

Automaten und Formale Sprachen

7. Vorlesung



Prof. Dr. Dietrich Kuske



FG Automaten und Logik, TU Ilmenau

Wintersemester 2024/25

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

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

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

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

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

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 $z = \hat{\delta}(z_0, u)$.
Dann wird der Linksquotient $u^{-1}L$ von dem DFA

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

akzeptiert.

Beweis: Für $w \in \Sigma^*$ gilt

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

d.h. wir haben die behauptete Gleichheit $L(M_z) = u^{-1}L$ gezeigt. □

Folgerung

Sei $L \subseteq \Sigma^*$ regulär.

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

Beispiel (Fortsetzung von Folie 6.21)

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 $p_1 < q_1 < p_2 < q_2 < \dots$, 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 $0^{q_i - p_i} \in (0^{p_i})^{-1}L \setminus (0^{p_j})^{-1}L$, und damit

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

Satz von Myhill und Nerode

Für $L \subseteq \Sigma^*$ gilt

$$L \text{ regulär} \iff LQ_L \text{ endlich.}$$

Beweis: „ $\Rightarrow$ “: Folgerung auf Folie 7.7

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

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

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

$$a^{-1}K = a^{-1}(u^{-1}L) = (ua)^{-1}L \in LQ_L = Z_{\text{MN}}.$$

q.e.d.

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

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

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

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

q.e.d.

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

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

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



Zwischenzusammenfassung

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

- hat jeder DFA für L wenigstens $|LQ_L|$ viele Zustände und
- der DFA MN_L aus dem obigen Beweis akzeptiert L und hat genau $|LQ_L|$ 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 die Sprache 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“.

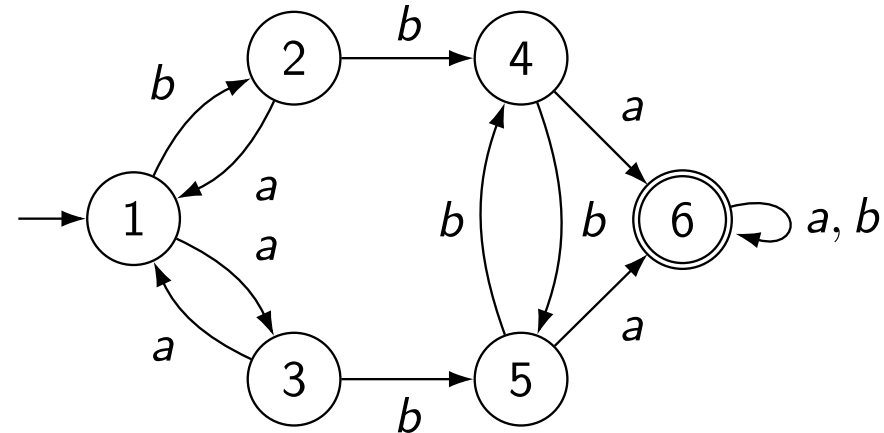
Die Streichung nicht erreichbarer Zustände ist trivial. Im Ergebnis erhält man einen „reduzierten“ DFA:

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 $\hat{\delta}(z_0, w_z) = z$.

Beispiel

Betrachte die
Zustände 4 und 5 im
reduzierten DFA M :

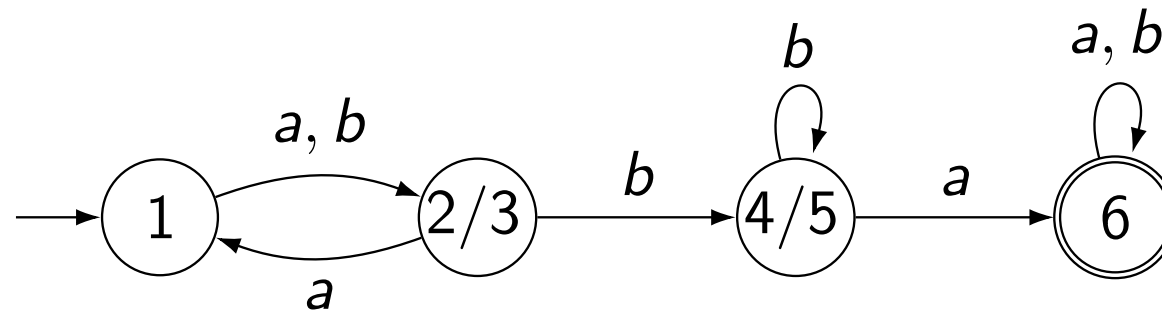


Feststellung:

- 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 „erkennungäquivalent“ und werden sie „verschmelzen“ (analog für 2 und 3).

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



Jetzt sind keine Zustände mehr erkenntnisäquivalent, 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 **erkennungäquivalent** (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

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

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.

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

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 $M_{\equiv} = (Z_{\equiv}, \Sigma, [z_0], \delta_{\equiv}, E_{\equiv})$ mit

- $Z_{\equiv} = Z / \equiv$,
- $\delta_{\equiv}([z], a) = [\delta(z, a)]$ für $z \in Z$ und $a \in \Sigma$ und
- $E_{\equiv} = \{[z] \mid z \in E\}$

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)

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



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 $f: Z_M \rightarrow Z_N$ gibt mit

- $f(\iota_M) = \iota_N$,
- $f(\delta_M(z, a)) = \delta_N(f(z), a)$ 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
- $MN_L = (Z_{MN}, \Sigma, \iota_{MN}, \delta_{MN}, E_{MN})$ 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

$f: Z_{MN} = LQ_L \rightarrow Z/\equiv = Z_{\equiv}$ mit

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

wohldefiniert. Man zeigt nun, daß sie ein Isomorphismus von MN_L auf $M_{\equiv}$ ist. (Zusatzmaterial auf Folien 7.25 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:

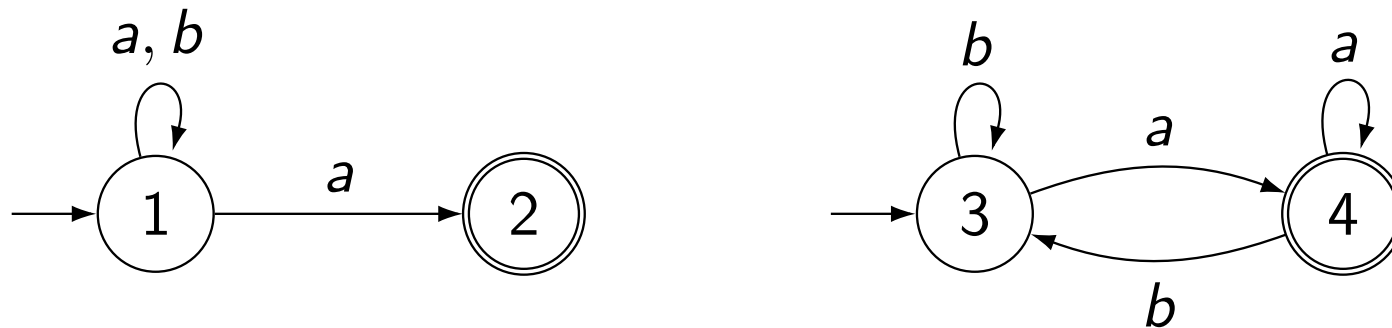
1. Es gelten $N \cong MN_L$ und $L(MN_L) = L$.
2. Sei N' DFA mit $L(N') = L$ und n' Zuständen.
 $\implies N' /_{\equiv} \cong MN_L \cong M /_{\equiv} = N$ hat n Zustände
 $\implies n' \geq n$
3. Sei N' DFA mit $L(N') = L$ und n Zuständen.
 $\implies N' /_{\equiv} \cong MN_L \cong M /_{\equiv} = N$ hat ebenfalls n Zustände
 $\implies N' \cong N' /_{\equiv}$, 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 $L = L((a + b)^* a)$ 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 $L_k = \{0, 1\}^* \{0\} \{0, 1\}^{k-1}$.

Beispielhafte Testfragen aus dieser Vorlesung (andere sind möglich):

- Definition Linksquotient
- Definition erkenntungsäquivalent
- Definition Quotient eines DFA
- Definition Isomorphie von DFAs

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

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

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

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

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

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

$$M \xrightarrow{\text{reduziert}} \exists u \in \Sigma^* : \hat{\delta}(\iota, u) = z$$

$$\implies f(u^{-1}L) = [\hat{\delta}(\iota, u)] = [z] = x$$

- Injektivität:

Seien $K_1, K_2 \in Z_{\text{MN}} = \text{LQ}_L$ 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

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

$$\implies \hat{\delta}(\iota, u_1) \equiv \hat{\delta}(\iota, u_2)$$

$$\implies K_1 = u_1^{-1}L = L(M_{\hat{\delta}(\iota, u_1)}) = L(M_{\hat{\delta}(\iota, u_2)}) = u_2^{-1}L = K_2$$

□