Grundlagen Theoretischer Informatik I

SoSe 2011 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Grundlagen Theoretischer Informatik I Gesamtübersicht

- Organisatorisches; Einführung
- Logik & Beweisverfahren
- Mengenlehre
- reguläre Sprachen

Nicht-Regularität durch Abschlusseigenschaften

Beispiel: Betrachte die Menge $L \subseteq \{a, b\}^*$ mit der Eigenschaft, dass $w \in L$ liegt gdw. w gleich viele a's wie b's besitzt.

Behauptung: L ist nicht regulär.

Beweis durch Widerspruch: Wäre L regulär, so auch $L' = L \cap \{a\}^*\{b\}^*$, denn $\{a\}^*\{b\}^*$ ist regulär, und der Schnitt zweier regulärer Sprachen ist wiederum regulär.
Offenbar gilt: $L' = \{a^k b^k \mid k \in \mathbb{N}\}$, und von dieser Sprache wissen wir bereits, dass sie nicht-regulär ist.
↯ zu unserer Annahme, L wäre regulär.

Auch hier Schwierigkeit: "Geschickte" Wahl der Operation...

Äquivalenzrelationen (hoffentlich noch bekannt ?!)

Eine Relation $R \subseteq X \times X$ heißt *Äquivalenzrelation* gdw.

(1) $R^0 = \Delta_X \subseteq R$ (Reflexivität)

(2) $R^2 = R \circ R \subseteq R$ (Transitivität)

(3) Mit $R^{-1} = \{(y, x) \mid (x, y) \in R\}$ gilt $R^{-1} \subseteq R$ (Symmetrie)

Eine ÄR auf X induziert eine *Partition* von X

in *Äquivalenzklassen* $[x]_R = \{y \in X \mid xRy\}$.

Eine Äquivalenzrelation auf Σ^*

Es sei $A = (Q, \Sigma, \delta, q_0, F)$ ein DEA.

Definiere $u \equiv_A v$ gdw. $\exists q \in Q : ((q_0, u) \vdash_A^* (q, \lambda)) \wedge ((q_0, v) \vdash_A^* (q, \lambda))$.

(Es ist klar, dass diese Relation reflexiv, symmetrisch und transitiv ist ?!)

. . . und noch eine Äquivalenzrelation auf Σ^*

Es sei $L \subseteq \Sigma^*$. L *trennt* zwei Wörter $u, v \in \Sigma^*$ gdw. $|\{u, v\} \cap L| = 1$.

Zwei Wörter u und v heißen *kongruent modulo* L (i.Z.: $u \equiv_L v$), wenn für jedes beliebige Wort w aus Σ^* die Sprache L die Wörter uw und vw *nicht* trennt, d.h. wenn gilt:

$$(\forall w \in \Sigma^*)\ (\ uw \in L \Leftrightarrow vw \in L\ )$$

Satz: Für jede Sprache $L \subseteq \Sigma^*$ ist $\equiv_L$ eine Äquivalenzrelation.

Beweis: Reflexivität: $\forall u \in \Sigma^* : u \equiv_L u$ ✓

Symmetrie: $\forall u, v \in \Sigma^* : u \equiv_L v \Rightarrow v \equiv_L u$ ✓

Transitivität: $\forall u, v, x \in \Sigma^* : (u \equiv_L v \wedge v \equiv_L x) \Rightarrow u \equiv_L x$

Betrachte $u, v, x, w \in \Sigma^*$.

(a) Falls $uw \in L$, so auch $vw \in L$, denn $u \equiv_L v$; wegen $v \equiv_L x$ gilt daher $xw \in L$, d.h., $u \equiv_L x$.

(b) Falls $uw \notin L$, ... (analog)

Beispiel: Betrachte

$$L = \{a^k b^k | k > 0\}$$

$a^i b \not\equiv_L a^j b$ für $i \neq j$:
Verwende $w = b^{i-1}$ mit $a^i b w \in L$ und $a^j b w \notin L$.
Damit hat man für $i = 1, 2, 3, ...$ bereits unendlich viele verschiedene Äquivalenzklassen $[a^i b]$ gefunden.
Genauer gilt: $[a^i b] = \{a^i b, a^{i+1} b^2, a^{i+2} b^3, ...\}$.
Ferner gilt: $[ab] = L$.

Lemma: Es sei $L \subseteq \Sigma^*$ regulär, d.h., L ist durch einen DEA A beschrieben. Dann gilt: Falls $u \equiv_A v$, so $u \equiv_L v$.

Beweis: Betrachte zwei Wörter $u, v \in \Sigma^*$ mit $u \equiv_A v$, also $((q_0, u) \vdash_A^* (q, \lambda)) \wedge ((q_0, v) \vdash_A^* (q, \lambda))$
Da A deterministisch, ist für $w \in \Sigma^*$: $((q, w) \vdash_A^* (q', \lambda))$, also $((q_0, uw) \vdash_A^* (q', \lambda)) \wedge ((q_0, vw) \vdash_A^* (q', \lambda))$ Also liegen entweder sowohl uw als auch vw in $L(A) = L$ oder beide nicht.
Daher gilt $u \equiv_L v$.

Folgerung: Ist L regulär, so hat $\equiv_L$ nur endlich viele Äquivalenzklassen.

Noch mehr Folgerungen aus dem letzten Beweis:

Betrachte reguläre Sprache $L \subseteq \Sigma^*$ und sie beschreibende Automaten A:

Ist $\mathcal{L} := \{L_1, \ldots, L_n\}$ die durch $\equiv_L$ induzierte Partition von Σ^*, so gilt für die durch $\equiv_A$ induzierte Partition $\mathcal{A} := \{A_1, \ldots, A_\ell\}$ von Σ^*:
Für jedes A_i gibt es ein L_j mit $A_i \subseteq L_j$.
Daher heißt $\mathcal{A}$ auch *Verfeinerung* von $\mathcal{L}$.

Satz: [Myhill und Nerode] Eine Sprache $L \subseteq \Sigma^*$ ist genau dann regulär, wenn es nur endlich viele Äquivalenzklassen bezüglich $\equiv_L$ gibt.

Beweis: 1. L regulär $\Rightarrow$ L induziert endlich viele Äquivalenzklassen (siehe Folgerung).

2. Umkehrung: Sei k Zahl der Klassen von $\equiv_L$, d.h. $\Sigma^* = [x_1] \cup ... \cup [x_k]$.
Definiere den *Minimalautomaten* $A(L) = (S, \Sigma, \delta, s_0, F)$ durch
$Q = \{[x_1], ..., [x_k]\}$
$q_0 := [\lambda]$
F bestehe aus allen Äquivalenzklassen $[x_i]$ mit $x_i \in L$
$\delta([x], a) := [xa]$

Wichtig: Mit $[x] = [y]$ ist $xaw \in L \Leftrightarrow yaw \in L$,
also auch $[xa] = [ya]$, $\rightsquigarrow$

$$\delta([x], a) = [xa] = [ya] = \delta([y], a)$$

$\rightsquigarrow$ δ ist wohldefiniert!

Offensichtlich gilt $([\lambda], x) \vdash_A^* ([x], \lambda)$ $\rightsquigarrow$

$$x \in L(A) \Longleftrightarrow \exists q \in F : ([\lambda], x) \vdash_A^* (q, \lambda) \Longleftrightarrow [x] \in F \Longleftrightarrow x \in L$$

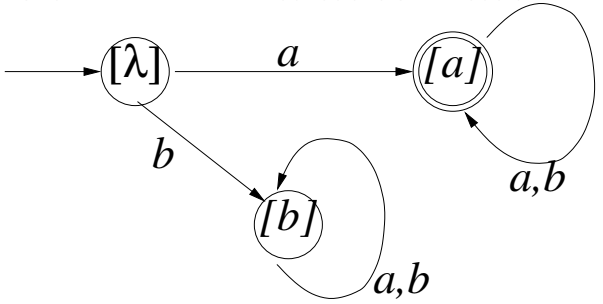
Beispiel: Betrachte $L = \{a\}\{b, a\}^*$

- $\lambda \not\equiv_L a$ mit $\lambda\lambda = \lambda \notin L$, $a\lambda = a \in L$.
- $b \not\equiv_L a$ mit $b\lambda = b \notin L$, $a\lambda = a \in L$
- $\lambda \not\equiv_L b$ mit $\lambda a = a \in L$, $ba \notin L$.
- $bw \equiv_L b$
- $aw \equiv_L a$

Also gilt

$$\Sigma^* = [\lambda] \cup [b] \cup [a]$$

mit dem Minimalautomaten



Warum heißt der Minimalautomat so?

Lemma: Ist L regulär, so ist $A(\mathrm{L})$ der DEA mit der kleinsten Anzahl von Zuständen.

Beweis: Zunächst sieht man: $\equiv_{\mathrm{L}} = \equiv_{A(\mathrm{L})} \rightsquigarrow$
Zustände von $A(\mathrm{L})$ ist gleich # Äquivalenzklassen von $\equiv_{\mathrm{L}}$.

Aus dem Beweis von obigem Lemma lesen wir ab:

Ist A ein DEA mit $\mathrm{L} = \mathrm{L}(A)$, so ist:

Zustände von A ist gleich

Äquivalenzklassen von $\equiv_A$ ist größer gleich

Äquivalenzklassen von $\equiv_{\mathrm{L}}$.

Es gibt nur einen Minimalautomaten

Lemma: Der Minimalautomat ist “bis auf Isomorphie” (Umbenennen der Zustände) eindeutig bestimmt.

Beweis: Es sei L regulär und n die Zustandsanzahl von $A(L)$ sowie die eines evtl. anderen DEA $A = (Q, \Sigma, \delta, q_0, F)$ mit $L(A) = L$.
(Erinnerung: allgemein gilt $|Q(A)| \geq n$ für DEAs A mit $L(A) = L$, denn $\equiv_A$ ist eine Verfeinerung von $\equiv_L$.)
Gilt nun sogar $|Q| = n$, so ist $\equiv_L = \equiv_A$.
$\rightsquigarrow x \equiv_L y \iff x \equiv_A y \iff \exists q \in Q : ((q_0, x) \vdash_A^* (q, \lambda)) \wedge ((q_0, y) \vdash_A^* (q, \lambda))$ für alle $x, y \in \Sigma^*$.
Definiere $\phi : Q \to 2^{\Sigma^*}, q \mapsto \{w \in \Sigma^* \mid (q_0, w) \vdash_A^* (q, \lambda)\}$. ϕ identifiziert die Zustände von A mit den Äquivalenzklassen von $\equiv_A$ und somit mit denen von $\equiv_L$. Anfangs- und Endzustände werden erhalten. Für irgendein Wort $w_q \in \phi(q)$ gilt: (1) $([w_q]_L, a) \vdash_{A(L)} ([w_q a]_L, \lambda)$ sowie (2) $(q, a) \vdash_A (q', \lambda)$ mit $\phi(q') = [w_q a]_L$. Daher wird auch die Übergangsfunktion mit ϕ erhalten, liefert also insgesamt den behaupteten “Automatenisomorphismus”.

Eine Anwendung des Satzes von Myhill und Nerode

Folgerung: Hat $\equiv_L$ unendlich viele Äquivalenzklassen, so ist L nicht regulär.

Beispiel: Zu

$$L = \{a^k b^k | k > 0\}$$

hat $\equiv_L$ unendlich viele Äquivalenzklassen, ist also nicht regulär.

Wann ist nun ein DEA A nicht minimal ?

- Wenn es nicht-erreichbare Zustände gibt, d.h. es gibt q mit $(q_0, y) \vdash_A^* (q, \lambda)$ für kein Wort $y \in \Sigma^*$.
  Im Folgenden: A hat nur erreichbare Zustände! (s.u.)

- Wenn es Zustände $q \neq q'$ gibt mit

  $\forall w \exists p, p' \in Q : |\{p, p'\} \cap F| \neq 1 \Longrightarrow ((q, w) \vdash_A^* (p, \lambda) \Longleftrightarrow (q', w) \vdash_A^* (p', \lambda))$

  d.h. q und q' sind nicht *trennbar*, sondern *äquivalent*.

Es bezeichne $[q]$ die Menge aller Zustände, die zu q äquivalent sind.

Eigenschaften äquivalenter Zustände

1. Sind q und q' äquivalent, dann auch $\delta(q, a)$ und $\delta(q', a)$, denn $(\delta(q, a), w) = (q, aw)$ und $(q', aw) = (\delta(q', a), w)$.

2. Sind q und q' äquivalent, dann gilt $q \in F \iff q' \in F$.

Zur Konstruktion des Minimalautomaten I

Definiere zu $A = (Q, \Sigma, \delta, q_0, F)$ neuen Automaten $A_{[]} = (Q_{[]}, \Sigma, \delta_{[]}, [q_0], F_{[]})$ mit

- Anfangszustand $[q_0]$
- Endzuständen $F_{[]} := \{[q] \mid q \in F\}$
- Übergangsfunktion $\delta_{[]}([q], a) := [\delta(q, a)]$

Mit A hat auch $A_{[]}$ hat keine nicht-erreichbaren Zustände.
Betrachte $f : Q \to Q_{[]}$ mit $f(q) := [q]$. Aus den aufgeführten Eigenschaften folgt:

Satz: f ist Automatenmorphismus; und damit gilt $L(A) = L(A_{[]})$.

Zur Konstruktion des Minimalautomaten II

Satz: $A_{[]}$ isomorph zum Minimalautomaten.

Beweis: Vergleiche $\equiv_{A_{[]}}$ und $x \equiv_L y$ für $L := L(A)$:

- $\equiv_{A_{[]}}$ ist Verfeinerung von $\equiv_L$, da $L = L(A_{[]})$.
- Sei $x \equiv_L y$. Da $L = L(A)$, gilt für q_x mit $(q_0, x) \vdash_A^* (q_x, \lambda)$ und für q_y mit $(q_0, y) \vdash_A^* (q_y, \lambda)$: $[q_x] = [q_y]$. Daher gilt:

$$([q_0], x) \vdash_{A_{[]}}^* ([q_x], \lambda) \quad \wedge \quad ([q_0], y) \vdash_{A_{[]}}^* ([q_x], \lambda).$$

  $\rightsquigarrow x \equiv_{A_{[]}} y.$

Konstruktion des Minimalautomaten III

Gegeben sei DEA $A = (Q, \Sigma, \delta, q_0, F)$.

Schritt (a): Bestimme die Menge der von q_0 erreichbaren Zustände E!
Bezeichne E_i die Menge der in $\leq i$ Schritten erreichbaren Zustände.

- Setze $E_0 = \{q_0\}$ (und $E_{-1} := \emptyset$)
- Wiederhole

  $$E_{i+1} = E_i \cup \{\delta(q, a) \mid q \in E_i \setminus E_{i-1}, a \in E\}$$

  bis erstmals $E_i = E_{i+1}$ gilt.
- Dann ist $E = E_i$.
- Entferne die Zustände $Q \setminus E$ aus dem Automaten.

Alternative Darstellung

Hinweis: reflexive transitive Hülle der 1-Einschritt-Erreichbarkeitsrelation

Genauer: Definiere zu DEA $A = (Q, \Sigma, \delta, q_0, F)$ die *1-Schritt-Zustandserreichbarkeitsrelation* $R = \{(p, q) \in Q \times Q \mid \exists a \in \Sigma : \delta(p, a) = q\}$.
Ist R^* die reflexive transitive Hülle von R, so ist

$$\{q \in Q \mid (q_0, q) \in R^*\}$$

die Menge der von q_0 erreichbaren Zustände.

Frage: Welches Verfahren ist besser ?!

Konstruktion des Minimalautomaten IV

Schritt (b): Bestimme die Äquivalenzrelation $\equiv_A$ im nach (a) verkleinerten Automaten wie folgt mit folgenden *Markierungsalgorithmus*:

- Verwende eine Tabelle aller ungeordneten Zustandspaare $\{q, q'\}$ mit $q \neq q'$.
- Markiere alle Paare $\{q, q'\}$ als nicht-äquivalent, bei denen $|\{q, q'\} \cap F| = 1$.
- Wiederhole, solange noch Änderungen in der Tabelle entstehen:

  Für jedes nicht-markierte Paar $\{q, q'\}$ und jedes $a \in \Sigma$
  Teste, ob $(\delta(q, a), \delta(q', a))$ bereits markiert ist.
  Wenn ja $\rightsquigarrow$ markiere $\{q, q'\}$.

- Alle am Ende nicht-markierten Paare sind äquivalent!

Gesamtaufwand (mit geeigneten Datenstrukturen und $k = |E|$ und $n = |Q|$, ohne Beweis):

$$O(k \cdot n^2)$$

Ein Beispiel:

Früher haben wir zu $L = \{a, aa, ab, abb\}$ den *Präfixbaumakzeptor* konstruiert:

δ	a	b
$\to Q_0$	Q_1	$\emptyset$
$Q_1 \to$	Q_2	Q_3
$Q_2 \to$	$\emptyset$	$\emptyset$
$Q_3 \to$	$\emptyset$	Q_4
$Q_4 \to$	$\emptyset$	$\emptyset$
$\emptyset$	$\emptyset$	$\emptyset$

Runde	neue markierte Paare
0	$M_0 = \{\{Q_i, \emptyset\}, \{Q_i, Q_0\} \mid i = 1, 2, 3, 4\}$
1	$\{\{Q_1, Q_2\}\}$ denn $\{\delta(Q_1, a), \delta(Q_2, a)\} \in M_0$
1	$\{\{Q_1, Q_3\}, \{Q_1, Q_4\}, \{Q_2, Q_3\}, \{Q_3, Q_4\}\}$
2	$\emptyset$
	übriggebliebene unmarkierte Paare
	$\{\{Q_2, Q_4\}\}$

Der Minimalautomat für $L = \{a, aa, ab, abb\}$ ist daher:

δ	a	b
$\rightarrow Q_0$	Q_1	$\emptyset$
$Q_1 \rightarrow$	Q_2	Q_3
$Q_2 \rightarrow$	$\emptyset$	$\emptyset$
$Q_3 \rightarrow$	$\emptyset$	Q_2
$\emptyset$	$\emptyset$	$\emptyset$

Andere Sprechweise: *Verschmelzung* der Zustände Q_2 und Q_4.