Institut für Theoretische Informatik
Lehrstuhl Prof. Dr. D. Wagner

Übungsblatt 1

Vorlesung Theoretische Grundlagen der Informatik im WS 17/18

Ausgabe 19. Oktober 2017
Abgabe 7. November 2017, 11:00 Uhr (im Kasten im UG von Gebäude 50.34)

Aufgabe 1

(1 + 1 + 1 + 1 = 4 Punkte)

Gegeben seien zwei Sprachen $L_1, L_2 \subseteq \Sigma$ über dem Alphabet $\Sigma = \{a, b\}$. Dabei sei L_1 die Sprache der Wörter, deren erstes und letztes Zeichen übereinstimmen und L_2 die Sprache der Wörter mit einer ungeraden Anzahl an b. Geben Sie reguläre Ausdrücke für folgende Sprachen an.

(a) $L_1 \cup L_2$

(b) $L_1 \cdot L_2$

(c) $L_2 \setminus L_1$

(d) L_1^c

Lösung:
Für $\alpha = \varepsilon \cup a \cup b \cup (a(a \cup b)^\star a) \cup (b(a \cup b)^\star b)$ und $\beta = a^\star(ba^\star ba^\star)^\star ba^\star$ gilt $L_1 = L(\alpha)$ und $L_2 = L(\beta)$. Anders ausgedrückt: α und β beschreiben die Sprachen L_1 beziehungsweise L_2. Demnach gilt:

(a) $L_1 \cup L_2 = L(\alpha \cup \beta)$

(b) $L_1 \cdot L_2 = L(\alpha \cdot \beta)$

(c) $L_2 \setminus L_1 = L((a^+(ba^\star ba^\star)^\star b) \cup (b(a^\star ba^\star b)^\star aa^\star))$

(d) $L_1^c = L((a(a \cup b)^\star b) \cup (b(a \cup b)^\star a))$

Aufgabe 2

(2 + 2 = 4 Punkte)

Sei L eine reguläre Sprache über einem endlichen Alphabet Σ. Für ein Wort $w \in \Sigma^\star$ sei $\overleftarrow{w}$ definiert als das Wort in $\Sigma^\star$ dessen Umkehrung w ist. Es gilt also $\overleftarrow{\varepsilon} = \varepsilon$ und für jedes Wort $w \in \Sigma^+$ mit letztem Zeichen a gilt $\overleftarrow{w} = a \cdot \overleftarrow{(w/a)}$.

(a) Ist die Sprache $L_1 := \{\overleftarrow{w} \mid w \in L\}$ eine reguläre Sprache? Begründen Sie.

(b) Ist die Sprache $L_2 := \{w \cdot \overleftarrow{w} \mid w \in L\}$ eine reguläre Sprache? Begründen Sie.

Lösung:

(a) Ja, L_1 is eine reguläre Sprache. Definiere allgemeiner für jede reguläre Sprache L die Sprache $\overleftarrow{L} := \{\overleftarrow{w} \mid w \in L\}$. Da L regulär ist, wird L durch einen regulären Ausdruck α beschrieben. Wir zeigen per Induktion nach der Anzahl n der Operationen $\cup$, $\cdot$, * in α, dass es einen regulären Ausdruck β gibt, der $\overleftarrow{L}$ beschreibt.

$n = 0$**:** Dann ist $\alpha = \varepsilon$ oder $\alpha = a$ mit $a \in \Sigma$ oder $\alpha = \emptyset$. In jedem Fall gilt $\overleftarrow{L} = L$ und wir wählen $\beta = \alpha$.

$n \geq 1$**:** Dann ist $\alpha = \alpha_1 \cup \alpha_2$ oder $\alpha = \alpha_1 \cdot \alpha_2$ oder $\alpha = \alpha_1^*$ für reguläre Ausdrücke α_1, α_2, je mit höchstens $n-1$ Operationen $\cup$, $\cdot$, *. Nach IV existieren reguläre Ausdrücke β_1 und β_2 die $\overleftarrow{L(\alpha_1)}$ beziehungsweise $\overleftarrow{L(\alpha_2)}$ beschreiben. Wir wählen β wie folgt:

$$\begin{aligned} \alpha = \alpha_1 \cup \alpha_2 \quad &\Rightarrow \quad \beta = \beta_1 \cup \beta_2 \\ \alpha = \alpha_1 \cdot \alpha_2 \quad &\Rightarrow \quad \beta = \beta_2 \cdot \beta_1 \\ \alpha = \alpha_1^\star \quad &\Rightarrow \quad \beta = \beta_1^\star \end{aligned}$$

Nun ist β ein regulärer Ausdruck der die Sprache $\overleftarrow{L}$ beschreibt.

(b) Nein, L_1 is im Allgemeinen keine reguläre Sprache. Betrachte dazu folgendes Bespiel: $L = \{10\}^\star$ ist die Sprache über dem Alphabet $\Sigma = \{0, 1\}$ die nur aus beliebigen Konkatenationen des Wortes 10 besteht. Dann ist $L_2 = \{w \cdot \overleftarrow{w} \mid w \in L\} = \{(10)^n(01)^n \mid n \in \mathbb{N}_{\geq 0}\}$ keine reguläre Sprache, weil auch $L' = \{1^n0^n \mid n \in \mathbb{N}_{\geq 0}\}$ keine reguläre Sprache ist[1].

Aufgabe 3 (1 + 1 = 2 Punkte)

Gegeben seien zwei Grammatiken $G_i = (\Sigma, V, S, R_i), i = 1, 2$ mit $\Sigma = \{a, b, c\}, V = \{S, A, B, C\}$ und folgenden Produktionsregeln

(a) $R_1 = \{S \to ABC, A \to aA \mid a, B \to bB \mid b, C \to cC \mid c\}$

(b) $R_2 = \{S \to aSc \mid B \mid ac, B \to bBc \mid bc\}$

Ist $L(G_i)$ eine reguläre Sprache? Wenn ja, geben Sie einen regulären Ausdruck an. Wenn nicht, begründen Sie dies kurz und geben sie eine (informale) Beschreibung der Sprache an.

Lösung:

(a) $a^+b^+c^+$

(b) $a^ib^jc^{j+i}, i, j \in \mathbb{N}_0, i + j > 0$. Nein, DEA können nicht zählen.

[1]Die Intuition dafür ist, dass man mit regulären Sprachen nicht „zählen“ kann. Bald werden wir diese Intuition formalisieren.

Aufgabe 4 (2 + 1 + 2 = 5 Punkte)

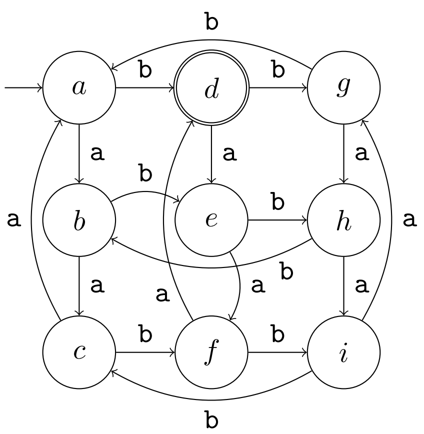
(a) Geben Sie einen deterministischen endlichen Automaten an, der die reguläre Sprache $L_1 = \{w \mid |w|_a \equiv 0 \pmod 3 \wedge |w|_b \equiv 1 \pmod 3\}$ erkennt.
Hinweis: $|w|_x$ gibt an, wie oft x in w vorkommt, z.B. $|\texttt{aba}|_a = 2$.

(b) Wie würden Sie einen deterministischen endlichen Automaten konstruieren, der die reguläre Sprache $L_2 = \{w \mid |w|_a \equiv 0 \pmod{2017} \wedge |w|_b \equiv 1 \pmod{42}\}$ erkennt?

(c) Geben Sie eine nichtdeterministischen endlichen Automaten an, der alle Wörter über dem Alphabet $\{\texttt{0}, \texttt{1}\}$ erkennt, in denen sowohl `0110` als auch `101` als Teilwort vorkommt.

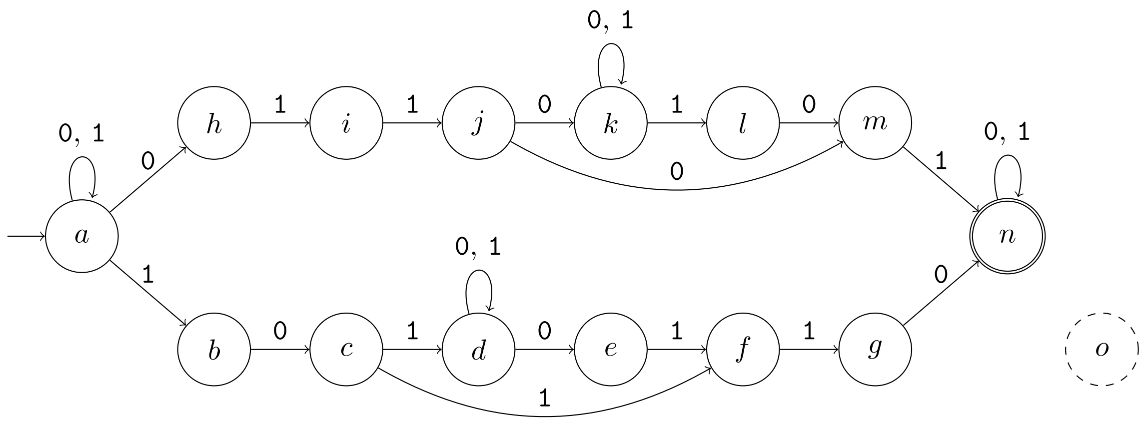
Lösung:

(a)



(b) Gleiche Idee wie in Teil (a), aber konstruiere statt einem 3×3 Gitter ein 42×2017 Gitter.

(c)

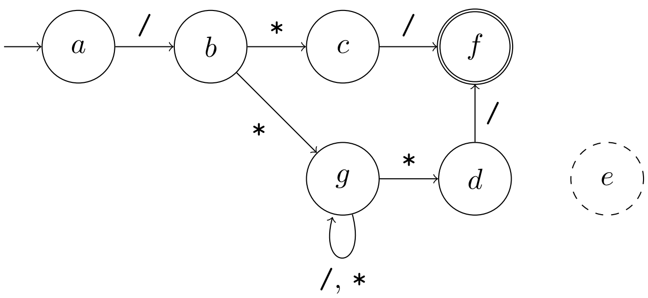


Hinweis: alle nicht explizit angegebenen Übergänge führen zu Zustand o.

Aufgabe 5 (1 + 2 = 3 Punkte)

(a) Geben Sie die reguläre Sprache über dem Alphabet $\Sigma = \{\texttt{/}, \texttt{*}\}$ an, die von dem unten abgebildeten Automaten erkannt wird.
Hinweis: alle nicht explizit angegebenen Übergänge führen zu Zustand e.

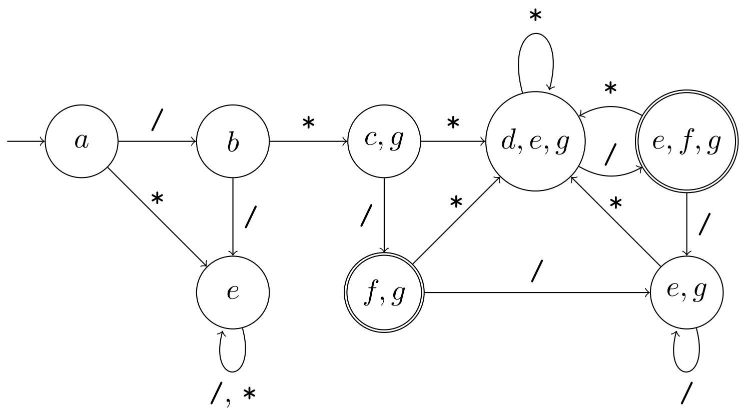
(b) Nutzen Sie die Potenzmengenkonstruktion aus der Vorlesung, um den Automat in einen deterministischen endlichen Automaten zu überführen.



Lösung:

(a) Der Automat erkennt genau die Wörter, die mit „`/*`“ beginnen und mit „`*/`“ enden.

(b)



Aufgabe 6

(1 + 2 + 1 = 4 Punkte)

In dieser Aufgabe geht es darum, einen Fehler in einem Beweis zu finden, zu verstehen und zu beheben.

Theorem. $\sqrt{9}$ *ist irrational.*

Beweis. Durch Widerspruch; nehme an, dass $\sqrt{9}$ rational sei. Dann müssen ganze Zahlen p, q existieren, so dass $q \neq 0, p/q = \sqrt{9}$ gilt, und p und q teilerfremd sind.

Wegen $p/q = \sqrt{9}$ gilt $p^2/q^2 = 9$ und deshalb $p^2 = 9q^2$. Weil q^2 eine ganze Zahl ist, ist p^2 ein Vielfaches von 9, und damit ist p ein Vielfaches von 9. Also gilt $p = 9k$ für eine Ganzzahl k.

Mit $9q^2 = p^2$ und $p = 9k$ ergibt sich $9q^2 = (9k)^2 = 81k^2$, also $q^2 = 9k^2$. Weil k^2 ganzzahlig ist, ist q^2 ein Vielfaches von 9, und damit ist q ebenso ein Vielfaches von 9. Also sind p und q Vielfache von 9. Dies ist aber ein Widerspruch dazu, dass p und q teilerfremd bis auf ± 1 sind. Deshalb ist $\sqrt{9}$ irrational. □

(a) Dieser Beweis ist offensichtlich falsch, da $\sqrt{9} = 3$ nicht irrational ist. Wo *genau* ist der Beweis falsch und wieso?

(b) Der analoge Beweis, um zu zeigen, dass $\sqrt{2}$ irrational ist, stimmt. Ergänzen Sie den Beweis für $\sqrt{2}$ so, dass klar wird, welche Eigenschaft von $\sqrt{2}$ im Gegensatz zu $\sqrt{9}$ wichtig ist, damit der Beweis korrekt ist.

(c) Formulieren Sie mit ihrem Wissen aus Teilaufgabe (b) das obige Theorem für eine allgemeinere Mengen von Zahlen $\{\sqrt{n} \mid \ldots\}$, so dass der Beweis stimmt.

Lösung:

(a) Man kann daraus, dass p^2 ein Vielfaches von 9 ist nicht folgern, dass auch p ein Vielfaches von 9 ist (und analog für q), wähle z.B. $p = 3$.

(b) Aus der Tatsache, dass p^2 ein Vielfaches von 2 ist *kann* man folgern, dass auch p ein Vielfaches von 2 ist. Da p ganzzahlig ist, enthält die Primfaktorzerlegung von p^2 jeden Faktor aus der Primfaktorzerlegung von p doppelt. Enthält also die Primfaktorzerlegung von p^2 eine 2, so muss auch die Primfaktorzerlegung von p eine 2 enthalten.

Für $\sqrt{9}$ gilt das nicht, da die Primfaktorzerlegung von p^2 z.B. genau zweimal den Primfaktor 3 enthalten kann. Dann wird p zwar von 3, aber nicht von 9 geteilt.

(c) Die Argumentation aus Teilaufgabe (b) funktioniert, solange $\sqrt{n} = p/q$ gilt für teilerfremde, jeweils quadratfreie[2] p, q. Das gilt insbesondere wenn n selbst quadratfrei oder sogar prim ist.

Aufgabe 7

(1 + 3 + 2 = 6 Punkte)

Der ebenso geniale, wie auch vergessliche Wissenschaftler und Superbösewicht Doktor Meta ist im Baufieber. Der Hauptzugang zu seinem unterirdischen Geheimlabor soll von einer unüberwindbaren Stahltür geschützt werden, die sich nur durch Eingabe eines gültigen Passworts öffnen lässt. Bei einer falschen Eingabe wird der Eindringling stattdessen durch eine Falltür im Boden den Haien vorgeworfen. Da sich Doktor Meta, aufgrund seiner Vergesslichkeit, nur schlecht an Passwörter erinnern kann, hat er die Tür so eingestellt, dass Sie jedes Wort aus einer zuvor festgelegten formalen Sprache L über einem endlichen Alphabet Σ akzeptiert. Dieses - sicherheitstechnisch fragwürdige, aber für Doktor Meta sehr praktische - Verfahren soll intern durch einen deterministischen endlichen Automaten realisiert werden. Da Sie als Doktor Metas neuer Sicherheitsexperte eingestellt worden sind, sollen Sie ihm bei einigen letzten Konfigurationen helfen:

(a) Kann der Öffnungsmechanismus der Falltür für jede formale Sprache L durch einen deterministischen endlichen Automaten realisiert werden? Warum?

(b) Sie haben sich mit Doktor Meta auf eine geeignete Sprache L geeignet. Leider hat einer ihrer Bauarbeiter, namentlich Ingo N. Kompetenz, das Schloss falsch verbaut. Die Kontrolleinheit der Tür bekommt das Passwort genau umgedreht zur Überprüfung. Da die Bauarbeiten bereits weit fortgeschritten sind, beauftragt Doktor Meta Sie, sich – natürlich erst nachdem Sie Herrn Kompetenz den Haien vorgeworfen haben – um eine Lösung des Problems zu bemühen. Wie könnten Sie den Automaten mit möglichst wenigen Änderungen umbauen, sodass er dennoch die gleiche Passwortmenge erkennt? Wieso funktioniert Ihr Ansatz? Ist Ihr Automat deterministisch oder nichtdeterministisch? Begründen Sie!

[2] Eine Zahl heißt *quadratfrei*, wenn sie von keiner Quadratzahl außer 1 geteilt wird.

(c) Doktor Meta möchte einige Mitarbeiter unauffällig verschwinden lassen. Dafür hat er die Passwörter, die sie normalerweise eingeben, studiert und Muster[3] darin gefunden. Er beauftragt sie nun, die Kontrolleinheit so umzubauen, dass gerade die Muster der Leute, die er loswerden möchte von der Kontrolleinheit abgelehnt werden. Der Automat darf also nur noch eine Teilmenge der alten Sprache L akzeptieren. Können Sie den Automaten für jedes Muster entsprechend umbauen? Begründen Sie Ihre Antwort!

Lösung:

(a) Nein. Dafür muss L regulär sein.

(b) Sei $\mathcal{A} = \{Q, \Sigma, \delta, s, F\}$ ein deterministischer Automat, der L akzeptiert. Konstruiere NEA $\mathcal{A}' = \{Q', \Sigma', \delta', s', F'\}$ wie folgt:

- $Q' = Q \cup \{s'\}$ mit $s' \notin Q$, $\Sigma' = \Sigma$
- Für jedes $a \in \Sigma$ und alle $q_1, q_2 \in Q$, wenn $\delta(q_1, a) = q_2$, dann $\delta(q_2, a) = q_1$. Folglich werden alle Zustandsübergänge *umgedreht*. So kann es zu nichtdeterministischen Übergängen kommen.
- Der Startzustand von $\mathcal{A}$ wird der akzeptierende Zustand von $\mathcal{A}'$: $F' = s$
- s' ist der Startzustand von $\mathcal{A}'$ mit $q(s', \epsilon) = f$ für alle $f \in F$. Es gibt also ϵ-Übergänge.

Dieser NEA kann natürlich mit der Potenzmengenkonstruktion in einen DEA überführt werden.

(c) Nein. Denn die Sprache, die durch die Muster beschrieben wird, muss nicht regulär sein. Zum Beispiel könnten Muster der Form $\left\{a^i b^i \mid i \in \mathbb{N}\right\}$, also eine Teilmenge der regulären Sprache a^+b^+ ist, von einem DEA nicht erkannt werden kann.

[3] Muster sind beliebige Mengen von Wörtern über dem Alphabet Σ.