Prof. T. Nipkow
K. Kappelmann, J. Rädle, L. Stevens

KEINE ABGABE

Technische Universität München
Lehrstuhl für Logik und Verifikation

Einführung in die Theoretische Informatik

Sommersemester 2020 – Übungsblatt Lösungsskizze 4

AUFGABE 4.1. (*Wichtige Begriffe*) Stufe A

Überprüfen Sie, dass Sie die folgenden Begriffe korrekt definieren können.

- Äquivalenzklasse
- Kanonischer Minimalautomat
- Myhill-Nerode-Relation
- Syntaxbaum
- (inhärent-)mehrdeutige Grammatik

AUFGABE 4.2. (*Automata Tutor*) Stufe B

Im AutomataTutor stehen wieder neue Aufgaben zur Verfügung. Die Aufgaben finden Sie unter den Kategorie "Equivalence Classes".

AUFGABE 4.3. (*Myhill-Nerode-Relation und Äquivalenzklassen*) Stufe B

Sei $\mathsf{L} = \mathsf{L}(\mathsf{a}^*\mathsf{b}^*\mathsf{c}^*)$ über dem Alphabet $\Sigma = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$.

(a) Entscheiden Sie, welche der folgenden Äquivalenzen wahr sind und begründen Sie Ihre Antwort:

- $\varepsilon \stackrel{?}{\equiv}_\mathsf{L} \mathsf{a}$
- $\mathsf{b} \stackrel{?}{\equiv}_\mathsf{L} \mathsf{c}$
- $\mathsf{abc} \stackrel{?}{\equiv}_\mathsf{L} \mathsf{cba}$

(b) Sei $v = \mathsf{aababc}$. Geben Sie ein Wort $u \neq v$ an, so dass $u \equiv_\mathsf{L} v$.

(c) Geben Sie die Mengen $[\mathsf{ab}]_\mathsf{L}$, $[\mathsf{bc}]_\mathsf{L}$ und $[\mathsf{ca}]_\mathsf{L}$ an.

(d) Finden Sie nun L', sodass $\mathsf{c} \equiv_{\mathsf{L}'} \mathsf{ba}$, $\mathsf{c} \not\equiv_{\mathsf{L}'} \mathsf{ab}$ und $\mathsf{aba} \equiv_{\mathsf{L}'} \mathsf{bab}$. Weiterhin soll $\varepsilon, \mathsf{aba} \in \mathsf{L}'$ gelten.

Lösungsskizze

(a)
- $\varepsilon \equiv_\mathsf{L} \mathsf{a}$, da $\forall w \in \Sigma^*.\ w \in \mathsf{L} \Leftrightarrow \mathsf{a}w \in \mathsf{L}$.
- $\mathsf{b} \not\equiv_\mathsf{L} \mathsf{c}$, da $\mathsf{bb} \in \mathsf{L}$ aber $\mathsf{cb} \notin \mathsf{L}$.
- $\mathsf{abc} \not\equiv_\mathsf{L} \mathsf{cba}$, da $\mathsf{abc} \in \mathsf{L}$ aber $\mathsf{cba} \notin \mathsf{L}$.

(b) ba

(c) $[\mathsf{ab}]_\mathsf{L} = \mathsf{L}(\mathsf{a}^*\mathsf{b}^+)$, $[\mathsf{bc}]_\mathsf{L} = \mathsf{L}(\mathsf{a}^*\mathsf{b}^*\mathsf{c}^+)$ und $[\mathsf{ca}]_\mathsf{L} = \mathsf{L}(\mathsf{a}^*\mathsf{b}^+\mathsf{a} \mid \mathsf{a}^*\mathsf{b}^*\mathsf{c}^+(\mathsf{a} \mid \mathsf{b}))\Sigma^*$.

(d) $\mathsf{L}^{'} = \{\varepsilon, \mathsf{aba}, \mathsf{bab}, \mathsf{c}, \mathsf{ba}, \mathsf{cb}\}$.

AUFGABE 4.4. (*Myhill-Nerode-Relation*) Stufe D

Hinweis: Bei dieser Aufgabe ist es nicht essentiell dass Sie alle Teilaufgaben bearbeiten. Die ersten beiden Teilaufgaben reichen aus um das Prinzip zu verstehen.

Entscheiden Sie, ob folgende Sprachen über dem Alphabet $\Sigma = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ regulär sind. Bestimmen Sie hierzu die Äquivalenzklassen der dazugehörigen Myhill-Nerode-Relation. Falls die Sprache regulär ist, zählen Sie alle Äquivalenzklassen auf und zeichnen Sie den kanonischen Minimalautomat $M_\mathsf{L} = (\Sigma^*/\equiv_\mathsf{L}, \Sigma, \delta_\mathsf{L}, [\varepsilon]_{\equiv_\mathsf{L}}, F_\mathsf{L})$. Falls die Sprache nicht regulär ist, reicht es eine unendliche Menge von Äquivalenzklassen zu bestimmen.

(a) $\mathsf{L}_1 = \{\mathsf{a}^{2i} \mid i \in \mathbb{N}\}$

(b) $\mathsf{L}_2 = \{\mathsf{a}^i\mathsf{b}^i\mathsf{c}^i \mid i \in \mathbb{N}\}$

(c) $\mathsf{L}_3 = \{w \in \Sigma^* \mid |w|_\mathsf{a} = 2 \cdot |w|_\mathsf{b}\}$

(d) $\mathsf{L}_4 = \mathsf{L}((\mathsf{a}^*(\mathsf{b} \mid \mathsf{c}))^*)$

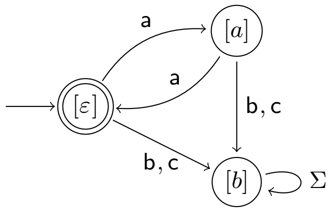
(e) $\mathsf{L}_5 = \{w\mathsf{c}w \mid w \in \{\mathsf{a}, \mathsf{b}\}^*\}$

Lösungsskizze
Hinweis: Da die Sprachen aus dem Kontext ersichtlich ist, lassen wir den L_i Subscript bei $\equiv$ und $[w]$ weg.

(a) • Bestimmen der Äquivalenzklassen:

$$[\varepsilon] = \mathsf{L}_1 \qquad [\mathsf{a}] = \{\mathsf{a}^{2i+1} \mid i \in \mathbb{N}\} \qquad [\mathsf{b}] = \{w \in \Sigma^* \mid |w|_b > 0 \vee |w|_c > 0\}$$

• Kanonischer DFA:

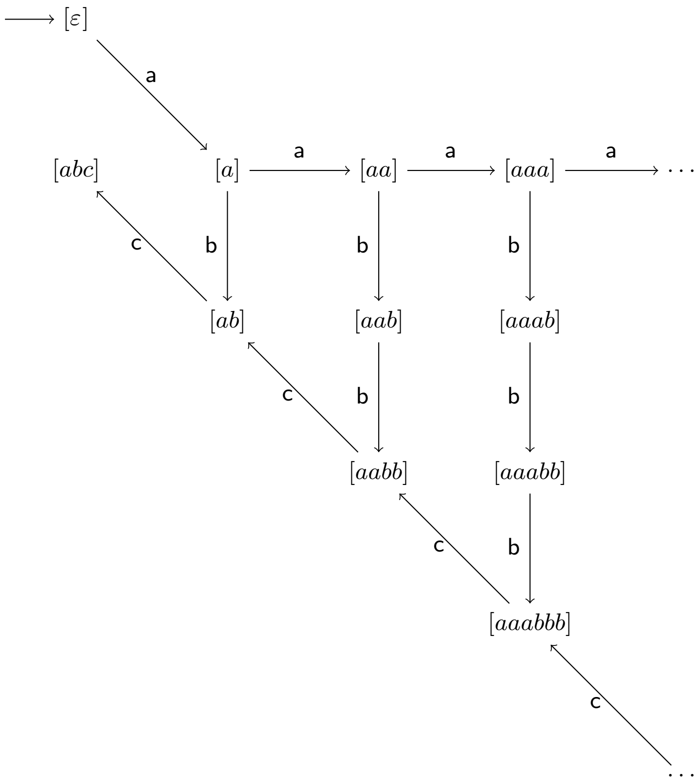


(b) • Bestimmen einer unendlichen Menge von Äquivalenzklassen:

$$\{[\mathsf{a}^i] \mid i \in \mathbb{N}\}$$

Beweis: Sei $i, j \in \mathbb{N}$ verschieden. Dann $\mathsf{a}^i\mathsf{b}^i\mathsf{c}^i \in \mathsf{L}_2$, aber $\mathsf{a}^j\mathsf{b}^i\mathsf{c}^i \notin \mathsf{L}_2$. Daher $[\mathsf{a}^i] \neq [\mathsf{a}^j]$. Somit ist die Menge unendlich und L_2 keine reguläre Sprache.

• Unendliches Transitionssystem (Ablehnende Äquivalenzklasse und entsprechende Transitionen sind nicht gezeichnet):



(c) • Bestimmen einer unendlichen Menge von Äquivalenzklassen:

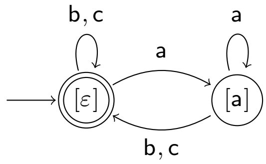
$$\{[\mathsf{b}^i] \mid i \in \mathbb{N}\}$$

Beweis: Sei $i, j \in \mathbb{N}$ verschieden. Dann $\mathsf{b}^i\mathsf{a}^{2\cdot i} \in \mathsf{L}_3$, aber $\mathsf{b}^j\mathsf{a}^{2\cdot i} \notin \mathsf{L}_3$. Daher $[\mathsf{b}^i] \neq [\mathsf{b}^j]$. Somit ist die Menge unendlich und L_3 keine reguläre Sprache.

(d) • Bestimmen der Äquivalenzklassen:

$$[\varepsilon] = \mathsf{L}((\mathsf{a}^*(\mathsf{b} \mid \mathsf{c}))^*) = \mathsf{L}_4 \qquad [\mathsf{a}] = \mathsf{L}((\mathsf{a} \mid \mathsf{b} \mid \mathsf{c})^*\mathsf{a})$$

• Kanonischer DFA:



(e) • Bestimmen der unendlichen Menge von Äquivalenzklassen:

$$\{[\mathsf{a}^i\mathsf{b}^i] \mid w \in \Sigma^*\}$$

Beweis: Sei $i, j \in \mathbb{N}$ verschieden. Dann $\mathsf{a}^i\mathsf{b}^i\mathsf{c}\mathsf{a}^i\mathsf{b}^i \in \mathsf{L}_5$, aber $\mathsf{a}^j\mathsf{b}^j\mathsf{c}\mathsf{a}^i\mathsf{b}^i \notin \mathsf{L}_5$. Somit ist die Menge unendlich und L_5 keine reguläre Sprache.

AUFGABE 4.5. (*Korrektheit von Grammatiken*) Stufe D

Mit $\mathsf{G} = (\{\mathsf{S}, \mathsf{T}\}, \{\mathsf{a}, \mathsf{b}\}, \mathsf{P}, \mathsf{S})$ sei die CFG mit folgenden Produktionen P bezeichnet:

$$\begin{array}{lcl} \mathsf{S} & \to & \mathsf{TaT} \\ \mathsf{T} & \to & \mathsf{aTb} \mid \mathsf{bTa} \mid \mathsf{TT} \mid \mathsf{aT} \mid \varepsilon \end{array}$$

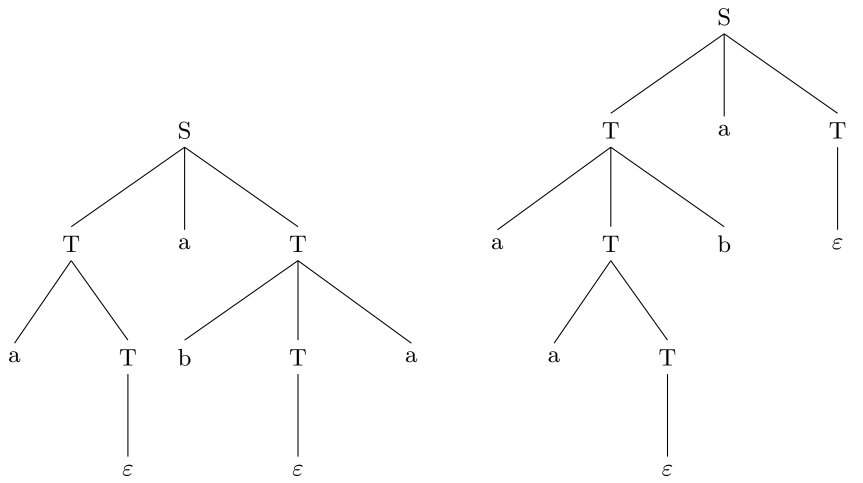
(a) Geben Sie den Syntaxbaum zweier verschiedener Ableitungen des Wortes aaba in G an.

(b) Studieren Sie vor der Bearbeitung der folgenden Aufgaben erneut den Beweis des Satzes 4.16 der Vorlesung. Zeigen Sie $\mathsf{L}_\mathsf{G}(\mathsf{T}) = \{w \in \{\mathsf{a}, \mathsf{b}\}^* \mid |w|_\mathsf{a} \geq |w|_\mathsf{b}\} =: \mathsf{L}$. Sie können dabei wie folgt vorgehen:
   (i) Zeigen Sie $\mathsf{L}_\mathsf{G}(\mathsf{T}) \subseteq \mathsf{L}$ per Induktion über die Erzeugung von Wörtern in $\mathsf{L}_\mathsf{G}(\mathsf{T})$.
   (ii) Zeigen Sie, dass für jedes $w \in \mathsf{L}$, das mit b beginnt, eine Zerlegung $\mathsf{b}x\mathsf{a}y$ existiert, sodass $x, y \in \mathsf{L}$. Verwenden Sie hierzu eine Höhenfunktion wie in der Vorlesung im Beweis zu Satz 4.16.
   (iii) Zeigen Sie $\mathsf{L} \subseteq \mathsf{L}_\mathsf{G}(\mathsf{T})$ per vollständiger Induktion über die Länge von Wörtern in L. Verwenden Sie das Ergebnis der vorherigen Aufgabe. Außerdem dürfen Sie ohne Beweis verwenden, dass für alle $w \in \mathsf{L}$, die mit a beginnen und für die $|w|_\mathsf{a} = |w|_\mathsf{b}$ gilt, eine Zerlegung $\mathsf{a}x\mathsf{b}y$ existiert, sodass $x, y \in \mathsf{L}$.

(c) Welche Sprache erzeugt G ausgehend von S?

Lösungsskizze

(a)



(b) (i) Sei $w \in \mathsf{L}_\mathsf{G}(\mathsf{T})$ beliebig. Das heißt es existiert eine Ableitung $\mathsf{T} \to^* w$. Wir zeigen $w \in \mathsf{L}$ mit Induktion über die Erzeugung von w.
   - Fall $w = \varepsilon$: Es gilt $\varepsilon \in \mathsf{L}$.
   - Fall $w = \mathsf{a}u\mathsf{b}$ mit $T \to^* u$: Per IH gilt $|u|_a \geq |u|_b$. Daraus folgt $|\mathsf{a}u\mathsf{b}|_a \geq |\mathsf{a}u\mathsf{b}|_b$ und damit $\mathsf{a}u\mathsf{b} \in \mathsf{L}$.
   - Fall $w = \mathsf{b}u\mathsf{a}$: Analog.
   - Fall $w = \mathsf{a}u$: Analog.
   - Fall $w = uv$: Per IH gilt $|u|_a \geq |u|_b$ und $|v|_a \geq |v|_b$. Damit folgt $uv \in \mathsf{L}$.

   (ii) Sei $w = x_1 \dots x_n$. Wir definieren eine Höhenfunktion $h(i) := |x_1 \dots x_i|_\mathsf{b} - |x_1 \dots x_i|_\mathsf{a}$. Da $w \in \mathsf{L}$, wissen wir dass $h(n) \leq 0$. Außerdem gilt $h(1) = 1$, da w mit b beginnt. Da sich h mit jedem weiteren Zeichen nur um 1 verändert, muss es also ein j geben, sodass $h(j) = 0$. Wir wählen das kleinste solche j und können mit $h(j-1) = 1$ schließen dass $x_j = \mathsf{a}$. Damit ergibt sich für w insgesamt:

$$w = \mathsf{b}x_2 \dots x_{j-1}\mathsf{a}x_{j+1} \dots x_n$$

Wegen $h(j) = 0$ wissen wir, dass $x_2 \dots x_{j-1}$ gleich viele a's und b's enthält, es gilt also $x_2 \dots x_{j-1} \in \mathsf{L}$. Wegen $h(n) \leq 0$ gilt außerdem, dass $x_{j+1} \dots x_n$ mindestens so viele a's wie b's enthält, womit $x_{j+1} \dots x_n \in \mathsf{L}$ folgt.
Ein analoger Beweis lässt sich für $w \in \mathsf{L}$ führen die mit a beginnen und für die $|w|_{\mathsf{a}} = |w|_{\mathsf{b}}$ gilt. Hier beginnt man mit $h(1) = -1$ und findet das kleinste j sodass $h(j) = 0$ um zu zeigen, dass eine Zerlegung $\mathsf{a}x\mathsf{b}y$ von w existiert, sodass $x, y \in \mathsf{L}$.

(iii) Sei $w \in \mathsf{L}$ beliebig. Wir zeigen $w \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$ mit vollständiger Induktion über $|w|$.
Fall $n = 0$: Folgt direkt aus $\varepsilon \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$.
Fall $n + 1$: Per IH erhalten wir

$$\forall w \in \Sigma^*.\ |w| \leq n \wedge w \in \mathsf{L} \implies w \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$$

Wir müssen zeigen:

$$\forall w \in \Sigma^{n+1}.\ w \in \mathsf{L} \implies w \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$$

Sei $w \in \mathsf{L}$ beliebig mit $|w| = n + 1$.

i. Beginnt w mit einem b, gibt es nach Aufgabe (ii) eine Zerlegung $\mathsf{b}x\mathsf{a}y$ von w mit $x, y \in \mathsf{L}$. Damit können wir w wie folgt ableiten: $\mathsf{T} \to \mathsf{TT} \to \mathsf{bTaT} \to^* \mathsf{b}x\mathsf{a}y = w$ wobei der letzte Schritt mit der IH folgt.
ii. Ist w von der Form $\mathsf{a}x$, gibt es zwei weitere Fälle. Entweder es gilt $|w|_{\mathsf{a}} > |w|_{\mathsf{b}}$, dann folgt mit der IH die Ableitung $\mathsf{T} \to \mathsf{aT} \to^* \mathsf{a}x = w$.
Andernfalls muss $|w|_{\mathsf{a}} = |w|_{\mathsf{b}}$ gelten. Dann gibt es eine Zerlegung $\mathsf{a}x\mathsf{b}y$ von w mit $x, y \in \mathsf{L}$ und wir leiten w mit Hilfe der IH wie folgt ab: $\mathsf{T} \to \mathsf{TT} \to \mathsf{aTbT} \to^* \mathsf{a}x\mathsf{b}y = w$.

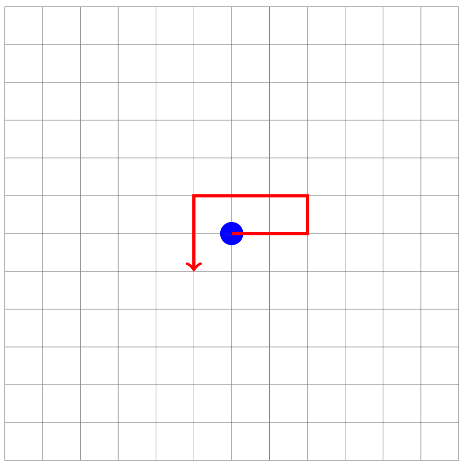
(c) $\mathsf{L}(\mathsf{G})$ enthält alle Wörter der Form $x\mathsf{a}y$ mit $x, y \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$. Wir behaupten

$$\mathsf{L}(\mathsf{G}) = \{w \in \{\mathsf{a}, \mathsf{b}\}^* \mid |w|_{\mathsf{a}} > |w|_{\mathsf{b}}\} =: \mathsf{L}'.$$

Sei $w \in \mathsf{L}(\mathsf{G})$. Dann gibt es $u, v \in \mathsf{L}_{\mathsf{G}}(\mathsf{T})$ mit $w = uav$. Nach vorheriger Aufgabe gilt $|u|_{\mathsf{a}} \geq |u|_{\mathsf{b}}$ und $|v|_{\mathsf{a}} \geq |v|_{\mathsf{b}}$. Somit $|uav|_{\mathsf{a}} > |uav|_{\mathsf{b}}$, also $w \in \mathsf{L}'$.
Nun sei $w \in \mathsf{L}'$. Wir haben $|w|_{\mathsf{a}} > |w|_{\mathsf{b}}$. Erneut betrachten wir den Anfangsbuchstaben von w.
Falls $w = au$, gilt $|u|_{\mathsf{a}} \geq |u|_{\mathsf{b}}$, also $u \in \mathsf{L}$. Es folgt $\mathsf{S} \to \mathsf{T}a\mathsf{T} \to^* \varepsilon au = w$ da $\varepsilon, u \in \mathsf{L} = \mathsf{L}_T(\mathsf{G})$.
Falls $w = bu$, gibt es $i < |w| =: n$ mit $h(i) = 0$. Sei i_m das größte solche i. Es folgt $w_{i_{m+1}} = a$ und $\left|w_{i_{m+2}} \cdots w_n\right|_{\mathsf{a}} \geq \left|w_{i_{m+2}} \cdots w_n\right|_{\mathsf{b}}$. Also $w_1 \cdots w_{i_m}, w_{i_{m+2}} \cdots w_n \in \mathsf{L} = \mathsf{L}_T(\mathsf{G})$ und somit $\mathsf{S} \to \mathsf{T}a\mathsf{T} \to^* w_1 \cdots w_{i_m} a w_{i_{m+2}} \cdots w_n = w$.

AUFGABE 4.6. (*Pfeilsprachen*) Stufe B – C

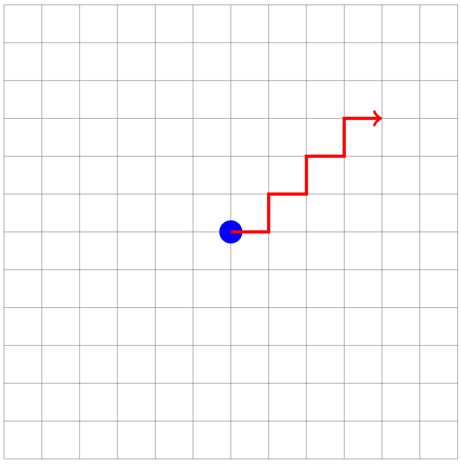
In dieser Aufgabe betrachten wir Sprachen, deren Worte Linienzüge in einem unendlichen zweidimensionalen Gitter von einem fixen Startpunkt aus beschreiben. Die folgende Grafik zeigt einen Ausschnitt aus dem Gitter:

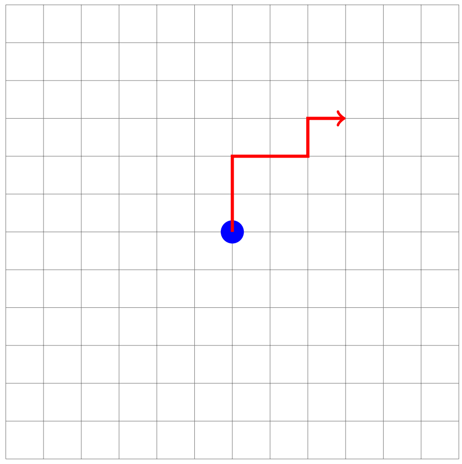


Wir haben Startpunkt blau markiert. Linienzüge beschreiben wir im Folgenden als eine Sequenz von Pfeilen, d.h. als Worte über dem Alphabet $\Sigma = \{\rightarrow, \leftarrow, \uparrow, \downarrow\}$. Die Pfeile beschreiben dabei (vom Startpunkt aus gesehen) einen ein Kästchen langen Schritt entlang des Gitters. Wir stellen daher den im Bild rot eingezeichnete Linienzug durch das Wort $w = \rightarrow\rightarrow\uparrow\leftarrow\leftarrow\leftarrow\downarrow\downarrow$ dar.

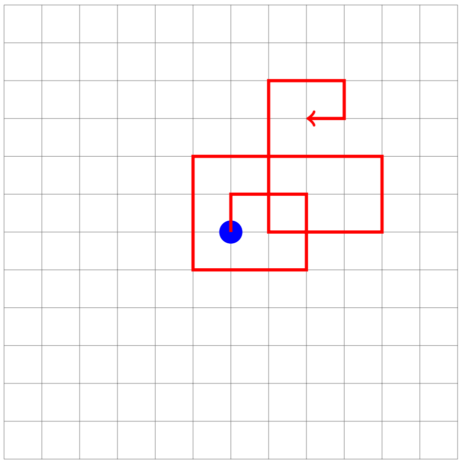
(a) Betrachten Sie die folgenden natürlich sprachlichen Beschreibungen zusammen mit jeweils einem Beispiel, welches in der Sprache liegt (auf der linken Seite), und einem Beispiel, das kein Element der Sprache ist (auf der rechten Seite). *Geben Sie für jede der Sprachen eine formale Definition der Form* $\{w \in \Sigma^* \mid \dots\}$ *an.*[1]

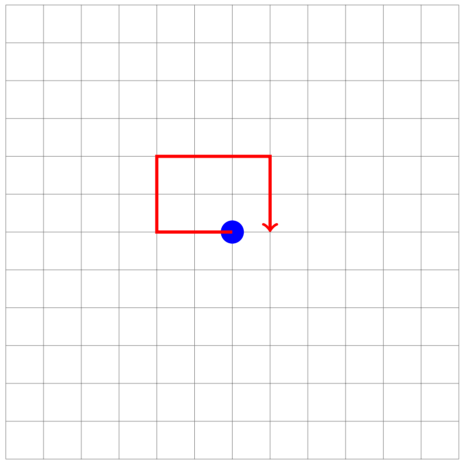
(i) die Sprache aller Treppen über dem Alphabet $\Sigma' = \{\rightarrow, \uparrow\}$



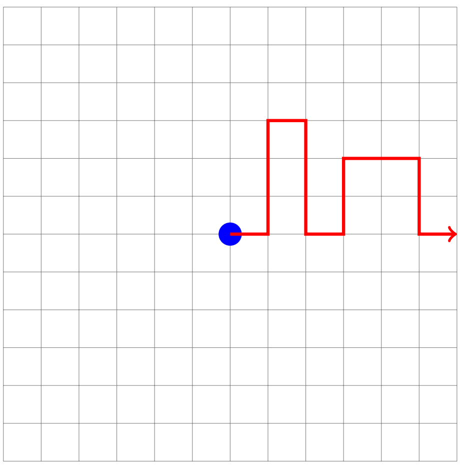


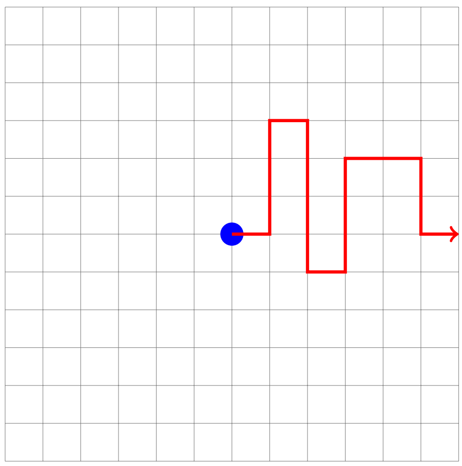
(ii) die Sprache aller im Uhrzeigersinn laufenden Spiralen über dem Alphabet Σ, die vom Startpunkt aus zuerst nach oben laufen





(iii) die Sprache aller "Skylines" über dem Alphabet $\Sigma'' = \{\rightarrow, \uparrow, \downarrow\}$





[1] Das heißt insbesondere, dass Sie in diesem Aufgabenteil keinen Automaten, keinen regulären Ausdruck, keine Grammatik oder ähnliches angeben sollen, die die Sprache beschreiben.

Hinweis: Die Sprachen sind mithilfe der Beispiele nicht eindeutig bestimmt! Ziel der Aufgabe ist es, die intuitive Beschreibung (z.B. “Sprache aller Skylines”) zusammen mit den Beispielen in eine möglichst allgemeine Sprachdefinition zu bringen.

(b) *Stellen Sie Vermutungen auf, ob die obigen Sprachen regulär oder kontextfrei sind.* Begründen Sie Ihre Antwort möglichst anschaulich anhand des Beispiels.

(c) *Geben Sie zu jeder der Sprachen* L *aus Aufgabenteil (a) eine Grammatik* G *an.*

Lösungsskizze

(a) (i) $\mathsf{L} = \{(\rightarrow\uparrow)^i \mid i \in \mathbb{N}\}\{\varepsilon, \rightarrow\}$

(ii) $\mathsf{L} = \{u \in \Sigma^* \mid \exists v \in \Sigma^*.\ uv \in \mathsf{L}((\uparrow^+\rightarrow^+\downarrow^+\leftarrow^+)^*)\}$

(iii) $\mathsf{L} = \{w \in \Sigma^* \mid (\forall u, v \in \Sigma^*.\ w = uv \rightarrow |u|_\uparrow \geq |u|_\downarrow) \wedge (\forall u, v \in \Sigma^*.\ \forall x, y \in \Sigma.\ w = uxyv \rightarrow xy \notin \{\uparrow\downarrow, \downarrow\uparrow\})\}$

(b) (i) regulär, da nur eine Alternierung konstanter Pfade verlangt wird.

(ii) regulär, da nur die Laufrichtung wichtig ist, aber nicht die Länge.

(iii) kontextfrei, da zwei Längen verglichen werden müssen.

(c) (i) $\mathsf{S} \mapsto \rightarrow\uparrow S \mid \rightarrow \mid \varepsilon$

(ii) $\mathsf{S} \mapsto \uparrow S \mid \uparrow T \mid \varepsilon \qquad T \mapsto \rightarrow T \mid \rightarrow U \mid \varepsilon \qquad U \mapsto \downarrow U \mid \downarrow V \mid \varepsilon \qquad V \mapsto \leftarrow V \mid \leftarrow S \mid \varepsilon$

(iii) $\mathsf{S} \mapsto T_? \mid T_? \rightarrow S \qquad T_? \mapsto \varepsilon \mid T \qquad T \mapsto \uparrow T \downarrow \mid T_? \rightarrow T_?$

AUFGABE 4.7. (***(Optional für Interessierte, wird nicht besprochen)*** *RegEx und das kürzeste Pfad-Problem)* Stufe E

In dieser Aufgabe abstrahieren die Interpretation von regulären Ausdrücken. Ziel ist, es den Zusammenhang mit Pfadproblemen und dem Lösen linearer Gleichungssysteme zu verdeutlichen. Insbesondere werden wir das kürzeste Pfad-Problem mit geschickter Interpretation regulärer Ausdrücke lösen.
Dafür führen wir sogenannte Kleene-Algebren ein. Kleene Algebren generalisieren die Operationen die Ihnen von regulären Ausdrücken bekannt sind. Nachfolgend finden Sie die Definition:

Definition (Monoid)

Ein Monoid $\langle M, \circ, 1\rangle$ besteht aus einer Trägermenge M, einer assoziativen Abbildung $\circ\colon M \times M \to M$ und einem bzgl. $\circ$ neutralen Element $1 \in M$ (d.h. $\forall m \in M.\ m \circ 1 = m = 1 \circ m$). Ist $\circ$ kommutativ, dann wird $\langle M, \circ, 1\rangle$ als kommutatives Monoid bezeichnet. Gilt $\forall m \in M.\ m \circ m = m$, so wird $\langle M, \circ, 1\rangle$ als *idempotentes* Monoid bezeichnet.

Definition (Kleene Algebra)

Eine *Kleene Algebra* $\langle K, +, \cdot, ^*, 0, 1\rangle$ besteht aus einer Trägermenge K, den binären Operationen $+\colon K \times K \to K$ (Addition), $\cdot\colon K \times K \to K$ (Multiplikation), der unären Operation $^*\colon K \to K$ (Stern) und zwei Konstanten $0, 1 \in K$. Mittels der Addition definiert man die binäre Relation $\sqsubseteq$ auf K durch

$$a \sqsubseteq b \ :\stackrel{\text{Def.}}{\Longleftrightarrow}\ a + b = b$$

Wie üblich schreibt man kurz ab für $a \cdot b$. Um Klammern zu sparen, gilt "Stern vor Punkt vor Strich".
Eine Kleene Algebra erfüllt folgende Eigenschaften für alle $a, b, c, x \in K$:

Ax1: $\langle K, +, 0\rangle$ ist ein kommutatives und idempotentes Monoid.

Ax2: $\langle K, \cdot, 1\rangle$ ist ein Monoid.

Ax3: $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$.

Ax4: $a0 = 0 = 0a$.

Ax5: $1 + aa^* \sqsubseteq a^*$ und $1 + a^*a \sqsubseteq a^*$.

Ax6: $b + ax \sqsubseteq x \to a^*b \sqsubseteq x$ und $b + xa \sqsubseteq x \to ba^* \sqsubseteq x$.

(a) Sei Σ ein Alphabet. Beweisen Sie, dass $\langle 2^{\Sigma^*}, \cup, \circ, ^*, \emptyset, \{\varepsilon\}\rangle$ eine Kleene Algebra ist für

$$LL' := L \circ L' := \{ww' \mid w \in L, w' \in L'\} \qquad \text{und} \qquad L^* := \bigcup_{k \in \mathbb{N}} L^k$$

(b) Die Addition und das Minimum auf $\mathbb{R}$ seien auf $[-\infty, \infty] = \mathbb{R} \cup \{\pm\infty\}$ wie folgt erweitert:

$$\infty + a = \infty \qquad -\infty + a = -\infty \qquad -\infty + \infty = \infty$$

$$\min(a, \infty) = a \qquad \min(a, -\infty) = -\infty \qquad \min(-\infty, \infty) = -\infty$$

Weiterhin gelte:

$$a^* := \begin{cases} -\infty & \text{falls } a \in [-\infty, 0) \\ 0 & \text{falls } a \in [0, \infty] \end{cases}$$

Beweisen Sie, dass $\langle \mathbb{R} \cup \{\pm\infty\}, \min, +, ^*, \infty, 0\rangle$ eine Kleene Algebra ist.

(c) Zeigen Sie, dass in jeder Kleene Algebra $\langle K, +, \cdot, ^*, 0, 1\rangle$ für beliebige $a, b, c, d, e, f \in K$ gilt:

(i) $\sqsubseteq$ ist eine partielle Ordnung auf K, die monoton bzgl. Addition, Multiplikation und Stern ist, d.h.:

$$a \sqsubseteq b \to (ca \sqsubseteq cb \wedge ac \sqsubseteq bc \wedge a + c \sqsubseteq b + c \wedge a^* \sqsubseteq b^*)$$

(ii) a^*b ist die bzgl. $\sqsubseteq$ kleinste Lösung der linearen Ungleichung $b + aX \sqsubseteq X$ in K (X Variable), genauer:

$$b + a(a^*b) \sqsubseteq a^*b \qquad \wedge \qquad \forall x \in K\colon b + ax \sqsubseteq x \to a^*b \sqsubseteq x$$

Entsprechend ist ba^* die kleinste Lösung in K von $b + Xa \sqsubseteq X$.

Man kann zeigen, dass jedes lineare Ungleichungssystem

$$\begin{aligned} a_{1,1}X_1 + a_{1,2}X_2 + \dots a_{1,n}X_n + b_1 \quad &\sqsubseteq \quad X_1 \\ &\vdots \\ a_{n,1}X_1 + a_{n,2}X_2 + \dots a_{n,n}X_n + b_n \quad &\sqsubseteq \quad X_n \end{aligned}$$

mit $a_{i,j}, b_i \in K$ und $X_1, \ldots, X_n$ Variablen stets eine eindeutige $\sqsubseteq$-kleinste Lösung in K hat, d.h. dass es konkrete Elemente $x_1, \ldots, x_n \in K$ gibt, sodass für $X_1 = x_1, \ldots, X_n = x_n$ alle obigen Ungleichungen erfüllt sind, und für jede weitere Lösung $X_1 = y_1, \ldots, X_n = y_n \in K$ stets $x_i \sqsubseteq y_i$ gilt. Insbesondere gilt

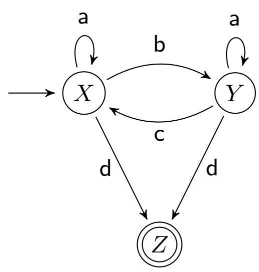
$$x_1 = a_{1,1}^*(a_{1,2}x_2 + \ldots + a_{1,n}x_n + b_1)$$

Somit kann das Gauß-Verfahren zur Bestimmung von $x_1, \ldots, x_n$ verwendet werden.

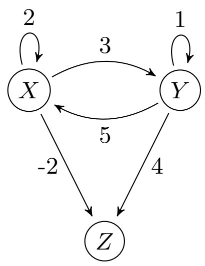
(d) Bestimmen Sie die kleinste Lösung x_1, x_2, x_3, x_4 für folgendes System:

$$\begin{array}{rcl} aX + bY + eZ & \sqsubseteq & X \\ cX + dY + fZ & \sqsubseteq & Y \\ 1 & \sqsubseteq & Z \end{array}$$

(e) Bestimmen Sie den regulären Ausdruck für den Zustand X. Durch welche Werte muss man a, b, c, d, e, f konkret ersetzen, damit sich die in (d) berechneten Terme in $\langle 2^{\Sigma^*}, \cup, \circ, {}^*, \emptyset, \{\varepsilon\}\rangle$ zu dem gewünschten Ausdruck auswertet?



(f) Bestimmen Sie die Länge eines kürzesten Pfades von jedem Knoten zum Knoten Z in folgendem gewichteten Graphen. Durch welche Werte muss man a, b, c, d, e, f konkret ersetzen, damit sich die in (d) berechneten Terme in $\langle \mathbb{R} \cup \{\pm\infty\}, \min, +, \infty, 0\rangle$ zu den gesuchten Pfadlängen auswerten?



Lösungsskizze

(a) Nur Stern überprüfen, Rest sollte klar sein. $\sqsubseteq$ entspricht hier $\subseteq$.
$1 + aa^* \sqsubseteq a^*$ wird zu $\{\varepsilon\} \cup AA^* \subseteq A^*$ mit $A \subseteq \Sigma^*$, was man leicht nachrechnet:

$$\{\varepsilon\} \cup AA^* = \{\varepsilon\} \cup A \bigcup_{k \geq 0} A^k = A^0 \cup \bigcup_{k \geq 1} A^k = A^*$$

Entsprechend für $1 + a^*a \sqsubseteq a^*$.
$b + ax \sqsubseteq x \to a^*b \sqsubseteq x$ wird zu

$$B \cup AX \subseteq X \to A^*B \subseteq X$$

mit $A, B, X \subseteq \Sigma^*$.
Mittels Induktion zeigt man nun, dass $A^kB \subseteq X$ für alle $k \in \mathbb{N}$ unter Verwendung von $B \cup AX \subseteq X$:
- $k = 0$: $A^0B = \{\varepsilon\}B = B \subseteq B \cup AX \subseteq X$.
- $k \to k+1$: Für $k \in \mathbb{N}$ beliebig fixiert gelte $A^kB \subseteq X$. Damit:

$$A^{k+1}B = A(A^kB) \subseteq AX \subseteq B \cup AX \subseteq X$$

Damit:

$$A^*B = \bigcup_{k \geq 0} A^kB \subseteq \bigcup_{k \geq 0} X = X$$

was zu zeigen war.

(b) Zur Verdeutlichung, welche Addition gemeint ist: $+_{\mathbb{R}}$ bezeichnet die übliche Addition auf den reellen Zahlen (erweitert auf $\pm\infty$).

Beachten: $\sqsubseteq$ auf K entspricht hier $\geq$ auf den reellen Zahlen

$$a \sqsubseteq b \text{ gdw. } \min(a,b) = b \text{ gdw. } a \geq b$$

$1 + aa^* \sqsubseteq a^*$ wird zu $\min(0, a +_{\mathbb{R}} a^*) \geq a^*$:
Gilt $a \geq 0$, so folgt $a^* = 0$ und damit $\min(0, a +_{\mathbb{R}} a^*) = 0 = a^*$; gilt $a < 0$, so folgt $a^* = -\infty$ und damit $\min(0, a +_{\mathbb{R}} a^*) = -\infty = a^*$. Für $1 +_{\mathbb{R}} a^* a \sqsubseteq a$ symmetrisch.
Aus $b + ax \sqsubseteq x \to a^* b \sqsubseteq x$ wird $\min(b, a +_{\mathbb{R}} x) \geq x \to a^* +_{\mathbb{R}} b \geq x$:
Aus $\min(b, a +_{\mathbb{R}} x) \geq x$ folgt $b \geq x \wedge a +_{\mathbb{R}} x \geq x$, damit $a \geq 0$ und somit auch $a^* = 0$, womit $a^* +_{\mathbb{R}} b \geq x$ stets gilt.

(c) (i) Reflexivität folgt aus der Definition von $\sqsubseteq$ und der Idempotenz von $+$:

$$a \sqsubseteq a \overset{\text{nDef}}{\longleftrightarrow} a + a = a$$

Antisymmetrie folgt aus der Definition von $\sqsubseteq$ und der Kommutativität von $+$:

$$b \overset{a \sqsubseteq b}{\equiv} a + b = b + a \overset{b \sqsubseteq a}{\equiv} a$$

Transitivität folgt aus der Definition von $\sqsubseteq$ und der Assoziativität von $+$:

$$c \overset{b \sqsubseteq c}{\equiv} c + b \overset{a \sqsubseteq b}{\equiv} c + (b + a) = (c + b) + a \overset{b \sqsubseteq c}{\equiv} c + a$$

Es gelte $a \sqsubseteq b$. Monotonie von $+$:

$$c + b \overset{a \sqsubseteq b}{\equiv} c + (b + a) = (c + a) + b \overset{\text{Def} \sqsubseteq}{\sqsupseteq} c + a$$

Entsprechend Monotonie von $\cdot$:

$$cb \overset{a \sqsubseteq b}{\equiv} c(b + a) = cb + ca \overset{\text{Def} \sqsubseteq}{\sqsupseteq} ca$$

Bleibt die Monotonie von *: mit Ax5 und der Monotonie von $\cdot$

$$b^* \sqsupseteq 1 + bb^* \sqsupseteq 1 + ab^*$$

womit sofort aus Ax6 $a^* \sqsubseteq b^*$ folgt (in Ax6 1 für b und b^* für x substituieren).

(ii) Wir zeigen zuerst den Speziallfall mit $b = 1$:
$1 + aa^* \sqsubseteq a^*$ ist Ax5. Bleibt $a^* \sqsubseteq 1 + aa^*$.
Nach Ax6 $b + ax \leq x \to a^* b \leq x$ mit 1 substituiert für b und $1 + aa^*$ substituiert für x reicht es zu zeigen, dass

$$1 + a(\underbrace{1 + aa^*}_{\sqsubseteq a^* (\text{Ax5})}) \sqsubseteq 1 + aa^*$$

was aber wegen Ax5 ($1 + aa^* \sqsubseteq a^*$) und der Monotonie von $\sqsubseteq$ gilt.
Symmetrisch folgt $1 + a^* a = a^*$.
Damit folgt auch sofort $b + a(a^* b) = (1 + aa^*)b = a^* b$ und symmetrisch $b + (ba^*)a = ba^*$.
Somit hat $b + aX \sqsubseteq X$ mit $X = a^* b$ mindestens eine Lösung, für – wie gerade gezeigt – die sogar Gleichheit gilt, nach Ax6 ist jede weitere Lösung größer als $a^* b$. Symmetrisch für $b + Xa \sqsubseteq X$ und $X = ba^*$.

(d) $1 \sqsubseteq Z$ führt auf $Z = 1$.
Damit ergibt sich $Y = d^*(cX + f)$ aus

$$cX + dY + fZ \sqsubseteq Y$$

Und damit $X = (a + bd^* c)^*(e + bd^* f)$ aus

$$aX + bY + eZ \sqsubseteq X$$

Damit schließlich $Y = d^* c(a + bd^* c)^*(e + bd^* f) + d^* f$.
Bemerkung: Man kann natürlich auch zuerst nach X und dann nach Y lösen, was auf

$$X = a^*(bY + e)$$

und damit auf

$$Y = (d + ca^* b)^*(f + ca^* e) \qquad X = a^* b(d + ca^* b)^*(f + ca^* e) + a^* e$$

führt.
Da die erhaltenen Terme jeweils die eindeutige kleinste Lösung beschreiben müssen, folgt z.B.

$$Y = (d + ca^* b)^*(f + ca^* e) = d^* c(a + bd^* c)^*(e + bd^* f) + d^* f$$

(e) Stellt man das LGS nach VL für den NFA auf, so erhält man genau das System aus (d) – mit der einzigen Aussnahme, dass statt der abstrakten Operationen die konkreten Operationen für Sprachen verwendet werden. Die Lösungsschritte aus (d) können somit auch im konkreten Fall angewendet werden. Insbesondere beschreiben die Terme aus (d) bzw. die entsprechenden regulären Ausdrücke gerade alle Pfade von X bzw. Y nach Z (siehe auch Folien).
Beispiel: aus

$$d^*c(a + bd^*c)^*(bd^*f + e) + d^*f$$

wird mit den Werten $a = \mathsf{a}, b = \mathsf{b}, c = \mathsf{c}, d = \mathsf{a}, e = f = \mathsf{d}$

$$L(\mathsf{a}^*\mathsf{c}(\mathsf{a} \mid \mathsf{ba}^*\mathsf{c})^*(\mathsf{ba}^*\mathsf{d} \mid \mathsf{d})|\mathsf{a}^*\mathsf{d})$$

(f) Von X nach Z geht man direkt: -2
Von Y nach Z geht man über X: $5 - 2 = 3$
Von Z nach Z: 0
Setzt man $a = 2$, $b = 3$, $c = 5$, $d = 1$, $e = -2$ und $f = 4$, so werten sich die Ausdrücke aus (d) mit min als Addition und + als Multiplikation gerade zu diesen Werten aus.
Beispiel: Aus

$$d^*c(a + bd^*c)^*(bd^*f + e) + d^*f$$

wird

$$\min(1^* + 5 + (\min(2, 3 + 1^* + 5))^* + \min(3 + 1^* + 4, -2), 1^* + 4) = \min(0 + 5 + 0 - 2, 0 + 4) = 3$$