Grundzüge der Theoretischen Informatik

10. November 2021

Markus Bläser

Universität des Saarlandes

Kapitel 5: Das Myhill-Nerode-Theorem

Die Myhill-Nerode-Relation

Definition (5.4, Myhill-Nerode-Relation)

Sei $L \subseteq \Sigma^*$. Die *Myhill-Nerode-Relation* $\sim_L$ ist auf Σ^* definiert durch

$$x \sim_L y :\iff [\text{für alle } z \in \Sigma^*\text{: } xz \in L \iff yz \in L].$$

Lemma (5.6)

Für jedes $L \subseteq \Sigma^*$ *ist* $\sim_L$ *eine rechtsinvariante Äquivalenzrelation.*

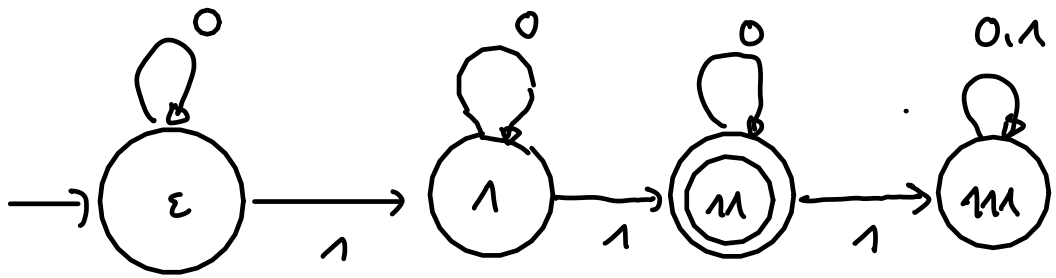
Beispiel

$$L = L(0^*10^*10^*)$$

[ε] [1] [11] [111]

1

{ 00100101000000100 }



Das Myhill-Nerode-Theorem

Theorem (5.8, Myhill-Nerode)

Sei $L \subseteq \Sigma^*$. *Die folgenden drei Aussagen sind äquivalent:*

1. L *ist regulär.*
2. L *ist die Vereinigung einiger Äquivalenzklassen einer rechtsinvarianten Äquivalenzrelation mit endlichem Index.*
3. $\sim_L$ *hat endlichen Index*

Jede Relation die 2. erfüllt,
ist eine Verfeinerung der Myhill-Nerode-Relation.
Jede Automatenrelation $\equiv_M$ erfüllt 2 $(L = L(M))$

Der Myhill-Nerode-Automat

- $Q =$ die Menge der Äquivalenzklassen von $\sim_L$,
- $\delta([x]_{\sim_L}, \sigma) = [x\sigma]_{\sim_L}$ für alle $\sigma \in \Sigma$,
- $q_0 = [\varepsilon]_{\sim_L}$,
- $Q_{acc} = \{[x]_{\sim_L} \mid x \in L\}$.

Beispiel

$$A = \{0^n 1^n \mid n \in \mathbb{N}\}$$

Alle Myhill-Nerode Klassen zu bestimmen kann mitunter schwierig sein. Aber um zu zeigen, dass $\text{index}(\sim_A)$ unendlich ist, reicht es unendlich viele Wörter $w_1, w_2, w_3, \ldots$ zu finden, so dass $w_i \not\sim_L w_j$ für alle $i \neq j$

$0 \not\sim_A 00$, da $01 \in A$, aber $001 \notin A$.

$0^i \not\sim_A 0^j$ für $i \neq j$,

da $0^i 1^i \in A$, aber $0^i 1^j \notin A$

Damit ist $\text{index}(\sim_A)$ unendlich $\Rightarrow A \notin REG$.

Isomorphismen von Automaten

- Seien $M = (Q, \Sigma, \delta, q_0, Q_{acc})$ und $M' = (Q', \Sigma, \delta', q_0', Q_{acc}')$ DEAs.
- δ und δ' seien total.

Definition

M und M' sind *isomorph* falls es eine Bijektion $b : Q \to Q'$ gibt mit:

1. Für alle $q \in Q$ und $\sigma \in \Sigma$ gilt $b(\delta(q, \sigma)) = \delta'(b(q), \sigma)$.
2. $b(q_0) = q_0'$.
3. $b(Q_{acc}) = Q_{acc}'$.

$b(Q_{acc}) = \{ b(q) \mid q \in Q_{acc} \}$

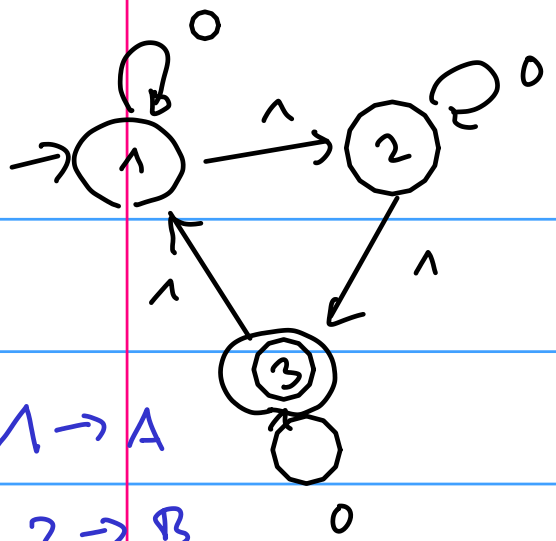
Solch ein b heißt *Isomorphismus*.

M

$$\begin{array}{ccc} Q \times \Sigma & \xrightarrow{\delta} & Q \\ \downarrow b \quad \downarrow \mathrm{id} & & \downarrow b \\ Q' \times \Sigma & \xrightarrow{\delta'} & Q' \end{array} \qquad b^{-1} \uparrow$$

M'

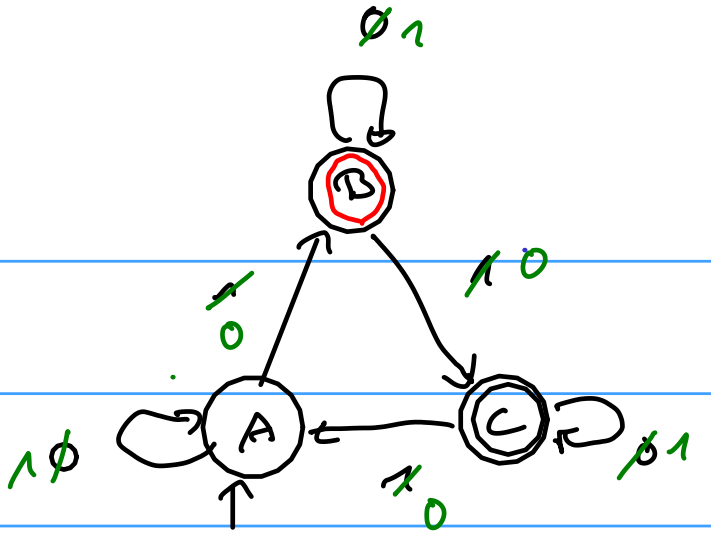
Wann sind zwei Automaten "gleich"?



b: 1 → A

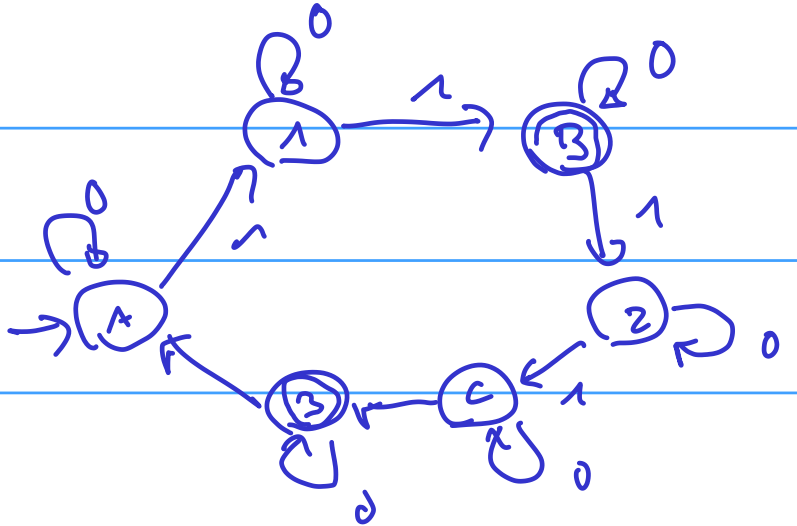
2 → B

3 → C



Zustände {1,2,3}

{A,B,C}



Der Minimalautomat

Theorem (5.9)

Sei $L \subseteq \Sigma^*$ *regulär.*

1. *Jeder DEA* $M' = (Q', \Sigma, \delta', q_0', Q_{acc}')$ *mit* δ' *total und* $L(M') = L$ *hat mindestens* $\text{index}(\sim_L)$ *Zustände.*
2. *Jeder DEA mit totaler Übergangsfunktion, der* L *erkennt und* $\text{index}(\sim_L)$ *Zustände hat, ist isomorph zum Myhill-Nerode-Automaten* $M = (Q, \Sigma, \delta, q_0, Q_{acc})$ *(aus dem Beweis von "3.* $\Longrightarrow$ *1." im Myhill-Nerode-Theorem).*

Myhill-Nerode-Automat heißt auch der Minimalautomat

Beweis 5.9.

1. Wir kombinieren den "1 ⇒ 2" und "2 ⇒ 3" Teilbeweis aus dem Myhill-Nerode-Thm.

"1 ⇒ 2": Die Automatenrelation ist eine Relation, die die Bedingung aus 2. erfüllt

"2 ⇒ 3" Relation aus 2 wird eine Verfeinerung von $\sim_L$.

$\Rightarrow \quad |Q| \geq \text{index}(\equiv_M) \geq \text{index}(\sim_L)$

2. Wir wissen $|Q'| = |Q|$

$\Rightarrow$ viele $(\equiv_{M'}) =$ viele $(\sim_L)$

Weil $\equiv_{M'}$ eine Verfeinerung von $\sim_L$, müssen beide Relationen gleich sein.

Für ein Wort x schreiben wir einfach $[x]$ für die Äquivalenzklasse in einer Relationen.

b: $Q' \to Q$

$q' \to [x]$ wobei x ein Wort mit $(\delta')^*(q_0', x) = q'$

b ist well def.

Denn gilt $\delta^*(q_0', y) = q'$, dann

ist $x \equiv_{M'} y$ und damit $x \equiv_L y$ und $[x] = [y]$

b ist total, denn alle Zustände in

M' sind erreichbar wegen der Minimalität

! $\delta(q, \sigma) = b(\delta'(b^{-1}(q), \sigma))$

$q = [x]$ und $b^{-1}(q) = q'$

$b(\delta'(q', \sigma)) = [x\sigma]$

$\delta(q, \sigma) = [x\sigma]$ //

$b(q_0') = q_0 = [\varepsilon]$

$\parallel$

$[\varepsilon]$

↳ nach der Definition von b.

↳ Nach Def von M.N-Automat

* $\supseteq$ folgt offensichtlich. □

$b(Q_{acc}') = Q_{acc}$

Sei $q' \in Q_{acc}'$ und x ist ein Wort mit $\delta'(q_0', x) = q'$

Dann ist $x \in L$

und $b(q') = [x] \in Q_{acc}$

↳ nach Def. von M.N-Automaten

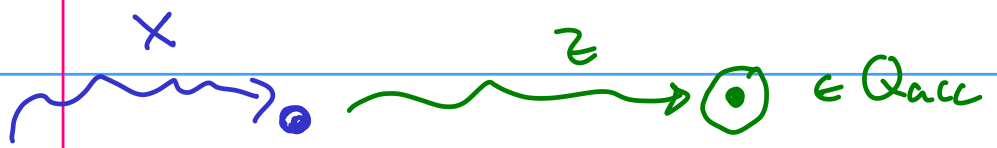
Dies zeigt $\subseteq$ *

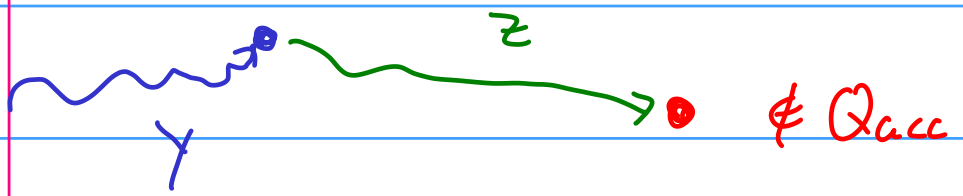
Es kann nur einen Minimalautomat geben.

Bis auf Isomorphie.

Man startet mit irgendeinem Automaten

$\equiv_n$ ist eine Verfeinerung von $\sim_L$





z ist ein Beweis, dass x und y nicht

äq bzgl. $\sim_L$

Lemma 5.11.

Falls es ein z gibt mit $\delta^*(q_1, z) \in Q_{acc}$ und $\delta^*(q', z) \notin Q_{acc}$ dann gibt es ein Wort z' mit $|z'| \leq \binom{|Q|}{2}$ mit $\delta^*(q_1, z') \in Q_{acc}$ und $\delta^*(q', z') \notin Q_{acc}$ oder umgedreht

Beweis

Sei $s_0, s_1, \dots, s_t \in Q_{acc}$ die Berechnung von M gestartet in $q = s_0$ auf das Wort z.

Sei $s_0', s_1', \dots, s_t' \notin Q_{acc}$ die Berechnung von M gestartet in $q' = s_0'$ auf das Wort z

Wenn $|z| \leq \binom{|Q|}{2}$, dann sind wir fertig.

Wenn $|z| > \binom{|Q|}{2}$, dann gibt es Indizes

$i \neq j$

i und j mit $\{s_i, s_i'\} = \{s_j, s_j'\}$

Falls $s_i = s_j$ und $s_i' = s_j'$ dann kann

beide Berechnungen simultan verkürzen

$$s_0, s_1, \ldots, s_i, s_{i+1}, \ldots, s_j, s_{j+1}, \ldots, s_t$$

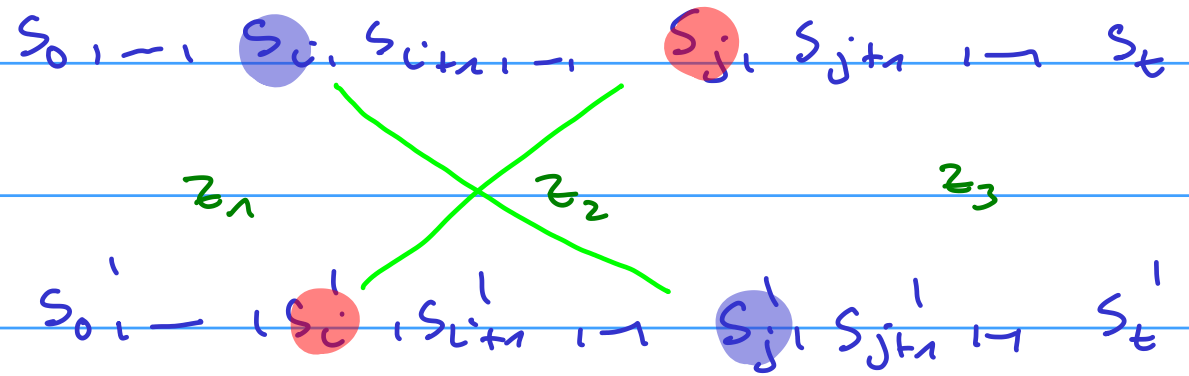
$z = z_1 z_2 z_3$ $\quad z_1 \quad \| \quad z_2 \quad \| \quad z_3$

$$s_0', s_1', \ldots, s_i', s_{i+1}', \ldots, s_j', s_{j+1}', \ldots, s_t'$$

$\delta^*(s_0, z_1 z_3) = s_t$ und $\delta^*(s_0', z_1 z_3) = s_t'$

Es kann aber auch sein, dass $s_i = s_j'$

und $s_i' = s_j$



Damit ist $\delta^*(s_0, z_1 z_3) = s_t'$ und

$$\delta^*(s_0', \underbrace{z_1 z_3}_{= z'}) = s_t$$

Vom z' wird noch zulange ist, dann wieder oder wie der Prozess. □