LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Formale Sprachen und Komplexität
Theoretische Informatik für Medieninformatiker
Sommersemester 2022

Der Satz von Myhill-Nerode

Prof. Dr. David Sabel

LFE Theoretische Informatik

Letzte Änderung der Folien: 29. Mai 2022

Die Nerode-Relation

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 Worte $u, v \in \Sigma^*$ 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 denselben Suffix.

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

1. Gilt $a \sim_L ab$? ✓
2. Gilt $a \sim_L b$? × (z.B. $w = \varepsilon$ oder $w = b^i$)
3. Gilt $\varepsilon \sim_L a$? × (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 $aau \sim_L bv$ mit $u, v \in \{a, b\}^*$? ✓

Die Nerode-Relation (2)

Satz

Die Nerode-Relation ist eine Äquivalenzrelation.

Beweis: einfach

Erinnerung: Index einer Äquivalenzrelation:

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

Beispiel: Index

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

$\mathit{Index}(\sim_L) = ?$

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

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

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
- $\mathit{Index}(\approx_M) = |Z|$ (und damit endlich)
- Wir zeigen: $u \approx_M v \implies u \sim_L v$ (d.h. $\approx_M$ verfeinert $\sim_L$)
  Dann gilt auch $\mathit{Index}(\sim_L) \leq \mathit{Index}(\approx_M) = |Z|$ (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

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

- Sei der Index von $\sim_L$ endlich.
- $\Sigma^* = [u_1]_{\sim_L} \cup \ldots \cup [u_n]_{\sim_L}$ 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
  - $E = \{[u_i]_{\sim_L} \mid i \in \{1, \ldots, n\}, u_i \in L\}$.
- Es gilt: $w \in L(M)$
  g.d.w. $\widehat{\delta}([\varepsilon]_{\sim_L}, w) \in E$
  g.d.w. $[w]_{\sim_L} \subseteq L$
  g.d.w. $w \in L$

  Daher gilt: $L(M) = L$

Anwendung des Satzes von Myhill und Nerode

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

1. Regularität nachzuweisen: Zeige $\mathit{Index}(\sim_L)$ ist endlich.
   „oft einfacher: gebe endlichen Automat an, der L akzeptiert / gebe regulären Ausdruck an, der L erzeugt / gebe 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 $Index(\sim_L) = \infty$?

Rezept: 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 $i \neq j$):

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

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

- 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 $\sim_L$.

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

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

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

- 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.

Bemerkung: $a^i \notin [u_i]_{\sim_L}$, denn $a^i a b^{i+1} \in L$ aber $u_i a b^{i+1} \notin L$

Nicht-reguläre Sprache, die die Pumping-Eigenschaft hat

Satz

Die Sprache $L = \{a^k b^l c^l \mid k, l \in \mathbb{N}\} \cup \{b, c\}^*$ ist nicht regulär.

Beweis:

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

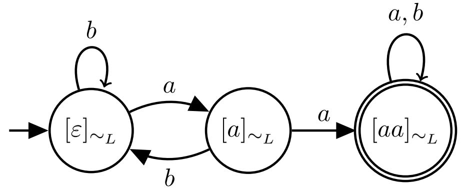
Beispiel: Reguläre Sprache

Sei L Sprache über $\{a, b\}$ mit $L = \{uaav \mid uv \in \{a, b\}^*\}$
Die disjunkten Äquivalenzklassen von $\sim_L$ sind:

- $[\varepsilon]_{\sim_L}$ = alle Worte ohne zwei aufeinanderfolgende a's, die nicht mit a enden
- $[a]_{\sim_L}$ = alle Worte ohne zwei aufeinanderfolgende a's, die mit a enden
- $[aa]_{\sim_L} = L$

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

Nerode-Automat dazu:



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

Minimalautomat

Beweis (Teil 2): (alle minimalen DFAs 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 minimaler DFA mit $L(M') = L$
- Minimalität impliziert $|Z| = |Z'|$.
- Da $\approx_{M'} \subseteq \sim_L$ gilt: $\approx_{M'} = \sim_L$.
- Da auch $\sim_L = \approx_M$ gilt, folgt:
  $$f : Z \to Z' \text{ mit } f([u]_{\approx_M}) = f([u]_{\sim_L}) := [u]_{\approx'_M}$$
  ist ein Isomorphismus auf den Zuständen
- Es gilt auch
  $$\begin{aligned} f(\delta([u]_{\sim_L}, a)) &= f([ua]_{\sim_L}) \\ &= [ua]_{\approx_{M'}} \\ &= \delta'([u]_{\approx_{M'}}, a) \\ &= \delta'(f([u]_{\sim_L}, a)) \end{aligned}$$
- D.h. die Automaten M und M' verhalten sich (bis auf die Umbenennung f) identisch.

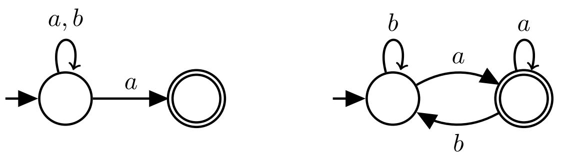
Minimalautomaten: NFAs

Der vorherige Satz zeigt:

Der Nerode-Automat ist eindeutig und minimal.

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:

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

Der Äquivalenzklassenautomat zu M ist der DFA $M' = (Z', \Sigma, \delta', z'_0, E')$ mit

$$\begin{aligned} Z' &= \{[z]_\equiv \mid z \in Z\}, \\ z'_0 &= [z_0]_\equiv, \\ E' &= \{[z]_\equiv \mid z \in E\} \text{ und} \\ \delta'([z]_\equiv, a) &= [\delta(z, a)]_\equiv. \end{aligned}$$

Äquivalenzklassenautomat (2)

Der Automat ist wohldefiniert:

- E' ist wohldefiniert:
  Aus $z \equiv z'$ folgt, dass $z \in E \iff z' \in E$ gilt (dies folgt mit $w = \varepsilon$ aus $z \equiv z'$, denn $\widehat{\delta}(z, w) \in E \iff \widehat{\delta}(z', w) \in E$)
- $\delta([z]_\equiv, a)$ ist eindeutig für alle $[z]_\equiv \in Z', a \in \Sigma$,
  d.h aus $z \equiv z'$ folgt $\delta(z, a) \equiv \delta(z', a)$:

  Sei $z \equiv z'$, dann gilt $\widehat{\delta}(z, w) \in E \iff \widehat{\delta}(z', w) \in E$ und damit auch
  $\widehat{\delta}(z, aw) \in E \iff \widehat{\delta}(z', aw) \in E$ und damit auch
  $\widehat{\delta}(\delta(z, a), w) \in E \iff \widehat{\delta}(\delta(z', a), w) \in E$. D. h. es gilt dann auch
  $\delta(z, a) \equiv \delta(z', a)$.

Äquivalenzklassenautomat: Korrektheit und Minimalität

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 Vorlesung

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):

- Da alle $z \in Z$ erreichbar, 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
  (dann gibt es nicht mehr als $\mathit{Index}(\sim_L)$ erreichbare Zustände.)
- Da alle $z' \in Z'$ erreichbar, gilt damit $|Z'| = \mathit{Index}(\sim_L)$

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, Forts.):

- Seien $u, u' \in [v]_{\sim_L}$, d. h. $u \sim_L u'$. Dann gilt
  $\forall w \in \Sigma^* : uw \in L \iff u'w \in L,$
  woraus folgt: $\forall w \in \Sigma^* : \widehat{\delta'}(z'_0, uw) \in E' \iff \widehat{\delta'}(z'_0, u'w) \in E'$
  woraus folgt: $\forall w \in \Sigma^* : \widehat{\delta'}(\widehat{\delta'}(z'_0, u), w) \in E' \iff \widehat{\delta'}(\widehat{\delta'}(z'_0, u'), w) \in E'$
  woraus folgt: $\widehat{\delta'}(z'_0, u) \equiv \widehat{\delta'}(z'_0, u')$
  woraus folgt: $[\widehat{\delta'}(z'_0, u)]_\equiv = [\widehat{\delta'}(z'_0, u')]_\equiv$.