Der Satz von Myhill und Nerode

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für
Theoretische Informatik

Stand: 16. Mai 2023
Folien ursprünglich von PD Dr. David Sabel

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$?
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$?
3. Gilt $\varepsilon \sim_L a$?
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$?
5. Gilt $ab^i \sim_L ab^j$?
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$?
3. Gilt $\varepsilon \sim_L a$?
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$?
5. Gilt $ab^i \sim_L ab^j$?
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ja
3. Gilt $\varepsilon \sim_L a$?
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$?
5. Gilt $ab^i \sim_L ab^j$?
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ja
3. Gilt $\varepsilon \sim_L a$? nein
   (z.B. $w = b^i$ oder $w = ab^i$)
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$?
5. Gilt $ab^i \sim_L ab^j$?
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ja
3. Gilt $\varepsilon \sim_L a$? nein
   (z.B. $w = b^i$ oder $w = ab^i$)
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$? ja
5. Gilt $ab^i \sim_L ab^j$?
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ja
3. Gilt $\varepsilon \sim_L a$? nein (z.B. $w = b^i$ oder $w = ab^i$)
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$? ja
5. Gilt $ab^i \sim_L ab^j$? ja
6. Gilt $a \sim_L b$?

Die Nerode-Relation (1)

Definition (Nerode-Relation $\sim_L$)

Sei L eine formale Sprache über Σ. Die Nerode-Relation $\sim_L \subseteq \Sigma^* \times \Sigma^*$ zu L ist definiert für alle Wörter $u, v \in \Sigma^*$ durch

$$u \sim_L v \iff (\forall w \in \Sigma^* : uw \in L \iff vw \in L)$$

Informell: $u \sim_L v$, wenn sich ihr Enthaltensein in L gleich verhält bezüglich beliebiger Erweiterung um dasselbe Suffix.

Beispiel: $L = \{ab^n \mid n \in \mathbb{N}\}$

1. Gilt $a \sim_L ab$? ja
2. Gilt $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ja
3. Gilt $\varepsilon \sim_L a$? nein (z.B. $w = b^i$ oder $w = ab^i$)
4. Gilt $aau \sim_L aav$ mit $u, v \in \{b\}^*$? ja
5. Gilt $ab^i \sim_L ab^j$? ja
6. Gilt $a \sim_L b$? nein (z.B. $w = \varepsilon$ oder $w = b^i$)

Die Nerode-Relation (2)

Satz

Die Nerode-Relation ist eine Äquivalenzrelation.

Beweis: einfach

Die Nerode-Relation (2)

Satz

Die Nerode-Relation ist eine Äquivalenzrelation.

Beweis: einfach

Zur Erinnerung:

- Die Äquivalenzklasse $[u]_{\sim_L}$ ist definiert als $\{w \mid u \sim_L w\}$.
- Der Index einer Äquivalenzrelation ist die Anzahl ihrer disjunkten Äquivalenzklassen $\Sigma^* = [u_1]_{\sim_L} \dot\cup [u_2]_{\sim_L} \dot\cup \cdots$.
- Der Index kann unendlich sein.

Beispiel: Index

$L = \{ab^n \mid n \in \mathbb{N}\}$

$Index(\sim_L) = ?$

Beispiel: Index

$L = \{ab^n \mid n \in \mathbb{N}\}$

$Index(\sim_L) = ?$

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$

Beispiel: Index

$L = \{ab^n \mid n \in \mathbb{N}\}$

$Index(\sim_L) = ?$

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$
- $[a]_{\sim_L} = \{a, ab, abb, abbb, \ldots\}$

Beispiel: Index

$$L = \{ab^n \mid n \in \mathbb{N}\}$$

$$Index(\sim_L) = \,?$$

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$
- $[a]_{\sim_L} = \{a, ab, abb, abbb, \ldots\}$
- $[aa]_{\sim_L} = \{aau \mid u \in \{a, b\}^*\}$
  $\cup \{bu \mid u \in \{a, b\}^*\}$
  $\cup \{abuav \mid u, v \in \{a, b\}^*\}$

Beispiel: Index

$L = \{ab^n \mid n \in \mathbb{N}\}$

$Index(\sim_L) = ?$

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$
- $[a]_{\sim_L} = \{a, ab, abb, abbb, \dots\}$
- $[aa]_{\sim_L} = \{aau \mid u \in \{a,b\}^*\} \cup \{bu \mid u \in \{a,b\}^*\} \cup \{abuav \mid u, v \in \{a,b\}^*\}$
- $\{a,b\}^* = [\varepsilon]_{\sim_L} \mathbin{\dot\cup} [a]_{\sim_L} \mathbin{\dot\cup} [aa]_{\sim_L}$

Beispiel: Index

$L = \{ab^n \mid n \in \mathbb{N}\}$

$Index(\sim_L) = ?$

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$
- $[a]_{\sim_L} = \{a, ab, abb, abbb, \ldots\}$
- $$\begin{aligned}[aa]_{\sim_L} = \{&aau \mid u \in \{a,b\}^*\} \\ &\cup \{bu \mid u \in \{a,b\}^*\} \\ &\cup \{abuav \mid u, v \in \{a,b\}^*\}\end{aligned}$$
- $\{a, b\}^* = [\varepsilon]_{\sim_L} \dot\cup [a]_{\sim_L} \dot\cup [aa]_{\sim_L}$
- Daher $Index(\sim_L) = 3$

Satz von Myhill und Nerode

Theorem (Satz von Myhill und Nerode)

Eine formale Sprache L ist genau dann **regulär**, wenn der **Index** von $\sim_L$ **endlich** ist.

Unabhängig bewiesen von John Myhill (1957) und Anil Nerode (1958)

Damit haben wir eine genaue Charakterisierung der regulären Sprachen.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.
- Sei $\approx_M \; \subseteq \Sigma^* \times \Sigma^*$ definiert als: $u \approx_M v \iff \widehat{\delta}(z_0, u) = \widehat{\delta}(z_0, v)$

  „$u \approx_M v$, wenn u, v auf M zum gleichen Zustand führen."

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.
- Sei $\approx_M \ \subseteq \Sigma^* \times \Sigma^*$ definiert als: $u \approx_M v \iff \widehat{\delta}(z_0, u) = \widehat{\delta}(z_0, v)$

  „$u \approx_M v$, wenn u, v auf M zum gleichen Zustand führen.“
- $\approx_M$ ist eine Äquivalenzrelation.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.
- Sei $\approx_M \subseteq \Sigma^* \times \Sigma^*$ definiert als: $u \approx_M v \iff \widehat{\delta}(z_0, u) = \widehat{\delta}(z_0, v)$

  „$u \approx_M v$, wenn u, v auf M zum gleichen Zustand führen."
- $\approx_M$ ist eine Äquivalenzrelation.
- $\mathit{Index}(\approx_M) \leq |Z|$ (und damit endlich).

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.
- Sei $\approx_M \; \subseteq \Sigma^* \times \Sigma^*$ definiert als: $u \approx_M v \iff \widehat{\delta}(z_0, u) = \widehat{\delta}(z_0, v)$

  „$u \approx_M v$, wenn u, v auf M zum gleichen Zustand führen.“
- $\approx_M$ ist eine Äquivalenzrelation.
- $\mathit{Index}(\approx_M) \leq |Z|$ (und damit endlich).
- Wir zeigen: $u \approx_M v \implies u \sim_L v$ (d.h. $\approx_M$ verfeinert $\sim_L$).
  Dann gilt auch $\mathit{Index}(\sim_L) \leq \mathit{Index}(\approx_M) \leq |Z|$ (und damit endlich).

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 1: Wenn L regulär ist, dann ist der Index von $\sim_L$ endlich.

- Sei L regulär und $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA mit $L(M) = L$.
- Sei $\approx_M \; \subseteq \Sigma^* \times \Sigma^*$ definiert als: $u \approx_M v \iff \widehat{\delta}(z_0, u) = \widehat{\delta}(z_0, v)$

  „$u \approx_M v$, wenn u, v auf M zum gleichen Zustand führen.“
- $\approx_M$ ist eine Äquivalenzrelation.
- $\mathit{Index}(\approx_M) \leq |Z|$ (und damit endlich).
- Wir zeigen: $u \approx_M v \implies u \sim_L v$ (d.h. $\approx_M$ verfeinert $\sim_L$).

  Dann gilt auch $\mathit{Index}(\sim_L) \leq \mathit{Index}(\approx_M) \leq |Z|$ (und damit endlich).
- Sei $u \approx_M v$ und $w \in \Sigma^*$. Dann gilt:

$$\begin{aligned} \widehat{\delta}(z_0, uw) &= \widehat{\delta}(\widehat{\delta}(z_0, u), w) \\ &= \widehat{\delta}(\widehat{\delta}(z_0, v), w) = \widehat{\delta}(z_0, vw) \end{aligned}$$

  und damit $uw \in L \iff vw \in L$. Da w beliebig, zeigt dies $u \sim_L v$.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 2: Wenn der Index von $\sim_L$ endlich ist, dann ist L regulär.

- Sei der Index von $\sim_L$ endlich.
- $\Sigma^* = [u_1]_{\sim_L} \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} [u_n]_{\sim_L}$ für $n \in \mathbb{N}_{>0}$.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 2: Wenn der Index von $\sim_L$ endlich ist, dann ist L regulär.

- Sei der Index von $\sim_L$ endlich.
- $\Sigma^* = [u_1]_{\sim_L} \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} [u_n]_{\sim_L}$ für $n \in \mathbb{N}_{>0}$.
- Konstruiere **Nerode-Automaten**:

  DFA $M = (Z, \Sigma, \delta, [\varepsilon]_{\sim_L}, E)$ mit
  - $Z = \{[u_1]_{\sim_L}, \ldots, [u_n]_{\sim_L}\}$,
  - $\delta([u_i]_{\sim_L}, a) = [u_i a]_{\sim_L}$ für alle $a \in \Sigma$ und
  - $E = \{[u_i]_{\sim_L} \mid i \in \{1, \ldots, n\}, u_i \in L\}$.

Beweis des Satzes von Myhill und Nerode

Beweis, Teil 2: Wenn der Index von $\sim_L$ endlich ist, dann ist L regulär.

- Sei der Index von $\sim_L$ endlich.
- $\Sigma^* = [u_1]_{\sim_L} \cup \cdots \cup [u_n]_{\sim_L}$ für $n \in \mathbb{N}_{>0}$.
- Konstruiere **Nerode-Automaten**:

  DFA $M = (Z, \Sigma, \delta, [\varepsilon]_{\sim_L}, E)$ mit
  - $Z = \{[u_1]_{\sim_L}, \ldots, [u_n]_{\sim_L}\}$,
  - $\delta([u_i]_{\sim_L}, a) = [u_i a]_{\sim_L}$ für alle $a \in \Sigma$ und
  - $E = \{[u_i]_{\sim_L} \mid i \in \{1, \ldots, n\}, u_i \in L\}$.
- $L(M) = L$:

$$
\begin{array}{ll}
 & w \in L(M) \\
\text{g.d.w.} & \widehat{\delta}([\varepsilon]_{\sim_L}, w) \in E \\
\text{g.d.w.} & [w]_{\sim_L} \in E \\
\text{g.d.w.} & w \in L
\end{array}
$$

□

Anwendung des Satzes von Myhill und Nerode

Da der Satz eine hinreichende und notwendige Bedingung für reguläre Sprachen liefert, kann man ihn verwenden, um

1. Regularität nachzuweisen: Zeige $Index(\sim_L)$ ist endlich.

2. Nichtregularität nachzuweisen: Zeige $Index(\sim_L)$ ist unendlich.

Anwendung des Satzes von Myhill und Nerode

Da der Satz eine hinreichende und notwendige Bedingung für reguläre Sprachen liefert, kann man ihn verwenden, um

1. Regularität nachzuweisen: Zeige $\mathit{Index}(\sim_L)$ ist endlich.

   „oft einfacher: gib endlichen Automaten an, der L akzeptiert / gib regulären Ausdruck an, der L erzeugt / gib reguläre Grammatik an, die L erzeugt"

2. Nichtregularität nachzuweisen: Zeige $\mathit{Index}(\sim_L)$ ist unendlich.

Anwendung des Satzes von Myhill und Nerode

Da der Satz eine hinreichende und notwendige Bedingung für reguläre Sprachen liefert, kann man ihn verwenden, um

1. Regularität nachzuweisen: Zeige $\mathit{Index}(\sim_L)$ ist endlich.

   „oft einfacher: gib endlichen Automaten an, der L akzeptiert / gib regulären Ausdruck an, der L erzeugt / gib reguläre Grammatik an, die L erzeugt"

2. Nichtregularität nachzuweisen: Zeige $\mathit{Index}(\sim_L)$ ist unendlich.

   „wird insbesondere dann benutzt, wenn das Pumping-Lemma nicht funktioniert"

Wie zeigt man $Index(\sim_L) = \infty$?

Idee: Finde unendlich viele Äquivalenzklassen $[u_1]_{\sim_L}, [u_2]_{\sim_L}, \ldots,$
die paarweise verschieden sind ($[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ für $i \neq j$).

Rezept:

Wie zeigt man $Index(\sim_L) = \infty$?

Idee: Finde unendlich viele Äquivalenzklassen $[u_1]_{\sim_L}, [u_2]_{\sim_L}, \ldots,$
die paarweise verschieden sind ($[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ für $i \neq j$).

Rezept:

- Finde für $i = 1, 2, \ldots$ Wörter u_i und w_i, sodass alle u_i paarweise verschieden und alle w_i paarweise verschieden sind und

$$u_i w_i \in L \text{ aber } u_i w_j \notin L \text{ für alle } i \neq j$$

Wie zeigt man $\mathit{Index}(\sim_L) = \infty$?

Idee: Finde unendlich viele Äquivalenzklassen $[u_1]_{\sim_L}, [u_2]_{\sim_L}, \ldots,$
die paarweise verschieden sind ($[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ für $i \neq j$).

Rezept:

- Finde für $i = 1, 2, \ldots$ Wörter u_i und w_i, sodass alle u_i paarweise verschieden und alle w_i paarweise verschieden sind und

$$u_i w_i \in L \text{ aber } u_i w_j \notin L \text{ für alle } i \neq j$$

- Dann sind $[u_1]_{\sim_L}$,$[u_2]_{\sim_L}$,$[u_3]_{\sim_L}$,... paarweise disjunkt.

Wie zeigt man $Index(\sim_L) = \infty$?

Idee: Finde unendlich viele Äquivalenzklassen $[u_1]_{\sim_L}, [u_2]_{\sim_L}, \ldots,$
die paarweise verschieden sind ($[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ für $i \neq j$).

Rezept:

- Finde für $i = 1, 2, \ldots$ Wörter u_i und w_i, sodass alle u_i paarweise verschieden und alle w_i paarweise verschieden sind und

$$u_i w_i \in L \text{ aber } u_i w_j \notin L \text{ für alle } i \neq j$$

- Dann sind $[u_1]_{\sim_L}, [u_2]_{\sim_L}, [u_3]_{\sim_L}, \ldots$ paarweise disjunkt.

Beachte: Es ist hierfür **nicht** notwendig, **alle** Äquivalenzklassen der disjunkten Zerlegung von Σ^* zu finden.

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

- Für $u_i = a^i b$ für $i \in \mathbb{N}_{>0}$ gilt:

  $[u_i]_{\sim_L} =$ alle Wörter, denen noch $i-1$ b's fehlen, um in L enthalten zu sein

$$\begin{aligned}
[u_1]_{\sim_L} &= \{ab, a^2b^2, \ldots\} = L \\
[u_2]_{\sim_L} &= \{a^2b, a^3b^2, a^4b^3, \ldots\} \\
[u_3]_{\sim_L} &= \{a^3b, a^4b^2, a^5b^3, \ldots\} \\
&\vdots
\end{aligned}$$

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

- Für $u_i = a^i b$ für $i \in \mathbb{N}_{>0}$ gilt:

  $[u_i]_{\sim_L} =$ alle Wörter, denen noch $i - 1$ b's fehlen, um in L enthalten zu sein

$$
\begin{aligned}
[u_1]_{\sim_L} &= \{ab, a^2b^2, \ldots\} = L \\
[u_2]_{\sim_L} &= \{a^2b, a^3b^2, a^4b^3, \ldots\} \\
[u_3]_{\sim_L} &= \{a^3b, a^4b^2, a^5b^3, \ldots\} \\
&\vdots
\end{aligned}
$$

- Sei $w_i = b^{i-1}$ für $i \in \mathbb{N}_{>0}$.

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

- Für $u_i = a^i b$ für $i \in \mathbb{N}_{>0}$ gilt:

  $[u_i]_{\sim_L} =$ alle Wörter, denen noch $i-1$ b's fehlen, um in L enthalten zu sein

$$\begin{aligned}
[u_1]_{\sim_L} &= \{ab, a^2b^2, \ldots\} = L \\
[u_2]_{\sim_L} &= \{a^2b, a^3b^2, a^4b^3, \ldots\} \\
[u_3]_{\sim_L} &= \{a^3b, a^4b^2, a^5b^3, \ldots\} \\
&\vdots
\end{aligned}$$

- Sei $w_i = b^{i-1}$ für $i \in \mathbb{N}_{>0}$.
- $u_i w_i = a^i b^i \in L$, aber $u_i w_j = a^i b^j \notin L$ für $i \neq j$.

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

- Für $u_i = a^i b$ für $i \in \mathbb{N}_{>0}$ gilt:

  $[u_i]_{\sim_L} =$ alle Wörter, denen noch $i-1$ b's fehlen, um in L enthalten zu sein

$$\begin{aligned}
[u_1]_{\sim_L} &= \{ab, a^2b^2, \ldots\} = L \\
[u_2]_{\sim_L} &= \{a^2b, a^3b^2, a^4b^3, \ldots\} \\
[u_3]_{\sim_L} &= \{a^3b, a^4b^2, a^5b^3, \ldots\} \\
&\vdots
\end{aligned}$$

- Sei $w_i = b^{i-1}$ für $i \in \mathbb{N}_{>0}$.
- $u_i w_i = a^i b^i \in L$, aber $u_i w_j = a^i b^j \notin L$ für $i \neq j$.
- Daher gilt: $[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ und $Index(\sim_L) = \infty$.

Beispiel

Betrachte $L = \{a^n b^n \mid n \in \mathbb{N}_{>0}\}$ und deren Nerode-Relation $\sim_L$.

- Für $u_i = a^i b$ für $i \in \mathbb{N}_{>0}$ gilt:

  $[u_i]_{\sim_L} =$ alle Wörter, denen noch $i-1$ b's fehlen, um in L enthalten zu sein

$$\begin{aligned} [u_1]_{\sim_L} &= \{ab, a^2b^2, \ldots\} = L \\ [u_2]_{\sim_L} &= \{a^2b, a^3b^2, a^4b^3, \ldots\} \\ [u_3]_{\sim_L} &= \{a^3b, a^4b^2, a^5b^3, \ldots\} \\ &\vdots \end{aligned}$$

- Sei $w_i = b^{i-1}$ für $i \in \mathbb{N}_{>0}$.
- $u_i w_i = a^i b^i \in L$, aber $u_i w_j = a^i b^j \notin L$ für $i \neq j$.
- Daher gilt: $[u_i]_{\sim_L} \cap [u_j]_{\sim_L} = \emptyset$ und $Index(\sim_L) = \infty$.
- Mit dem Satz von Myhill und Nerode folgt: L ist nicht regulär.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Beweis:

- Sei $u_i = ab^i c$ für $i \in \mathbb{N}_{>0}$.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Beweis:

- Sei $u_i = ab^i c$ für $i \in \mathbb{N}_{>0}$.
- Sei $w_i = c^{i-1}$.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Beweis:

- Sei $u_i = ab^i c$ für $i \in \mathbb{N}_{>0}$.
- Sei $w_i = c^{i-1}$.
- $u_i w_i = ab^i c^i \in L$, aber $u_i w_j = ab^i c^j \notin L$ für $i \neq j$.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Beweis:

- Sei $u_i = ab^i c$ für $i \in \mathbb{N}_{>0}$.
- Sei $w_i = c^{i-1}$.
- $u_i w_i = ab^i c^i \in L$, aber $u_i w_j = ab^i c^j \notin L$ für $i \neq j$.
- Daher sind alle $[u_i]_{\sim_L}$ disjunkt und $Index(\sim_L) = \infty$.

Nicht reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^\ell c^\ell \mid k, \ell \in \mathbb{N}_{>0}\}$ ist nicht regulär.

Beweis:

- Sei $u_i = ab^i c$ für $i \in \mathbb{N}_{>0}$.
- Sei $w_i = c^{i-1}$.
- $u_i w_i = ab^i c^i \in L$, aber $u_i w_j = ab^i c^j \notin L$ für $i \neq j$.
- Daher sind alle $[u_i]_{\sim_L}$ disjunkt und $\mathit{Index}(\sim_L) = \infty$.
- Mit dem Satz von Myhill und Nerode folgt: L ist nicht regulär. $\square$

Beispiel: Reguläre Sprache

Sei $L = \{ab^n \mid n \in \mathbb{N}\}$. Die disjunkten Äquivalenzklassen von $\sim_L$ sind:

- $[\varepsilon]_{\sim_L} = \{\varepsilon\}$
- $[a]_{\sim_L} = \{a, ab, abb, abbb, \ldots\}$
- $$\begin{aligned}[aa]_{\sim_L} &= \{aau \mid u \in \{a,b\}^*\} \\ &\cup \{bu \mid u \in \{a,b\}^*\} \\ &\cup \{abuav \mid u, v \in \{a,b\}^*\}\end{aligned}$$

Daher folgt $\mathit{Index}(\sim_L) = 3$ und L ist regulär.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 1, Minimalität):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 1, Minimalität):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L.
- Sei $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger DFA mit $L(M') = L$.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 1, Minimalität):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L.
- Sei $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger DFA mit $L(M') = L$.
- Der Beweis des Satzes von Myhill und Nerode zeigt:
  1. $\approx_{M'}$ ist eine Verfeinerung von $\sim_L$ ($\approx_{M'} \subseteq \sim_L$)

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 1, Minimalität):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L.
- Sei $M' = (Z', \Sigma, \delta', z'_0, E')$ ein beliebiger DFA mit $L(M') = L$.
- Der Beweis des Satzes von Myhill und Nerode zeigt:
  1. $\approx_{M'}$ ist eine Verfeinerung von $\sim_L$ ($\approx_{M'} \subseteq \sim_L$)
  2. $\approx_M = \sim_L$

  Daher ist $Index(\approx_{M'}) \geq Index(\approx_M)$ und daher auch
  $|Z'| \geq Index(\approx_{M'}) \geq Index(\approx_M) = Index(\sim_L) = |Z|$.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 2, alle minimalen DFAs sind bis auf Umbenennung identisch):

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 2, alle minimalen DFAs sind bis auf Umbenennung identisch):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L und $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger minimaler DFA mit $L(M') = L$.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 2, alle minimalen DFAs sind bis auf Umbenennung identisch):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L und $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger minimaler DFA mit $L(M') = L$.
- Minimalität impliziert $|Z'| = |Z|$.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 2, alle minimalen DFAs sind bis auf Umbenennung identisch):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L und $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger minimaler DFA mit $L(M') = L$.
- Minimalität impliziert $|Z'| = |Z|$.
- Da $\approx_{M'} \subseteq \sim_L$ gilt, gilt entweder $\approx_{M'} \subset \sim_L$ oder $\approx_{M'} = \sim_L$. Im ersten Fall hätten wir $|Z'| \geq Index(\approx_{M'}) > Index(\sim_L) = |Z|$. Widerspruch. Daher $\approx_{M'} = \sim_L$.

Minimalautomat

Satz

Der Nerode-Automat einer regulären Sprache L ist der sogenannte Minimalautomat, d.h. jeder DFA M', mit $L(M') = L$ hat mindestens so viele Zustände wie der Nerode-Automat. Zudem sind alle minimalen DFAs bis auf Umbenennung von Zuständen identisch.

Beweis (Teil 2, alle minimalen DFAs sind bis auf Umbenennung identisch):

- Sei $M = (Z, \Sigma, \delta, z_0, E)$ der Nerode-Automat der Sprache L und $M' = (Z', \Sigma, \delta', z_0', E')$ ein beliebiger minimaler DFA mit $L(M') = L$.
- Minimalität impliziert $|Z'| = |Z|$.
- Da $\approx_{M'} \subseteq \sim_L$ gilt, gilt entweder $\approx_{M'} \subset \sim_L$ oder $\approx_{M'} = \sim_L$. Im ersten Fall hätten wir $|Z'| \geq \mathit{Index}(\approx_{M'}) > \mathit{Index}(\sim_L) = |Z|$. Widerspruch.
  Daher $\approx_{M'} = \sim_L$.
- Da $\approx_{M'} = \sim_L = \approx_M$ gilt, folgt dass M und M' strukturell identisch sind (siehe Skript).

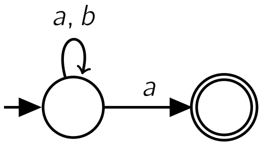
Minimalautomaten: NFAs

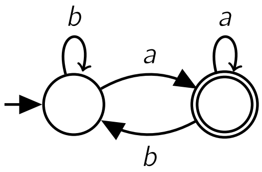
Der vorherige Satz zeigt:

Alle minimalen DFAs sind bis auf Umbenennung identisch.

Für **NFAs** git das im Allgemeinen nicht.

Beispiel:





Beide Automaten erkennen $\{ua \mid u \in \{a, b\}^*\}$ und haben eine minimale Zustandsanzahl, aber sind strukturell verschieden.

Äquivalenzklassenautomat

Definition (Äquivalenzklassenautomat)

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA. Wir nennen zwei Zustände $z, z' \in Z$ äquivalent und schreiben $z \equiv z'$ falls gilt:

$$\text{für alle } w \in \Sigma^*\colon \widehat{\delta}(z, w) \in E \iff \widehat{\delta}(z', w) \in E$$

Äquivalenzklassenautomat

Definition (Äquivalenzklassenautomat)

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA. Wir nennen zwei Zustände $z, z' \in Z$ äquivalent und schreiben $z \equiv z'$ falls gilt:

$$\text{für alle } w \in \Sigma^*\colon \widehat{\delta}(z, w) \in E \iff \widehat{\delta}(z', w) \in E$$

Der Äquivalenzklassenautomat zu M ist der DFA $M' = (Z', \Sigma, \delta', z_0', E')$ mit

$$\begin{aligned} Z' &= \{[z]_\equiv \mid z \in Z\} \\ z_0' &= [z_0]_\equiv \\ E' &= \{[z]_\equiv \mid z \in E\} \\ \delta'([z]_\equiv, a) &= [\delta(z, a)]_\equiv \end{aligned}$$

Äquivalenzklassenautomat: Korrektheit und Minimalität (1)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 1): nächste Stunde

Äquivalenzklassenautomat: Korrektheit und Minimalität (2)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2): Sei $L = L(M') = L(M)$.

Äquivalenzklassenautomat: Korrektheit und Minimalität (2)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2): Sei $L = L(M') = L(M)$.

- Da alle $z \in Z$ erreichbar sind, sind alle $z' \in Z'$ erreichbar.

Äquivalenzklassenautomat: Korrektheit und Minimalität (2)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2): Sei $L = L(M') = L(M)$.

- Da alle $z \in Z$ erreichbar sind, sind alle $z' \in Z'$ erreichbar.
- Für Minimalität genügt es zu zeigen: $|Z'| \leq \mathit{Index}(\sim_L)$.

Äquivalenzklassenautomat: Korrektheit und Minimalität (2)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2): Sei $L = L(M') = L(M)$.

- Da alle $z \in Z$ erreichbar sind, sind alle $z' \in Z'$ erreichbar.
- Für Minimalität genügt es zu zeigen: $|Z'| \leq \mathit{Index}(\sim_L)$.
- Zeige für jede Äquivalenzklasse $[v]_{\sim_L}$:
  für alle $u \in [v]_{\sim_L}$ ist $\widehat{\delta}(z_0', u)$ derselbe Zustand (Beweis folgt).
  Dann gibt es nicht mehr als $\mathit{Index}(\sim_L)$ erreichbare Zustände.

Äquivalenzklassenautomat: Korrektheit und Minimalität (2)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2): Sei $L = L(M') = L(M)$.

- Da alle $z \in Z$ erreichbar sind, sind alle $z' \in Z'$ erreichbar.
- Für Minimalität genügt es zu zeigen: $|Z'| \leq \mathit{Index}(\sim_L)$.
- Zeige für jede Äquivalenzklasse $[v]_{\sim_L}$:
  für alle $u \in [v]_{\sim_L}$ ist $\widehat{\delta}(z_0', u)$ derselbe Zustand (Beweis folgt).
  Dann gibt es nicht mehr als $\mathit{Index}(\sim_L)$ erreichbare Zustände.
- Da alle $z' \in Z'$ erreichbar sind, gilt damit $|Z'| \leq \mathit{Index}(\sim_L)$.

Äquivalenzklassenautomat: Korrektheit und Minimalität (3)

Satz

Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DFA und $M' = (Z', \Sigma, \delta', z_0', E')$ der Äquivalenzklassenautomat zu M. Dann gilt

1. $L(M') = L(M)$.
2. Falls alle Zustände in Z vom Startzustand z_0 erreichbar sind, dann ist M' minimal.

Beweis (Teil 2, Fortsetzung):

- Seien $u, u' \in [v]_{\sim_L}$, d.h. $u \sim_L u'$. Dann gilt

  $$\forall w \in \Sigma^*\colon uw \in L \iff u'w \in L$$

  woraus folgt: $\forall w \in \Sigma^*\colon \widehat{\delta'}(z_0', uw) \in E' \iff \widehat{\delta'}(z_0', u'w) \in E'$

  woraus folgt: $\forall w \in \Sigma^*\colon \widehat{\delta'}(\widehat{\delta'}(z_0', u), w) \in E' \iff \widehat{\delta'}(\widehat{\delta'}(z_0', u'), w) \in E'$

  woraus folgt: $\widehat{\delta'}(z_0', u) \equiv \widehat{\delta'}(z_0', u')$

  woraus folgt: $[\widehat{\delta'}(z_0', u)]_\equiv = [\widehat{\delta'}(z_0', u')]_\equiv$ $\square$