

FORMALE SYSTEME

9. Vorlesung: Minimale Automaten (2)

Hannes Straß

Folien: © Markus Krötzsch, <https://iccl.inf.tu-dresden.de/web/FS2020>, CC BY 3.0 DE

TU Dresden, 8. November 2021

Verschiedene Äquivalenzrelationen

Für einen DFA \mathcal{M} und eine Sprache \mathbf{L} haben wir verschiedene Äquivalenzrelationen verwendet:

DFA-Zustandsäquivalenz $\sim_{\mathcal{M}} \subseteq Q \times Q$:
 $q \sim_{\mathcal{M}} p$ genau dann, wenn für alle $w \in \Sigma^*$ gilt: $\delta(q, w) \in F$ gdw. $\delta(p, w) \in F$.

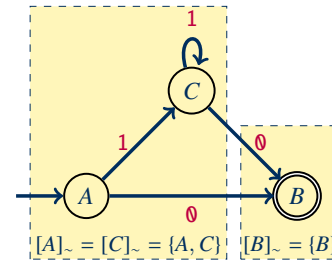
Anwendung: Vereinfachung von DFAs durch Quotientenbildung

Nerode-Rechtskongruenz $\approx_{\mathbf{L}} \subseteq \Sigma^* \times \Sigma^*$:
 $u \approx_{\mathbf{L}} v$ genau dann, wenn für alle $w \in \Sigma^*$ gilt: $uw \in \mathbf{L}$ gdw. $vw \in \mathbf{L}$.

Anwendung: automatenunabhängige Analyse von Sprachen; alternative Konstruktion eines Minimalautomaten

Automaten verkleinern mit Quotientenbildung

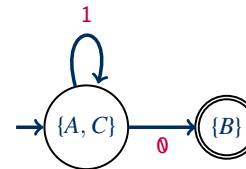
Wir betrachten DFAs mit totaler Übergangsfunktion.



Ermittlung der Zustandsäquivalenz \sim :

	A	B
C		ϵ
B	ϵ	

Quotientenautomat:



Hannes Straß, TU Dresden

Sei \mathcal{M} ein DFA mit totaler Übergangsfunktion. Der **reduzierte Automat** \mathcal{M} , ergibt sich durch folgende Schritte:

- (1) Entferne alle unerreichbaren Zustände aus \mathcal{M}
- (2) Berechne den Quotientenautomaten

Formale Systeme, VL 9

Folie 3 von 29

Der Satz von Myhill und Nerode

\simeq und reguläre Sprachen

Satz: Wenn L regulär ist, dann hat \simeq_L endlich viele Äquivalenzklassen.

(Die Anzahl der Äquivalenzklassen wird auch als **Index** bezeichnet.)

Beweis: Wir erhalten diese Eigenschaft aus der Darstellung von L mit einem DFA.

Für einen DFA $\mathcal{M} = \langle Q, \Sigma, \delta, q_0, F \rangle$ definieren wir eine Relation $\simeq_{\mathcal{M}}$ wie folgt. Für Wörter $u, v \in \Sigma^*$ sei $u \simeq_{\mathcal{M}} v$ genau dann, wenn gilt:

$$\delta(q_0, u) = \delta(q_0, v).$$

Offensichtlich ist $\simeq_{\mathcal{M}}$ eine Äquivalenzrelation (Eigenschaften „geerbt“ von =) mit endlichem Index (es gibt nur endlich viele Zustände).

\simeq und reguläre Sprachen (3)

Satz: Wenn L regulär ist, dann hat \simeq_L endlich viele Äquivalenzklassen.

Beweis (Fortsetzung): Wir haben gezeigt, dass $\simeq_{\mathcal{M}} \subseteq \simeq_L$.

- Jede \simeq_L -Äquivalenzklasse besteht aus einer oder mehreren $\simeq_{\mathcal{M}}$ -Äquivalenzklassen.
- Der Index von \simeq_L ist kleiner oder gleich dem Index von $\simeq_{\mathcal{M}}$.
- Der Index von \simeq_L ist endlich. □

Anmerkung: Der letzte Teil ist eine allgemeine Eigenschaft aller Äquivalenzrelationen. Für Äquivalenzrelationen $R, S \subseteq M \times M$ gilt: Wenn $R \subseteq S$, dann ist der Index von R größer oder gleich dem Index von S .

Die „kleinste“ Äquivalenzrelation, die Gleichheit $\{(m, m) \mid m \in M\}$, hat den größten Index (die Anzahl der Elemente der Grundmenge M); die „größte“ Äquivalenzrelation, $M \times M$, hat nur eine Äquivalenzklasse (alle Elemente sind zueinander äquivalent). Formal gilt: $\{(m, m) \mid m \in M\} \subseteq R \subseteq S \subseteq M \times M$.

\simeq und reguläre Sprachen (2)

Satz: Wenn L regulär ist, dann hat \simeq_L endlich viele Äquivalenzklassen.

Beweis (Fortsetzung): Behauptung: $\simeq_{\mathcal{M}} \subseteq \simeq_L$, also:

Für alle $u, v \in \Sigma^*$ folgt aus $u \simeq_{\mathcal{M}} v$ stets $u \simeq_L v$.

Wir betrachten einen DFA \mathcal{M} mit $L = L(\mathcal{M})$.

- Seien $u, v \in \Sigma^*$ Wörter mit $u \simeq_{\mathcal{M}} v$.
- Dann ist $\delta(q_0, u) = \delta(q_0, v)$.
- Dann gilt für alle $w \in \Sigma^*$: $\delta(q_0, uw) = \delta(q_0, vw)$.
- Dann gilt für alle $w \in \Sigma^*$: $\delta(q_0, uw) \in F$ gdw. $\delta(q_0, vw) \in F$.
- Dann gilt für alle $w \in \Sigma^*$: $uw \in L(\mathcal{M})$ gdw. $vw \in L(\mathcal{M})$.
- Dann ist $u \simeq_{L(\mathcal{M})} v$ und daher $u \simeq_L v$.

Damit ist die Behauptung gezeigt.

Verschiedene Äquivalenzrelationen

Für einen DFA \mathcal{M} und eine Sprache L haben wir verschiedene Äquivalenzrelationen verwendet:

DFA-Zustandsäquivalenz $\sim_{\mathcal{M}} \subseteq Q \times Q$:

$q \sim_{\mathcal{M}} p$ genau dann, wenn für alle $w \in \Sigma^*$ gilt: $\delta(q, w) \in F$ gdw. $\delta(p, w) \in F$.

Anwendung: Vereinfachung von DFAs durch Quotientenbildung

Nerode-Rechtskongruenz $\simeq_L \subseteq \Sigma^* \times \Sigma^*$:

$u \simeq_L v$ genau dann, wenn für alle $w \in \Sigma^*$ gilt: $uw \in L$ gdw. $vw \in L$.

Anwendung: automatenunabhängige Analyse von Sprachen; alternative Konstruktion eines Minimalautomaten

DFA-Präfixäquivalenz $\simeq_{\mathcal{M}} \subseteq \Sigma^* \times \Sigma^*$:

$u \simeq_{\mathcal{M}} v$ genau dann, wenn gilt: $\delta(q_0, u) = \delta(q_0, v)$.

Anwendung: Beweis der Endlichkeit des \simeq_L -Indexes regulärer Sprachen

Der Satz von Myhill und Nerode

Das vorige Resultat kann noch verstärkt werden:

Satz (Myhill & Nerode):

Eine Sprache L ist genau dann regulär, wenn \approx_L endlich viele Äquivalenzklassen hat.

Beweis: Die Richtung „ \Rightarrow “ haben wir soeben gezeigt.

Für die Richtung „ \Leftarrow “ zeigen wir, wie man einen DFA M_L für L erhalten kann, wenn \approx_L endlich viele Äquivalenzklassen hat.

Der DFA $M_L = \langle Q, \Sigma, \delta, q_0, F \rangle$ ist wie folgt definiert:

- $Q = \{[w]_{\approx} \mid w \in \Sigma^*\}$ ist die (endliche) Menge der \approx -Äquivalenzklassen
- $q_0 = [\epsilon]_{\approx}$
- $F = \{[w]_{\approx} \mid w \in L\}$
- $\delta([w]_{\approx}, a) = [wa]_{\approx}$

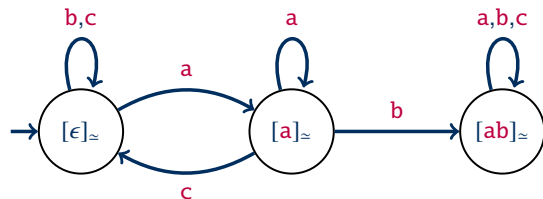
Anmerkung: Diese Definition von F und δ ist zulässig, weil sie nicht vom gewählten Repräsentanten w abhängt. (\approx ist eine Rechtskongruenz.)

Beispiel

Wir betrachten die Konstruktion von Myhill & Nerode für die Sprache

$L = \{w \mid w \text{ enthält kein Infix } ab\}$ über dem Alphabet $\Sigma = \{a, b, c\}$:

Klasse C	erlaubte Suffixe w mit $C \cdot \{w\} \subseteq L$	C als Menge
$[\epsilon]_{\approx}$	$w \in L$	$\{v \in L \mid v \text{ endet nicht auf } a\}$
$[a]_{\approx}$	$w \in L, w$ beginnt nicht mit b	$\{v \in L \mid v \text{ endet auf } a\}$
$[ab]_{\approx}$	keine	$\{v \mid v \notin L\}$



Satz von Myhill und Nerode: Beweis

Beweis (Fortsetzung): Wir müssen noch zeigen, dass $L = L(M_L)$.

$$\begin{aligned}
 w \in L(M_L) &\text{ gdw. } \delta(q_0, w) \in F \\
 &\text{ gdw. } \delta([\epsilon]_{\approx}, w) \in F \\
 &\text{ gdw. } [w]_{\approx} \in F \quad \text{wegen } \delta([u], v) = [uv] \\
 &\hspace{10em} \text{(Induktion über } |v|) \\
 &\text{ gdw. } w \in L
 \end{aligned}$$

□

Quiz: Konstruktion von Myhill und Nerode

$\approx_L \subseteq \Sigma^* \times \Sigma^*$: $u \approx_L v$ genau dann, wenn für alle $w \in \Sigma^*$ gilt: $uw \in L$ gdw. $vw \in L$.

Quiz: Wir betrachten das Alphabet $\Sigma = \{0, 1\}$ und darüber die formale Sprache ...

$\mathcal{M}_{\mathbf{L}}$ ist minimal

Für reguläre \mathbf{L} haben wir bereits gezeigt:

- $\mathcal{M}_{\mathbf{L}}$ ist ein DFA, da er insbesondere endlich viele Zustände hat (Index von \approx).
- $\mathbf{L}(\mathcal{M}_{\mathbf{L}}) = \mathbf{L}$

Als nächstes interessiert uns der Bezug zum Minimalautomaten:

Satz: $\mathcal{M}_{\mathbf{L}}$ hat unter allen totalen DFAs, die \mathbf{L} erkennen, eine minimale Anzahl an Zuständen.

Beweis: Sei \mathcal{M} ein beliebiger totaler DFA mit $\mathbf{L}(\mathcal{M}) = \mathbf{L}$.

- Wir haben bereits gezeigt: $\approx_{\mathcal{M}} \subseteq \approx_{\mathbf{L}}$.
- Daraus folgerten wir:
„Zahl der $\approx_{\mathbf{L}}$ -Äquivalenzklassen \leq Anzahl der erreichbaren Zustände von \mathcal{M} .“
- Die Zahl der $\approx_{\mathbf{L}}$ -Äquivalenzklassen ist aber genau die Anzahl der Zustände von $\mathcal{M}_{\mathbf{L}}$.
- Also hat \mathcal{M} mindestens so viele erreichbare Zustände, wie $\mathcal{M}_{\mathbf{L}}$ Zustände hat. \square

Isomorphismen von Automaten

„Isomorph“ bedeutet „gleich bis auf Umbenennung von Zuständen“:

Ein **Isomorphismus** zwischen zwei DFAs $\mathcal{M}_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle$ und $\mathcal{M}_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ ist eine bijektive Funktion $f : Q_1 \rightarrow Q_2$, so dass gilt:

- $f(q_1) = q_2$
- $f(\delta_1(q, \mathbf{a})) = \delta_2(f(q), \mathbf{a})$ für alle $\mathbf{a} \in \Sigma$
- $\{f(q) \mid q \in F_1\} = F_2$

Zwei Automaten sind **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

Man kann leicht zeigen, dass isomorphe Automaten die selbe Sprache akzeptieren.

Weitere Eigenschaften von $\mathcal{M}_{\mathbf{L}}$

Für reguläre \mathbf{L} haben wir bereits gezeigt:

- $\mathcal{M}_{\mathbf{L}}$ ist ein DFA, da er insbesondere endlich viele Zustände hat (Index von \approx).
- $\mathbf{L}(\mathcal{M}_{\mathbf{L}}) = \mathbf{L}$
- Jeder Zustand $q \in Q$ von $\mathcal{M}_{\mathbf{L}}$ ist vom Startzustand aus erreichbar:
Für jedes $w \in \Sigma^+ \neq \emptyset$ gilt $\delta(q_0, w) = \delta([\epsilon]_{\approx}, w) = [w]_{\approx} = q$.
- $\approx_{\mathcal{M}_{\mathbf{L}}} = \approx_{\mathbf{L}}$ (\clubsuit)

Beweis (\clubsuit): $\approx_{\mathcal{M}_{\mathbf{L}}} \subseteq \approx_{\mathbf{L}}$ haben wir bereits für beliebige DFA gezeigt

$\approx_{\mathcal{M}_{\mathbf{L}}} \supseteq \approx_{\mathbf{L}}$ kann wie folgt gezeigt werden:

- Seien $u, v \in \Sigma^*$ beliebige Wörter mit $u \approx_{\mathbf{L}} v$.
- Dann gilt für $\mathcal{M}_{\mathbf{L}}$: $\delta(q_0, u) = \delta([\epsilon]_{\approx}, u) = [u]_{\approx} = [v]_{\approx} = \delta([\epsilon]_{\approx}, v) = \delta(q_0, v)$.
- Also ist $u \approx_{\mathcal{M}_{\mathbf{L}}} v$. \square

Quiz: Isomorphismen von Automaten

Ein **Isomorphismus** zwischen zwei DFAs $\mathcal{M}_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle$ und $\mathcal{M}_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ ist eine bijektive Funktion $f : Q_1 \rightarrow Q_2$, so dass gilt:

$$f(q_1) = q_2, \quad f(\delta_1(q, \mathbf{a})) = \delta_2(f(q), \mathbf{a}) \text{ für alle } \mathbf{a} \in \Sigma, \quad \{f(q) \mid q \in F_1\} = F_2.$$

Zwei Automaten sind **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

Quiz: Gegeben seien die beiden Automaten \mathcal{M}_1 und \mathcal{M}_2 über $\Sigma = \{0, 1\}$:

...

Eindeutigkeit des Minimalautomaten

Satz: Ist L eine reguläre Sprache, M ein DFA mit totaler Übergangsfunktion und $L(M) = L$, so sind der reduzierte Automat M_r und der Myhill-Nerode-Minimalautomat M_L isomorph.

Beweis: Sei $M_L = \langle Q, \Sigma, \delta, q_0, F \rangle$ und $M_r = \langle Q_r, \Sigma, \delta_r, q_r, F_r \rangle$.

$M_L = \langle Q, \Sigma, \delta, q_0, F \rangle$ mit:

- $Q = \{[w]_{\simeq} \mid w \in \Sigma^*\}$
- $q_0 = [\epsilon]_{\simeq}$
- $F = \{[w]_{\simeq} \mid w \in L\}$
- $\delta([w]_{\simeq}, a) = [wa]_{\simeq}$

$M_r = \langle Q_r, \Sigma, \delta_r, q_r, F_r \rangle$:

- (1) Entferne unerreichbare Zustände
- (2) Berechne den Quotienten-DFA bzgl. \sim

Wir definieren eine Funktion $f : Q_r \rightarrow Q$ wie folgt:

Für $q \in Q_r$ wähle ein Wort w mit $\delta_r(q_r, w) = q$ und setze $f(q) = [w]_{\simeq}$.

Eindeutigkeit des Minimalautomaten (3)

Es bleibt zu zeigen: f ist ein Isomorphismus von M_r zu M_L .

- (1) „ $f(q_r) = q_0$ “: Es gilt $\delta_r(q_r, \epsilon) = q_r$ und daher $f(q_r) = [\epsilon]_{\simeq} = q_0$.
- (2) „ $f(\delta_r(q, a)) = \delta(f(q), a)$ “:
 - Sei w ein Wort mit $\delta_r(q_r, w) = q$.
 - Dann ist $\delta_r(q_r, wa) = \delta_r(q, a)$ und daher $f(\delta_r(q, a)) = [wa]_{\simeq}$.
 - Andererseits gilt $f(q) = [w]_{\simeq}$ und daher auch $\delta(f(q), a) = [wa]_{\simeq}$.
- (3) „ $\{f(q) \mid q \in F_r\} = F$ “: Übung

□

Damit ist der Satz bewiesen:

Satz: Ist L eine reguläre Sprache, M ein DFA mit totaler Übergangsfunktion und $L(M) = L$, so sind der reduzierte Automat M_r und der Myhill-Nerode-Minimalautomat M_L isomorph.

Eindeutigkeit des Minimalautomaten (2)

Für $q \in Q_r$ wähle ein Wort w mit $\delta_r(q_r, w) = q$ und setze $f(q) = [w]_{\simeq}$.

Ist f wohldefiniert?

- Für jeden Zustand $q \in Q_r$ gibt es ein geeignetes Wort w , da alle Zustände in M_r vom Startzustand q_r aus erreichbar sind.
- Die konkrete Wahl von w ist dabei unerheblich:
 - Wenn $\delta_r(q_r, w) = q = \delta_r(q_r, w')$,
 - dann $w \simeq_{M_r} w'$,
 - dann $w \simeq_L w'$ (wie zuvor gezeigt),
 - dann $[w]_{\simeq} = [w']_{\simeq}$.

$\leadsto f$ ist wohldefiniert.

Zusammenfassung: Eigenschaften von M_L

Für reguläre L haben wir bereits gezeigt:

- M_L ist ein DFA, da er insbesondere endlich viele Zustände hat (Index von \simeq).
- $L(M_L) = L$
- Jeder Zustand von M_L ist vom Startzustand aus erreichbar, da $\delta([\epsilon]_{\simeq}, w) = [w]_{\simeq}$.
- $\simeq_{M_L} = \simeq_L$
- M_L ist isomorph zu jedem reduzierten Automaten für L .

Daraus folgt auch:

Satz: Alle minimalen DFA mit totaler Übergangsfunktion, die $L(M)$ erkennen, sind bis auf Umbenennung von Zuständen gleich (sie sind **isomorph**). Daher hängt M_r nur von $L(M)$ ab, nicht von M .

Automaten vergleichen

Wir wissen, dass reduzierte Automaten isomorph sind, wenn sie die selbe Sprache akzeptieren.

Damit können wir Äquivalenz zweier Automaten testen:

Eingabe: Zwei endliche Automaten \mathcal{M}_1 und \mathcal{M}_2

Ausgabe: Ist $L(\mathcal{M}_1) = L(\mathcal{M}_2)$?

- Transformiere \mathcal{M}_1 und \mathcal{M}_2 falls nötig in DFAs mit totaler Übergangsfunktion
- Bestimme die reduzierten Automaten
- Teste, ob die reduzierten Automaten isomorph sind (z.B. naiv durch systematisches Durchprobieren aller Bijektionen)

Auf ähnlichem Weg kann man auch reguläre Ausdrücke und reguläre Grammatiken vergleichen. Es gibt allerdings zum Teil effizientere Verfahren ...

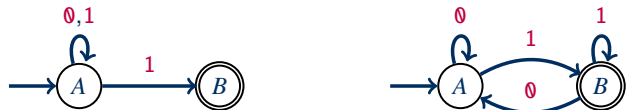
Minimale NFAs?

Alle Ergebnisse zu Minimalautomaten gehen von DFAs aus ...

→ NFAs könnten viel kleiner sein als minimale DFAs!

Für NFAs gibt es keine vergleichbar elegante Art der Minimierung.

Beispiel: Die folgenden beiden NFAs akzeptieren die selbe Sprache („Wörter die auf 1 enden“) und sind von minimaler Größe, aber sie sind nicht isomorph:



- NFA-Minimierung ist algorithmisch aufwändiger
- ... und liefert kein eindeutiges Ergebnis,
- ... ist aber durchaus praktisch machbar.

Minimieren ohne totale Übergänge?

Alle Ergebnisse zu Minimalautomaten gehen von DFAs mit totaler Übergangsfunktion aus.

Diskussion:

- Jeder DFA kann leicht in einen totalen umgewandelt werden (ein zusätzlicher Fangzustand).
- Der Fangzustand entspricht der Nerode-Kongruenzklasse $\{w \mid w \text{ ist kein Präfix eines Wortes in } L\}$.
- In minimalen Automaten gibt es daher maximal einen entsprechenden Fangzustand, den man weglassen könnte, ohne die akzeptierte Sprache zu ändern.¹
- Man kann DFAs ohne totale Übergangsfunktion auch direkt reduzieren, wobei der Algorithmus zur Bestimmung von \sim ausgeführt wird, als ob man einen Fangzustand definiert hätte.

¹Ausnahme: Der DFA der leeren Sprache benötigt diese (einzige!) Klasse.

Sind NFAs wirklich kompakter?

Beispiel aus Vorlesung 4: $L_n = \{0, 1\}^* 1 \{0, 1\}^{n-1}$ („Wörter mit 1 an n -letzter Stelle“)

Wir haben gesehen, dass es dafür NFAs der Größe $n + 1$ gibt.

DFAs benötigen dagegen mindestens 2^n Zustände.

Beweis: Mit Hilfe von Myhill/Nerode:

- Die Kongruenzklassen haben die Form $[w]_{\sim}$ mit $w \in \{0, 1\}^n$.
- Jede dieser Klassen ist unterschiedlich, z.B. für $n = 3$:
wenn $v \in [011]$ dann $v \notin L_3$, $v0 \in L_3$ und $v00 \in L_3$.
wenn $v \in [101]$ dann $v \in L_3$, $v0 \notin L_3$ und $v00 \in L_3$.
...
- Es gibt also mindestens 2^n Kongruenzklassen, daher mindestens 2^n Zustände im Minimal-DFA.

Ausblick: Nichtreguläre Sprachen

Nichtreguläre Sprachen

Sind alle Sprachen regulär?

Sicher nicht – dazu gibt es zu viele Sprachen.

Sind alle Typ-0-Sprachen regulär?

Nein, auch das gilt nicht.

Wie aber zeigt man das?

- Behauptung „Sprache **L** ist regulär!“ \leadsto Es genügt, **einen** Automaten, regulären Ausdruck oder eine Typ-3-Grammatik für **L** anzugeben.
- Behauptung „Sprache **L** ist nicht regulär!“ \leadsto Man müsste zeigen, dass es **keinen** Automaten, **keinen** regulären Ausdruck bzw. **keine** Typ-3-Grammatik für **L** gibt.

Zusammenfassung und Ausblick

Der **Satz von Myhill und Nerode** charakterisiert reguläre Sprachen und liefert einen direkt konstruierten DFA für eine Sprache.

Der **reduzierte DFA** ist minimal und eindeutig.

NFAs können viel kleiner sein als minimale DFAs, aber ihre Minimierung ist viel komplizierter.

Offene Fragen:

- Wie findet man nichtreguläre Sprachen?
- Welche weiteren Berechnungsaufgaben gibt es im Zusammenhang mit regulären Sprachen?
- Und was ist mit kontextfreien Sprachen?