Formale Grundlagen der Informatik

2

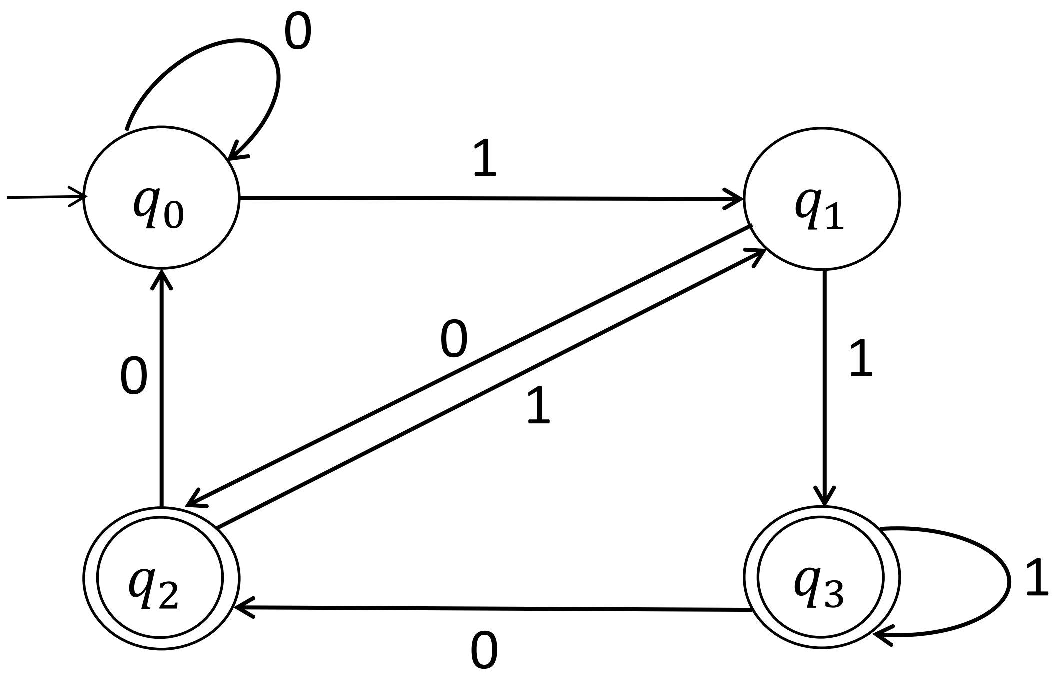
Korrektheitsbeweise
Nichtdeterminismus (NEA)

Recap: DEA und seine Sprache

- Ein **deterministischer endlicher Automat (DEA)** ist ein 5-Tupel
$$A = (Q, \Sigma, \delta, q_0, F),$$
wobei Q die endliche Zustandsmenge und Σ das Eingabealphabet, $\delta: (\mathrm{Q} \times \Sigma) \to Q$ die Überführungsfunktion, $\mathrm{q}_0 \in Q$ und $F \subseteq Q$ ist.
- Für alle $q \in Q$, $a \in \Sigma$ und $w \in \Sigma^*$ sei $\hat{\delta}: (\mathrm{Q} \times \Sigma^*) \to Q$ definiert durch
$\hat{\delta}(q, \varepsilon) = q$ und $\hat{\delta}(q, wa) = \delta(\hat{\delta}(q, w), a)$.
- Die von A **akzeptierte Sprache $L(A)$** ist die Sprache
$L(A) = \{\, w \mid \hat{\delta}(q_0, w) \in F \,\}$.

DEA – Beispiel 2

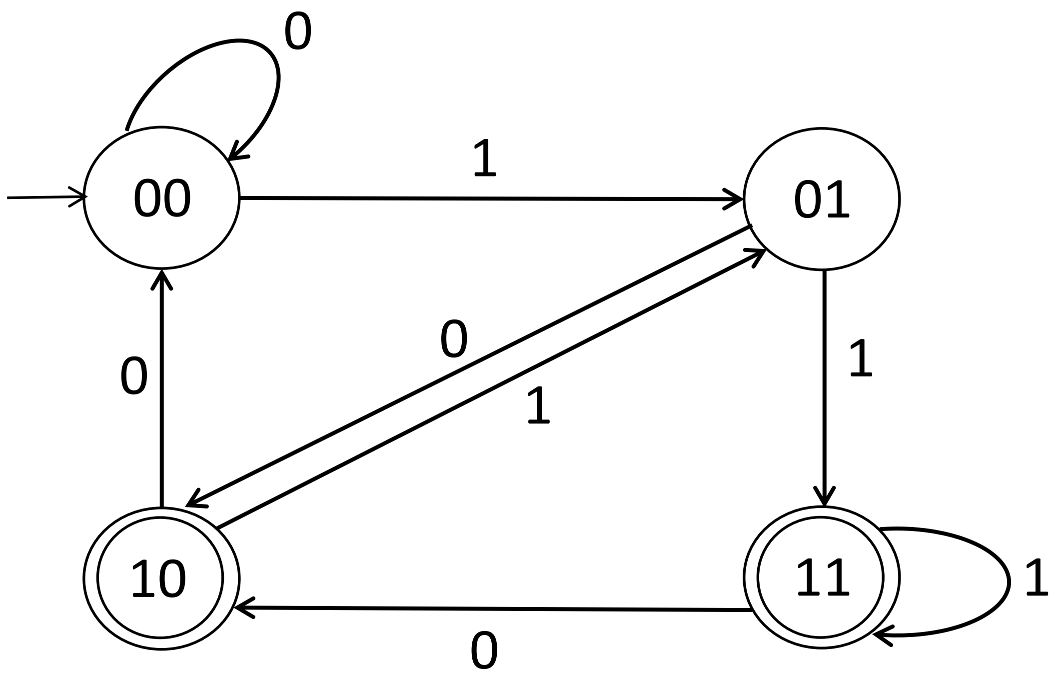
- $A_2 = (\{q_0, q_1, q_2, q_3\}, \{0,1\}, \delta_2, q_0, \{q_2, q_3\})$, δ_2 nach Transitionsgraph:



… suggestive Umbenennung der Zustände

DEA – Beispiel 2

- $A_2 = (\{00{,}01{,}10{,}11\}, \{0{,}1\}, \delta_2, 00, \{10{,}11\})$, δ_2 nach Transitionsgraph:



Behauptung:
Alle Wörter führen in den Zustand
- 00, die auf 00 enden,
- 01, die auf 01 enden,
- 10, die auf 10 enden,
- 11, die auf 11 enden.

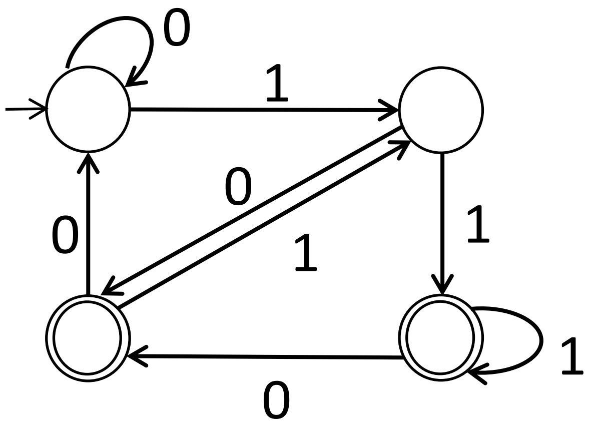
Keine weiteren Wörter führen in die Zustände 10 und 11.

→ $L(A_2) = \{\, w1x \mid w \in \{0{,}1\}^*, x \in \{0{,}1\}\,\}$

Korrektheitsbeweise - Prinzip

- Gegeben sind ein DEA A und eine Sprache L.

A:

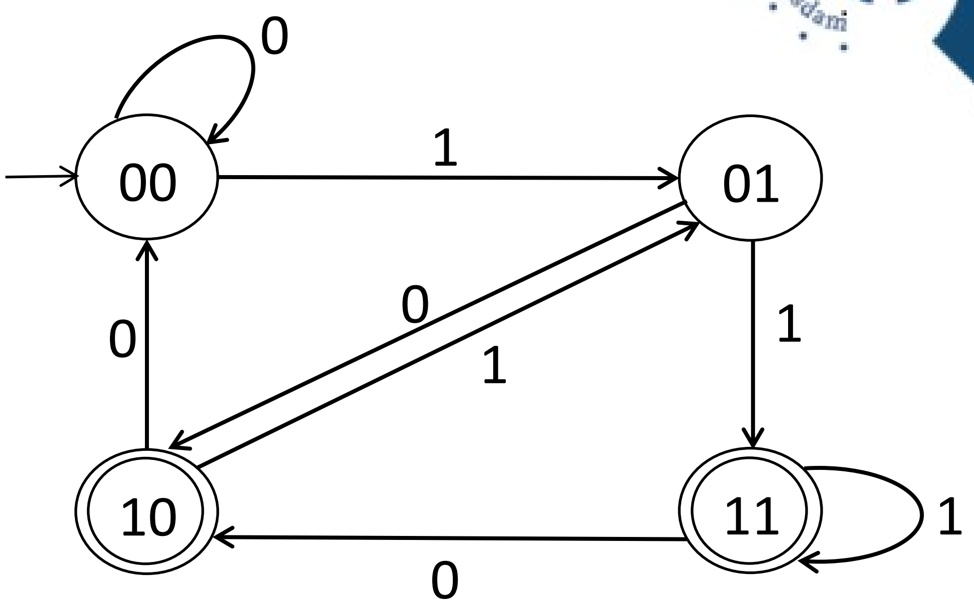


$\longleftrightarrow$

$$L = \{\, w1x \mid w \in \{0,1\}^*, x \in \{0,1\} \,\}$$

- *zu zeigen:* $\boldsymbol{L(A) = L}$
  1. Alle Wörter, die A akzeptiert, sind in L: $\boldsymbol{L(A) \subseteq L}$
  2. Alle Wörter aus L werden von A akzeptiert: $\boldsymbol{L \subseteq L(A)}$
  - *Ggf. auf* genau-dann-wenn-*Aussagen achten!*

Beweis der Korrektheit



Behauptung:

Alle Wörter führen in den Zustand

- 00, die auf 00 enden,
- 01, die auf 01 enden,
- 10, die auf 10 enden,
- 11, die auf 11 enden.

Präzisierung:

$\hat{\delta}(00, w) = 00$ gdw. $w \in \{ v00 \mid v \in \{0,1\}^* \} \cup \{\varepsilon, 0\}$

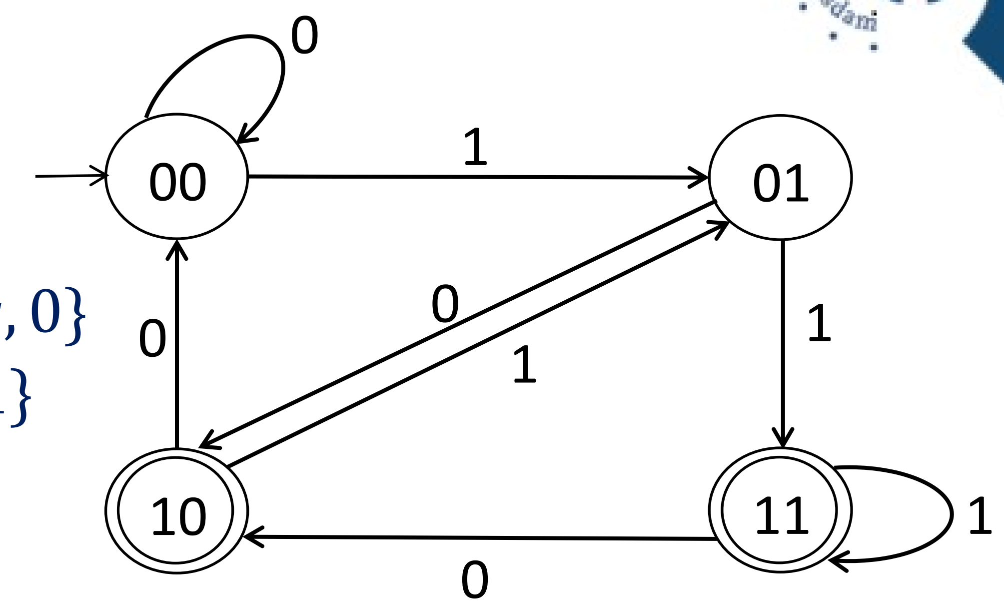
$\hat{\delta}(00, w) = 01$ gdw. $\mathrm{w} \in \{ v01 \mid v \in \{0,1\}^* \} \cup \{1\}$

$\hat{\delta}(00, w) = 10$ gdw. $\mathrm{w} \in \{ v10 \mid v \in \{0,1\}^* \}$

$\hat{\delta}(00, w) = 11$ gdw. $\mathrm{w} \in \{ v11 \mid v \in \{0,1\}^* \}$

Keine weiteren Wörter führen in diese Zustände („gdw.“).

Beweis der Korrektheit



Behauptung:

$\hat{\delta}(00, w) = 00$ gdw. $w \in \{ v00 \mid v \in \{0,1\}^* \} \cup \{\varepsilon, 0\}$
$\hat{\delta}(00, w) = 01$ gdw. $w \in \{ v01 \mid v \in \{0,1\}^* \} \cup \{1\}$
$\hat{\delta}(00, w) = 10$ gdw. $w \in \{ v10 \mid v \in \{0,1\}^* \}$
$\hat{\delta}(00, w) = 11$ gdw. $w \in \{ v11 \mid v \in \{0,1\}^* \}$

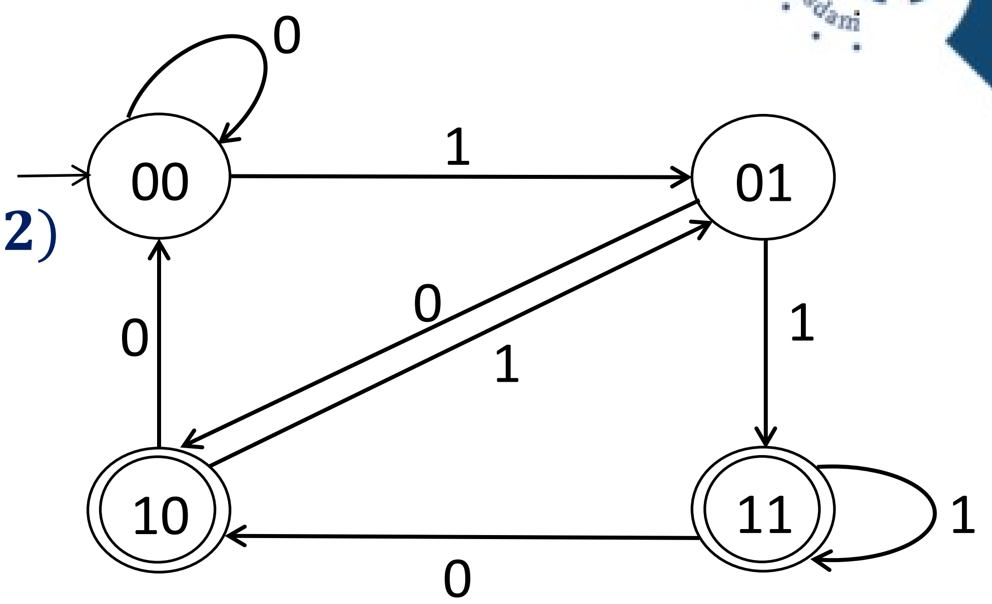
Induktion über die Länge des Eingabewortes w:

Induktionsanfang: $|w| \leq 2$

$\hat{\delta}(00, \varepsilon) = 00$, $\quad \hat{\delta}(00,0) = 00$, $\quad \hat{\delta}(00,00) = 00$,
$\hat{\delta}(00,1) = 01$, $\quad \hat{\delta}(00,01) = 01$,
$\hat{\delta}(00,10) = 10$, $\quad \hat{\delta}(00,11) = 11$

Dies sind alle Wörter der Länge ≤ 2.

Beweis der Korrektheit



Induktionsvoraussetzung: (für Wörter der Länge $n \geq 2$)

$\hat{\delta}(00, v00) = 00$ für alle $v \in \{0,1\}^*$

$\hat{\delta}(00, v01) = 01$ für alle $v \in \{0,1\}^*$

$\hat{\delta}(00, v10) = 10$ für alle $v \in \{0,1\}^*$

$\hat{\delta}(00, v11) = 11$ für alle $v \in \{0,1\}^*$

Induktionsschritt: (zu Wörtern der Länge $n+1$, $n \geq 2$)

$$\hat{\delta}(00, v000) = \delta\left(\hat{\delta}(00, v00), 0\right) = \delta(00,0) = 00$$

$$\hat{\delta}(00, v100) = \delta(10,0) = 00$$

$$\hat{\delta}(00, v001) = \delta(00,1) = 01$$

$$\hat{\delta}(00, v101) = \delta(10,1) = 01$$

$$\hat{\delta}(00, v010) = \delta(01,0) = 10$$

$$\hat{\delta}(00, v110) = \delta(11,0) = 10$$

$$\hat{\delta}(00, v011) = \delta(01,1) = 11$$

$$\hat{\delta}(00, v111) = \delta(11,1) = 11$$

■

Verallgemeinerung

- Sprache aller Wörter über $\{0,1\}$ der Form $w1u$ mit $|u| = n - 1$

- $Q \;= \{\, q \mid q \in \{0,1\}^*, |q| = n \,\}$
- $q_0 = 0^n$
- $F \;= \{\, 1r \mid r \in \{0,1\}^*, |r| = n - 1 \,\}$
- Für alle $r \in \{0,1\}^*, |r| = n - 1$:

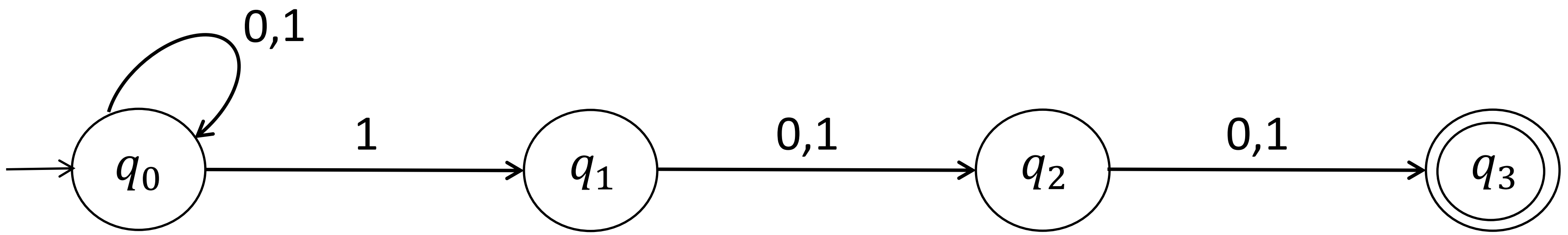
$$\delta(0r, 0) = r0 \qquad \delta(0r, 1) = r1$$

$$\delta(1r, 0) = r0 \qquad \delta(1r, 1) = r1$$

$$\boldsymbol{|Q| = 2^n}$$

Nichtdeterminismus

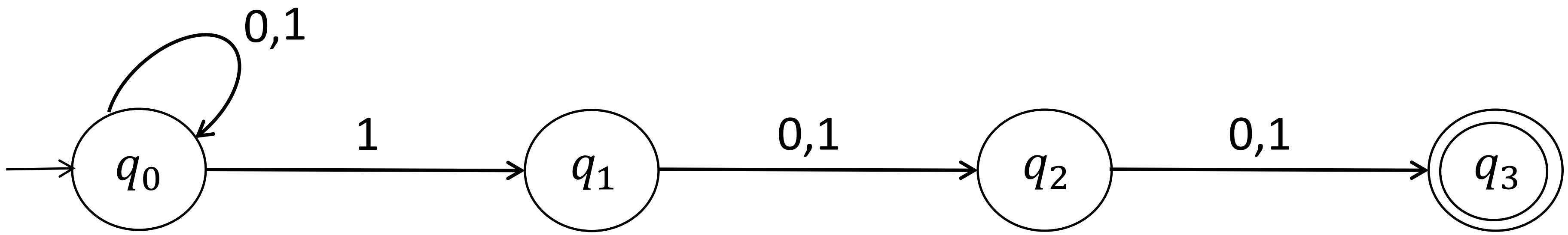
- noch einfacher, hier für $L = \{\, w1u \mid w, u \in \{0,1\}^*, |u| = 2 \,\}$:



- Der Automat ist **nichtdeterministisch**, weil in q_0 nicht bestimmt ist, in welchen Zustand der Automat bei Eingabe einer **1** wechselt.
- Dies ist ein Denkmodell, das so nicht implementiert werden kann.
- *Vorteil:* bei $w1u$ mit $|u| = n - 1$ nur $n + 1$ Zustände statt 2^n

Nichtdeterminismus

- $\delta(q_0, 1) = \{q_0, q_1\}$ $\longleftrightarrow$ Folgezustand wird „geraten“



- Der Automat akzeptiert, wenn er „bei der richtigen 1“ in q_1 wechselt.

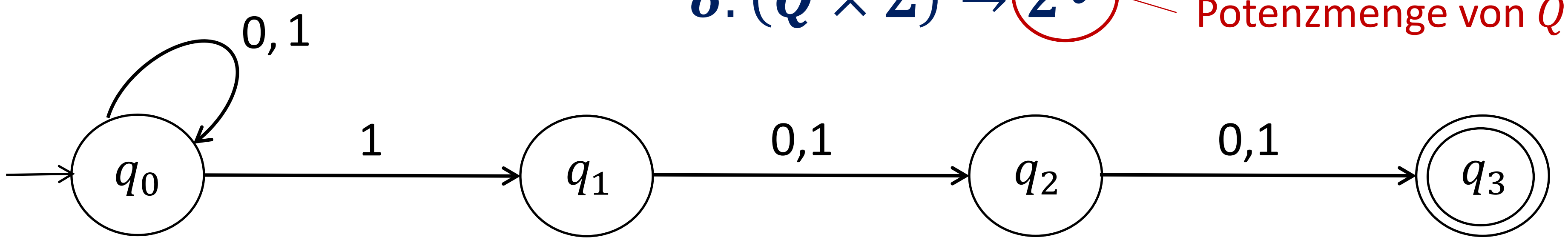
➢ Der Automat akzeptiert, wenn es *eine* *erfolgreiche Berechnung* *gibt*.

Nichtdeterministischer endlicher Automat

Definition: Ein **nichtdeterministischer endlicher Automat (NEA)** ist ein 5-Tupel $A = (Q, \Sigma, \delta, q_0, F)$, wobei Q, Σ, q_0 und F wie bei einem DEA definiert sind und die Überführungsfunktion δ ist eine Abbildung mit

$$\boldsymbol{\delta}: (\boldsymbol{Q} \times \boldsymbol{\Sigma}) \rightarrow \boldsymbol{2^Q}$$

Potenzmenge von Q

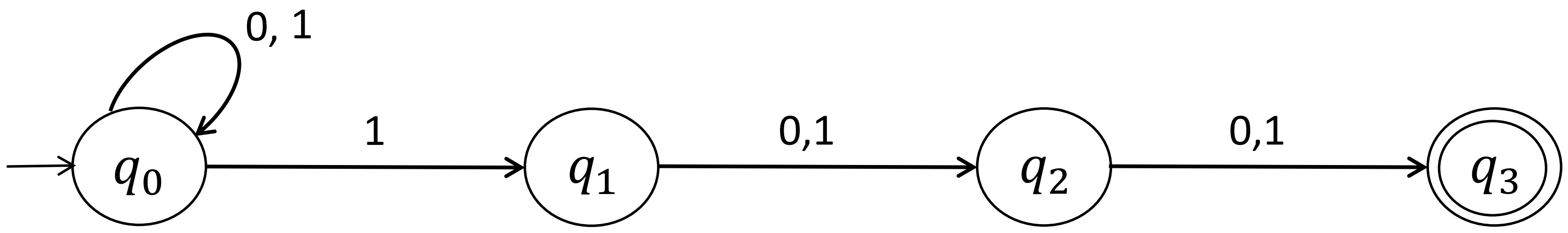


$\delta(q_0, 0) = \{q_0\}$ $\delta(q_0, 1) = \{q_0, q_1\}$

$\delta(q_1, 0) = \delta(q_1, 1) = \{q_2\}$ $\delta(q_2, 0) = \delta(q_2, 1) = \{q_3\}$

$\delta(q_3, 0) = \delta(q_3, 1) = \emptyset$ ⟶ $\emptyset \in 2^Q$ ⟶ *kein neuer Fehlerzustand nötig*

NEA – erweiterte Überführungsfunktion



$\delta(q_0, 0) = \{q_0\}$ $\quad$ $\delta(q_0, 1) = \{q_0, q_1\}$

$\delta(q_1, 0) = \delta(q_1, 1) = \{q_2\}$ $\quad$ $\delta(q_2, 0) = \delta(q_2, 1) = \{q_3\}$ $\quad$ $\delta(q_3, 0) = \delta(q_3, 1) = \emptyset$

- $\hat{\delta}: (Q \times \Sigma^*) \to 2^Q$
- $\hat{\delta}(q_0, \varepsilon) = \{q_0\}$
- $\hat{\delta}(q_0, 00) = \{q_0\}$
- $\hat{\delta}(q_0, 10) = \delta(q_0, 0) \cup \delta(q_1, 0) = \{q_0\} \cup \{q_2\} = \{q_0, q_2\}$
- $\hat{\delta}(q_0, 100) = \delta(q_0, 0) \cup \delta(q_2, 0) = \{q_0\} \cup \{q_3\} = \{q_0, q_3\}$

NEA – erweiterte Überführungsfunktion

- $\hat{\delta}: (Q \times \Sigma^*) \to 2^Q$
- Für alle $q \in Q$, $a \in \Sigma$ und $w \in \Sigma^*$:

$$\hat{\delta}(q, \varepsilon) = \{q\}$$

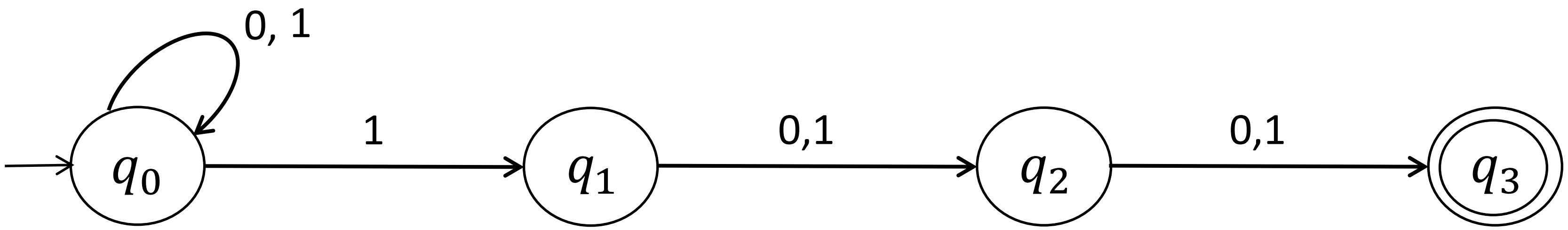
$$\hat{\delta}(q, wa) = \bigcup_{p \in \hat{\delta}(q,w)} \delta(p, a)$$

$\hat{\delta}(q_0, 10) = \delta(q_0, 0) \cup \delta(q_1, 0)$

$\hat{\delta}(q_0, 100) = \delta(q_0, 0) \cup \delta(q_2, 0)$

NEA A – akzeptierte Sprache

- *intuitiv:* Menge aller Eingabewörter, für die eine Berechnung vom Anfangszustand in einen akzeptierenden Zustand **existiert**



$\hat{\delta}(q_0, 100) = \{q_0, q_3\}$ ✓ $\qquad$ $\hat{\delta}(q_0, 000) = \{q_0\}$ ✗

- *formal:* $L(A) = \{\, w \mid \hat{\delta}(q_0, w) \cap F \neq \emptyset \,\}$

Äquivalenz von DEAs und NEAs

- Zwei Automaten A_1 und A_2 heißen **äquivalent**, wenn $L(A_1) = L(A_2)$.

- **Sprachfamilien:**
  - $\mathcal{L}$**(DEA)** $= \{ L \mid L = L(A)$ für einen DEA $A \}$
  - $\mathcal{L}$**(NEA)** $= \{ L \mid L = L(A)$ für einen NEA $A \}$

- **Satz 2.1:** Zu jedem DEA kann ein äquivalenter DEA konstruiert werden und umgekehrt. Somit gilt

$$\mathcal{L}(\text{DEA}) = \mathcal{L}(\text{NEA})\ .$$

Vom DEA zum NEA

- **Beweis:** Konstruktion eines NEA aus gegebenem DEA und umgekehrt:

- Jeder DEA ist ein spezieller NEA:
  - ➢ Der einzige Unterschied liegt in der Definition der Überführungsfunktion.

DEA		**NEA**
$\delta: (Q \times \Sigma) \rightarrow Q$		$\delta: (Q \times \Sigma) \rightarrow 2^Q$
$\delta(q, a) = q$	$\longrightarrow$	$\delta(q, a) = \{q\}$

Vom NEA zum DEA

- *Ziel:* Konstruktion eines *äquivalenten* DEA von einem NEA

- *Idee:*

$\hat{\delta}(q_0, \varepsilon) = \{q_0\}$

$\hat{\delta}(q_0, 10) = \{q_0, q_2\}$

$\hat{\delta}(q_0, 00) = \{q_0\}$

$\hat{\delta}(q_0, 100) = \{q_0, q_3\}$

Zustände

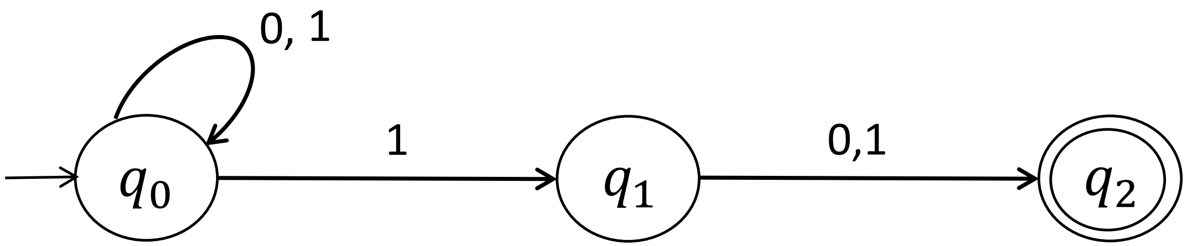
Startzustand: $\{q_0\}$

akzeptierend wenn ein Element aus F enthalten ist

Potenzmengenkonstruktion

- Sei $A = (Q, \Sigma, \delta, q_0, F)$ ein NEA.
- Konstruieren den DEA
$$A' = (Q', \Sigma, \delta', q_0', F')$$
- Schreiben die Zustände von A' als $[q_1, q_2, \ldots, q_i]$ (*statt* $\{q_1, q_2, \ldots, q_i\}$)
$Q' = \{ [q_1, q_2, \ldots, q_i] \mid \{q_1, q_2, \ldots, q_i\} \in 2^Q \}$
- $q_0' = [q_0]$
- $F' = \{ [q_1, q_2, \ldots, q_i] \mid \{q_1, q_2, \ldots, q_i\} \cap F \neq \emptyset \}$
- Für alle $\{q_1, q_2, \ldots, q_i\} \in 2^Q$ und alle $a \in \Sigma$:
$\delta'([q_1, q_2, \ldots, q_i], a) = [p_1, p_2, \ldots, p_j]$ gdw. $\bigcup_{1 \leq k \leq i} \delta(q_k, a) = \{p_1, p_2, \ldots, p_j\}$

Potenzmengenkonstruktion - Beispiel

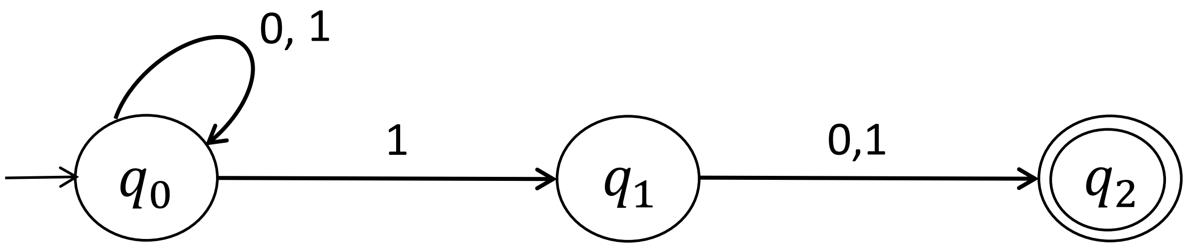


für $\{\, w1x \mid w \in \{0,1\}^*, x \in \{0,1\} \,\}$

- $Q' = \{\emptyset, [q_0], [q_1], [q_2], [q_0, q_1], [q_0, q_2], [q_1, q_2], [q_0, q_1, q_2]\}$
- $q_0' = [q_0]$
- $F' = \{[q_2], [q_0, q_2], [q_1, q_2], [q_0, q_1, q_2]\}$
- $$\begin{aligned} \delta'([q_0], 0) &= [q_0] & \delta'([q_0], 1) &= [q_0, q_1] \\ \delta'([q_0, q_1], 0) &= [q_0, q_2] & \delta'([q_0, q_1], 1) &= [q_0, q_1, q_2] \\ \delta'([q_0, q_2], 0) &= [q_0] & \delta'([q_0, q_2], 1) &= [q_0, q_1] \\ \delta'([q_0, q_1, q_2], 0) &= [q_0, q_2] & \delta'([q_0, q_1, q_2], 1) &= [q_0, q_1, q_2] \end{aligned}$$

  und $\delta(q, a) = \emptyset$ für alle anderen $q \in Q'$ und $a \in \{0,1\}$

Optimierte Potenzmengenkonstruktion

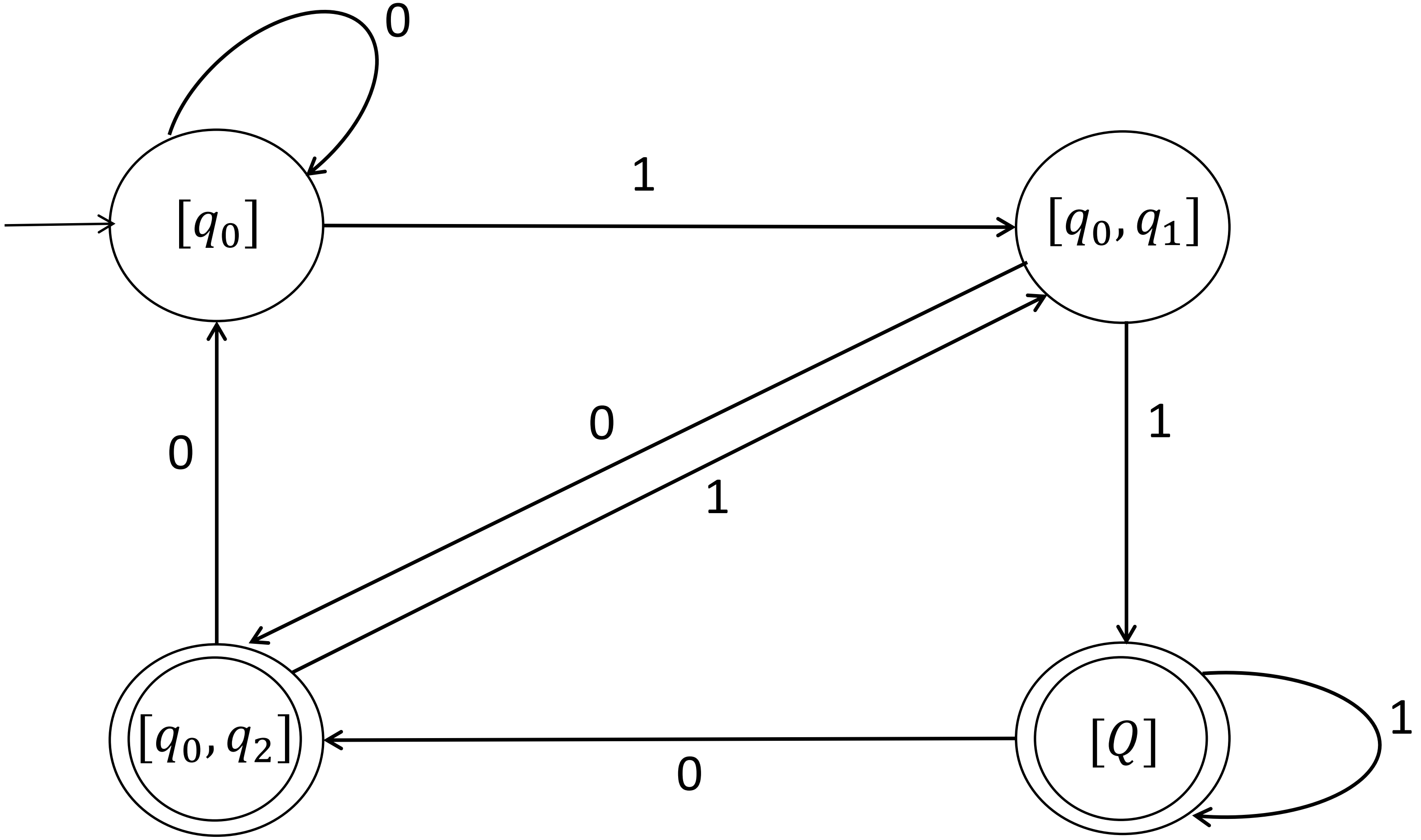


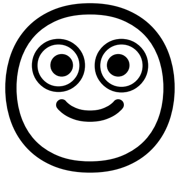
	$\rightarrow [q_0]$	$[q_0, q_1]$	$* [q_0, q_2]$	$* [q_0, q_1, q_2]$
0	$[q_0]$	$[q_0, q_2]$	$[q_0]$	$[q_0, q_2]$
1	$[q_0, q_1]$	$[q_0, q_1, q_2]$	$[q_0, q_1]$	$[q_0, q_1, q_2]$

***optimiert:** neue Tabellenspalten, wenn neue Zustände entstehen*

→ nur vier Zustände

Ergebnis vom Beispiel als Transitionsgraph





Recap: Potenzmengenkonstruktion

- Sei $A = (Q, \Sigma, \delta, q_0, F)$ ein NEA.
- Konstruieren den DEA
$$A' = (Q', \Sigma, \delta', q_0', F')$$
- Schreiben die Zustände von A' als $[q_1, q_2, \dots, q_i]$ (*statt* $\{q_1, q_2, \dots, q_i\}$)
$Q' = \{ [q_1, q_2, \dots, q_i] \mid \{q_1, q_2, \dots, q_i\} \in 2^Q \}$
- $q_0' = [q_0]$
- $F' = \{ [q_1, q_2, \dots, q_i] \mid \{q_1, q_2, \dots, q_i\} \cap F \neq \emptyset \}$
- Für alle $\{q_1, q_2, \dots, q_i\} \in 2^Q$ und alle $a \in \Sigma$:
$\delta'([q_1, q_2, \dots, q_i], a) = [p_1, p_2, \dots, p_j]$ gdw. $\bigcup_{1 \leq k \leq i} \delta(q_k, a) = \{p_1, p_2, \dots, p_j\}$

Potenzmengenkonstruktion - Korrektheit

- NEA $A = (Q, \Sigma, \delta, q_0, F)$ $\longrightarrow$ DEA $A' = (Q', \Sigma, \delta', q_0', F')$
- Induktion über die Länge des Eingabewortes w, dass
  $\widehat{\delta'}(q_0', w) = [q_1, q_2, \dots, q_i]$ gdw. $\hat{\delta}(q_0, w) = \{q_1, q_2, \dots, q_i\}$:
  - I.A. ($|w| = 0$): $\widehat{\delta'}(q_0', \varepsilon) = \hat{\delta}'([q_0], \varepsilon) = [q_0]$ und $\hat{\delta}(q_0, \varepsilon) = \{q_0\}$
  - I.V. ($|w| = n$): $\hat{\delta}'(q_0', w) = [p_1, p_2, \dots, p_j]$ gdw. $\hat{\delta}(q_0, w) = \{p_1, p_2, \dots, p_j\}$
  - I.S. (zu $|wa| = n + 1$):

    $\hat{\delta}'(q_0', wa) = [q_1, q_2, \dots, q_i]$ gdw. $\bigcup_{1 \leq k \leq j} \delta(p_k, a) = \{q_1, q_2, \dots, q_i\}$
- $\widehat{\delta'}(q_0', w) = [q_1, q_2, \dots, q_i] \in F'$ gdw. $\{q_1, q_2, \dots, q_i\} \cap F \neq \emptyset$

➢ $L(A') = L(A)$ ■