Automaten und Formale Sprachen
7. Vorlesung

Prof. Dr. Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Wintersemester 2023/24

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

$$M_z = \big(Z, \Sigma, z, \delta, E\big)$$

akzeptiert.

Beweis: Für $w \in \Sigma^*$ gilt

$$\begin{aligned} w \in L(M_z) &\iff E \ni \widehat{\delta}(z, w) = \widehat{\delta}\big(\widehat{\delta}(z_0, u), w\big) = \widehat{\delta}(z_0, uw) \\ &\iff uw \in L(M) = L \\ &\iff w \in u^{-1}L\,, \end{aligned}$$

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).

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 $p^{q_i - p_i} \in \left(0^{p_i}\right)^{-1} L \setminus \left(0^{p_j}\right)^{-1} L$, und damit $\left(0^{p_i}\right)^{-1} L \neq \left(0^{p_j}\right)^{-1} L$, d.h. L hat unendlich viele Linksquotienten und ist somit nicht regulär. □

Satz von Myhill und Nerode

Für $L \subseteq \Sigma^*$ gilt

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

Beweis: „$\Rightarrow$“: Lemma auf vorheriger Folie

„$\Leftarrow$“: Sei LQ_L endlich. Konstruiere DFA $\mathrm{MN}_L = (Z_{\mathrm{MN}}, \Sigma, \iota_{\mathrm{MN}}, \delta_{\mathrm{MN}}, E_{\mathrm{MN}})$ wie folgt:

$$\begin{aligned} Z_{\mathrm{MN}} &= \mathrm{LQ}_L & \qquad \delta_{\mathrm{MN}}(K, a) &= a^{-1}K \\ \iota_{\mathrm{MN}} &= \varepsilon^{-1}L = L & \qquad E_{\mathrm{MN}} &= \{K \in \mathrm{LQ}_L \mid \varepsilon \in K\} \end{aligned}$$

Behauptung 1: Die Funktion $\delta_{\mathrm{MN}} \colon Z_{\mathrm{MN}} \times \Sigma \to Z_{\mathrm{MN}}$ ist wohldefiniert,
denn: Seien $K \in Z_{\mathrm{MN}} = \mathrm{LQ}_L$ und $a \in \Sigma$. Dann existiert $u \in \Sigma^*$ mit $K = u^{-1}L$. Damit erhalten wir

$$a^{-1}K = a^{-1}(u^{-1}L) = (ua)^{-1}L \in \mathrm{LQ}_L = Z_{\mathrm{MN}}\,.$$

q.e.d.

Behauptung 2: Für $u \in \Sigma^*$ gilt $\widehat{\delta_{\mathrm{MN}}}(\iota_{\mathrm{MN}}, u) = u^{-1}L$.
denn (per Induktion über $|u|$):

IA $\widehat{\delta_{\mathrm{MN}}}(\iota_{\mathrm{MN}}, \varepsilon) = \iota_{\mathrm{MN}} = L = \varepsilon^{-1}L$

IS Für $u \in \Sigma^*$ und $a \in \Sigma$ erhalten wir

$$\begin{aligned}
\widehat{\delta_{\mathrm{MN}}}(\iota_{\mathrm{MN}}, ua) &= \delta_{\mathrm{MN}}\big(\widehat{\delta_{\mathrm{MN}}}(\iota_{\mathrm{MN}}, u), a\big) \\
&\overset{IV}{=} \delta_{\mathrm{MN}}(u^{-1}L, a) \\
&= a^{-1}(u^{-1}L) = (ua)^{-1}L
\end{aligned}$$

q.e.d.

Damit erhalten wir für alle $u \in \Sigma^*$:

$$\begin{aligned}
u \in L(\mathrm{MN}_L) &\iff \widehat{\delta_{\mathrm{MN}}}(\iota_{\mathrm{MN}}, u) \in E_{\mathrm{MN}} \\
&\overset{\text{Beh. 2}}{\iff} u^{-1}L \in E_{\mathrm{MN}} \\
&\iff \varepsilon \in u^{-1}L \\
&\iff u \in L\,.
\end{aligned}$$

Es gilt also $L = L(\mathrm{MN}_L)$, die Sprache L ist also regulär. □

Zwischenzusammenfassung

Sei $L \subseteq \Sigma^*$ regulär. Dann

- hat jeder DFA für L wenigstens $|\mathrm{LQ}_L|$ viele Zustände und
- der DFA MN_L aus dem obigen Beweis akzeptiert L und hat genau $|\mathrm{LQ}_L|$ viele Zustände, hat also die minimale mögliche Größe.

Aber wie kann man den DFA MN_L berechnen?

Wir werden jetzt zeigen, wie MN_L aus einem beliebigen DFA M für L konstruiert werden kann. Hierfür werden wir M „minimieren“.

Der Minimalautomat

Wir werden den gegebenen DFA M „minimieren“ (oder zumindest „verkleinern“), indem wir unerreichbare Zustände streichen und „ununterscheidbare“ „verschmelzen“.

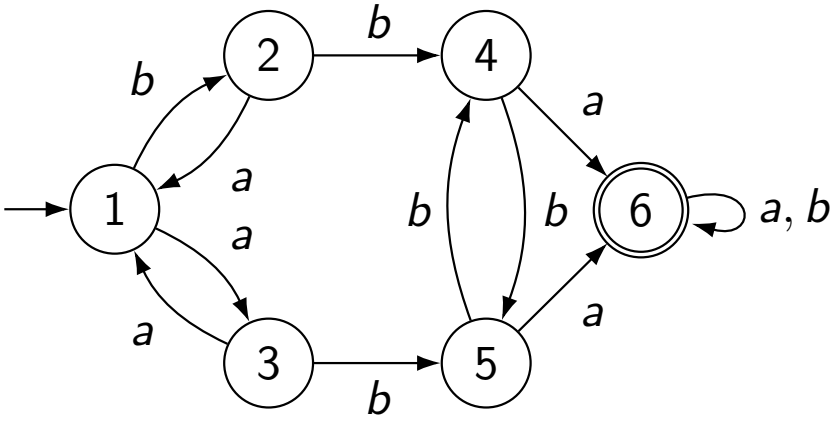
Die Streichung nicht erreichbarer Zustände ist trivial. Im Ergebnis erhält man einen „reduzierten“ DFA:

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:

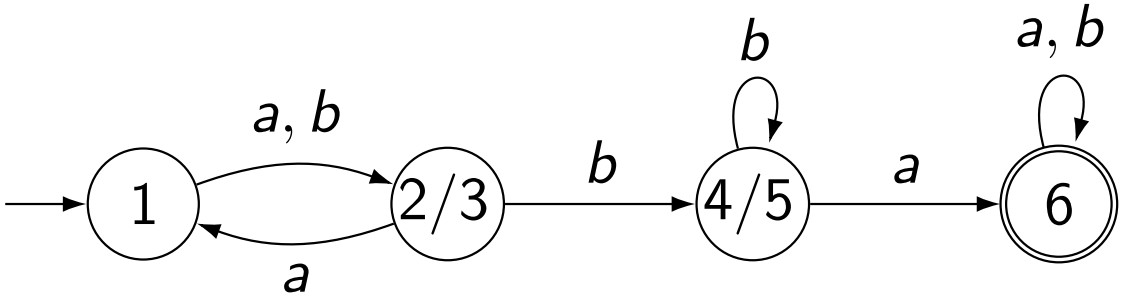


Feststellung:

- 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?

Erinnerung

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.

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

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

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

Definition

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

- $Z_{\equiv} = Z/_{\equiv}$,
- $\delta_{\equiv}\big([z], a\big) = \big[\delta(z, a)\big]$ 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 7.13 ist auf Folie 7.14 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 7.16)

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

Sei M ein reduzierter DFA und $L = L(M)$.
Wir wissen, daß der DFA MN_L „ein kleinstmöglicher DFA“ für die Sprache L ist. Wir werden zeigen, daß der Quotient $M_{\equiv}$ „so aussieht wie MN_L“, 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.

Lemma

Sei $M = (Z, \Sigma, \iota, \delta, E)$ ein reduzierter DFA und $L = L(M)$. Seien

- $M_\equiv = (Z_\equiv, \Sigma, \iota_\equiv, \delta_\equiv, E_\equiv)$ sein Quotient und
- $\mathrm{MN}_L = (Z_{\mathrm{MN}}, \Sigma, \iota_{\mathrm{MN}}, \delta_{\mathrm{MN}}, E_{\mathrm{MN}})$ der DFA aus dem Beweis des Satzes auf Folie 7.9.

Dann sind $M_\equiv$ und MN_L isomorph.

Beweis:

Für $u, v \in \Sigma^*$ mit $u^{-1}L = v^{-1}L$ gilt

$$L(M_{\widehat{\delta}(\iota,u)}) = u^{-1}L = v^{-1}L = L(M_{\widehat{\delta}(\iota,v)})$$

und daher $\widehat{\delta}(\iota, u) \equiv \widehat{\delta}(\iota, v)$. Also ist die Abbildung
$f : Z_{\mathrm{MN}} = \mathrm{LQ}_L \to Z/_\equiv = Z_\equiv$ mit

$$f(u^{-1}L) = \left[\widehat{\delta}(\iota, u)\right]$$

wohldefiniert. Man zeigt nun, daß sie ein Isomorphismus von MN_L auf $M_\equiv$ ist. (Zusatzmaterial auf Folien 7.24 ff.) □

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:

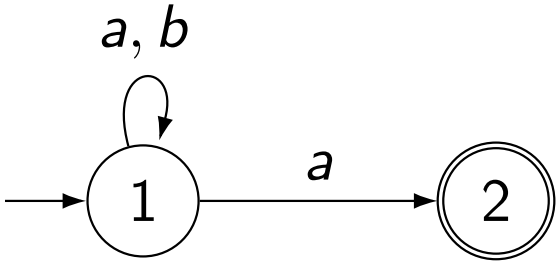
1. Es gelten $N \cong \mathrm{MN}_L$ und $L(\mathrm{MN}_L) = L$.
2. Sei N' DFA mit $L(N') = L$ und n' Zuständen.
   $\Longrightarrow N'/_{\equiv} \cong \mathrm{MN}_L \cong M/_{\equiv} = N$ hat n Zustände
   $\Longrightarrow n' \geq n$
3. Sei N' DFA mit $L(N') = L$ und n Zuständen.
   $\Longrightarrow N'/_{\equiv} \cong \mathrm{MN}_L \cong M/_{\equiv} = N$ hat ebenfalls n Zustände
   $\Longrightarrow N' \cong N'/_{\equiv}$, also $N' \cong N$.

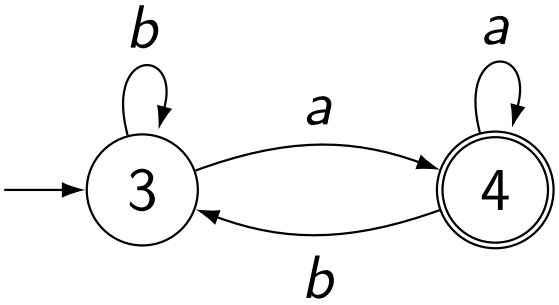
□

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

Zusatzmaterial

- $f(\iota_{\mathrm{MN}}) = f(\varepsilon^{-1}L) = \left[\widehat{\delta}(\iota, \varepsilon)\right] = [\iota] = \iota_{\equiv}$
- Sei $K \in Z_{\mathrm{MN}} = \mathrm{LQ}_L$ und $a \in \Sigma$. Dann existiert $u \in \Sigma^*$ mit $K = u^{-1}L$ und es gilt

$$\begin{aligned} f\big(\delta(K,a)\big) = f\big(\delta(u^{-1}L,a)\big) &= f\big(a^{-1}(u^{-1}L)\big) = f\big((ua)^{-1}L\big) \\ &= \left[\widehat{\delta}(\iota, ua)\right] = \left[\delta\big(\widehat{\delta}(\iota,u),a\big)\right] \\ &= \delta_{\equiv}\Big(\left[\widehat{\delta}(\iota,u)\right], a\Big) \\ &= \delta_{\equiv}\big(f(u^{-1}L), a\big) = \delta_{\equiv}\big(f(K), a\big) \end{aligned}$$

- Sei wieder $K \in Z_{\mathrm{MN}} = \mathrm{LQ}_L$. Dann existiert $u \in \Sigma^*$ mit $K = u^{-1}L$ und es gilt

$$\begin{aligned} K \in E_{\mathrm{MN}} &\iff u^{-1}L \in E_{\mathrm{MN}} \iff \varepsilon \in u^{-1}L = L\big(M_{\widehat{\delta}(\iota,u)}\big) \\ &\iff \widehat{\delta}(\iota,u) \in E \\ &\iff E_{\equiv} \ni \big[\widehat{\delta}(\iota,u)\big] = f(u^{-1}L) = f(K) \end{aligned}$$

- Surjektivität: Sei $x \in Z_{\equiv}$. Dann existiert $z \in Z$ mit $x = [z]$.

$$\begin{aligned} &\overset{M \text{ reduziert}}{\Longrightarrow} \exists u \in \Sigma^* \colon \widehat{\delta}(\iota,u) = z \\ &\Longrightarrow \quad f(u^{-1}L) = \big[\widehat{\delta}(\iota,u)\big] = [z] = x \end{aligned}$$

- Injektivität:
  Seien $K_1, K_2 \in Z_{\mathrm{MN}} = \mathrm{LQ}_L$ mit $f(K_1) = f(K_2)$. Dann existieren $u_1, u_2 \in \Sigma^*$ mit $K_i = u_i^{-1}L$ und es gilt

$$[\widehat{\delta}(\iota,u_1)] = f(u_1^{-1}L) = f(K_1) = f(K_2) = f(u_2^{-1}L) = [\widehat{\delta}(\iota,u_2)]$$

$$\Longrightarrow \widehat{\delta}(\iota,u_1) \equiv \widehat{\delta}(\iota,u_2)$$

$$\Longrightarrow K_1 = u_1^{-1}L = L(M_{\widehat{\delta}(\iota,u_1)}) = L(M_{\widehat{\delta}(\iota,u_2)}) = u_2^{-1}L = K_2$$ □