Automaten und Formale Sprachen
7. Vorlesung

Prof. Dr. Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Wintersemester 2022/23

Der Satz von Myhill und Nerode

Wir werden ein Verfahren von Myhill und Nerode kennenlernen, die Nicht-Regularität zu zeigen. (Im Gegensatz zum Pumping-Lemma kann es auch genutzt werden, die Regularität zu beweisen.)

Definition

Für eine Sprache $L \subseteq \Sigma^*$ und ein Wort $u \in \Sigma^*$ sei

$$u^{-1}L = \{v \in \Sigma^* \mid uv \in L\}$$

der Linksquotient von L bzgl. u. Wir werden die Menge der Linksquotienten von L mit LQ_L bezeichnen.

Beispiel

Gegeben sei die Sprache

$$L = \left\{ w \in \{a, b\}^* : |w|_a \text{ gerade} \right\}.$$

Für $u \in \{a, b\}^*$ gilt

$$\begin{aligned} u^{-1}L &= \{v \in \{a, b\}^* : |u\,v|_a \text{ gerade}\} \\ &= \begin{cases} L & \text{falls } |u|_a \text{ gerade} \\ \{a, b\}^* \setminus L & \text{falls } |u|_a \text{ ungerade} \end{cases} \end{aligned}$$

Die Sprache L hat nur zwei verschiedene Linksquotienten, die Menge LQ_L ist also endlich.

Beispiel

Gegeben sei die Sprache $L = \Sigma^*\{abc\}$ mit $\Sigma = \{a, b, c\}$.
Es gelten

- $\varepsilon^{-1}L = L$
- $a^{-1}L = \{w \in \Sigma^* \mid a\,w \in L\} = \{bc\} \cup L$
- $(ab)^{-1}L = \{w \in \Sigma^* \mid ab\,w \in L\} = \{c\} \cup L$
- $(abc)^{-1}L = \{w \in \Sigma^* \mid abc\,w \in L\} = \{\varepsilon\} \cup L$

Allgemeiner erhält man für alle $u \in \Sigma^*$:

$$u^{-1}L = \begin{cases} \{bc\} \cup L & \text{falls } u \in \Sigma^*\{a\} \\ \{c\} \cup L & \text{falls } u \in \Sigma^*\{ab\} \\ \{\varepsilon\} \cup L & \text{falls } u \in \Sigma^*\{abc\} \\ L & \text{sonst.} \end{cases}$$

Die Sprache L hat vier verschiedene Linksquotienten, die Menge LQ_L ist also wieder endlich.

Beispiel

Gegeben sei die Sprache

$$L = \{a^n\, b^n \mid n \in \mathbb{N}\}\,.$$

Für $u \in \{a, b\}^*$ gilt

$$u^{-1}L \;=\; \begin{cases} \{a^n b^{m+n} \mid n \in \mathbb{N}\} & \text{falls } u = a^m \text{ mit } m \in \mathbb{N} \\ \{b^n\} & \text{falls } u = a^{m+n}\, b^m \text{ mit } m, n \in \mathbb{N}, m > 0 \\ \emptyset & \text{sonst} \end{cases}$$

Diese Sprache hat unendlich viele verschiedene Linksquotienten, die Menge LQ_L ist also unendlich.

Lemma

Seien $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA, $L = L(M)$ und $u \in \Sigma^*$. Dann wird der Linksquotient $u^{-1}L$ von dem DFA

$$\big(Z, \Sigma, \widehat{\delta}(z_0, u), \delta, E\big)$$

akzeptiert.

Beweis: Für $w \in \Sigma^*$ gilt

$$\begin{aligned} w \in L\Big(\big(Z, \Sigma, \widehat{\delta}(z_0, u), \delta, E\big)\Big) \quad &\Longleftrightarrow \quad E \ni \widehat{\delta}\big(\widehat{\delta}(z_0, u), w\big) = \widehat{\delta}(z_0, uw) \\ &\Longleftrightarrow \quad uw \in L(M) = L \\ &\Longleftrightarrow \quad w \in u^{-1}L\,, \end{aligned}$$

d.h. wir haben die behauptete Gleichheit gezeigt. □

Folgerung

Sei $L \subseteq \Sigma^*$ regulär.

- L hat endlich viele Linksquotienten.
- Jeder Linksquotient von L ist regulär.
- Jeder DFA für L hat wenigstens $|\mathrm{LQ}_L|$ viele Zustände.

Beispiel (Fortsetzung von Folie 6.20)

Die Sprache $L = \{ab^\ell c^\ell \mid \ell \in \mathbb{N}\}$ ist nicht regulär, denn ihr Linksquotient $a^{-1}L = \{b^\ell c^\ell \mid \ell \in \mathbb{N}\}$ ist nicht regulär (siehe Beispiel auf Folie 6.13).

Es gilt sogar:

Satz von Myhill und Nerode

$$L \text{ regulär} \iff \mathrm{LQ}_L \text{ endlich.}$$

Die Implikation „$\Leftarrow$“ werden wir nicht beweisen.

Beispiel

$L = \{0^p \mid p \text{ ist eine Primzahl}\}$ ist nicht regulär.

Beweis: Es gibt Primzahlen $p_1 < q_1 < p_2 < q_2 < \cdots$, so daß gilt:

- zwischen p_i und q_i existiert keine Primzahl (f.a. $i \geq 1$)
- $q_i - p_i < q_j - p_j$ f.a. $1 \leq i < j$

Sei $1 \leq i < j$. Dann gelten

- $0^{p_i}\, 0^{q_i - p_i} = 0^{q_i} \in L$
- $0^{p_j}\, 0^{q_i - p_i}$ ist Wort der Länge $p_j + (q_i - p_i)$. Wegen $p_j < p_j + q_i - p_i < p_j + q_j - p_j = q_j$ ist dies keine Primzahl, also ist das Wort nicht in L.

Damit haben wir $\left(0^{p_i}\right)^{-1} L \neq \left(0^{p_j}\right)^{-1} L$, d.h. L hat unendlich viele Linksquotienten und ist somit nicht regulär. □

Der Minimalautomat

Eine reguläre Sprache kann von sehr verschiedenen DFAs akzeptiert werden. Unser Ziel ist es, einen möglichst kleinen zu bestimmen. Hierzu werden wir einen gegebenen DFA „verkleinern“, indem wir unerreichbare Zustände streichen und „ununterscheidbare“ „verschmelzen“.

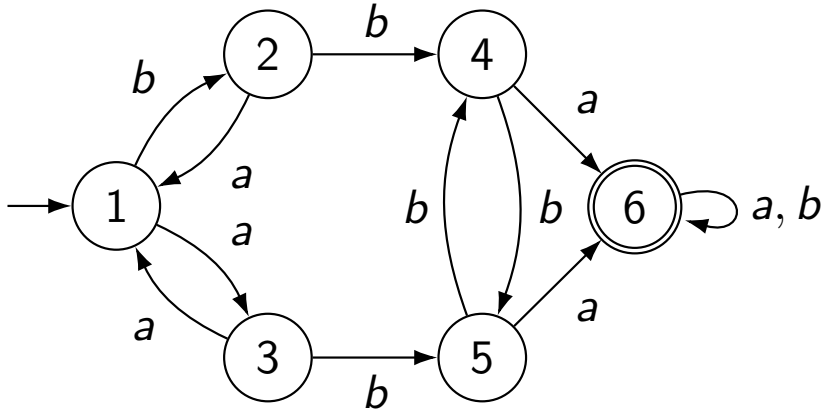
Die Streichung nicht erreichbarer Zustände ist trivial. Im Ergebnis erhält man einen „reduzierten“ DFA:

Definition

Ein DFA $M = (Z, \Sigma, z_0, \delta, E)$ heißt reduziert, wenn es für jeden Zustand $z \in Z$ ein Wort $w_z \in \Sigma^*$ gibt mit $\widehat{\delta}(z_0, w_z) = z$.

Beispiel

Betrachte die Zustände 4 und 5 im reduzierten DFA M:

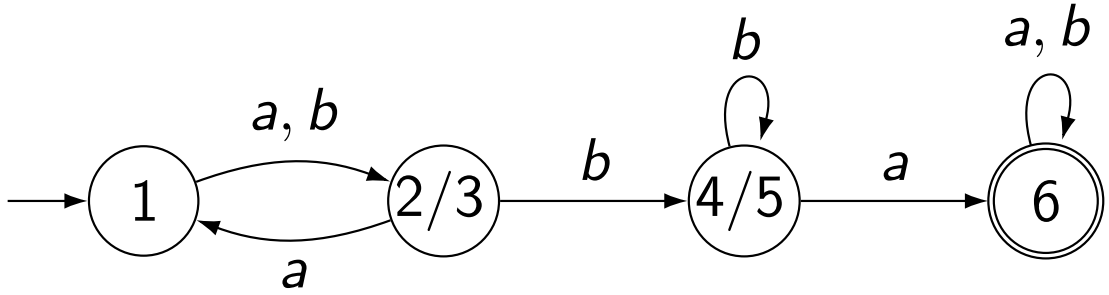


Feststellung:

- Mit einem Wort, das ein a enthält, landet man von dort aus immer im Zustand 6 (Endzustand).
- Mit einem Wort, das kein a enthält, landet man von dort aus immer im Zustand 5 bzw. 4 (kein Endzustand).

Der DFA M mit Startzustand 4 und der mit Startzustand 5 akzeptieren also dieselbe Sprache. Wir nennen die Zustände 4 und 5 daher „erkennungsäquivalent“ und werden sie „verschmelzen“ (analog für 2 und 3).

Entstehender DFA $M_{\equiv}$ (nach der Verschmelzung):



Jetzt sind keine Zustände mehr erkennungsäquivalent, und es können daher keine weiteren verschmolzen werden.

Es gilt:

- M und $M_{\equiv}$ akzeptieren dieselbe Sprache: $L(M) = L(M_{\equiv})$.
- Jeder DFA N mit vier Zuständen, der $L(M)$ akzeptiert, sieht so aus wie $M_{\equiv}$ (bis auf die Benennung der Zustände).
- Es gibt keinen DFA N mit < 4 Zuständen, der $L(M)$ akzeptiert.

Frage

Wirklich? Geht das vielleicht immer?

Definition

Sei $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA und $z \in Z$. Dann schreiben wir M_z für den DFA $(Z, \Sigma, z, \delta, E)$.

Definition

Sei $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA.

Zwei Zustände $z, z' \in Z$ heißen erkennungsäquivalent (in Zeichen: $z \equiv z'$), wenn die DFAs M_z und $M_{z'}$ dieselbe Sprache akzeptieren, d.h. wenn $L(M_z) = L(M_{z'})$ gilt.

Beobachtung

$z \equiv z'$ gilt genau dann, wenn für alle $w \in \Sigma^*$ gilt

$$\widehat{\delta}(z, w) \in E \iff \widehat{\delta}(z', w) \in E\,.$$

Lemma

Sei $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA, $z, z' \in Z$ und $a \in \Sigma$.

1. $\equiv$ ist eine Äquivalenzrelation auf Z.
2. $z \equiv z'$ impliziert $(z \in E \iff z' \in E)$.
3. $z \equiv z'$ impliziert $\delta(z, a) \equiv \delta(z', a)$.

Beweis:

1. klar
2. $z \in E \iff \varepsilon \in L(M_z) \iff \varepsilon \in L(M_{z'}) \iff z' \in E$
3. Sei $w \in \Sigma^*$ beliebig.

$$\begin{aligned} w \in L(M_{\delta(z,a)}) &\iff E \ni \widehat{\delta}\big(\delta(z,a), w\big) = \widehat{\delta}(z, aw) \\ &\iff aw \in L(M_z) = L(M_{z'}) \\ &\iff E \ni \widehat{\delta}(z', aw) = \widehat{\delta}\big(\delta(z',a), w\big) \\ &\iff w \in L\big(M_{\delta(z',a)}\big)\,. \end{aligned}$$

Also gilt $L(M_{\delta(z,a)}) = L(M_{\delta(z',a)})$, d.h. $\delta(z, a) \equiv \delta(z', a)$. □

Erinnerung

Sei $\equiv$ eine Äquivalenzrelation auf einer Menge Z. Für $z \in Z$ ist die Äquivalenzklasse von z die Menge

$$[z] = \{z' \in Z \mid z \equiv z'\}.$$

Der Quotient von Z bzgl. $\equiv$ ist die Menge aller Äquivalenzklassen

$$Z/_{\equiv} = \left\{[z] \;\middle|\; z \in Z\right\}.$$

Definition

Sei $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA. Dann ist $M_{\equiv} = (Z/_{\equiv}, \Sigma, [z_0], \delta_{\equiv}, E_{\equiv})$ mit

- $\delta_{\equiv}\big([z], a\big) = \big[\delta(z, a)\big]$ für $z \in Z$ und $a \in \Sigma$ und
- $E_{\equiv} = \big\{[z] \;\big|\; z \in E\big\}$

der Quotient von M bzgl. $\equiv$.

Beispiel: Der Quotient des DFA auf Folie 7.10 ist auf Folie 7.11 abgebildet.

Bemerkung

$\delta_{\equiv}$ ist wohldefiniert, d.h. $M_{\equiv}$ ist ein DFA.

Beweis:

seien $z, z' \in Z$ mit $[z] = [z'] \implies z \equiv z'$

$\implies \delta(z, a) \equiv \delta(z', a)$ (nach Lemma auf Folie 7.13)

$\implies \big[\delta(z, a)\big] = \big[\delta(z', a)\big]$ □

Lemma

Sei $M = (Z, \Sigma, z_0, \delta, E)$ ein DFA und $M_{\equiv} = (Z/\equiv, \Sigma, [z_0], \delta_{\equiv}, E_{\equiv})$ sein Quotient. Dann gilt $L(M) = L(M_{\equiv})$.

Beweis:

Behauptung: Für alle Wörter $w \in \Sigma^*$ gilt $\big[\widehat{\delta}(z_0, w)\big] = \widehat{\delta_{\equiv}}\big([z_0], w\big)$,

denn

$$
\begin{aligned}
\big[\widehat{\delta}(z_0, \varepsilon)\big] &= [z_0] = \widehat{\delta_{\equiv}}\big([z_0], \varepsilon\big) \\
\big[\widehat{\delta}(z_0, wa)\big] &= \Big[\delta\big(\widehat{\delta}(z_0, w), a\big)\Big] \\
&= \delta_{\equiv}\Big(\big[\widehat{\delta}(z_0, w)\big], a\Big) \overset{\text{IV}}{=} \delta_{\equiv}\Big(\widehat{\delta_{\equiv}}\big([z_0], w\big), a\Big) \\
&= \widehat{\delta_{\equiv}}\big([z_0], wa\big)
\end{aligned}
$$

q.e.d.

Damit erhalten wir für alle Wörter w

$$
\begin{aligned}
w \in L(M) &\iff \widehat{\delta}(z_0, w) \in E \iff \big[\widehat{\delta}(z_0, w)\big] \in E_{\equiv} \\
&\overset{\text{Beh.}}{\iff} \widehat{\delta_{\equiv}}\big([z_0], w\big) \in E_{\equiv} \iff w \in L(M_{\equiv})
\end{aligned}
$$

□

Damit ist $M_{\equiv}$ „ein kleiner DFA“ für die Sprache $L(M)$. Wir werden zeigen, daß es keinen kleineren gibt und daß jeder DFA dieser Größe für $L(M)$ „so aussieht wie $M_{\equiv}$“, d.h. „sich nur in der Bezeichnung der Zustände unterscheidet“ oder „isomorph ist“:

Definition

Seien $M = (Z_M, \Sigma, \iota_M, \delta_M, E_M)$ und $N = (Z_N, \Sigma, \iota_N, \delta_N, E_N)$ DFAs. Sie heißen isomorph (in Zeichen: $M \cong N$), wenn es eine Abbildung $f : Z_M \to Z_N$ gibt mit

- $f(\iota_M) = \iota_N$,
- $f\big(\delta_M(z, a)\big) = \delta_N\big(f(z), a\big)$ für alle $z \in Z_M$ und $a \in \Sigma$,
- $z \in E_M \iff f(z) \in E_N$ für alle $z \in Z_M$,
- f ist surjektiv und
- f ist injektiv.

Definition

Sei M ein DFA. Seine Erkennungsäquivalenz $\equiv$ ist trivial, wenn für alle Zustände z und z' gilt

$$z \equiv z' \implies z = z' .$$

Beobachtung

Sei M DFA. Dann gilt

$$M \text{ hat triviale Erkennungsäquivalenz} \iff M \cong M_{\equiv} .$$

DFAs mit trivialer Erkennungsäquivalenz werden durch die Quotientenbildung also nicht weiter verkleinert.

Das folgende Lemma zeigt daher insbesondere, daß die wiederholte Anwendung der Quotientenbildung keine weitere Verkleinerung bringt.

Lemma

Sei M ein reduzierter DFA und $N = M_{\equiv}$ sein Quotient. Dann hat N eine triviale Erkennungsäquivalenz.

Beweis: Wir schreiben $\equiv_M$ bzw. $\equiv_N$ für die Erkennungsäquivalenzen von $M = (Z_M, \Sigma, \iota_M, \delta_M, E_M)$ bzw. $N = (Z_N, \Sigma, \iota_N, \delta_N, E_N)$.
Seien $[z], [z'] \in Z_N = Z/\equiv_M$ Zustände von N mit $[z] \equiv_N [z']$. Dann gilt

$$
\begin{aligned}
& \forall w \in \Sigma^* \colon \delta_N\big([z], w\big) \in E_N \iff \delta_N\big([z'], w\big) \in E_N \\
\Rightarrow\ & \forall w \in \Sigma^* \colon \big[\delta_M(z, w)\big] \in E_N \iff \big[\delta_M(z', w)\big] \in E_N \\
\overset{(*)}{\Rightarrow}\ & \forall w \in \Sigma^* \colon \delta_M(z, w) \in E_M \iff \delta_M(z', w) \in E_M \\
\Rightarrow\ & z \equiv_M z' \\
\Rightarrow\ & [z] = [z'] \,.
\end{aligned}
$$

$(*)$ nach dem Lemma auf Folie 7.13 □

Während es für eine reguläre Sprache L sehr viele verschiedene DFAs geben kann, gibt es nur einen reduzieren DFA mit trivialer Erkennungsäquivalenz:

Lemma

Seien M und N reduzierte DFAs mit trivialer Erkennungsäquivalenz und gelte $L(M) = L(N)$. Dann gilt $M \cong N$.

Beweis: Wir schreiben $\equiv_M$ bzw. $\equiv_N$ für die Erkennungsäquivalenzen von $M = (Z_M, \Sigma, \iota_M, \delta_M, E_M)$ bzw. $N = (Z_N, \Sigma, \iota_N, \delta_N, E_N)$.

Als erstes definieren wir eine Abbildung $f : Z_M \to Z_N$:

Sei $z \in Z_M$. Da M reduziert ist, existiert ein Wort $w_z \in \Sigma^*$ mit $\widehat{\delta_M}(\iota_M, w_z) = z$. Setze $f(z) = \widehat{\delta_N}(\iota_N, w_z)$.

Wir werden zeigen, daß diese Abbildung f ein Isomorphismus ist.

Zunächst zeigen wir aber folgendes:

Behauptung Für alle $u, v \in \Sigma^*$ gilt

$$\widehat{\delta_M}(\iota_M, u) = \widehat{\delta_M}(\iota_M, v) \iff \widehat{\delta_N}(\iota_N, u) = \widehat{\delta_N}(\iota_N, v)$$

Begründung Sei $w \in \Sigma^*$ beliebig.

$$\begin{aligned}
\widehat{\delta_N}\big(\widehat{\delta_N}(\iota_N, u), w\big) \in E_N \quad &\iff \quad uw \in L(N) \\
&\iff \quad uw \in L(M) \\
&\iff \quad \widehat{\delta_M}\big(\widehat{\delta_M}(\iota_M, u), w\big) \in E_M \\
&\iff \quad \widehat{\delta_M}\big(\widehat{\delta_M}(\iota_M, v), w\big) \in E_M \\
&\iff \quad \widehat{\delta_N}\big(\widehat{\delta_N}(\iota_N, v), w\big) \in E_N\,.
\end{aligned}$$

Da dies für alle $w \in \Sigma^*$ gilt, erhalten wir $\widehat{\delta_N}(\iota_N, u) \equiv_N \widehat{\delta_N}(\iota_N, v)$. Da die Erkennungsäquivalenz von N trivial ist, folgt $\widehat{\delta_N}(\iota_N, u) = \widehat{\delta_N}(\iota_N, v)$.

Aus Symmetriegründen haben wir also die Behauptung gezeigt. **q.e.d.**

- Wir haben $\widehat{\delta_M}(\iota_M, w_{\iota_M}) = \iota_M = \widehat{\delta_M}(\iota_M, \varepsilon)$ und daher

$$f(\iota_M) = \widehat{\delta_N}(\iota_N, w_{\iota_M}) \overset{\text{Beh.}}{=} \widehat{\delta_N}(\iota_N, \varepsilon) = \iota_N$$

- Seien $z \in Z_M$ und $a \in \Sigma$. Betrachte $\overline{z} = \widehat{\delta_M}(\iota_M, w_z\, a)$ und das Wort $w_{\overline{z}}$. Dann gilt $\widehat{\delta_M}(\iota_M, w_z a) = \overline{z} = \widehat{\delta_M}(\iota_M, w_{\overline{z}})$. Damit ergibt sich

$$\begin{aligned}
f\big(\delta_M(z,a)\big) &= f\Big(\widehat{\delta_M}(\iota_M, w_z\, a)\Big) \\
&= f\Big(\widehat{\delta_M}(\iota_M, w_{\overline{z}})\Big) \\
&= \widehat{\delta_N}\big(\iota_N, w_{\overline{z}}\big) \\
&\overset{\text{Beh.}}{=} \widehat{\delta_N}(\iota_N, w_z\, a) \\
&= \delta_N\Big(\widehat{\delta_N}(\iota_N, w_z), a\Big) \\
&= \delta_N\big(f(z), a\big)
\end{aligned}$$

- Für $z \in Z_M$ erhalten wir

$$\begin{aligned} z \in E_M &\iff w_z \in L(M) \\ &\iff w_z \in L(N) \\ &\iff \widehat{\delta_N}(\iota_N, w_z) \in E_N \\ &\iff f(z) \in E_N \end{aligned}$$

- Injektivität von f: Für $z_1, z_2 \in E_M$ erhalten wir

$$\begin{aligned} f(z_1) = f(z_2) &\Rightarrow \widehat{\delta_N}(\iota_N, w_{z_1}) = \widehat{\delta_N}(\iota_N, w_{z_2}) \\ &\overset{\text{Beh.}}{\Rightarrow} \widehat{\delta_M}(\iota_M, w_{z_1}) = \widehat{\delta_M}(\iota_M, w_{z_2}) \\ &\Rightarrow z_1 = z_2 \end{aligned}$$

- Surjektivität von f: Sei $z_N \in Z_N$. Da N reduziert ist, existiert $w \in \Sigma^*$ mit $\widehat{\delta_N}(\iota_N, w) = z_N$. Setze $z := \widehat{\delta_M}(\iota_M, w)$. Dann gilt

$$\widehat{\delta_M}(\iota_M, w) = z = \widehat{\delta_M}(\iota_M, w_z)\,.$$

Wir erhalten

$$\begin{aligned} f(z) &= \widehat{\delta_N}(\iota_N, w_z) \\ &\overset{\text{Beh.}}{=} \widehat{\delta_N}(\iota_N, w) \\ &= z_N\,. \end{aligned}$$

□

Satz

Sei M ein reduzierter DFA und $L = L(M)$. Sei $N = M_{\equiv}$ der Quotient von M und sei n die Anzahl der Zustände von N. Dann gelten

1. $L(N) = L$,
2. jeder DFA für L hat $\geq n$ Zustände und
3. ist N' DFA mit n Zuständen und $L(N') = L$, so gilt $N \cong N'$.

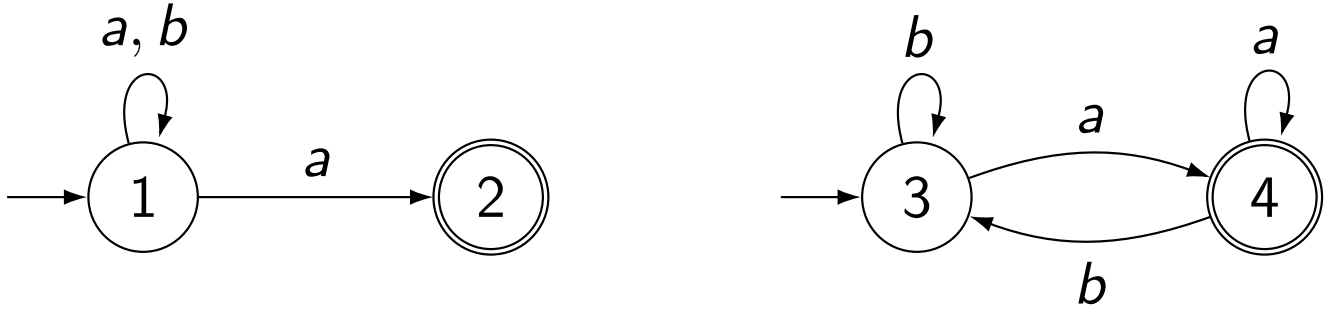
Beweis:

1. Lemma auf Folie 7.16
2. Sei N' DFA mit $L(N') = L$ und seien n' und $n'_{\equiv}$ die Anzahl der Zustände von N' bzw. $N'_{\equiv}$.
   $\Longrightarrow$ N und $N'_{\equiv}$ haben triviale Erkennungsäquivalenz und akzeptieren L (Folien 7.19 und 7.16)
   $\Longrightarrow$ $N \cong N'_{\equiv}$ (Folie 7.20)
   $\Longrightarrow$ $n = n'_{\equiv} \leq n'$.
3. Gilt $n = n'$, so folgt $n'_{\equiv} = n'$ und damit $N' \cong N'_{\equiv} \cong N$. □

Für nicht-deterministische Automaten kann man folgende Aussagen treffen:

- Es gibt nicht den minimalen NFA, sondern es kann mehrere geben.

  Folgende zwei NFAs minimaler Größe akzeptieren die Sprache $L = L\big((a+b)^*a\big)$ und haben beide zwei Zustände (mit nur einem Zustand kann L nicht akzeptiert werden).



- Gegeben ein DFA M. Dann hat ein minimaler NFA, der $L(M)$ erkennt, immer höchstens so viel Zustände wie M, denn M selbst ist schon ein NFA.

  Außerdem kann ein minimaler NFA exponentiell kleiner sein als der minimale DFA.
  Beispiel hierfür $L_k = \{0,1\}^* \{0\} \{0,1\}^{k-1}$.

Zusammenfassung 7. Vorlesung

in dieser Vorlesung neu

- Satz von Myhill und Nerode: eine weitere notwendige Bedingung für die Regularität einer Sprache (diese Bedingung ist auch hinreichend)
- für jeden reduzierten DFA M ist $M_{\equiv}$ **der** minimale DFA für $L(M)$

kommende Vorlesung

- Algorithmus für die Berechnung des Quotienten $M_{\equiv}$
- Algorithmen für Leerheits- u.a. Probleme für reguläre Sprachen
- Anwendung dieser Algorithmen für die Verifikation von Protokollen