM  $D$ , die  $\bar{L}_d$  akzeptiert, kann wie folgt arbeiten:



1. Berechne  $i$ , so dass  $w$  das  $i$ -te Wort  $w_i$  in der kanonischen Reihenfolge ist
2. Generiere die  $\text{Kod}(M_i)$  der  $i$ -ten TM  $M_i$
3. Simuliere die Berechnung von  $M_i$  auf dem Wort  $w_i$ :
  - Falls  $M_i$  das Wort  $w_i$  akzeptiert, dann akzeptiert auch  $D$ .
  - Falls  $M_i$  das Wort  $w_i$  verwirft, dann verwirft auch  $D$ .
  - Falls  $M_i$  auf  $w_i$  unendlich lange arbeitet, dann auch  $D$ .

## 35 Die universelle Sprache

Zeigen, dass eine generelle Programmverifikation nicht möglich ist.

Sei  $L_u = \{\text{Kod}(M)\# \mid M \text{ ist eine TM, die } w \text{ akzeptiert}\}$  die universelle Sprache.

Wir haben bereits gesehen, dass es eine universelle TM gibt, also ist  $L_u$  rekursiv aufzählbar:  $L_u \in \mathcal{L}_{\text{RE}}$ .

**Theorem 11.**  $L_u \notin \mathcal{L}_{\text{R}}$ .

*Beweis.* Idee: wir zeigen, dass wir eine TM, die  $L_u$  entscheidet, verwenden können, um  $\bar{L}_d$  zu entscheiden. Da wir bereits wissen, dass  $\bar{L}_d \notin \mathcal{L}_{\text{R}}$ , kann  $L_u$  nicht rekursiv sein.

Anders formuliert: Wir zeigen  $\bar{L}_d \leq_{\text{R}} L_u$ , d.h. wir zeigen, dass  $L_u$  mindestens so schwer ist wie  $\bar{L}_d$ .

Sei  $A$  eine TM, die  $L_u$  entscheidet. Wir bauen daraus eine TM  $B$ , die  $\bar{L}_d$  akzeptiert.

Die TM  $B$  hält immer, weil wir angenommen haben, dass  $A$  immer hält. Daraus folgt  $B$  entscheidet  $\bar{L}_d$ .

Dies ist ein Widerspruch, da wir schon gezeigt haben, dass  $\bar{L}_d \notin \mathcal{L}_{\text{R}}$ . Da die TM  $C$  offenbar existiert, muss die Annahme falsch gewesen sein, dass es eine TM  $A$  gibt, die  $L_u$  entscheidet.

Daraus folgt  $\bar{L}_u \notin \mathcal{L}_{\text{R}}$ .

□