Grundbegriffe der Theoretischen Informatik

Sommersemester 2018 - Thomas Schwentick

Teil A: Reguläre Sprachen

4: Minimierung von Automaten

Version von: 24. April 2018 (12:31)

Der Borussia-Newsticker-Automat (1/3)

- Ich habe einen Bekannten, der ein ziemlich großer Fan von Borussia ist
- Er sammelt auch Fanartikel, die mit Borussia zu tun haben und verfolgt einen Newsticker, der ihn über Auktionen informiert
- Dabei möchte er vor allem Auktionen finden, in deren Beschreibung der Name „Borussia“ falsch geschrieben wurde (borusssia, borusia, borrussia, brussia, borissia)
- Können wir ihm dabei helfen?

Definition (MultiSearch)

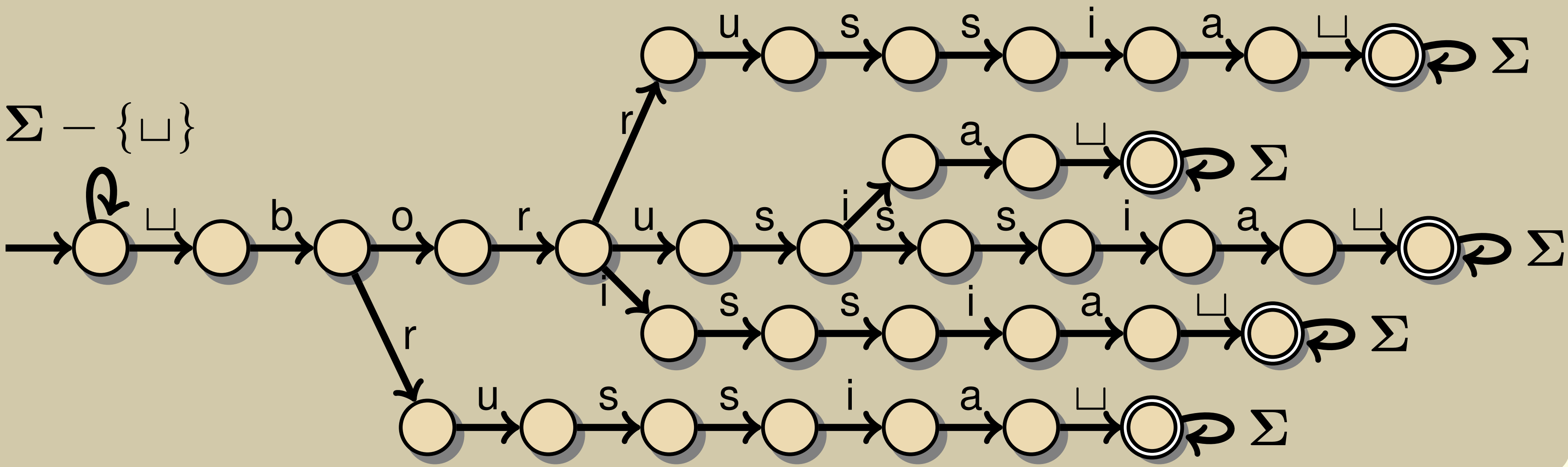
Gegeben: Menge $M = \{w_1, \ldots, w_n\}$ von Zeichenketten, String v

Frage: Kommt einer der Strings $w_1, \ldots, w_n$ in v vor?

- v entspricht also dem Newsticker
- $w_1, \ldots, w_n$ entsprechen den möglichen (richtigen und falschen) Schreibweisen von „Borussia“

Der Borussia-Newsticker-Automat (2/3)

Beispiel: Umsetzung als DFA



- $\Sigma = \{a, \dots, z, \sqcup\}$ ☞ $\sqcup$ steht für das Leerzeichen

- Jeder Zustand hat ausgehende Transitionen für alle Symbole aus Σ
  - Nicht angezeigte Transitionen, bei denen Blanks gelesen werden, führen in den zweiten Zustand
  - Alle anderen nicht angezeigten Transitionen führen in den Startzustand

- **Ist diese Lösung optimal?**
- Oder gibt es einen kleineren Automaten für die „Borussia-Sprache“?

Idee: Wim Martens

Minimierung endlicher Automaten: Fragen & Antworten

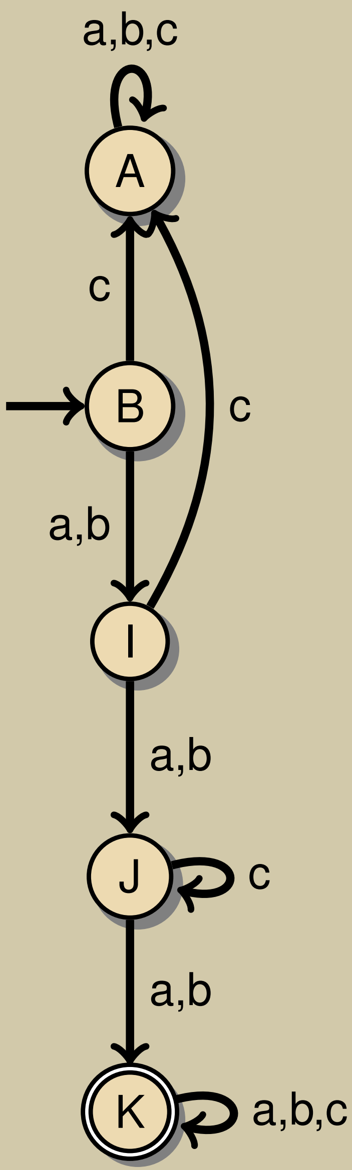
- Gibt es zu jedem DFA einen kleinsten äquivalenten DFA? ☞ Natürlich!

- Wieviele verschiedene kleinste äquivalente DFAs kann es geben? ☞ Nur einen, bis auf Isomorphie
- Kann man zu jedem DFA effizient den kleinsten äquivalenten DFA konstruieren?
  ☞ Ja, das ist sogar ziemlich einfach

- Zur genaueren Beantwortung dieser Fragen müssen wir die Struktur regulärer Sprachen etwas besser verstehen
- Dabei hilft uns eine etwas „mathematischere“ Sicht auf reguläre Sprachen

Minimierung: Grundidee

Beispiel



Beispiel

- Unerreichbare Zustände können gelöscht werden: ☞ G und H
- Mehrere Zustände, für die alle Übergänge in dieselben Zustände führen, und die alle akzeptierend oder alle ablehnend sind, können verschmolzen werden: ☞ E und K
- Senkenzustände können verschmolzen werden: ☞ L und A
- Allgemein: Zustände, von denen aus das Akzeptierverhalten für alle nachfolgenden Eingabesequenzen (inklusive ϵ) gleich ist, können verschmolzen werden:
  - D, F, und J
  - C und I

- Was heißt „das Akzeptierverhalten für alle nachfolgenden Eingabesequenzen ist gleich“ genau?
- Wie lassen sich die verschmelzbaren Zustände systematisch berechnen?

Inhalt

Nerode-Relation: Definition und Beispiel

- Die folgende Definition präzisiert den vagen Begriff „das Akzeptierverhalten für alle möglichen nachfolgenden Eingabesequenzen ist gleich“ durch eine Äquivalenzrelation für Strings

Definition (Nerode-Relation, $\sim_L$)

- Sei $L \subseteq \Sigma^*$ eine Sprache
- Die **Nerode-Relation** $\sim_L$ auf Σ^* ist auf Σ^* definiert durch:
  - $x \sim_L y \overset{\text{def}}{\Leftrightarrow}$ für alle $z \in \Sigma^*$ gilt:
    $$xz \in L \iff yz \in L$$

- Wir werden sehen: ein DFA ist minimal für L, wenn jeweils alle Strings, die bezüglich $\sim_L$ äquivalent sind, den DFA in den selben Zustand bringen

Beispiel

- Sei $L = L_g$ ☞ gerade vielen Einsen und Nullen
- Wann sind zwei Strings x und y bezüglich $\sim_L$ äquivalent?
  - Gilt $011 \sim_L 01$?
    - Nein: denn die Wahl von $z = 0$ ergibt:
      - $(xz =)\ 0110 \in L$ aber
      - $(yz =)\ 010 \notin L$
  - Gilt $10 \sim_L 010$?
    - Nein: denn die Wahl von $z = 1$ ergibt:
      - $(xz =)\ 101 \notin L$ aber
      - $(yz =)\ 0101 \in L$
  - Gilt $100 \sim_L 10110$?
    - Ja: Beide haben ungerade viele Einsen und gerade viele Nullen und erreichen L durch Anhängen von Strings mit ungerade vielen Einsen und gerade vielen Nullen
- Beobachtung: $\sim_L$ hat vier Äquivalenzklassen

Exkurs: Äquivalenzrelationen (1/3)

- Sei A eine Menge
- $\underline{A^n} \stackrel{\text{def}}{=}$ Menge der n-Tupel mit Einträgen aus A
- Eine Menge $R \subseteq A^n$ heißt **n-stellige Relation über A**

Beispiel

- **Gleiches-Semester-Relation**:
  - A: Menge aller Studierenden, $R \subseteq A^2$
  - $(x, y) \in R$, falls x und y im selben Semester sind

- **Gleicher-Rest-Relation modulo k**:
  - A : Menge $\mathbb{N}$ der natürlichen Zahlen, $R \subseteq \mathbb{N}^2$
  - $(x, y) \in R$ falls x und y bei Division durch k den selben Rest haben
    - Schreibweise: $x \equiv_k y$

Exkurs: Äquivalenzrelationen (2/3)

Definition (Äquivalenzrelation)

- Eine 2-stellige (binäre) Relation $\boldsymbol{R}$ über $\boldsymbol{A}$ heißt
  - **reflexiv** $\overset{\text{def}}{\Leftrightarrow}$ für alle $\boldsymbol{x} \in \boldsymbol{A}$ gilt: $(\boldsymbol{x}, \boldsymbol{x}) \in \boldsymbol{R}$
  - **symmetrisch** $\overset{\text{def}}{\Leftrightarrow}$ für alle $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{A}$ gilt: $(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{R} \Rightarrow (\boldsymbol{y}, \boldsymbol{x}) \in \boldsymbol{R}$
  - **transitiv** $\overset{\text{def}}{\Leftrightarrow}$ für alle $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \boldsymbol{A}$ gilt: $(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{R}, (\boldsymbol{y}, \boldsymbol{z}) \in \boldsymbol{R} \Rightarrow (\boldsymbol{x}, \boldsymbol{z}) \in \boldsymbol{R}$

- Eine 2-stellige reflexive, symmetrische, transitive Relation heißt **Äquivalenzrelation**

Beobachtung

- $\sim_{\boldsymbol{L}}$ ist eine **Äquivalenzrelation**

- Äquivalenzrelationen werden oft mit $\sim$ statt $\boldsymbol{R}$ bezeichnet
- Infix-Notation: $\boldsymbol{x} \sim \boldsymbol{y}$ statt $(\boldsymbol{x}, \boldsymbol{y}) \in \sim$
- Beispiele: Gleiches-Semester-Relation, Gleicher-Rest-Relation

- **Äquivalenzklasse:** maximale Menge $\boldsymbol{K}$ von Elementen, so dass für alle $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{K}$: $\boldsymbol{x} \sim \boldsymbol{y}$
- $[\boldsymbol{x}] \overset{\text{def}}{=}$ Äquivalenzklasse von $\boldsymbol{x}$, also die Menge aller $\boldsymbol{y}$ mit $\boldsymbol{x} \sim \boldsymbol{y}$
- Wird eine Äquivalenzklasse in der Form $[\boldsymbol{x}]$ benannt, so wird $\boldsymbol{x}$ oft als **Repräsentant** dieser Klasse bezeichnet

- Es gilt: $\boldsymbol{y} \in [\boldsymbol{x}] \iff [\boldsymbol{y}] = [\boldsymbol{x}]$

Beispiel

- Bezüglich der $\equiv_6$-Relation gilt:
  $$[2] = \{2, 8, 14, 20, \dots\}$$

Satz von Myhill und Nerode (1/5)

- Zur Erinnerung:
  $x \sim_L y \overset{\text{def}}{\Leftrightarrow}$ für alle $z \in \Sigma^*$ gilt
  $$(xz \in L \iff yz \in L)$$

Satz 4.1 (Myhill, Nerode)

- Eine Sprache L ist genau dann regulär, wenn $\sim_L$ endlich viele Äquivalenzklassen hat

- Dieser Satz ist das Herzstück dieses Kapitels

- Er liefert uns:
  - eine Methode zum Nachweis, dass eine Sprache regulär ist
  - eine Methode zum Nachweis, dass eine Sprache nicht regulär ist

- Sein Beweis wird uns außerdem liefern:
  - einen Beweis, dass der minimale DFA für eine reguläre Sprache eindeutig ist

    ☞ bis auf Isomorphie
  - einen Ansatz zur Berechnung des minimalen DFAs

- Der Beweis des Satzes beruht auf zwei einfachen Ideen

- „$\sim_L$ endlich $\Rightarrow$ L regulär“:
  - Aus den Äquivalenzklassen der Relation $\sim_L$ lässt sich ein Automat für L konstruieren: der Äquivalenzklassenautomat
  - Und wenn $\sim_L$ nur endlich viele Klassen hat, ist das ein DFA

- „L regulär $\Rightarrow$ $\sim_L$ endlich“:
  - Jeder DFA für L „bezeugt“, dass $\sim_L$ endlich ist

Satz von Myhill und Nerode (2/5)

Satz 4.1

- Eine Sprache L ist genau dann regulär, wenn $\sim_L$ endlich viele Äquivalenzklassen hat

Beweis

- Wir zeigen zuerst:
  $\sim_L$ hat endlich viele Klassen $\Rightarrow$ L ist regulär

- Wir definieren den **Äquivalenzklassenautomaten** $\mathcal{A}_L \stackrel{\text{def}}{=} (Q, \Sigma, \delta, s, F)$ für L wie folgt:
  - Q ist die Menge der Äquivalenzklassen von $\sim_L$
  - $s \stackrel{\text{def}}{=} [\epsilon]$
  - $F \stackrel{\text{def}}{=} \{[x] \mid x \in L\}$
  - für alle $x \in \Sigma^*, \sigma \in \Sigma$:
    $$\delta([x], \sigma) \stackrel{\text{def}}{=} [x\sigma]$$

Beweis (Forts.)

- Vorsicht: δ ist mit Hilfe von Repräsentanten der Klassen definiert
  - ➞ wir müssen zeigen, dass die Definitionen des Funktionswertes nicht von der Wahl des Repräsentanten abhängen
  - Also: wenn wir zwei verschiedene Strings x, y aus einer Äquivalenzklasse von $\sim_L$ für die Definition von δ verwenden, erhalten wir jeweils das selbe Ergebnis

- Behauptungen:
  - (1) δ ist wohldefiniert:
    $$x \sim_L y \Rightarrow x\sigma \sim_L y\sigma$$
  - (2) F ist sinnvoll definiert:
    $$[x] \in F \iff x \in L$$
  - (3) $L(\mathcal{A}_L) = L$

Satz von Myhill und Nerode: Beweis (3/5)

Beweis (Forts.)

(1) Zu zeigen: falls $x \sim_L y$, so gilt für alle $\sigma \in \Sigma$:
- $x\sigma \sim_L y\sigma$

- Sei also $x \sim_L y$ und $\sigma \in \Sigma$
- Sei $z \in \Sigma^*$ beliebig:

$$\begin{aligned}(x\sigma)z \in L &\iff x(\sigma z) \in L \\ &\iff y(\sigma z) \in L \quad \text{☞ wegen } x \sim_L y \\ &\iff (y\sigma)z \in L\end{aligned}$$

(2) Zu zeigen: $[x] \in F \iff x \in L$
- $[x] \in F \Rightarrow$ es gibt y mit $x \sim_L y$ und $y \in L$

➨ Mit $z = \epsilon$ ergibt sich $x \in L \iff y \in L$, also: $x \in L$

- Umgekehrt folgt aus $x \in L$ auch $[x] \in F$

☞ Definition von F

Satz von Myhill und Nerode: Beweis (4/5)

Beweis (Forts.)

(3) Wir zeigen zunächst durch Induktion, dass für alle $w \in \Sigma^*$ gilt:

$$\delta^*(s, w) = [w] \qquad (\#)$$

– $w = \epsilon$ ✓ ☞ Definition von s

– $w = u\sigma$:

$$\begin{aligned} \delta^*(s, u\sigma) &= \delta(\delta^*(s, u), \sigma) && \text{☞ Def. } \delta^* \\ &= \delta([u], \sigma) && \text{☞ Ind.} \\ &= [u\sigma] && \text{☞ Def. } \delta \end{aligned}$$

– Also:

$$\begin{aligned} w \in L(\mathcal{A}_L) &\iff \delta^*(s, w) \in F && \text{☞ Def } L(\mathcal{A}_L) \\ &\iff [w] \in F && \text{☞ } (\#) \\ &\iff w \in L && \text{☞ (2)} \end{aligned}$$

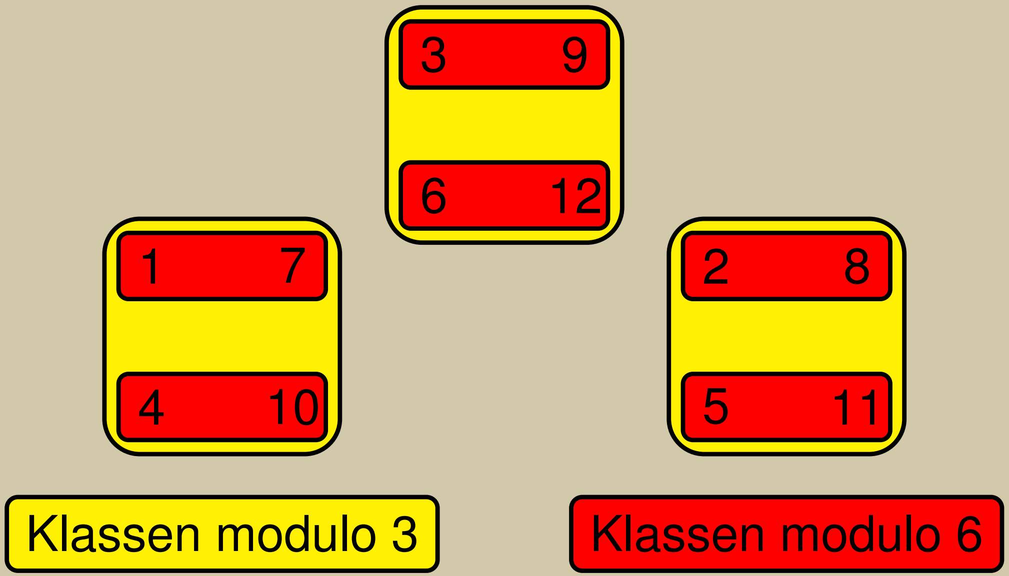
- Aus (1)-(3) folgt, dass $\mathcal{A}_L$ ein DFA für L ist

➨ L ist regulär

Exkurs: Äquivalenzrelationen (3/3)

- Für die „Rückrichtung“ des Beweises benötigen wir den Begriff der *Verfeinerung einer Äquivalenzrelation*

Beispiel



- Die Äquivalenzrelation $\equiv_6$ ist eine Verfeinerung der Äquivalenzrelation $\equiv_3$

Definition (Verfeinerung)

- Seien $\sim_1, \sim_2$ Äquivalenzrelationen über derselben Grundmenge
- $\sim_1$ heißt **Verfeinerung von** $\sim_2$, wenn für alle x, y gilt: $x \sim_1 y \Rightarrow x \sim_2 y$

- Falls $\sim_1$ Verfeinerung von $\sim_2$ ist, gilt: Anzahl Klassen von $\sim_1$ $\geqslant$ Anzahl Klassen von $\sim_2$

- Weiteres Beispiel: die Gleiches-Semester-und-gleicher-Studiengang-Relation ist eine Verfeinerung der Gleiches-Semester-Relation

Satz von Myhill und Nerode: Beweis (5/5)

Beweis (Forts.)

- Jetzt zeigen wir:
  L regulär $\Rightarrow \sim_L$ hat endlich viele Klassen

- Sei $\mathcal{A} = (Q, \Sigma, \delta, s, F)$ ein DFA für L

- Wir definieren eine Äquivalenzrelation $\sim_\mathcal{A}$ mit $|Q|$ Klassen und zeigen:
  $\sim_\mathcal{A}$ ist eine Verfeinerung von $\sim_L$

- Dann folgt:
  - Anzahl Klassen von $\sim_L$
    $\leqslant$ Anzahl Klassen von $\sim_\mathcal{A}$
    $= |Q| < \infty$

Beweis (Forts.)

- Wir definieren $\sim_\mathcal{A}$ durch:
  $$\underline{x \sim_\mathcal{A} y} \overset{\text{def}}{\Leftrightarrow} \delta^*(s, x) = \delta^*(s, y)$$

- **Behauptung:** $\sim_\mathcal{A}$ ist eine Verfeinerung von $\sim_L$, also:
  für alle x, y gilt: $x \sim_\mathcal{A} y \Rightarrow x \sim_L y$

- Seien also $x, y \in \Sigma^*$ mit $x \sim_\mathcal{A} y$

➡ $\delta^*(s, x) = \delta^*(s, y)$

➡ für alle $z \in \Sigma^*$ gilt:
$$\delta^*(s, xz) = \delta^*(s, yz)$$

➡ für alle $z \in \Sigma^*$ gilt:
$$xz \in L \iff yz \in L$$

➡ $x \sim_L y$

- Damit ist der Beweis des Satzes von Myhill und Nerode vollständig

Minimaler Automat: Eindeutigkeit (1/3)

- Was bringt uns der Satz von Myhill und Nerode für die Minimierung von Automaten?
- Aus dem Beweis können wir direkt die folgende Aussage schließen

Lemma 4.2

- Ist L eine reguläre Sprache und $\mathcal{A} = (Q, \Sigma, \delta, s, F)$ ein DFA für L, dann gilt:

$$|Q| \geqslant \text{Anzahl Klassen von } \sim_L$$

- Also: Jeder DFA für L hat mindestens so viele Zustände wie der Äquivalenzklassenautomat $\mathcal{A}_L$
- $\mathcal{A}_L$ ist also *ein* minimaler DFA für L

- Wir zeigen gleich:
  - In einem gewissen Sinne ist $\mathcal{A}_L$ sogar in jedem DFA für L enthalten
  - Und: falls $|Q|$ gleich der Anzahl der Klassen von $\sim_L$ ist, sind $\mathcal{A}$ und $\mathcal{A}_L$ „praktisch identisch“
- $\mathcal{A}_L$ ist also *der* minimale DFA für L

✎ Wir betrachten zuerst die Formalisierung von „praktisch identisch“: Isomorphie von DFAs

Minimaler Automat: Eindeutigkeit (2/3)

Definition (Isomorphie von DFAs, $\cong$)

- Seien $\mathcal{A}_1 = (Q_1, \Sigma, \delta_1, s_1, F_1)$ und $\mathcal{A}_2 = (Q_2, \Sigma, \delta_2, s_2, F_2)$ DFAs mit dem selben Eingabe-Alphabet

- $\mathcal{A}_1$ und $\mathcal{A}_2$ heißen **isomorph**, falls es eine Bijektion $\pi : Q_1 \to Q_2$ gibt mit:
  (1) $\pi(s_1) = s_2$,
  (2) für alle $q \in Q_1$ gilt:
  $$q \in F_1 \iff \pi(q) \in F_2, \text{ und}$$
  (3) für alle $q \in Q_1$ und $\sigma \in \Sigma$ gilt:
  $$\pi(\delta_1(q, \sigma)) = \delta_2(\pi(q), \sigma)$$
- Notation: $\mathcal{A}_1 \cong \mathcal{A}_2$

- Informell bedeutet $\mathcal{A}_1 \cong \mathcal{A}_2$:
  - $\mathcal{A}_1$ und $\mathcal{A}_2$ unterscheiden sich nur hinsichtlich der Namen der Zustände:
    * Wenn in $\mathcal{A}_1$ die Zustände gemäß π umbenannt werden, ergibt sich $\mathcal{A}_2$

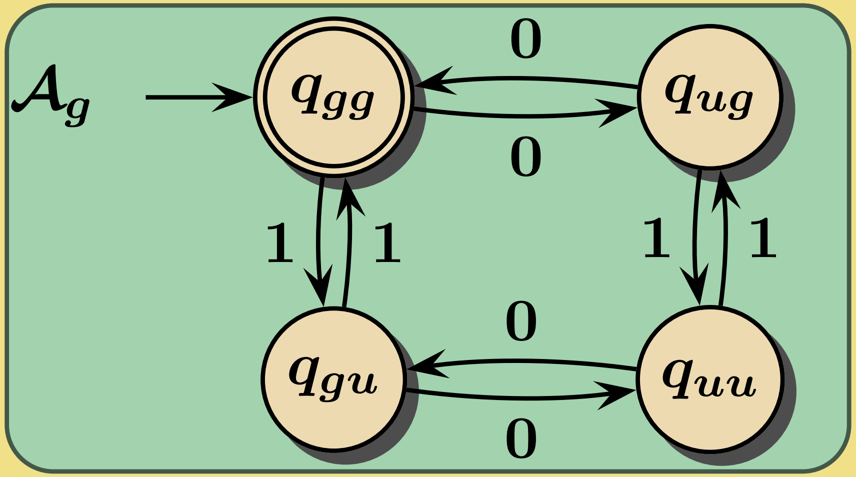
Minimaler Automat: Eindeutigkeit (3/3)

Lemma 4.3

- Ist $\mathcal{A}$ ein DFA für eine Sprache L, der die selbe Anzahl von Zuständen wie $\mathcal{A}_L$ hat, so gilt:
$$\mathcal{A} \cong \mathcal{A}_L$$

- Der Beweis findet sich im Anhang

- Der Äquivalenzklassenautomat für L_g ist isomorph zu:



Minimalautomat

- Insgesamt haben wir bisher gezeigt:

Satz 4.4

- Für jede reguläre Sprache L ist $\mathcal{A}_L$ der bis auf Isomorphie eindeutig bestimmte minimale DFA für L

Beweisskizze

- Wegen Lemma 4.2 hat jeder DFA für L mindestens soviele Zustände wie $\mathcal{A}_L$
- Wegen Lemma 4.3 ist jeder DFA für L, der genau so viele Zustände wie $\mathcal{A}_L$ hat, isomorph zu $\mathcal{A}_L$

- Wir betrachten jetzt, wie sich $\mathcal{A}_L$ aus einem gegebenen DFA für L berechnen lässt

Inhalt

Vom DFA zum minimalen DFA

- Nehmen wir an, wir haben einen DFA $\mathcal{A}$ für eine reguläre Sprache L gegeben und hätten gerne einen minimalen DFA für L

- Der Satz von Myhill/Nerode sagt uns, dass der minimale DFA für L in $\mathcal{A}$ schon „drin“ ist
- Wir müssen ihn nur finden

- Ein naiver Ansatz wäre jede Teilmenge $Q' \subseteq Q$ als „Trägermenge“ für den minimalen DFA auszuprobieren
- Das würde allerdings zu exponentiellem Aufwand führen

- Wir werden jetzt sehen: der minimale DFA lässt sich erheblich direkter und damit auch schneller berechnen

Minimaler Automat: Berechnung

- Wie lässt sich $\mathcal{A}_L$ aus $\mathcal{A}$ konstruieren?
- Hierfür liefert der Beweis von Satz 4.1 einen Hinweis

- Ist $\mathcal{A}$ ein DFA für L, so ist $\sim_{\mathcal{A}}$ eine Verfeinerung von $\sim_L$

➡ $\mathcal{A}_L$ kann durch Zusammenlegen von Zuständen (Äquivalenzklassen) aus $\mathcal{A}$ erzeugt werden

- Genauer: zwei Zustände p, q von $\mathcal{A}$ können zusammengelegt werden, wenn sie im folgenden Sinne **äquivalent** sind:

$(**)$ für alle $z \in \Sigma^*$ gilt:
$$\delta^*(p, z) \in F \iff \delta^*(q, z) \in F$$

➡ Um den minimalen DFA zu konstruieren, genügt es also, zu berechnen, welche Zustände zusammen gelegt werden können

- Das ist „direkt“ jedoch nicht so leicht möglich

- Die grundlegende Idee für unseren Minimierungsalgorithmus ist, zunächst zu berechnen, welche Zustände *nicht* zusammen gelegt werden können

- Deshalb betrachten wir jetzt einen Algorithmus, der die Menge $N(\mathcal{A})$ der **nicht äquivalenten Paare** berechnet:
$$\underline{N(\mathcal{A})} \stackrel{\text{def}}{=} \{(p, q) \mid p, q \in Q,$$
$$\exists w : (\delta^*(p, w) \in F \not\Leftrightarrow \delta^*(q, w) \in F)\}$$

- Die Berechnung erfolgt induktiv:
  - Zuerst werden Paare berechnet, deren Inäquivalenz durch $w = \epsilon$ bezeugt wird
  - Dann werden Paare bestimmt, deren Inäquivalenz sich durch Übergänge in andere inäquivalente Paare ergibt

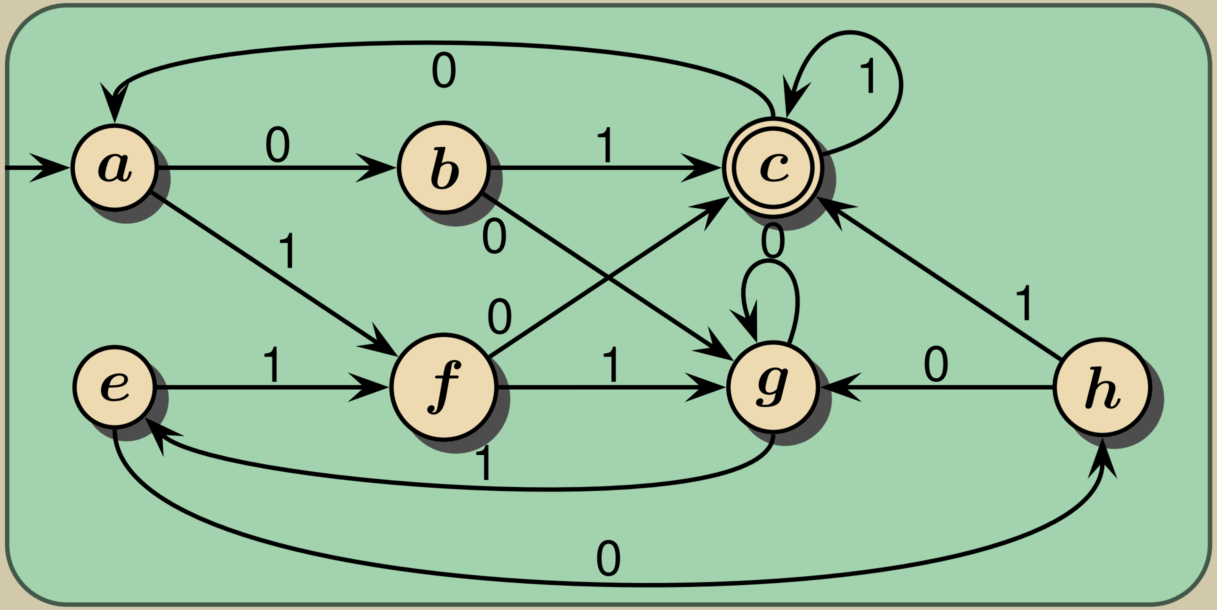
Der Markierungsalgorithmus

Markierungsalgorithmus

- Eingabe:
  $$\mathcal{A} = (Q, \Sigma, \delta, s, F)$$
- Ausgabe: Relation $N(\mathcal{A})$

1. $M := \{(p,q),(q,p) \mid p \in F, q \notin F\}$
2. $M' := \{(p,q) \notin M \mid \exists \sigma \in \Sigma : (\delta(p,\sigma),\delta(q,\sigma)) \in M\}$
3. $M := M \cup M'$
4. Falls $M' \neq \varnothing$, weiter mit 2.
5. Ausgabe M

Beispiel



	a	b	c	e	f	g	h
a		X^1	X^0		X^1	X^2	X^1
b			X^0	X^1	X^1	X^1	
c				X^0	X^0	X^0	X^0
e					X^1	X^2	X^1
f						X^1	X^1
g							X^1
h							

Nicht markiert: $(a,e),(b,h)$

Markierungsalgorithmus: Korrektheit (1/2)

Lemma 4.5

- Der Markierungsalgorithmus berechnet $N(\mathcal{A})$

Beweisskizze

- Zur Erinnerung:
  $N(\mathcal{A}) = \{(p,q) \mid p,q \in Q, \exists w : (\delta^*(p,w) \in F \not\Leftrightarrow \delta^*(q,w) \in F)\}$

- Wir zeigen:
  (a) Wenn (p,q) im k-ten Durchlauf (von 2.) markiert wird, dann gibt es einen String w der Länge k mit
  $$\delta^*(p,w) \in F \not\Leftrightarrow \delta^*(q,w) \in F$$
  (b) Wenn (p,q) durch den Algorithmus nicht markiert wird, dann gilt für alle Strings $w \in \Sigma^*$:
  $$\delta^*(p,w) \in F \Longleftrightarrow \delta^*(q,w) \in F$$

Beweisskizze für (a)

- Beweis durch Induktion nach k
  - $k = 0$ ✓ ☞ $w = \epsilon$
  - Von $k-1$ zu k:
  - Zu jedem Paar (p,q), das im k-ten Durchlauf markiert wird, gibt es ein Paar (p',q'), das im $(k-1)$-ten Durchlauf markiert wird mit
    $$\delta(p,\sigma) = p', \delta(q,\sigma) = q'$$
  - Nach Induktion gibt es also einen String v der Länge $k-1$ mit
    $$\delta^*(p',v) \in F \not\Leftrightarrow \delta^*(q',v) \in F$$
    ☞ $w = \sigma v$

➡ $\delta^*(p,\sigma v) \in F \not\Leftrightarrow \delta^*(q,\sigma v) \in F$

Markierungsalgorithmus: Korrektheit (2/2)

Lemma 4.5

- Der Markierungsalgorithmus berechnet $N(\mathcal{A})$

Beweisskizze

- Zur Erinnerung:
  $N(\mathcal{A}) = \{(p,q) \mid p,q \in Q,$
  $\exists w : (\delta^*(p,w) \in F \not\Leftrightarrow \delta^*(q,w) \in F)\}$

- Wir zeigen:
  (a) Wenn (p,q) im k-ten Durchlauf (von 2.) markiert wird,
  dann gibt es einen String w der Länge k mit
  $$\delta^*(p,w) \in F \not\Leftrightarrow \delta^*(q,w) \in F$$
  (b) Wenn (p,q) durch den Algorithmus nicht markiert wird,
  dann gilt für alle Strings $w \in \Sigma^*$:
  $$\delta^*(p,w) \in F \Longleftrightarrow \delta^*(q,w) \in F$$

Beweisskizze für (b)

- Beweis durch Widerspruch:

- Angenommen, es gibt ein **Gegenbeispiel** (p,q,w), so dass
  - der Algorithmus (p,q) nicht markiert, aber
  - $\delta^*(p,w) \in F \not\Leftrightarrow \delta^*(q,w) \in F$

- Sei (p,q,w) ein Gegenbeispiel mit dem kürzest möglichen w
- Klar: $w \neq \epsilon$ wegen Schritt (1) des Alg.

- Seien $v \in \Sigma^*$, $\sigma \in \Sigma$ mit $w = \sigma v$
- Da (p,q) unmarkiert ist, ist auch $(\delta(p,\sigma),\delta(q,\sigma))$ unmarkiert

➡ $(\delta(p,\sigma),\delta(q,\sigma),v)$ ist auch ein Gegenbeispiel, aber v ist kürzer als w

- Widerspruch zur Wahl von (p,q,w)

Wiederholung: $\mathcal{O}$-Notation

Definition

- Seien $f, g : \mathbb{N} \to \mathbb{R}$ zwei Funktionen
- $f = \mathcal{O}(g)$: es gibt c, d, so dass für alle $n \geqslant d$ gilt: $f(n) \leqslant cg(n)$ ☞ 4.1

Beispiel

- $12n \log n = \mathcal{O}(n^2)$
- $5n^3 + 12n^2 + 17n + 100 = \mathcal{O}(n^3 n)$

Minimierungsalgorithmus

Minimierungsalgorithmus für DFA

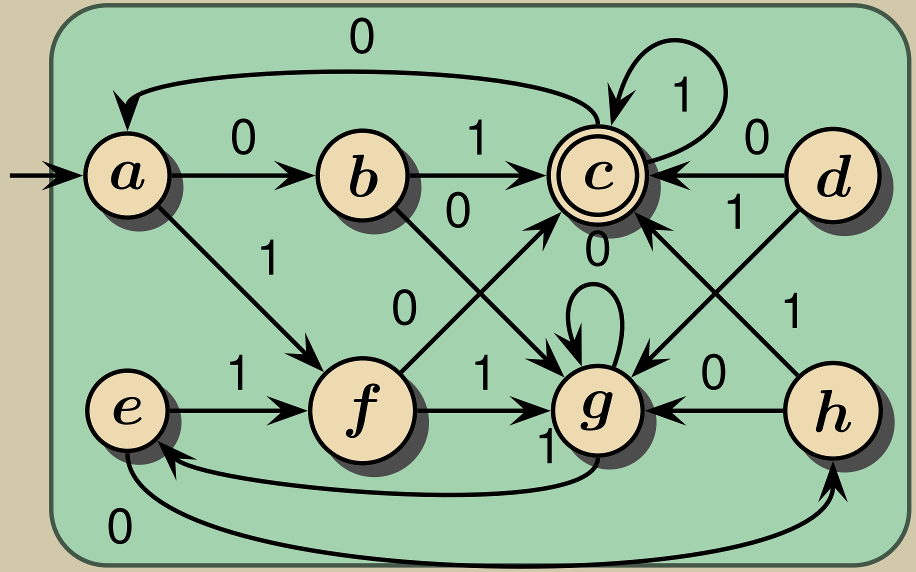
- Eingabe: $\mathcal{A} = (Q, \Sigma, \delta, s, F)$
- Ausgabe: minimaler DFA $\mathcal{A}'$ mit $L(\mathcal{A}') = L(\mathcal{A})$

1. Entferne alle Zustände von $\mathcal{A}$, die von s aus nicht erreichbar sind.
2. Berechne die Relation $N(\mathcal{A})$ mit dem Markierungs-Algorithmus
3. Verschmelze sukzessive alle nicht markierten Zustandspaare zu jeweils einem Zustand.

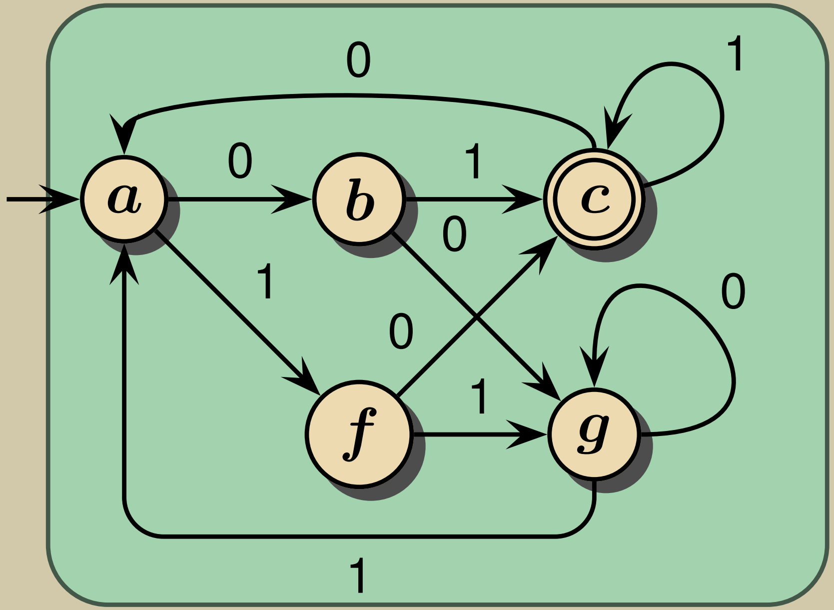
- Laufzeit des Minimierungsalgorithmus:
  1. $\mathcal{O}(|\delta|) = \mathcal{O}(|Q|^2|\Sigma|)$
     ☞ nächstes Kapitel
  2. $\mathcal{O}(|Q|^2|\Sigma|)$ bei geschickter Implementierung
  3. $\mathcal{O}(|Q|^2|\Sigma|)$

  Zusammen: $\mathcal{O}(|Q|^2|\Sigma|)$

Beispiel



Minimaler DFA:



Vom RE zum DFA: vollständig

- Damit kennen wir nun alle Teilschritte von der Spezifikation einer regulären Sprache bis zur Berechnung eines möglichst kleinen endlichen Automaten

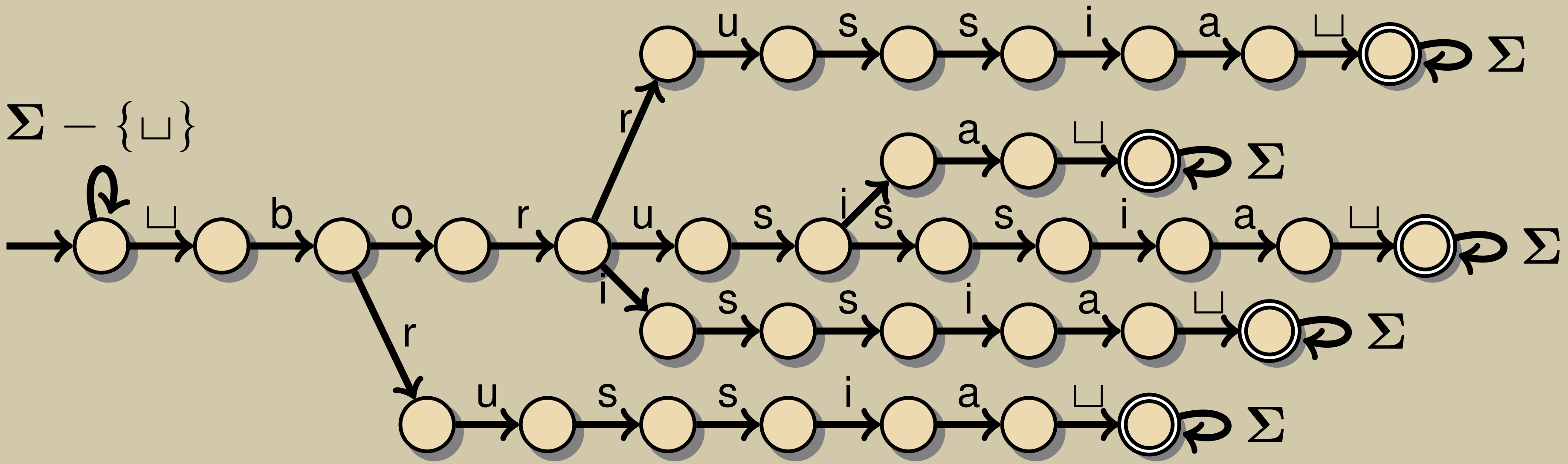
1. Spezifiziere die Sprache durch einen regulären Ausdruck α
2. Wandle α in einen ϵ-NFA $\mathcal{A}_1$ um
3. Wandle $\mathcal{A}_1$ in einen DFA $\mathcal{A}_2$ um
4. Wandle $\mathcal{A}_2$ in einen minimalen DFA $\mathcal{A}_3$ um

✎ Der e-Mail-Adressen-DFA ist übrigens schon minimal...

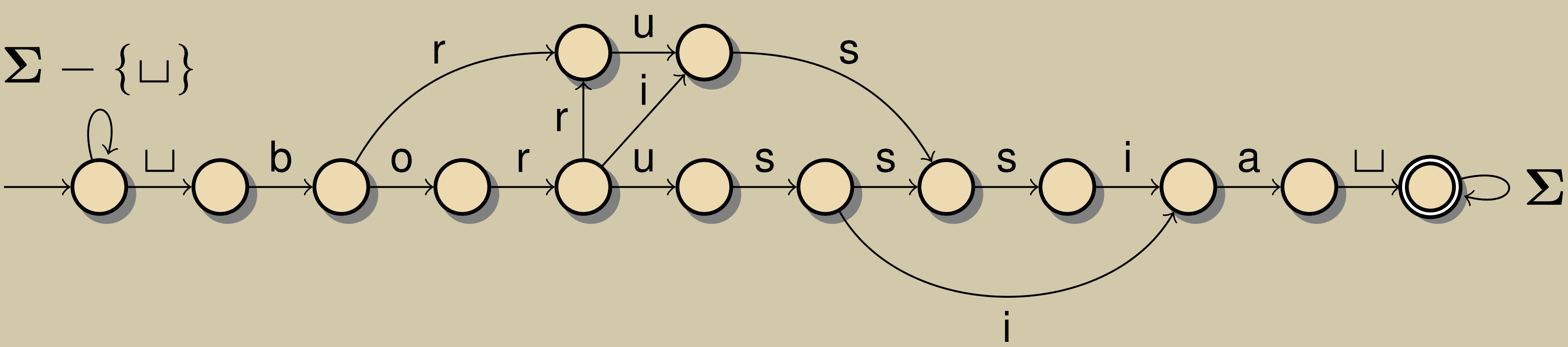
Der Borussia-Newsticker-Automat (3/3)

Beispiel

- Ist der Borussia-Automat minimal?



- Nein, dies ist der minimale DFA:



Inhalt

Satz von Myhill und Nerode: Weitere Anwendungen (1/3)

- Mit dem Satz von Myhill und Nerode lässt sich herausfinden, ob eine gegebene Sprache regulär ist
  - Z.B.: da die Relation $\sim_{\boldsymbol{L_g}}$ vier Klassen hat, ist $\boldsymbol{L_g}$ regulär

- Der Satz ist aber auch für den Nachweis, dass eine gegebene Sprache *nicht* regulär ist, nützlich

Satz von Myhill und Nerode: Weitere Anwendungen (2/3)

Beispiel

- Wir berechnen die Äquivalenzklassen von $L_{ab} = \{a^n b^n \mid n \geqslant 0\}$
- Es gilt z.B.:
  $a^4 b \sim_{L_{ab}} a^5 b^2 \sim_{L_{ab}} a^6 b^3 \dots$

- $\sim_{L_{ab}}$ hat die Klassen:
  - $B_k \stackrel{\text{def}}{=} \{a^{i+k} b^i \mid i \geqslant 1\}$, für jedes $k \geqslant 0$,
  - $A_k \stackrel{\text{def}}{=} \{a^k\}$, für jedes $k \geqslant 0$,
  - $C \stackrel{\text{def}}{=} \{a^i b^j \mid i < j\} \cup \overline{L(a^* b^*)}$, die Klasse aller Strings, für die es überhaupt keine Verlängerung gibt, die in L_{ab} liegt:

- Notation:
  - Sei L eine Sprache über Σ und $v \in \Sigma^*$
  - $\underline{L/v} \stackrel{\text{def}}{=} \{z \in \Sigma^* \mid vz \in L\}$

Beispiel (Forts.)

- Um nachzuweisen, dass dies die Äquivalenzklassen von $\sim_{L_{ab}}$ sind, ist zu zeigen:
  (1) Jeder String kommt in einer Klasse vor ✓
  (2) Für alle Strings u, v in derselben Klasse gilt: $u \sim_{L_{ab}} v$
  (3) Für Strings u, v aus verschiedenen Klassen gilt: $u \not\sim_{L_{ab}} v$

- Dazu genügt es zu zeigen, dass
  (2') für alle Strings v einer Klasse die Menge L_{ab}/v gleich ist
  (3') für verschiedene Klassen die Mengen L_{ab}/v verschieden sind

- Für jedes k gilt:
  - Für $v \in B_k$ ist $L_{ab}/v = \{b^k\}$
  - Für $v \in A_k$ ist $L_{ab}/v = \{a^i b^{i+k} \mid i \geqslant 0\}$
- Für $v \in C$ ist $L_{ab}/v = \varnothing$

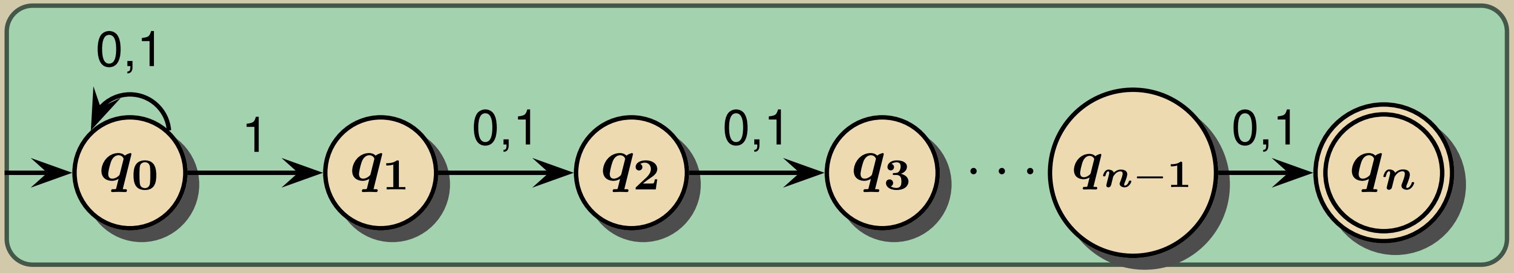
➡ Die Äquivalenzklassen sind korrekt angegeben
➡ unendlich viele Klassen $\Rightarrow$ L_{ab} nicht regulär

Satz von Myhill und Nerode: Weitere Anwendungen (3/3)

- Der Satz von Myhill und Nerode liefert auch eine Methode um die Größe des Minimalautomaten für eine reguläre Sprache zu berechnen:
  - Zähle die Klassen von $\sim_L$

Beispiel

- Wir betrachten wieder die Sprache L_n aller 0-1-Strings, deren n-tes Zeichen von rechts eine 1 ist:



- Es ist leicht zu zeigen, dass zwei Strings x, y genau dann in derselben Äquivalenzklasse von $\sim_{L_n}$ sind, wenn sie dasselbe Suffix der Länge n haben

✎ Dabei werden bei Strings der Länge $< n$ führende Nullen „hinzugedacht“

➡ Es gibt soviele Klassen in $\sim_L$ wie es 0-1-Strings der Länge n gibt

➡ $\sim_{L_n}$ hat 2^n Klassen

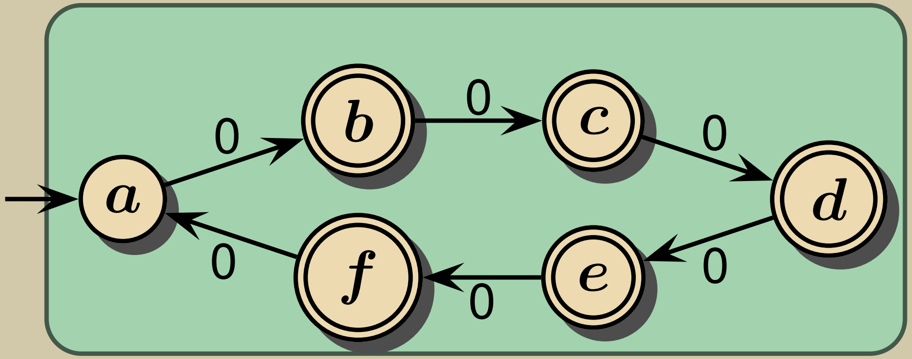
➡ Jeder DFA für L_n hat mindestens 2^n Zustände

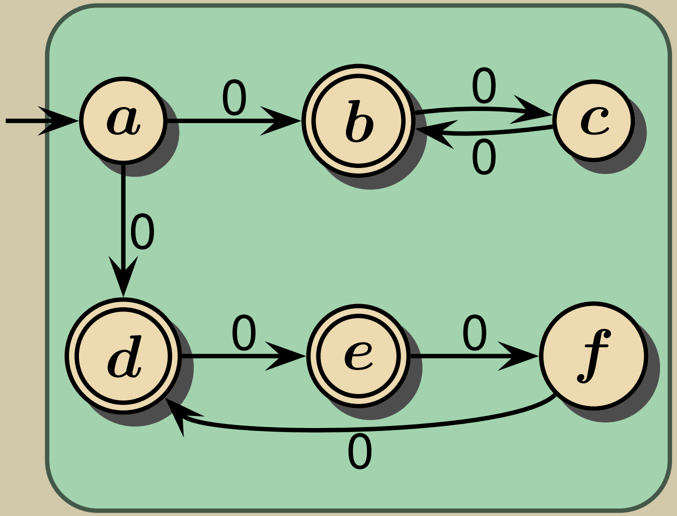
Minimale NFAs

- Es gibt zwar auch zu jedem NFA $\mathcal{A}$ einen kleinsten NFA $\mathcal{A}'$ mit
$$L(\mathcal{A}') = L(\mathcal{A})$$
- Aber der kleinste NFA ist im Allgemeinen nicht bis auf Isomorphie eindeutig

Beispiel

- Die Menge aller Strings der Form 0^n, für die 6 *kein* Teiler von n ist, hat zwei kleinste NFAs:





- Idee: 6 ist genau dann kein Teiler von n wenn 2 oder 3 kein Teiler von n ist

Rot, Gelb, Grün

- Minimale Automaten haben höchstens einen Zustand, von dem aus kein akzeptierender Zustand mehr erreichbar ist
  - Dieser Zustand entspricht der roten Ampel im Webformular-Beispiel
  - Akzeptierende Zustände entsprechen der grünen Ampel
  - Alle übrigen Zustände entsprechen der gelben Ampel
- Wir nennen diesen Zustand Fehlerzustand oder Senkenzustand (im Englischen: *sink state*)

- Dass ein solche Zustand nicht immer existiert, zeigt der DFA $\mathcal{A}_g$ von Kapitel 2

Zusammenfassung

- Zu einem gegebenen DFA ist der minimale äquivalente DFA bis auf Isomorphie eindeutig bestimmt und kann mit Hilfe des Markierungsalgorithmus in Zeit $\mathcal{O}(|Q|^2|\Sigma|)$ berechnet werden

- **Literatur:**

  - John R. Myhill. Finite automata and the representation of events. Technical Report WADC TR-57-624, Wright-Paterson Air Force Base, 1957
  - A. Nerode. Linear automaton transformations. *Proc. Amer. Math. Soc.*, 9:541–544, 1958

Erläuterungen

Bemerkung 4.1

- Die Notation $f = \mathcal{O}(g)$ kann leicht zu Missverständnissen führen:
  - Denn: das Gleichheitszeichen wird hier, anders als sonst üblich, in einem nicht symmetrischen Sinn verwendet
  - Es gilt z.B.
    - $n^2 = \mathcal{O}(n^3) = \mathcal{O}(n^4)$,
    - aber nicht $n^2 = \mathcal{O}(n^4) = \mathcal{O}(n^3)$
- Sauberer ist es, (wie in MafI) $\mathcal{O}(g)$ als Notation für eine Menge von Funktionen (oder Folgen) zu betrachten:
  - $\mathcal{O}(g) \stackrel{\text{def}}{=} \{h \mid \exists c, d\ \forall n \geqslant d : \ h(n) \leqslant cg(n)\}$
  - Schreibweise dann: $f \in \mathcal{O}(g)$
- Aber: Wir folgen hier der Tradition...

Minimaler Automat: Eindeutigkeit (3/3)

Lemma 4.3

- Ist $\mathcal{A}$ ein DFA für eine Sprache L, der die selbe Anzahl von Zuständen wie $\mathcal{A}_L$ hat, so gilt: $\mathcal{A} \cong \mathcal{A}_L$

Beweisidee

- Sei $\mathcal{A} = (Q, \Sigma, \delta, s, F)$ ein solcher DFA
- $\mathcal{A}$ minimal $\Rightarrow$ in $\mathcal{A}$ sind alle Zustände erreichbar

➡ für jeden Zustand q von $\mathcal{A}$ gibt es einen String w_q mit $\delta^*(s, w_q) = q$

- Wir definieren eine Abbildung π durch: $\pi(q) \stackrel{\text{def}}{=} [w_q]$
- **Behauptung:** π ist ein Isomorphismus von $\mathcal{A}$ auf $\mathcal{A}_L$

Beweisdetails

(1) $\pi(s) = [\epsilon]$ ✓

(2) $q \in F \iff w_q \in L \iff$ $\pi(q) = [w_q]$ ist akzeptierender Zustand von $\mathcal{A}_L$

(3) Für $q \in Q, \sigma \in \Sigma$ gilt:

$$\begin{aligned}\pi(\delta(q,\sigma)) &= \pi(\delta(\delta^*(s,w_q),\sigma))\\ &= \pi(\delta^*(s,w_q\sigma))\\ &= [w_q\sigma]\\ &= \delta'([w_q],\sigma)\\ &= \delta'(\pi(q),\sigma)\end{aligned}$$

✎ δ' bezeichnet die Überführungsfunktion von $\mathcal{A}_L$

- π ist bijektiv, denn:
  - Aus dem Beweis von Satz 4.1 folgt: $\sim_\mathcal{A}$ ist eine Verfeinerung von $\sim_L$
  - Da $\sim_\mathcal{A}$ und $\sim_L$ gleich viele Klassen haben gilt also: $\sim_\mathcal{A} = \sim_L$

➡ π ist eine Bijektion

- Also ist π ein Isomorphismus und es folgt: $\mathcal{A} \cong \mathcal{A}_L$