2.4 Minimierung von endlichen Automaten

Die Komplementierung eines endlichen Automaten, die u.a. in einigen Algorithmen wie dem Inklusionstest benötigt wird, setzt einen deterministischen Automaten voraus. Ist der Ausgangspunkt ein nichtdeterministischer endlicher Automat, so kann dieser zwar durch die Potenzmengenkonstruktion determinisiert werden, jedoch ist der resultierende DFA dann oftmals sehr viel größer als der ursprüngliche NFA, selbst dann, wenn man alle unerreichbaren Zustände des Potenzmengen-DFA entfernt. In diesem Abschnitt stellen wir ein Verfahren vor, wie man aus einem gegebenen DFA einen äquivalenten DFA minimaler Größe konstruieren kann. Der Algorithmus beruht auf dem Satz von Myhill & Nerode, der eine weitere Charakterisierung regulärer Sprachen angibt und der – abgesehen von der Minimierung von DFA – auch für andere Zwecke nützlich ist. So kann der Satz von Myhill & Nerode z.B. genutzt werden, um den Nachweis zu erbringen, dass eine gegebene Sprache nicht regulär ist, oder auch um untere Schranken für kleinste DFA für gegebene reguläre Sprache anzugeben.

Zunächst erinnern wir kurz an den Begriff einer *Äquivalenzrelation*. Sei X eine Menge. Eine Äquivalenzrelation auf X ist eine binäre Relation $\mathcal{R} \subseteq X \times X$, die folgende drei Eigenschaften besitzt:

Reflexivität:	$(x,x) \in \mathcal{R}$ für alle $x \in X$
Transitivität:	aus $(x,y) \in \mathcal{R}$ und $(y,z) \in \mathcal{R}$ folgt $(x,z) \in \mathcal{R}$
Symmetrie:	aus $(x,y) \in \mathcal{R}$ folgt $(y,x) \in \mathcal{R}$.

Für Äquivalenzrelationen wird oftmals eine Infixschreibweise benutzt, also $x\mathcal{R}y$ für $(x,y) \in \mathcal{R}$. Die Äquivalenzklasse eines Elements $x \in X$ ist $[x]_{\mathcal{R}} = \{y \in X : x\mathcal{R}y\}$. Es gilt $x\mathcal{R}y$ genau dann, wenn $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$ und genau dann, wenn $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \varnothing$. $X/\mathcal{R} = \big\{[x]_{\mathcal{R}} : x \in X\big\}$ bezeichnet den Quotientenraum, d.h., die Menge aller Äquivalenzklassen. Der *Index* von $\mathcal{R}$ bezeichnet die Anzahl an Äquivalenzklassen (möglicherweise ∞). Sind $\mathcal{R}_1$ und $\mathcal{R}_2$ Äquivalenzrelationen auf X mit $\mathcal{R}_1 \subseteq \mathcal{R}_2$, so wird $\mathcal{R}_1$ feiner als $\mathcal{R}_2$ und $\mathcal{R}_2$ gröber als $\mathcal{R}_1$ genannt.

Definition 2.33 (Nerode-Äquivalenz $\sim_L$, Nerode-Index). Sei $L \subseteq \Sigma^*$ eine Sprache. Die Nerodeäquivalenz für L bezeichnet diejenige Äquivalenzrelation $\sim_L$ auf Σ^*, so dass für alle Wörter x, $y \in \Sigma^*$ gilt:

$$x \sim_L y \quad \text{gdw} \quad \left\{ \begin{array}{l} \text{für alle } z \in \Sigma^* \text{ gilt:} \\ xz \in L \iff yz \in L \end{array} \right.$$

Wir schreiben $[x]_L$ für die Äquivalenzklasse von x bzgl. $\sim_L$. Es gilt also $[x]_L = \{y \in \Sigma^* : x \sim_L y\}$. Σ^*/L bezeichnet den Quotientenraum unter $\sim_L$ $[x]_L$ und Σ^*/L sind also lediglich eine Kurzschreibweisen für $[x]_{\sim_L}$ bzw. $\Sigma^*/\sim_L$. Der *Nerode-Index* von L bezeichnet den Index von $\sim_L$, also die Anzahl an Elementen im Quotientenraum Σ^*/L. ■

Man überzeugt sich leicht davon, dass $\sim_L$ tasächlich eine Äquivalenzrelation ist, also reflexiv, transitiv und symmetrisch.

Beispiel 2.34 (Nerode-Äquivalenz $\sim_L$). Wir betrachten die reguläre Sprache $L = \mathcal{L}(0^*1^*)$. Die Wörter 0^n mit $n \geqslant 0$ sind paarweise $\sim_L$-äquivalent, da $0^n z \in L$ genau dann, wenn $z \in \mathcal{L}(0^*1^*)$:

$$\varepsilon \sim_L 0 \sim_L 00 \sim_L 000 \sim_L \ldots,$$

Sämtliche Wörter $x \in \mathcal{L}(0^*)$ liegen also in derselben Äquivalenzklasse. Diese ist $\mathcal{L}(0^*)$. Entsprechend sind alle Wörter der Form 0^n1^m mit $n \geqslant 0$ und $m \geqslant 1$ paarweise $\sim_L$-äquivalent, da da $0^n1^mz \in L$ genau dann gilt, wenn $z \in \mathcal{L}(1^*)$. Also:

$$1 \sim_L 01 \sim_L 001 \sim_L \ldots,$$

Alle anderen Wörter $x \in \mathcal{L}(\,0^*1^+0(0+1)^*\,)$, also alle Wörter, in denen eine Eins vor einer Null steht, sind paarweise Nerode-äquivalent, da $xz \notin L$ für alle Wörter $z \in \{0,1\}^*$. Der Quotientenraum bzgl. $\sim_L$ ist also

$$\Sigma^*/L \;=\; \big\{\mathcal{L}(0^*), \mathcal{L}(0^*1^+), \mathcal{L}(0^*1^+(0+1)^*)\big\}.$$

Der Nerode-Index von L ist somit 3. ■

Satz 2.35 (Satz von Myhill & Nerode). *Sei L eine Sprache. L ist genau dann regulär, wenn der Nerode-Index von L endlich ist.*

Der Beweis von Satz 2.35 beruht auf mehreren Hilfsaussagen, die wir im Folgenden diskutieren werden. Der eigentliche Beweis wird dann auf Seite 64 geführt. Bevor wir auf die für den Satz von Myhill & Nerode zentralen Hilfsaussagen eingehen, überzeugen wir uns von der Aussage an zwei Beispielen. Für die reguläre Sprache $L = \mathcal{L}(0^*1^*)$ besteht Σ^*/L aus drei Elementen, siehe Beispiel 2.34 auf Seite 61. Der Nerode-Index von L ist also endlich (nämlich 3). Die Sprache

$$K \;=\; \{0^n1^n : n \geqslant 0\}$$

ist nicht regulär (siehe Seite 46). In der Tat sind die Wörter 0^n1^ℓ und 0^m1^k mit $0 \leqslant n \leqslant \ell$ und $0 \leqslant m \leqslant k$ und $n-\ell \neq m-k$ paarweise nicht Nerode-äquivalent bezüglich $\sim_K$. Es gilt nämlich

$$0^n1^\ell1^{n-\ell} = 0^n1^n \in K, \text{ aber } 0^m1^k1^{n-\ell} = 0^m1^{m+n-\ell} \notin K.$$

Somit ist der Quotientenraum $\{0,1\}^*/K$ und damit der Nerode-Index von K unendlich.

Der Beweis von Satz 2.35 benutzt einige Aussagen über die wie folgt definierte Äquivalenzrelation $\sim_{\mathcal{M}}$ für gegebenen DFA $\mathcal{M}$.

Definition 2.36 (DFA-Äquivalenz $\sim_{\mathcal{M}}$). Sei $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ ein DFA. Die Äquivalenzrelation $\sim_{\mathcal{M}} \subseteq \Sigma^* \times \Sigma^*$ ist wie folgt definiert:

$$x \sim_{\mathcal{M}} y \quad \text{gdw} \quad \delta(q_0, x) = \delta(q_0, y)$$

Dabei sind x, y beliebige Wörter über dem Alphabet Σ. $\Sigma^*/\mathcal{M}$ und $[x]_{\mathcal{M}}$ sind Kurzschreibweisen für den Quotientenraum $\Sigma^*/\sim_{\mathcal{M}}$ bzw. die Äquivalenzklasse $[x]_{\mathcal{M}}$. ■

Wir betrachten den DFA $\mathcal{M}$ aus Abbildung 22, der die Sprache $\mathcal{L}(0^*1^*)$ akzeptiert. Der Quotientenraum $\Sigma^*/\sim_{\mathcal{M}}$ besteht aus drei Äquivalenzklassen.

Lemma 2.37 (DFA-Äquivalenz hat endlichen Index). *Für jeden DFA $\mathcal{M}$ ist der Quotientenraum $\Sigma^*/\mathcal{M}$ endlich.*

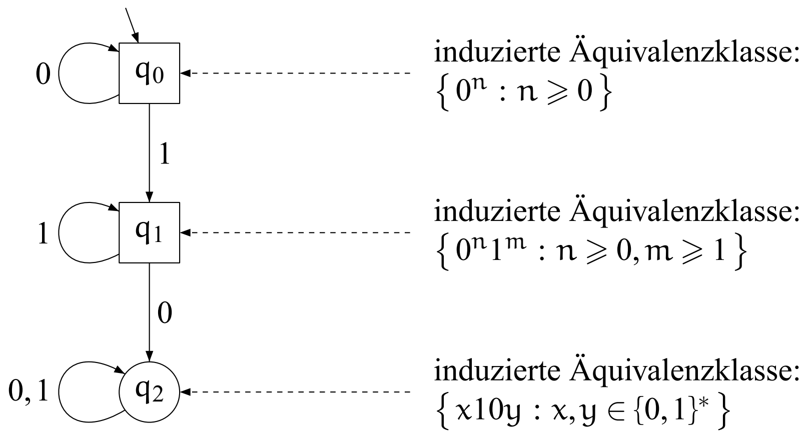


Abbildung 22: DFA $\mathcal{M}$ und die induzierten $\sim_{\mathcal{M}}$-Äquivalenzklassen

Beweis. Wir betrachten zunächst einen DFA $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ mit totaler Übergangsfunktion. Für jeden Zustand q sind die Wörter aus der Sprache

$$K_q \stackrel{\text{def}}{=} \{x \in \Sigma^* : \delta(q_0, x) = q\}$$

paarweise äquivalent bzgl. $\sim_{\mathcal{M}}$. Andererseits gilt $x \not\sim_{\mathcal{M}} y$ für $q \neq p$, $x \in K_q$, $y \in K_p$. Somit gilt $[x]_{\mathcal{M}} = K_q$, falls $\delta(q_0, x) = q$. Der Quotientenraum bzgl. $\sim_{\mathcal{M}}$ ist daher

$$\Sigma^*/\mathcal{M} \;=\; \{K_q : q \in Q\} \setminus \{\varnothing\}.$$

Also ist $|\Sigma^*/\mathcal{M}| \leqslant |Q| < \infty$. Insbesondere ist $|\Sigma^*/\mathcal{M}| = |Q'|$, wobei Q' die Menge der von q_0 erreichbaren Zustände ist.

Für DFA mit partieller Übergangsfunktion ist die Argumentation analog, jedoch muss (gedanklich) ein zusätzlicher Fangzustand eingefügt werden, der alle Wörter x mit $\delta(q_0, x) = \perp$ repräsentiert. Es ergibt sich dann $|\Sigma^*/\mathcal{M}| \leqslant |Q|+1 < \infty$. Insbesondere ist in diesem Falle $|\Sigma^*/\mathcal{M}| = |Q'|+1$, wenn Q' die Menge der von q_0 erreichbaren Zustände ist. $\square$

Lemma 2.38 (Zusammenhang $\sim_L$ und $\sim_{\mathcal{M}}$). *Sei* $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ *ein totaler DFA und* $L = \mathcal{L}(\mathcal{M})$. *Dann gilt:*

(a) $\sim_{\mathcal{M}}$ *ist feiner als* $\sim_L$*, d.h., für alle* $x, y \in \Sigma^*$ *mit* $x \sim_{\mathcal{M}} y$ *gilt* $x \sim_L y$.

(b) $|Q| \geqslant |\Sigma^*/\mathcal{M}| \geqslant |\Sigma^*/L|$.

Beweis. Wir zeigen zunächst Aussage (a). Es gelte $x \sim_{\mathcal{M}} y$. Weiter sei $z \in \Sigma^*$. Dann gilt:

$$\delta(q_0, xz) \;=\; \delta(\,\delta(q_0, x),\, z\,) \;=\; \delta(\,\delta(q_0, y),\, z\,) \;=\; \delta(q_0, yz)$$

Hieraus folgt:

$$\begin{aligned} xz \in L = \mathcal{L}(\mathcal{M}) \quad &\text{gdw} \quad \delta(q_0, xz) \in F \\ &\text{gdw} \quad \delta(q_0, yz) \in F \\ &\text{gdw} \quad yz \in \mathcal{L}(\mathcal{M}) = L \end{aligned}$$

Somit gilt $x \sim_L y$.

Nun zum Nachweis von Aussage (b). Da die Relation $\sim_{\mathcal{M}}$ stets eine Verfeinerung von $\sim_L$ (Aussage (a)) ist jede DFA-Äquivalenzklasse in (genau) einer Nerode-Äquivalenzklasse enthalten. Sei nun Q' die Menge aller vom Anfangszustand q_0 erreichbaren Zustände. Für $q \in Q'$ sei L_q diejenige Nerode-Äquivalenzklasse, welche die durch q induzierte DFA-Äquivalenzklasse

$$K_q = \{x \in \Sigma^* : \delta(q_0, x) = q\}$$

enthält. Also $K_q \subseteq L_q \in \Sigma^*/L$. Man beachte, dass $K_q \neq \varnothing$ für $q \in Q'$ und dass $L_q = L_p$ für $q \neq p$ möglich ist. Dann gilt:

$$\Sigma^*/L = \{L_q : q \in Q'\}.$$

Also ist $|\Sigma^*/L| \leqslant |Q'| = |\Sigma^*/\mathcal{M}| < \infty$ (siehe Lemma 2.37 auf Seite 62). □

Beweis von Satz 2.35 (Satz von Myhill & Nerode, Seite 62). Zu zeigen ist, dass eine gegebene Sprache L genau dann regulär ist, wenn der Nerode-Index von L (also die Anzahl an Äquivalenzklassen unter der Nerode-Äquivalenz $\sim_L$) endlich ist. Sei L regulär und $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ ein totaler DFA mit $\mathcal{L}(\mathcal{M}) = L$. Aus Lemma 2.38 (siehe Seite 63). folgt:

$$|\Sigma^*/L| \leqslant |\Sigma^*/\mathcal{M}| \leqslant |Q| < \infty$$

Wir nehmen nun an, dass L eine Sprache mit endlichem Nerode-Index ist. Wir zeigen, dass L regulär ist. Zunächst stellen wir fest, dass für alle $x, y \in \Sigma^*$ und $a \in \Sigma$ gilt:

(1) Aus $x \sim_L y$ folgt $xa \sim_L ya$.

Insbesondere ist $[xa]_L = [ya]_L$. Wir definieren einen DFA

$$\mathcal{M}_L \stackrel{\text{def}}{=} (Q_L, \Sigma, \delta_L, q_{0,L}, F_L),$$

dessen Zustände die Äquivalenzklassen bzgl. $\sim_L$ sind.

$$\begin{array}{rclcrcl} Q_L & = & \Sigma^*/L & \qquad & F_L & = & \{[x]_L : x \in L\} \\ q_{0,L} & = & [\varepsilon]_L & & \delta_L([x]_L, a) & = & [xa]_L \end{array}$$

Aussage (1) stellt die Wohldefiniertheit der Übergangsfunktion δ_L sicher. Ferner gilt für alle $x \in \Sigma^*$:

(2) $\delta_L([\varepsilon]_L, x) = [x]_L$

(3) $x \in L$ gdw $[x]_L \in F_L$

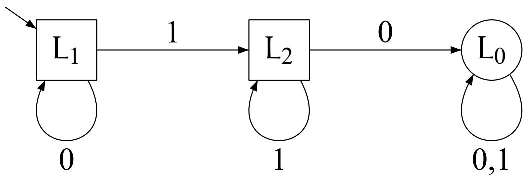
Aussage (2) kann durch Induktion nach der Länge von x gezeigt werden. Nun zum Nachweis von Aussage (3). Die Implikation "$\Longrightarrow$" ist klar, da F_L aus allen Äquivalenzklassen $[x]_L$ mit $x \in L$ besteht. Für den Nachweis der Implikation "$\Longleftarrow$" müssen wir die spezielle Form der Relation $\sim_L$ benutzen. Ist nämlich $[x]_L \in F_L$, dann gibt es ein $y \in L$, so dass $[y]_L = [x]_L$; also $x \sim_L y$. Wir betrachten nun das Wort $z = \varepsilon$ und erhalten $x = x\varepsilon = xz \in L$, da $yz = y\varepsilon = y \in L$. Damit ist Aussage (3) bewiesen. Aus (3) folgt:

$$\begin{aligned} x \in \mathcal{L}(\mathcal{M}_L) \quad &\text{gdw} \quad \delta_L([\varepsilon]_L, x) \in F_L \\ &\text{gdw} \quad [x]_L \in F_L \\ &\text{gdw} \quad x \in L \end{aligned}$$

Also ist $\mathcal{L}(\mathcal{M}_L) = L$ und L regulär. ■

Definition 2.39 (Minimalautomat $\mathcal{M}_L$). Sei L eine reguläre Sprache. Der im Beweis von Satz 2.35 konstruierte DFA für L wird *Minimalautomat* von L genannt und mit $\mathcal{M}_L$ bezeichnet. ■

Beispiel 2.40 (Minimalautomat). Der Minimalautomat für die Sprache $L = \mathcal{L}(0^*1^*) = \{0^n1^m : n, m \geqslant 0\}$ hat folgende Gestalt:



Dabei ist $L_1 = \mathcal{L}(0^*)$, $L_2 = \mathcal{L}(0^*11^*)$ und $L_0 = \{0,1\}^* \setminus (L_1 \cup L_2)$. ■

Teil (b) des folgenden Satzes 2.43 zeigt, dass die Anzahl der Zustände im Minimalautomaten minimal unter allen DFA für die betreffende Sprache ist (was die Bezeichnung „Minimalautomat" rechtfertigt). In Teil (a) zeigen wir die Eindeutigkeit des Minimalautomaten als DFA, für den die induzierte Äquivalenzrelation $\sim_{\mathcal{M}}$ mit $\sim_L$ übereinstimmt. Tatsächlich haben wir nur Eindeutigkeit "bis auf Isomorphie", d.h., Gleichheit bis auf eventuelles Umbenennen der Zustandsnamen. Auch wenn der Begriff der Isomorphie intuitiv klar ist, geben wir die präzise Definition von Isomorphie an.

Definition 2.41 (Isomorphie). Zwei DFA $\mathcal{M}_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$, $\mathcal{M}_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$ heißen *isomorph*, wenn es eine bijektive Abbildung $\varphi : Q_1 \to Q_2$ gibt, so dass $q_2 = \varphi(q_1)$, $F_2 = \varphi(F_1)$ und

$$\delta_2(\varphi(q), a) = \varphi(\delta_1(q, a)) \text{ für alle } q \in Q_1 \text{ und } a \in \Sigma$$

Die Abbildung φ wird *Isomorphismus* genannt. ■

DFA $\mathcal{M}_1$ und $\mathcal{M}_2$ sind also genau dann isomorph, wenn $\mathcal{M}_1$ und $\mathcal{M}_2$ bis auf die Namen der erreichbaren Zustände übereinstimmen. Intuitiv identifizieren wir isomorphe DFA, da die Zustandsnamen völlig irrelevant für die akzeptierte Sprache sind. Offensichtlich gilt folgendes Lemma:

Lemma 2.42 (Isomorphismus erhält die akzeptierte Sprache). *Sind $\mathcal{M}_1$ und $\mathcal{M}_2$ isomorphe DFA, so gilt $\mathcal{L}(\mathcal{M}_1) = \mathcal{L}(\mathcal{M}_2)$.*

Satz 2.43 (Eindeutigkeit und Minimalität des Minimalautomaten). *Für jede reguläre Sprache L gilt:*

(a) Der Minimalautomat $\mathcal{M}_L$ für L ist der bis auf Isomorphie eindeutig bestimmte DFA mit totaler Übergangsfunktion, der folgende drei Eigenschaften besitzt:

- $\mathcal{L}(\mathcal{M}_L) = L$
- $\sim_{\mathcal{M}_L} = \sim_L$
- *Jeder Zustand ist vom Anfangszustand erreichbar.*

(b) Ist $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ *ein totaler DFA mit* $\mathcal{L}(\mathcal{M}) = L$*, dann ist* $|Q| \geqslant |\Sigma^*/L|$.

Beweis. Teil (b) folgt sofort aus Lemma 2.38 (Seite 63). Wir zeigen Aussage (a). Zunächst ist klar, dass jeder Zustand in $\mathcal{M}_L$ vom Anfangszustand erreichbar ist. Dies folgt aus der Beobachtung:

$$\text{Ist } x \in \Sigma^*\text{, so ist } [x]_L = \delta_L([\varepsilon]_L, x).$$

Also ist jeder Zustand $[x]_L$ in $\mathcal{M}_L$ vom Anfangszustand $[\varepsilon]_L$ erreichbar. Die Aussage $\mathcal{L}(\mathcal{M}_L) = L$ wurde im Beweis von Satz 2.35 nachgewiesen. Nun zeigen wir, dass die Relationen $\sim_{\mathcal{M}_L}$ und $\sim_L$ übereinstimmen. Wegen Teil (a) von Lemma 2.38 (Seite 63) genügt es zu zeigen, dass $\sim_L$ eine Verfeinerung von $\sim_{\mathcal{M}_L}$ ist. Seien $x, y \in \Sigma^*$ und $x \sim_L y$. Es folgt:

$$\delta_L([\varepsilon]_L, x) = [x]_L = [y]_L = \delta_L([\varepsilon]_L, y)$$

Also ist $x \sim_{\mathcal{M}_L} y$. Es folgt, dass $\sim_L$ und $\sim_{\mathcal{M}_L}$ übereinstimmen.

Damit erfüllt $\mathcal{M}_L$ die drei genannten Eigenschaften.

Wir zeigen nun, dass jeder weitere DFA mit den genannten drei Eigenschaften zu $\mathcal{M}_L$ isomorph ist. Sei nun $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$ ein weiterer DFA mit $\mathcal{L}(\mathcal{M}) = L$, $\sim_{\mathcal{M}} = \sim_L$ und für den alle Zustände $q \in Q$ vom Anfangszustand q_0 erreichbar sind. Für jeden Zustand $q \in Q$ definieren wir die Sprache

$$K_q \stackrel{\text{def}}{=} \{x \in \Sigma^* : \delta(q_0, x) = q\}.$$

Dann ist K_q eine Äquivalenzklasse unter $\sim_{\mathcal{M}} = \sim_L$.[6] Also ist $K_q \in \Sigma^*/L$ ein Zustand im Minimalautomaten $\mathcal{M}_L$. Es ist leicht zu sehen, dass die Abbildung $\varphi : Q \to \Sigma^*/L$, $\varphi(q) = K_q$, ein Isomorphismus ist. □

Bemerkung 2.44 (Totale versus partielle Übergangsfunktion im Minimalautomaten). Die Übergangsfunktion des Minimalautomaten ist total. Unter allen DFA mit totaler Übergangsfunktion ist $\mathcal{M}_L$ minimal. Jedoch ist eine weitere Zustandsreduktion möglich, wenn man partielle Übergangsfunktionen zulässt. Sei

$$L_0 \stackrel{\text{def}}{=} \{ x \in \Sigma^* : xz \notin L \text{ für alle } z \in \Sigma^* \}.$$

Falls $L_0 \neq \varnothing$, so ist L_0 ein Zustand im Minimalautomaten, von dem aus kein Endzustand erreichbar ist. Daher können L_0 und alle zugehörigen Kanten entfernt werden. Der resultierende Automat ist nun minimal unter allen DFA $\mathcal{M}$ mit $\mathcal{L}(\mathcal{M}) = L$. Beispielsweise kann L_0 im Beispiel 2.40 aus dem Minimalautomaten $\mathcal{M}_L$ für die Sprache $L = \mathcal{L}(0^*1^*)$ eliminiert werden. ■

[6] Beachte: Äquivalenzklassen sind (per Definition) nicht leer. Für die Zustände q in $\mathcal{M}$ ist $K_q \neq \varnothing$, da q vom Anfangszustand q_0 erreichbar ist.