Karlsruher Institut für Technologie

Institute of Information Security and Dependability
Dr. Mattias Ulbrich
https://formal.kastel.kit.edu/

Übungsblatt 10

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in: | Tutorium Nr.:

Nach-,Vorname: ,

Matr.nr.:

Ausgabe: 23. Januar 2023, 14:30 Uhr

Abgabe: 2. Februar 2024, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 10: / 19

Blätter 1 – 10: / 201

Aufgabe 1 - Dreifaltigkeit (5.5 Punkte)

Gegeben sei die Sprache

$$L = \{w \in Z_{10}^* \mid \mathrm{Num}_{10}(w) \text{ ist durch 3 teilbar}\} \quad .$$

a) Geben Sie 3991 **mod** 3, 43 **mod** 3 und 437 **mod** 3 an. (0.5 Punkte)

b) Geben Sie die Menge X_0 aller $x \in Z_{10}$ an, für die gilt: $\mathrm{Num}_{10}(wx)$ **mod** $3 = \mathrm{Num}_{10}(w)$ **mod** 3 für alle $w \in Z_{10}^*$. Begründen Sie Ihre Antwort. (0.5 Punkte)

c) Geben Sie die Menge X_1 aller $x \in Z_{10}$ an, für die gilt: $\mathrm{Num}_{10}(wx)$ **mod** $3 = (\mathrm{Num}_{10}(w) + 1)$ **mod** 3 für alle $w \in Z_{10}^*$. Begründen Sie Ihre Antwort. (0.5 Punkte)

d) Geben Sie einen endlichen Akzeptor $\mathcal{A}$ an, so dass $L(\mathcal{A}) = L$ gilt. (2 Punkte)

e) Geben Sie eine Produktionsmenge P an, so dass $G = (\{N_0, N_1, N_2\}, Z_{10}, N_0, P)$ eine rechtslineare Grammatik ist und $L(G) = L$ gilt. (2 Punkte)

   Hinweis: Die Menge P kann angegeben werden, ohne alle Produktionen einzeln aufzuzählen.

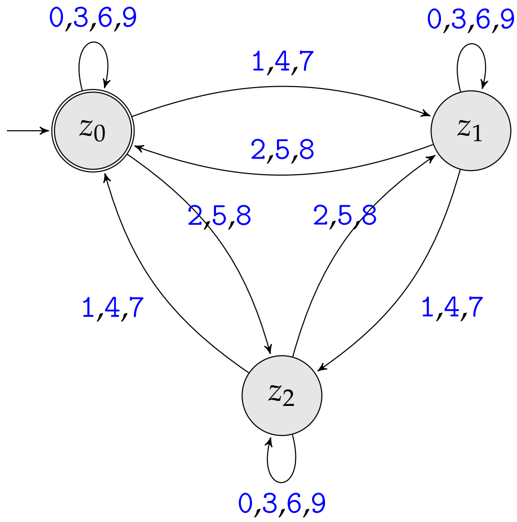
Lösung 1

a) $3991 \textbf{ mod } 3 = 1, \qquad 43 \textbf{ mod } 3 = 1, \qquad 437 \textbf{ mod } 3 = 2$

b) $X_0 = \{\mathtt{0}, \mathtt{3}, \mathtt{6}, \mathtt{9}\}$

c) $X_1 = \{\mathtt{1}, \mathtt{4}, \mathtt{7}\}$

d) $\mathcal{A} = (\{z_0, z_1, z_2\}, z_0, A, f, \{z_0\})$. Die Zustandsüberführungsfunktion f von $\mathcal{A}$ ist gegeben durch:



e)

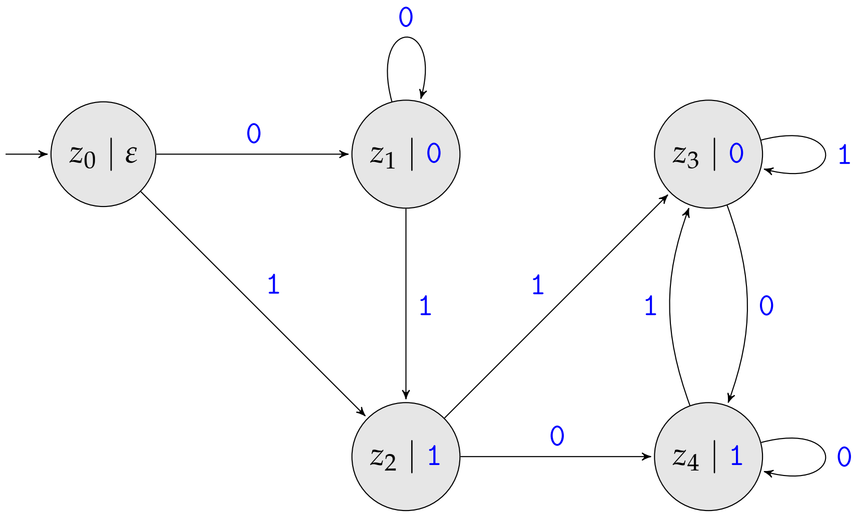
$$
\begin{aligned}
P = &\{N_0 \to \varepsilon\} \\
&\cup \{N_i \to xN_i \mid i \in \{0,1,2\} \text{ und } x \in \{0,3,6,9\}\} \\
&\cup \{N_i \to xN_{(i+1)\,\mathbf{mod}\,3} \mid i \in \{0,1,2\} \text{ und } x \in \{1,4,7\}\} \\
&\cup \{N_i \to xN_{(i+2)\,\mathbf{mod}\,3} \mid i \in \{0,1,2\} \text{ und } x \in \{2,5,8\}\}
\end{aligned}
$$

Aufgabe 2 - Moore-Automaten (4.5 Punkte)

Für einen Automaten (Z, z_0, X, f, Y, h) gemäß der Vorlesung ist die *Ausgabefunktion* $o : X^* \to Y^*$ folgendermaßen definiert:

$$o\colon X^* \to Y^*, w \mapsto h^{**}(f_{**}(z_0, w))$$

Für diese Aufgabe wird nun $X = \{0, 1\}$ als Ein- und Ausgabealphabet verwendet. Der Moore-Automat $\mathcal{A}$ ist durch folgende graphische Repräsentation gegeben:



Die Funktionen f_{**}, h^{**} und g_{**} beziehen sich auf die in der Vorlesung definierten Funktionen für den Automaten $\mathcal{A}$.

a) Berechnen Sie $f_{**}(z_0, 0001)$, $h^{**}(z_2z_3z_4z_3)$, $g_{**}(z_0, 1110)$ und $o(111)$. (1 Punkt)

b) Geben Sie die Menge M aller Wörter $w \in X^*$ an, für die $(o(w))(|w|-1) = 1$ gilt. (0.5 Punkte)

c) Gegeben sei die Funktion $k\colon X^* \to X^*, w \mapsto R(o(R(w)))$, wobei $R(w)$ die Umkehrung des Wortes w ist. Beschreiben Sie, was k für die Eingabe $w \in X^*$ berechnet. (1 Punkt)

   Hinweis: Es handelt sich um eine Funktion, die in Kapitel 8 der Vorlesung vorgestellt wurde.

d) Geben Sie einen Moore-Automaten $\mathcal{A}'$ an, so dass $o_{\mathcal{A}'}(o(w)) = w$ für alle $w \in X^*$. Die Funktion $o_{\mathcal{A}'}$ ist dabei die Ausgabefunktion des Automaten $\mathcal{A}'$. (1 Punkt)

e) Gibt es für jeden Moore-Automaten $\mathcal{B}$ einen Moore-Automaten $\mathcal{C}$, so dass $o_{\mathcal{B}}(o_{\mathcal{C}}(w)) = w$ für alle $w \in X^*$? Die Funktionen $o_{\mathcal{B}}$ und $o_{\mathcal{C}}$ bezeichnen die Ausgabefunktionen des jeweiligen Automaten. Begründen Sie Ihre Antwort. (1 Punkt)

Lösung 2

a) $f_{**}(z_0, 0001) = z_0z_1z_1z_1z_2$

   $h^{**}(z_2z_3z_4z_3) = 1010$

$g_{**}(z_0, \texttt{1110}) = \texttt{1001}$

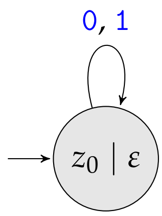
$o(\texttt{111}) = \texttt{100}$

b) $M = \{w\texttt{0} \in X^+ \mid N_{\texttt{1}}(w) > 0\}$

c) k berechnet für alle nichtleeren Wörter über X das Negat im Zweierkomplement, also $k(w) = \text{Zkpl}_{|w|}(w)$ für alle $w \in X^+$.

d) $\mathcal{A}' = \mathcal{A}$ liefert hier das Gewünschte.

e) Nein, der folgende graphisch repräsentierte Automat $\mathcal{B}$ ist ein Gegenbeispiel:



Es gilt $G_{\mathcal{B}}(w) = \varepsilon$ für alle $w \in X^*$. Also ist $G_{\mathcal{B}}$ nicht injektiv und kann keine Rechtsinverse besitzen.

Aufgabe 3 - Reguläre Ausdrücke (4+2 Punkte)

Gegeben seien das Alphabet $\Sigma = \{\texttt{a}, \texttt{b}\}$ und die folgenden beiden regulären Ausdrücke:

$$R_1 = \texttt{abb*(abb*)*}$$

$$R_2 = \texttt{(a*b(a|b)*a)*|a*}$$

a) Zählen Sie alle Wörter in $L(R_1) \cap \Sigma^3$ auf. (0.5 Punkte)

b) Zählen Sie alle Wörter in $L(R_2) \cap \Sigma^3$ auf. (0.5 Punkte)

c) Geben Sie reguläre Ausdrücke R_3, R_4 an, so dass $L(R_3) = L(R_1) \cup L(R_2)$ und $L(R_4) = L(R_1) \cap L(R_2)$ (1 Punkt)

d) Geben Sie einen endlichen Akzeptor $\mathcal{A}_1$ an, so dass $L(\mathcal{A}_1) = L(R_1)$ gilt. (2 Punkte)

e) **Bonusaufgabe:** Geben Sie einen endlichen Akzeptor $\mathcal{A}_2$ an, so dass $L(\mathcal{A}_2) = L(R_2)$ gilt. (2 Punkte)

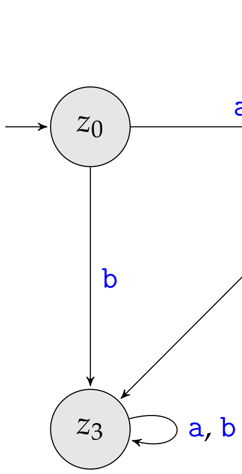
Lösung 3

a) $L(R_1) \cap \Sigma^3 = \{\texttt{abb}\}$

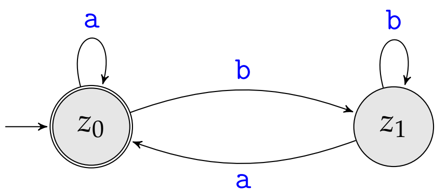
b) $L(R_2) \cap \Sigma^3 = \{\texttt{aaa}, \texttt{aba}, \texttt{baa}, \texttt{bba}\}$

c) $R_3 = R_1 \,|\, R_2$ und $R_4 = \emptyset$

d) $\mathcal{A}_1 = (Z, z_0, \Sigma, f, \{z_0\})$ mit der folgenden graphischen Repräsentation:



e) $\mathcal{A}_2 = (Z, z_0, \Sigma, f, \{z_0\})$ mit der folgenden graphischen Repräsentation:



Aufgabe 4 - Strukturelle Induktion (5 Punkte)

In Foliensatz 19 der Vorlesung wird ab Folie 30 eine Beweisskizze der folgenden Aussage gezeigt:

> Zu jedem regulären Ausdruck R über dem Alphabet A gibt es eine rechtslineare Grammatik G mit $L(G) = L(R)$.

Vervollständigen Sie diese Skizze zu einem Beweis. Orientieren Sie sich dabei an dem in den erwähnten Folien gezeigten Beweisschema.

a) Welche Aussagen sind im Induktionsanfang zu beweisen? Geben Sie für alle Fälle im Induktionsanfang eine rechtslineare Grammatik an, die die korrekte Sprache erzeugt. (1 Punkt)

b) Welche Aussagen sind im Induktionsschritt zu beweisen? Geben Sie für alle Fälle im Induktionsschritt eine rechtslineare Grammatik an, die die korrekte Sprache erzeugt. Beweisen Sie, dass die Grammatiken jeweils rechtslinear sind und die korrekte Sprache erzeugen. (4 Punkte)

Lösung 4

Induktionsanfang: Hier gibt es zwei Fälle zu betrachten.

I) $R = \emptyset$. Dann ist $L(R) = \emptyset$ und $G = (\{S\}, A, S, \emptyset)$ eine rechtslineare Grammatik mit $L(G) = L(R)$.

II) $R = \mathtt{x}$ für $\mathtt{x} \in A$. Dann ist $L(R) = \{\mathtt{x}\}$ und $G = (\{S\}, A, S, \{S \to \mathtt{x}\})$ eine rechtslineare Grammatik mit $L(G) = L(R)$.

Induktionsschritt: Seien R_1, R_2 beliebige reguläre Ausdrücke über A. Per Induktionsannahme gibt es rechtslineare Grammatiken $G_1 = (N_1, A, S_1, P_1), G_2 = (N_2, A, S_2, P_2)$, so dass $L(G_i) = L(R_i)$ für alle $i \in \{1, 2\}$. Wir können o.B.d.A. annehmen, dass $N_1 \cap N_2 = \emptyset$. Zu zeigen sind die folgenden drei Aussagen:

I) Es gibt eine rechtslineare Grammatik G_3, so dass $L(G_3) = L(R_1 \mathtt{|} R_2)$.

II) Es gibt eine rechtslineare Grammatik G_4, so dass $L(G_4) = L(R_1 R_2)$.

III) Es gibt eine rechtslineare Grammatik G_5, so dass $L(G_5) = L(R_1 \mathtt{*})$.

Wir beweisen diese Aussagen wie folgt:

I) In der Vorlesung wurde behauptet,

$$G_3 = (\{S\} \cup N_1 \cup N_2, A, S, \{S \to S_1 \mid S_2\} \cup P_1 \cup P_2)$$

wobei $S \notin N_1 \cup N_2$, sei eine solche Grammatik. G_3 ist offensichtlich rechtslinear. Außerdem gilt

$$\begin{aligned}
& w \in L(G_3) \\
\Longleftrightarrow\ & S \Rightarrow^* w \\
\Longleftrightarrow\ & S \Rightarrow S_1 \Rightarrow^* w \text{ oder } S \Rightarrow S_2 \Rightarrow^* w \\
\Longleftrightarrow\ & w \in L(G_1) \text{ oder } w \in L(G_2) \\
\overset{\text{IA}}{\Longleftrightarrow}\ & w \in L(R_1) \text{ oder } w \in L(R_1) \\
\Longleftrightarrow\ & w \in L(R_1 | R_2)
\end{aligned}$$

II) Sei $P_1' = \{X \to w \in P_1 \mid X \in N_1, w \in A^*\}$ die Menge aller Produktionen in P_1, deren rechte Seite kein Nichtterminal enthält. Sei $P_1'' = \{X \to wS_2 \mid X \to w \in P_1'\}$ die Menge der Produktionen, die man erhält, wenn man an jede Produktion in P_1' das Symbol S_2 hinten anfügt.

Dann erfüllt $G_4 = (N_1 \cup N_2, A, S_1, P_1'' \cup (P_1 \setminus P_1') \cup P_2$ die geforderten Bedingungen.

Sie ist rechtslinear, denn jede Produktion in P_1'' ist von der Form $X \to wY$ und jede Produktion in $(P_1 \setminus P_1') \cup P_2$ ist per Induktionsannahme von der richtigen Form.

Sie erzeugt die richtige Sprache, denn

$$\begin{aligned}
& w \in L(G_4) \\
\Longleftrightarrow\ & S_1 \Rightarrow^* w \\
\Longleftrightarrow\ & \exists u, v\ (w = uv \text{ und } S_1 \Rightarrow^* uS_2 \Rightarrow uv) \\
\Longleftrightarrow\ & \exists u, v\ (w = uv \text{ und } u \in L(G_1) \text{ und } v \in L(G_2)) \\
\overset{\text{IA}}{\Longleftrightarrow}\ & \exists u, v\ (w = uv \text{ und } u \in L(R_1) \text{ und } v \in L(R_2)) \\
\Longleftrightarrow\ & w \in L(R_1 R_2)
\end{aligned}$$

III) Sei P_1' wie oben. Sei $P_1'' = \{X \to wS_1 \mid X \to w \in P_1'\}$ die Menge der Produktionen, die man erhält, wenn man an jede Produktion in P_1' das Symbol S_1 hinten anfügt.

Dann erfüllt $G_5 = (N_1, A, S_1, P_1'' \cup (P_1 \setminus P_1') \cup \{S_1 \to \epsilon\} \cup P_2$ die geforderten Bedingungen.

Sie ist rechtslinear, denn jede Produktion in P_1'' ist von der Form $X \to wY$ und jede Produktion in $(P_1 \setminus P_1') \cup P_2$ ist per Induktionsannahme von der richtigen Form.

Sie erzeugt die richtige Sprache, denn

$$
\begin{aligned}
& w \in L(G_5) \\
\iff & S_1 \Rightarrow^* w \\
\iff & \exists n \in \mathbb{N}, (u_1, \dots, u_n)\ (w = u_1 \dots u_n \text{ und } \forall i \in \{0, \dots, n\}\ (S_1 \Rightarrow^* u_i)) \\
\iff & \exists n \in \mathbb{N}\ (w \in L(G_1)^n) \\
\iff & w \in L(G_1)^* \\
\overset{\text{IA}}{\iff} & w \in L(R_1)^* \\
\iff & w \in L(R_1*)
\end{aligned}
$$

Bitte beachten Sie die folgenden Hinweise:

- Lösungen **müssen** handschriftlich erstellt werden
- Ihre Abgabe sollte die erste Seite dieser Datei als Deckblatt haben
- Ihre Abgabe muss **rechtzeitig** erfolgen

Außerdem, wenn Sie Ihre Ausarbeitung über die Abgabekästen im Keller des Informatik-Gebäudes abgeben:

- Ihre Abgabe muss in der oberen **linken** Ecke zusammengeheftet werden
- Tablet-Ausdrucke sind zulässig

Wenn Sie Ihre Ausarbeitung online über ILIAS abgeben, dann achten Sie darauf:

- Ihre Abgabe muss **genau eine** PDF-Datei sein
- Scans und lesbare Fotos sind zulässig
- Abgabe erfolgt unter „Tutorien" im Ordner **Ihres** Tutoriums