Vorlesungsskript

Theoretische Informatik II

Wintersemester 2007/2008

Prof. Dr. Johannes Köbler
Humboldt-Universität zu Berlin
Lehrstuhl Komplexität und Kryptografie

19. Oktober 2007

Inhaltsverzeichnis

Kapitel 1

Reguläre Sprachen

1.1 Endliche Automaten

Rechenmaschinen spielen in der Informatik eine zentrale Rolle. Hier beschäftigen wir uns mit mathematischen Modellen für Maschinentypen von unterschiedlicher Berechnungskraft. In der Vorlesung Theoretische Informatik 1 wurde die Turingmaschine als ein universales Berechnungsmodell eingeführt. In dieser Vorlesung werden wir eine Reihe von Einschränkungen dieses Maschinenmodells kennenlernen, die vielfältige praktische Anwendungen haben. Dabei betrachten wir zunächst nur Entscheidungsprobleme, was der Berechnung von $\{0,1\}$-wertigen Funktionen entspricht. Zur Beschreibung der Problemeingaben wird ein Eingabealphabet Σ verwendet.

Definition 1 (Alphabet)

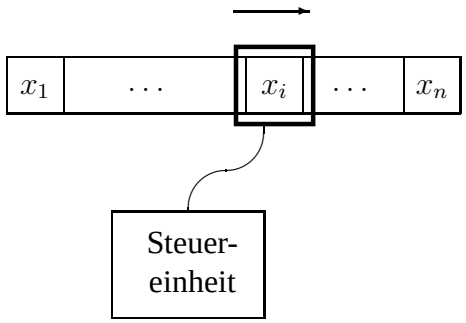
Ein **Alphabet** ist eine geordnete endliche Menge $\Sigma = \{a_1, \ldots, a_m\}$ von **Zeichen**. Eine Folge $x = x_1 \ldots x_n \in \Sigma^n$ heißt **Wort** (der **Länge** n). Die Menge aller Wörter über Σ ist

$$\Sigma^* = \bigcup_{n \geq 0} \Sigma^n = \{x_1 \cdots x_n \mid n \geq 0 \text{ und } x_i \in \Sigma \text{ für } i = 1, \ldots, n\}.$$

Das (einzige) Wort der Länge $n = 0$ ist das **leere Wort**, welches wir mit ε bezeichnen.

Ein endlicher Automat ist eine auf ein Minimum „abgespeckte“ Turingmaschine, die nur kostant viel Speicherplatz zur Verfügung hat und bei Eingaben der Länge

n nur n Rechenschritte ausführen darf. Um die gesamte Eingabe lesen zu können, muss der Automat also in jedem Schritt ein Zeichen der Eingabe verarbeiten.



Definition 2 (DFA)

Ein **endlicher Automat** (kurz: DFA; *deterministic finite automaton*) wird durch ein 5-Tupel $M = (Z, \Sigma, \delta, q_0, E)$ beschrieben, wobei

- Z eine endliche Menge von **Zuständen**,
- Σ das **Eingabealphabet**,
- $\delta : Z \times \Sigma \to Z$ die **Überführungsfunktion**,
- $q_0 \in Z$ der **Startzustand** und
- $E \subseteq Z$ die Menge der **Endzustände** ist.

Die von M **akzeptierte** oder **erkannte Sprache** ist

$$L(M) = \left\{ x_1 \cdots x_n \in \Sigma^* \;\middle|\; \begin{array}{c} \exists\, q_1, \ldots, q_{n-1} \in Z, q_n \in E: \\ \delta(q_i, x_{i+1}) = q_{i+1} \text{ für } i = 0, \ldots, n-1 \end{array} \right\}$$

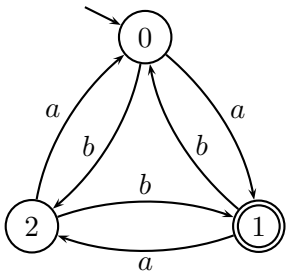
Beispiel 1.3 Betrachte den DFA $M = (Z, \Sigma, \delta, 0, E)$ mit

$$\begin{aligned} Z &= \{0, 1, 2\}, \\ \Sigma &= \{a, b\}, \\ E &= \{1\} \end{aligned}$$

und der Überführungsfunktion

δ	a	b
0	1	2
1	2	0
2	0	1

Graphische Darstellung von M:



Hierbei wird der Startzustand durch einen Pfeil und Endzustände werden durch einen doppelten Kreis gekennzeichnet.

Behauptung 1.4 *M akzeptiert die Sprache*

$$L(M) = \{x \in \Sigma^* \mid \#_a(x) - \#_b(x) \equiv 1 \pmod 3\},$$

wobei $\#_a(x)$ die Anzahl der Vorkommen des Buchstabens a in x bezeichnet. (Für $j \equiv k \pmod m$ schreiben wir im Folgenden auch kurz $j \equiv_m k$.)

Beweis Bezeichne $\hat{\delta}(q, x)$ denjenigen Zustand, in dem sich M nach Lesen von x befindet, wenn M im Zustand q gestartet wird. Dann können wir die Funktion

$$\hat{\delta} : Z \times \Sigma^* \to Z$$

induktiv wie folgt definieren. Für $q \in Z$, $x \in \Sigma^*$ und $a \in \Sigma$ sei

$$\begin{aligned} \hat{\delta}(q, \varepsilon) &= q, \\ \hat{\delta}(q, xa) &= \delta(\hat{\delta}(q, x), a). \end{aligned}$$

Da 1 der einzige Endzustand von M ist, reicht es, folgende Kongruenzgleichung zu zeigen:

$$\hat{\delta}(0, x) \equiv_3 \#_a(x) - \#_b(x),$$

Wir beweisen die Kongruenz induktiv über die Länge von x.

- $|x| = 0$: klar, da $\hat{\delta}(0, \varepsilon) = 0$ und $\#_a(\varepsilon) = \#_b(\varepsilon) = 0$ ist.
- $n \rightsquigarrow n + 1$: Sei $x = x_1 \cdots x_{n+1}$ gegeben. Nach IV ist

$$\hat{\delta}(0, x_1 \cdots x_n) \equiv_3 \#_a(x_1 \cdots x_n) - \#_b(x_1 \cdots x_n).$$

Wegen

$$\delta(i,a) \equiv_3 i+1 \text{ und } \delta(i,b) \equiv_3 i-1$$

folgt daher sofort

$$\hat{\delta}(0,x) = \delta(\hat{\delta}(0,x_1\cdots x_n),x_{n+1}) \equiv_3 \#_a(x) - \#_b(x).$$

■

Eine von einem DFA akzeptierte Sprache wird als **regulär** bezeichnet. Die zugehörige Sprachklasse ist

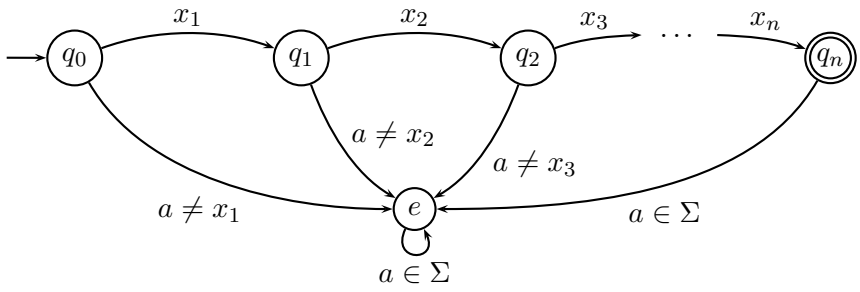
$$\mathrm{REG} = \{L(M) \mid M \text{ ist ein DFA}\}.$$

Um ein intuitives Verständnis für die Berechnungskraft von DFAs zu entwickeln, werden wir uns zunächst intensiv mit der Beantwortung folgender Frage beschäftigen.

Frage: Welche Sprachen gehören zu REG und welche nicht?

Dabei legen wir unseren Überlegungen ein beliebiges aber fest gewähltes Alphabet $\Sigma = \{a_1,\ldots,a_m\}$ zugrunde.

Beobachtung 1.5 *Alle Sprachen, die aus einem einzigen Wort $x = x_1\cdots x_n \in \Sigma^*$ bestehen, sind regulär. Für folgenden DFA M gilt nämlich $L(M) = \{x\}$.*



Formal lässt sich M also durch das Tupel $M = (Z,\Sigma,\delta,q_0,E)$ mit

$$\begin{aligned} Z &= \{q_0,\ldots,q_n,e\}, \\ E &= \{q_n\} \end{aligned}$$

und der Überführungsfunktion

$$\delta(q,a_j) = \begin{cases} q_{i+1}, & q = q_i \text{ für ein } i \text{ mit } 0 \leq i \leq n-1 \text{ und } a_j = x_{i+1} \\ e, & \text{sonst} \end{cases}$$

beschreiben.

Als nächstes betrachten wir Abschlusseigenschaften der Sprachklasse REG.

Definition 1.6 *Ein* **(k-stelliger) Sprachoperator** *ist eine Abbildung op, die k Sprachen $L_1, \ldots, L_k$ auf eine Sprache $op(L_1, \ldots, L_k)$ abbildet.*

Beispiel 1.7 Der 2-stellige Schnittoperator bildet zwei Sprachen L_1 und L_2 auf die Sprache $L_1 \cap L_2$ ab.

Definition 1.8 *Eine Sprachklasse $\mathcal{K}$ heißt unter op* **abgeschlossen***, wenn gilt:*

$$L_1, \ldots, L_k \in \mathcal{K} \Rightarrow op(L_1, \ldots, L_k) \in \mathcal{K}.$$

Der **Abschluss** *von $\mathcal{K}$ unter op ist die kleinste Sprachklasse $\mathcal{K}'$, die $\mathcal{K}$ enthält und unter op abgeschlossen ist.*

Beobachtung 1.9 *Mit $L_1, L_2 \in \mathrm{REG}$ sind auch die Sprachen $\overline{L_1} = \Sigma^* \setminus L_1$, $L_1 \cap L_2$ und $L_1 \cup L_2$ regulär. Sind nämlich $M_i = (Z_i, \Sigma, \delta_i, q_0, E_i)$, $i = 1, 2$, DFAs mit $L(M_i) = L_i$, so akzeptiert der DFA*

$$\overline{M_1} = (Z_1, \Sigma, \delta_1, q_0, Z_1 \setminus E_1)$$

das Komplement $\overline{L_1}$ von L_1. Der Schnitt $L_1 \cap L_2$ von L_1 und L_2 wird dagegen von dem DFA

$$M' = (Z_1 \times Z_2, \Sigma, \delta', (q_0, q_0), E_1 \times E_2)$$

mit

$$\delta'((q, p), a) = (\delta_1(q, a), \delta_2(p, a))$$

akzeptiert. Wegen $L_1 \cup L_2 = \overline{(\overline{L_1} \cap \overline{L_2})}$ ist dann aber auch die Vereinigung von L_1 und L_2 regulär. (Wie sieht der zugehörige DFA aus?)

Aus den beiden Beobachtungen folgt, dass alle endlichen und alle co-endlichen Sprachen regulär sind. Da die in Beispiel 1.3 betrachtete Sprache weder endlich noch co-endlich ist, haben wir damit allerdings noch nicht alle regulären Sprachen erfasst. Es stellt sich die Frage, ob REG neben den mengentheoretischen Operationen Schnitt, Vereinigung und Komplement unter weiteren Operationen wie etwa der **Produktbildung**

$$L_1 L_2 = \{xy \mid x \in L_1, y \in L_2\}$$

(auch **Verkettung** oder **Konkatenation** genannt) oder der Bildung der **Sternhülle**

$$L^* = \bigcup_{n \geq 0} L^n$$

abgeschlossen ist. Die n-fache Potenz L^n von L ist dabei induktiv durch

$$L^0 = \{\varepsilon\},\ L^{n+1} = L^n L$$

definiert.

Im übernächsten Abschnitt werden wir sehen, dass die Klasse REG als der Abschluss der endlichen Sprachen unter Vereinigung, Produktbildung und Sternhülle charakterisierbar ist. Beim Versuch, einen endlichen Automaten für das Produkt $L_1 L_2$ zweier regulärer Sprachen zu konstruieren, stößt man auf die Schwierigkeit, den richtigen Zeitpunkt für den Übergang von (der Simulation von) M_1 zu M_2 zu finden. Unter Verwendung eines nichtdeterministischen Automaten lässt sich dieses Problem jedoch leicht beheben, da dieser den richtigen Zeitpunkt „erraten“ kann. Im nächsten Abschnitt werden wir nachweisen, dass auch nichtdeterministische endliche Automaten nur reguläre Sprachen erkennen können.

1.2 Nichtdeterministische endliche Automaten

Definition 10 (NFA)

Ein **nichtdeterministischer endlicher Automat** (kurz: NFA; *nondeterministic finite automaton*) $N = (Z, \Sigma, \delta, Q_0, E)$ ist ähnlich aufgebaut wie ein DFA, nur dass er mehrere Startzustände (zusammengefasst in der Menge $Q_0 \subseteq Z$) haben kann und seine Überführungsfunktion

$$\delta : Z \times \Sigma \to \mathcal{P}(Z)$$

die Potenzmenge $\mathcal{P}(Z)$ von Z als Wertebereich hat. Die von N akzeptierte Sprache ist

$$L(N) = \left\{ x_1 \cdots x_n \in \Sigma^* \;\middle|\; \begin{array}{l} \exists\, q_0 \in Q_0, q_1, \ldots, q_{n-1} \in Z, q_n \in E: \\ q_{i+1} \in \delta(q_i, x_{i+1}) \text{ für } i = 0, \ldots, n-1 \end{array} \right\}$$

Ein NFA kann also nicht nur eine, sondern mehrere verschiedene Rechnungen ausführen. Die Eingabe gehört bereits dann zu $L(N)$, wenn bei einer dieser Rechnungen nach Lesen des gesamten Eingabewortes ein Endzustand erreicht wird. Im

Gegensatz zu einem DFA, dessen Überführungsfunktion auf der gesamten Menge $Z \times \Sigma$ definiert ist, kann ein NFA „stecken bleiben“. Das ist dann der Fall, wenn er in einen Zustand q gelangt, in dem das nächste Eingabezeichen x_i wegen $\delta(q, x_i) = \emptyset$ nicht gelesen werden kann.

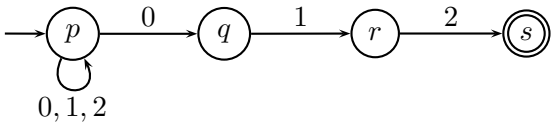
Beispiel 1.11 Betrachte den NFA $N = (Z, \Sigma, \delta, Q_0, E)$ mit

$$\begin{array}{rcl} Z & = & \{p, q, r, s\}, \\ \Sigma & = & \{0, 1, 2\}, \\ Q_0 & = & \{p\}, \\ E & = & \{s\} \end{array}$$

und der Überführungsfunktion

δ	p	q	r	s
0	$\{p, q\}$	$\emptyset$	$\emptyset$	$\emptyset$
1	$\{p\}$	$\{r\}$	$\emptyset$	$\emptyset$
2	$\{p\}$	$\emptyset$	$\{s\}$	$\emptyset$

Graphische Darstellung von N:



Offensichtlich akzeptiert N die Sprache

$$L(N) \quad = \quad \{x012 \mid x \in \Sigma^*\}$$

aller Wörter, die mit dem Suffix 012 enden.

Beobachtung 1.12 *Sind $N_i = (Z_i, \Sigma, \delta_i, Q_i, E_i)$ ($i = 1, 2$) NFAs, so werden auch die Sprachen $L(N_1)L(N_2)$ und $L(N_1)^*$ von einem NFA erkannt. Wir können $Z_1 \cap Z_2 = \emptyset$ annehmen. Dann akzeptiert der NFA*

$$N = (Z_1 \cup Z_2, \Sigma, \delta, Q_1, E)$$

mit

$$\delta(p, a) = \begin{cases} \delta_1(p, a), & p \in Z_1 \setminus E_1, \\ \delta_1(p, a) \cup \bigcup_{q \in Q_2} \delta_2(q, a), & p \in E_1, \\ \delta_2(p, a), & \textit{sonst} \end{cases}$$

und

$$E = \begin{cases} E_1 \cup E_2, & Q_2 \cap E_2 \neq \emptyset \\ E_2, & \textit{sonst} \end{cases}$$

die Sprache $L(N_1)L(N_2)$ *und der NFA*

$$N^* = (Z_1 \cup \{q_{neu}\}, \Sigma, \delta^*, Q_1 \cup \{q_{neu}\}, E_1 \cup \{q_{neu}\})$$

mit

$$\delta^*(p,a) = \begin{cases} \delta(p,a) \cup \bigcup_{q \in Q_1} \delta(q,a), & p \in E_1, \\ \delta(p,a), & \textit{sonst} \end{cases}$$

die Sprache $L(N_1)^*$.

Theorem 1.13 $\mathrm{REG} = \{L(N) \mid N \textit{ ist ein NFA}\}$.

Beweis Die Inklusion von links nach rechts ist klar, da jeder DFA auch als NFA aufgefasst werden kann. Für die Gegenrichtung konstruieren wir zu einem NFA $N = (Z, \Sigma, \delta, Q_0, E)$ einen DFA M mit $L(M) = L(N)$. Zunächst erweitern wir die Überführungsfunktion $\delta : Z \times \Sigma \to \mathcal{P}(Z)$ zu $\delta' : \mathcal{P}(Z) \times \Sigma \to \mathcal{P}(Z)$ mittels

$$\delta'(Q,a) = \bigcup_{q \in Q} \delta(q,a).$$

und zeigen folgende Behauptung:

> $\hat{\delta}'(Q_0, x)$ enthält alle von N bei Eingabe x in $|x|$ Schritten erreichbaren Zustände.

Wir beweisen die Behauptung induktiv über die Länge von x.

- $|x| = 0$: klar, da $\hat{\delta}'(Q_0, \varepsilon) = Q_0$.
- $n-1 \rightsquigarrow n$: Sei $x = x_1 \cdots x_n$ gegeben. Nach Induktionsvoraussetzung enthält
  $$Q_{n-1} = \hat{\delta}'(Q_0, x_1 \cdots x_{n-1})$$
  alle Zustände, die $N(x)$ in $n-1$ Schritten erreichen kann. Wegen
  $$\hat{\delta}'(Q_0, x) = \delta'(Q_{n-1}, x_n) = \bigcup_{q \in Q_{n-1}} \delta(q, x_n)$$
  enthält dann aber $\hat{\delta}'(Q_0, x)$ alle Zustände, die $N(x)$ in n Schritten erreichen kann.

Nun ist leicht zu sehen, dass der DFA

$$M = (\mathcal{P}(Z), \Sigma, \delta', Q_0, E')$$

mit

$$\delta'(Q, a) = \bigcup_{q \in Q} \delta(q, a)$$

und

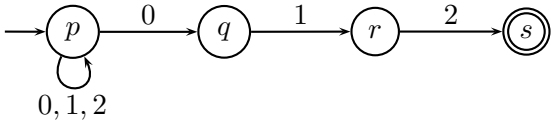
$$E' = \{Q \subseteq Z \mid Q \cap E \neq \emptyset\}$$

äquivalent zu N ist, da für alle Wörter $x \in \Sigma^*$ gilt:

$$\begin{aligned} x \in L(N) &\Leftrightarrow N(x) \text{ kann in genau } |x| \text{ Schritten einen Endzustand erreichen} \\ &\Leftrightarrow \hat{\delta}'(Q_0, x) \cap E \neq \emptyset \\ &\Leftrightarrow \hat{\delta}'(Q_0, x) \in E' \\ &\Leftrightarrow x \in L(M). \end{aligned}$$

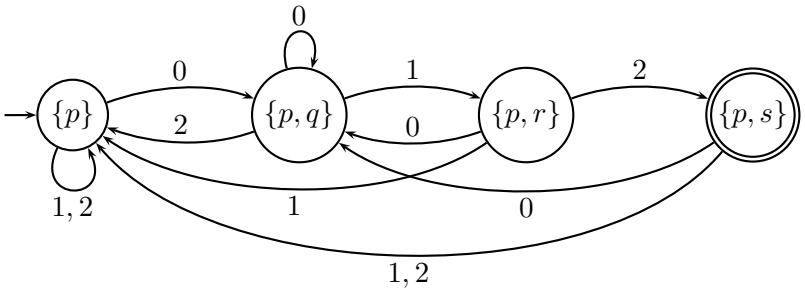
■

Beispiel 1.14 Für den NFA $N = (Z, \Sigma, \delta, Q_0, E)$ aus Beispiel 1.11



ergibt die Konstruktion des vorigen Satzes den folgenden DFA M (nach Entfernung aller vom Startzustand $Q_0 = \{p\}$ aus nicht erreichbaren Zustände):

δ'	0	1	2
$Q_0 = \{p\}$	$\{p, q\}$	$\{p\}$	$\{p\}$
$Q_1 = \{p, q\}$	$\{p, q\}$	$\{p, r\}$	$\{p\}$
$Q_2 = \{p, r\}$	$\{p, q\}$	$\{p\}$	$\{p, s\}$
$Q_3 = \{p, s\}$	$\{p, q\}$	$\{p\}$	$\{p\}$



Im obigen Beispiel wurden für die Konstruktion des DFA M aus dem NFA N nur 4 der insgesamt $2^{\|Z\|} = 16$ Zustände benötigt, da die übrigen 12 Zustände in $\mathcal{P}(Z)$ nicht vom Startzustand $Q_0 = \{p\}$ aus erreichbar sind. Es gibt jedoch Beispiele, bei denen alle $2^{\|Z\|}$ Zustände in $\mathcal{P}(Z)$ für die Konstruktion des so genannten **Potenzmengenautomaten** M benötigt werden (siehe Übungen).