ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Prof. Dr. Andreas Podelski
Matthias Heizmann
Alexander Nutz
Christian Schilling

21.11.2013

Präsenzübungen in der Vorlesung

Theoretische Informatik

Mit Lösungsskizze

Aufgabe 1: Reguläre Ausdrücke und endliche Automaten

Gegeben sei der folgende reguläre Ausdruck über dem Alphabet $\Sigma = \{a, b\}$:

$$\alpha = (a+b)^* aa(a+b)^*$$

(a) Welche Sprache wird durch α beschrieben? Es genügt, wenn Sie eine informelle Beschreibung von $L(\alpha)$ angeben.

(b) Geben Sie alle Residuen ($u^{-1}L(\alpha)$) von $L(\alpha)$ an. Beschreiben Sie jedes Residuum durch einen regulären Ausdruck.

(c) Geben Sie den Minimalautomaten für die Sprache $L(\alpha)$ an.

. . . . Lösungsskizze . . . .

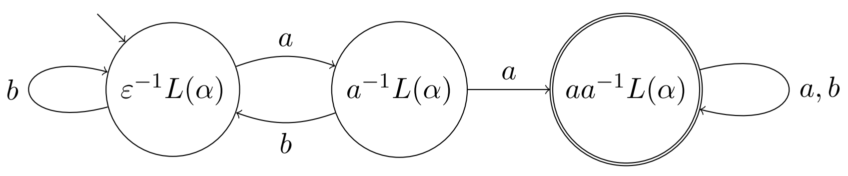
(a) $L(\alpha) = \{uaav \mid u, v \in \Sigma^*\} = \{w \in \Sigma^* \mid w \text{ enthält das Teilwort } aa\}$

(b) (i) $\varepsilon^{-1}L(\alpha) = \alpha$

(ii) $a^{-1}L(\alpha) = a(a+b)^* + \alpha$

(iii) $aa^{-1}L(\alpha) = (a+b)^*$

(c)



Aufgabe 2: Reguläre Sprachen

Zeigen Sie, dass folgende Sprache über dem Alphabet $\Sigma = \{a, b\}$ nicht regulär ist:

$$L = \{a^m b^n \mid m < n\}$$

.... Lösungsskizze ....

Angenommen, L sei regulär. Dann gibt es eine Wortlänge p aus dem Pumping Lemma. Wir wählen das Wort $z = a^p b^{p+1}$. Es gilt $|z| = 2p + 1 \geq p$.
Dann gibt es eine Zerlegung $z = uvw$ mit $|uv| \leq p$ und $|v| > 0$ und es gilt für alle $i \in \mathbb{N} : uv^i w \in L$.
Wir wissen, dass uv nur aus a besteht, also $u = a^{|u|}$ und $v = a^{|v|}$.
Wir wählen $i = 2$ und erhalten $z' := uv^2 w = a^{|u|} a^{2|v|} a^{p-|uv|} b^{p+1}$.
Die Anzahl der a ist $|u| + 2|v| + (p - |uv|) = p + |v|$ und $|v| > 0$. Also enthält z' mindestens so viele a wie b und damit gilt $z' \notin L$.
Widerspruch, also ist L nicht regulär.

Aufgabe 3: Abschluss unter Rückwärtsoperator

In den Übungen wurde bereits gezeigt: Reguläre Sprachen sind unter dem Rückwärtsoperator abgeschlossen. Beweisen Sie diesen Satz erneut, indem Sie nicht mit Automaten, sondern mit regulären Ausdrücken argumentieren.

Zur Erinnerung:
Der *Rückwärtsoperator* für Wörter $w = a_1 a_2 \dots a_n \in \Sigma^*$ ist wie folgt definiert:

$$w^R = a_n a_{n-1} \dots a_1$$

Basierend darauf ist der *Rückwärtsoperator* für Sprachen $L \subseteq \Sigma^*$ wie folgt definiert:

$$L^R = \{w^R \in \Sigma^* \mid w \in L\}$$

.... Lösungsskizze ....

Beweisidee: Wir wissen, dass jede reguläre Sprache durch einen regulären Ausdruck beschrieben werden kann. Wir zeigen, dass "Umdrehen" eines regulären Ausdruckes die Rückwärtssprache beschreibt. Daraus folgt direkt die zu zeigende Behauptung.

Zunächst beschreiben wir formal was wir mit "Umdrehen" meinen und definieren den Rückwärtsoperator $\cdot^R$ für reguläre Ausdrücke wie folgt.

- $\emptyset^R = \emptyset$
- $\varepsilon^R = \varepsilon$
- $a^R = a$ für $a \in \Sigma$
- $(\alpha + \beta)^R = (\alpha^R + \beta^R)$
- $(\alpha \cdot \beta)^R = (\beta^R \cdot \alpha^R)$
- $(\alpha^*)^R = (\alpha^R)^*$

Wir beweisen die folgende Aussage: Für jeden regulären Ausdruck α ist die Sprache des "Rückwärtsausdruckes" α^R, die Rückwärtsprache von α.

$$L(\alpha^R) = (L(\alpha))^R$$

Wir führen unseren Beweis mit Hilfe von struktureller Induktion über den Aufbau von regulären Ausdrücken.

- Induktionsanfang:
  - $L(\emptyset^R) = L(\emptyset) = L(\emptyset)^R$
  - $L(\varepsilon^R) = L(\varepsilon) = L(\varepsilon)^R$
  - $L(a^R) = L(a) = L(a)^R$
- Induktionsschritt:
  - $L((\alpha+\beta)^R) = L(\alpha^R+\beta^R) = L(\alpha^R) \cup L(\beta^R) \overset{IV}{=} L(\alpha)^R \cup L(\beta)^R = (L(\alpha) \cup L(\beta))^R = L(\alpha+\beta)^R$
  - $L((\alpha\cdot\beta)^R) = L(\beta^R \cdot \alpha^R) = L(\beta^R) \cdot L(\alpha^R) \overset{IV}{=} L(\beta)^R \cdot L(\alpha)^R \overset{(i)}{=} (L(\alpha) \cdot L(\beta))^R = L(\alpha\cdot\beta)^R$
  - $L((\alpha^*)^R) = L((\alpha^R)^*) = L(\alpha^R)^* \overset{IV}{=} (L(\alpha)^R)^* \overset{(iii)}{=} L(\alpha^*)^R$

Wir verwendeten dabei die folgenden Behauptungen.

- Behauptung (i): Für alle Wörter $w_1 \in \Sigma^*$,$w_1 \in \Sigma^*$ gilt die folgende Äquivalenz

$$w_2 \cdot w_1 \in L_2^R \cdot L_1^R \quad \Leftrightarrow \quad w_2 \cdot w_1 \in (L_1 \cdot L_2)^R$$

  Beweis zu (i):

$$\begin{array}{ll} & w_2 \cdot w_1 \in L_2^R \cdot L_1^R \\ \Leftrightarrow & w_1 \in L_1^R \text{ und } w_2 \in L_2^R \\ \Leftrightarrow & w_1^R \in L_1 \text{ und } w_2^R \in L_2 \\ \Leftrightarrow & w_1^R \cdot w_2^R \in L_1 \cdot L_2 \\ \overset{(ii)}{\Leftrightarrow} & (w_2 \cdot w_1)^R \in L_1 \cdot L_2 \\ \Leftrightarrow & w_2 \cdot w_1 \in (L_1 \cdot L_2)^R \end{array}$$

- Behauptung (ii): Für alle Wörter $u \in \Sigma^*$,$v \in \Sigma^*$ gilt die folgende Gleichheit

$$u^R \cdot v^R = (v \cdot u)^R$$

  Beweis zu (ii)

  Sei $u = a_1 \dots a_n$ und $v = b_1 \dots b_m$ mit $a_i \in \Sigma$ und $b_j \in \Sigma$, dann gilt

$$u^R \cdot v^R = a_n \dots a_1 \cdot b_m \dots b_1 = (v \cdot u)^R$$

- Behauptung (iii): Für alle Wörter $w \in \Sigma^*$ gilt:

$$w \in (L^R)^* \Leftrightarrow w \in (L^*)^R$$

  Beweis zu (iii)

  Nach Definition des Kleeneschen Sternoperators gilt:

$$w \in (L^R)^* \Leftrightarrow \text{ es gibt ein } n \in \mathbb{N} \text{ sodass } w \in (L^R)^n$$

  Wir zeigen durch vollständige Induktion über n, dass die Äquivalenz $w \in (L^R)^n \Leftrightarrow w \in (L^n)^R$ gilt.

- Induktionsanfang $n = 0$: klar.
- Induktionsschritt $n - 1 \rightsquigarrow n$:
  Sei $w = w_1 \cdot w_2$ für $w_1 \in (L^R)^{n-1}$ und $w_2 \in L^R$.
  Nach Induktionsvoraussetzung gilt die Äquivalenz $w_1 \in (L^R)^{n-1} \Leftrightarrow w_1 \in (L^{n-1})^R$, zusammen mit Behauptung (i) folgt die Äquivalenz $w_1 \cdot w_2 \in (L^R)^n \Leftrightarrow w_1 \cdot w_2 \in (L^n)^R$.

Hinweis: Dieser formale Beweis ist **keine** typische Klausuraufgabe!