Grundzüge der Theoretischen Informatik, WS 21/22: Musterlösung zum 3. Übungsblatt

Julian Dörfler

Aufgabe A3.1 (Nichtreguläre Sprachen) *(4 Punkte)*
Zeigen Sie mithilfe des Pumping Lemmas, dass folgende Sprachen nicht regulär sind:

(a) $A = \{1^{3n}0^{2n} \mid n \in \mathbb{N}\}$

(b) $B = \{xx^{\text{rev}} \mid x \in \{0,1\}^\star\}$
Hierbei definieren wir $x^{\text{rev}} := x_l x_{l-1} \cdots x_2 x_1$, wenn $x = x_1 x_2 \cdots x_{l-1} x_l$.

Lösung A3.1 (Nichtreguläre Sprachen)

(a) Wir verwenden das Pumping Lemma:

Sei $n \in \mathbb{N} \setminus \{0\}$ beliebig. Wähle $uvw = 1^{3n}0^{2n} \in A$ mit $u = \varepsilon, v = 1^{3n}$ und $w = 0^{2n}$. Sei nun $xyz = v$ mit $|y| = \ell \geq 1$. Wir wählen $i = 0$ und erhalten das Wort $uxy^0zw = 1^{3n-\ell}0^{2n} \notin A$, da wegen $\ell > 0$ das Wort $1^{3n-\ell}0^{2n}$ nicht mehr von der Form $1^{3m}0^{2m}$ ist.

A lässt sich also nicht pumpen und ist damit nicht regulär.

(b) Wir verwenden das Pumping Lemma:

Sei $n \in \mathbb{N} \setminus \{0\}$ beliebig. Wähle $uvw = 0^n 1 1 0^n \in B$ mit $u = 0^n 11$, $v = 0^n$ und $w = \varepsilon$. Sei nun $v = xyz$ mit $|y| = \ell > 0$ beliebig. Wir wählen $i = 0$. Dann ist $uxy^izw = 0^n110^{n-\ell} \notin B$, da $n - \ell \neq n$ und somit $(0^n1)^{\text{rev}} \neq 10^{n-\ell}$.

B lässt sich also nicht pumpen und ist damit nicht regulär.

Aufgabe A3.2 (Mehr nichtreguläre Sprachen) *(4 Punkte)*
Zeigen Sie, dass die Sprache

$$C = \{xy \mid x, y \in \{0,1\}^\star \text{ und } |x| = |y| \text{ und } x \neq y\}$$

nicht regulär ist.

Lösung A3.2 (Mehr nichtreguläre Sprachen) Wir verwenden die Abgeschlossenheit von REG unter Komplement und Schnitt. Es gilt

$$(\{0,1\}^\star \setminus C) \cap L(((0+1)(0+1))^\star) = \mathsf{COPY}$$

Angenommen C wäre regulär, dann wäre $\mathsf{COPY} = \{xx \mid x \in \{0,1\}^\star\}$ also auch regulär. Das dies nicht der Fall ist, zeigen wir mithilfe des Pumping Lemmas:

Sei $n \in \mathbb{N} \setminus \{0\}$ beliebig. Wähle $uvw = 10^n10^n \in \mathsf{COPY}$ mit $u = 1, v = 0^n$ und $w = 10^n$. Sei nun $xyz = v$ mit $|y| = \ell \geq 1$. Wir wählen $i = 0$ und erhalten das Wort $uxy^0zw = 10^{n-\ell}10^n \notin \mathsf{COPY}$, da wegen $\ell > 0$ das Wort $10^{n-\ell}10^n$ entweder eine ungerade Länge enthält, oder aber die erste Hälfte des Wortes zwei 1er enthält, aber die zweite Hälfte des Wortes keine 1er enthält.

COPY lässt sich also nicht pumpen und ist damit nicht regulär. Somit ist also auch C nicht regulär.

Aufgabe A3.3 (Nerode-Klassen) (4 Punkte)
Für $k \in \mathbb{N} \setminus \{0\}$ sei

$$L_k = \{xy \mid x \in \{0,1\}^\star, y \in \{0,1\}^k \text{ und } y \text{ enthält eine gerade Anzahl an 1en}\}$$

die Menge der Wörter, die mindestens k Zeichen lang sind und in den letzten k Zeichen eine gerade Anzahl an 1en haben.

(a) Wie viele Myhill-Nerode-Äquivalenzklassen besitzt L_k? Beweisen Sie Ihre Antwort.

(b) Konstruieren Sie für L_2 aus den Äquivalenzklassen einen minimalen deterministischen endlichen Automaten.

(c) Zeigen Sie, dass es einen NEA mit nur $2k$ Zuständen gibt, der L_k erkennt.

(d) *(2 Bonuspunkte)* Zeigen Sie, dass der Automat aus der vorhergehenden Teilaufgabe minimal ist, es also keinen NEA mit $2k-1$ Zuständen gibt, der L_k erkennt.

Lösung A3.3 (Nerode-Klassen)

(a) Wir behaupten die Menge $R = \{0,1\}^k \cup \bigcup_{i=0}^{k-2}\{0,1\}^i$ enthält genau einen Repräsentanten aus jeder Myhill-Nerode-Äquivalenzklasse von L_k. Die Menge R enthält keine Repräsentanten der Länge $k-1$, denn alle diese Wörter sind Myhill-Nerode-äquivalent zu einem Wort der Länge k mit einer ungeraden Anzahl 1er. *Alternativ können wir also auch $R' = \bigcup_{i=0}^{k-1}\{0,1\}^i \cup \{x \mid x \in \{0,1\}^k$ und Anzahl 1er in x ist gerade$\}$ wählen.*

Wir zeigen zuerst, dass diese paarweise verschieden sind. Sei hierzu $x \neq y$ mit $x, y \in R$. Wir betrachten zuerst den Fall, dass $|x| \neq |y|$. Sei o.B.d.A. $|x| > |y|$. Wir wählen $z \in \{0,1\}^\ell$ mit $\ell = \max(1, k - |x|)$ so, dass $xz \in L_k$. Solch ein z existiert immer, da $\ell \geq 1$ und $|xz| \geq k$. Nun ist aber $|yz| < k$, da $|y| \leq k-2$ nach Konstruktion von R, es gilt also $yz \notin L_k$ und somit $[x]_{\sim_{L_k}} \neq [y]_{\sim_{L_k}}$.

Sei nun alternativ $\ell := |x| = |y|$. Dann gibt es ein maximales $i \in \{1, \ldots, \ell\}$ mit $x_i \neq y_i$. O.B.d.A. sei $x_i = 1$ und $y_i = 0$. Wir unterscheiden nun zwei Fälle:

$x_ix_{i+1}\ldots x_\ell$ enthält eine gerade Anzahl 1en: Dann enthält $y_iy_{i+1}\ldots y_k = 0x_{i+1}\ldots x_\ell$ durch die Maximalität von i eine ungerade Anzahl 1en. Wir betrachten die letzten k Zeichen von $x0^{k-\ell+i-1}$, also $x_ix_{i+1}\ldots x_\ell 0^{k-\ell+i-1}$ und bemerken, dass

diese ebenfalls eine gerade Anzahl 1en besitzt. Gleichermassen enthalten die letzten k Zeichen von $y0^{i-1}$, also $y_i y_{i+1} \dots y_\ell 0^{k-\ell+i-1}$, eine ungerade Anzahl 1en. Es gilt also $x0^{k-\ell+i-1} \in L_k$ und $y0^{k-\ell+i-1} \notin L_k$.

$x_i x_{i+1} \dots x_k$ enthält eine ungerade Anzahl 1en: Dann enthält $y_i y_{i+1} \dots y_\ell = 0x_{i+1} \dots x_\ell$ durch die Maximalität von i eine gerade Anzahl 1en. Wir betrachten die letzten k Zeichen von $x0^{k-\ell+i-1}$, also $x_i x_{i+1} \dots x_\ell 0^{k-\ell+i-1}$ und bemerken, dass diese ebenfalls eine ungerade Anzahl 1en besitzt. Gleichermassen enthalten die letzten k Zeichen von $y0^{k-\ell+i-1}$, also $y_i y_{i+1} \dots y_\ell 0^{k-\ell+i-1}$, eine gerade Anzahl 1en. Es gilt also $x0^{k-\ell+i-1} \notin L_k$ und $y0^{k-\ell+i-1} \in L_k$.

Also ist in beiden Fällen $[x]_{\sim_{L_k}} \neq [y]_{\sim_{L_k}}$.

Da es $2^k + 2^{k-1} - 1$ unterschiedliche Strings in R gibt, muss $\sim_{L_k}$ mindestens $2^k + 2^{k-1} - 1$ Äquivalenzklassen haben.

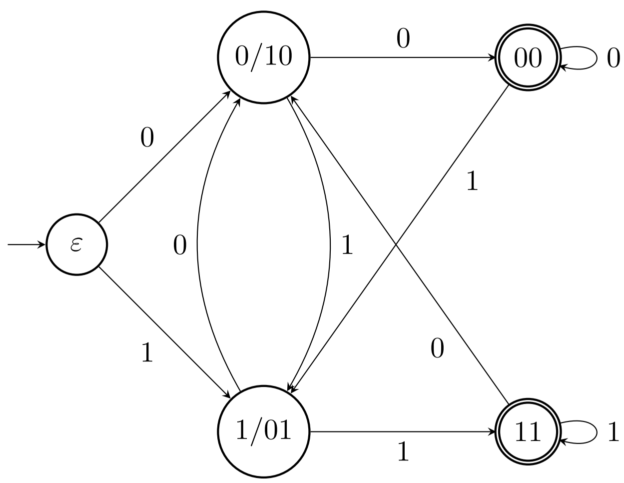
Es bleibt zu zeigen, dass $2^k + 2^{k-1} - 1$ Äquivalenzklassen genügen, es also für alle $x \in \{0,1\}^\star$ ein $z \in R$ gibt mit $x \sim_{L_k} z$, also $x \in [z]_{\sim_{L_k}}$.

$|x| = \ell > k$: Sei $x = yz$ mit $|z| = k$, dann ist $x \sim_{L_k} z$, da für beliebige $w \in \{0,1\}^\star$ der String xw die letzten k Zeichen identisch sind und somit xw genau dann in den letzten k Zeichen eine gerade Anzahl 1er hat, wenn zw in den letzten k Zeichen eine gerade Anzahl 1er hat. Weiterhin haben sowohl xw als auch zw Länge mindestens k.

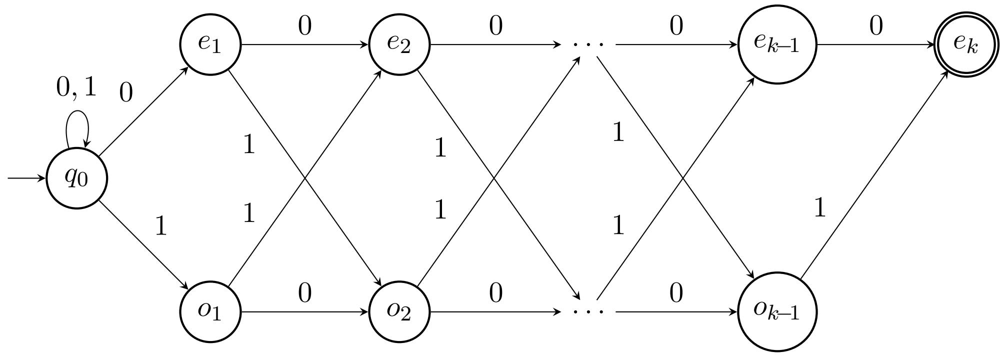
$|x| = \ell < k$: Falls $\ell \leq k-2$, dann ist $x \in R$, es ist also nichts weiteres zu zeigen. Es gilt also $\ell = k-1$.

Nun hat entweder $0x$ oder $1x$ eine ungerade Anzahl an 1en, wähle dieses Wort als z. Sei nun $w \in \Sigma^\star$ beliebig. Ist $w = \varepsilon$, so gilt $xw \notin L_k$ und $zw \notin L_k$. Ist $|w| \geq 1$, dann sind die letzten k Zeichen von xw und zw identisch, es gilt also $xw \in L_k$ genau dann, wenn $zw \in L_k$.

(b) Folgender deterministischer Automat erkennt L_2. Die Zustände sind benannt nach R, bzw bei Doppelbenennung zusätzlich auch nach den alternativen Repräsentanten.



(c) Folgender nichtdeterministischer Automat erkennt L_k indem die Parität der letzten k Zeichen mitberechnet wird und hat $2k$ Zustände.



(d) Es bleibt zu zeigen, dass $2k-1$ Zustände nicht ausreichend sind. Sei $N = (Q, \Sigma, \delta, q_0, Q_{\text{acc}})$ ein NEA ohne ε-Transitionen[1] mit $L(N) = L_k$.

Wir definieren für $u, v \in \Sigma^\star$ die Menge aller Zustände q, so dass eine akzeptierende Berechnung von uv auf N existiert, die nach Einlesen von u im Zustand q ist als $B_{u,uv}$. Formaler:

$$B_{u,uv} := \{q \in Q \mid q \in \delta^\star(q_0, u), \delta^\star(q, v) \cap Q_{\text{acc}} \neq \emptyset\}$$

Wir betrachten nun für $i \in \{1, 2, \dots, k-1\}$ die Wörter $x = 00^{i-1}$ und $y = 10^{i-1}$. Wir bemerken, dass $x0^{k-i} \in L_k$, sowie $y10^{k-i-1} \in L_k$. Daher sind $B_{x,x0^{k-i}}$ und $B_{y,y1^{k-i-1}}$ nicht leer. Weiterhin hat der kürzeste Pfad von Zuständen in $B_{x,x0^{k-i}} \cup B_{y,y1^{k-i-1}}$ zu Zuständen in Q_{acc} maximal Länge[2] $k - i$ da N keine ε-Transitionen hat. Nun ist aber $y0^{k-i} \notin L_k$, woraus wir schliessen $B_{x,x0^{k-i}} \cap B_{y,y1^{k-i-1}} = \emptyset$, da ansonsten für $q \in B_{x,x0^{k-i}} \cap B_{y,y1^{k-i-1}}$ gelten würde, dass $\delta^\star(q, 0^{k-i}) \in Q_{\text{acc}}$, ein Widerspruch zu $y1^{k-i-1} \notin L_k$.

Angenommen es gäbe einen Zustand $q \in B_{x,x0^{n-i}} \cup B_{y,y1^{n-i-1}}$, so dass der kürzeste Pfad von q zu einem Zustand aus Q_{acc} Länge kürzer als $n - i$ hat. Dann existiert ein z mit $|z| < k - i$, so dass $xz \in L_k$ oder $yz \in L_k$. Nun gilt entweder $|xz| < k$ oder $|yz| < k$, beides ein Widerspruch dazu, dass L_k nur Wörter enthält die mindestens Länge k haben. Somit hat der kürzeste Pfad zu Zuständen in Q_{acc} für alle solchen q genau Länge $ik - i$.

Setzen wir all dies zusammen bemerken wir also, dass es jeweils mindestens 2 unterschiedlich Zustände im Abstand $k - i$ von akzeptierenden Zuständen geben muss für alle $i \in \{1, 2, \dots, k-1\}$, also $2 \cdot (k-1)$ viele. Mit einem sehr ähnlichen Argument durch Wahl von $x = \varepsilon$ sehen wir, dass es weiterhin mindestens einen Zustand mit minimalem Abstand mindestens k geben muss, sowie durch Wahl von $x = 0^k$ einen Zustand mit minimalem Abstand 0, also einen akzeptierenden Zustand. Insgesamt muss es also mindestens $2k$ Zustände in N geben.

[1] Unser Verfahren zum Entfernen von ε-Transitionen verändert die Zuständsmenge, also insbesondere die Anzahl der Zustände nicht, dies ist also keine Einschränkung

[2] Zur Erinnerung: Die Länge eines Pfades ist die Anzahl Kanten entlang des Pfades

Aufgabe A3.4 (Transduktoren) *(4 Punkte)*
Wir hatten in Aufgabe A2.3 schon Transduktoren konstruiert. Nun zeigen wir, dass REG unter Transduktorberechnungen abgeschlossen ist. Sei dafür $M = (Q, \Sigma, \Gamma, \delta, f, q_0, Q_{\text{acc}})$ ein Transduktor. Wie gewohnt definieren wir

$$f_M(L) := \{f_M(x) \mid x \in L\}$$

und

$$f_M^{-1}(L) := \{x \in \Sigma^\star \mid f_M(x) \in L\}\,.$$

(a) Zeigen Sie, dass wenn $L \subseteq \Sigma^\star$ regulär ist, $f_M(L)$ ebenfalls regulär ist.

(b) Zeigen Sie, dass wenn $L \subseteq \Gamma^\star$ regulär ist, $f_M^{-1}(L)$ ebenfalls regulär ist.

(c) Zeigen Sie, dass Transduktoren eine Verallgemeinerung der Homomorphismen sind. Zeigen Sie dazu, dass wenn $h : \Sigma^\star \to \Gamma^\star$ ein Homomorphismus ist, dass es dann einen Transduktor M gibt mit $f_M = h$.

(d) Gibt es Transduktoren M, die eine Funktion f_M berechnen, die kein Homomorphismus $h : \Sigma^\star \to \Gamma^\star$ ist? Beweisen Sie Ihre Antwort.

Lösung A3.4 (Transduktoren)

(a) Sei $M_L = (Q_L, \Sigma, \delta_L, q_{0,L}, Q_{acc,L})$ ein DEA mit $L(M_L) = L$. Wir konstruieren nun einen NEA M' indem wir Q Kopien von M_L ähnlich zu einem Produktautomaten erzeugen. Darin fügen wir in der Kopie, die zu $q \in Q$ gehört für jeden Übergang $\delta_L(q_L, a) = q'_L$ einen Pfad ein, der $f(q, a)$ erkennt und in der Kopie endet, die zu $\delta(q, a)$ gehört.

Formal konstruieren wir einen NEA $M' = (Q', \Gamma, \delta', q'_0, Q'_{\text{acc}})$ mit

$$\begin{aligned} Q' &= Q \times Q_L \cup \{(q, q_L)_{f(q,a)_i} \mid q \in Q, q_L \in Q_L, a \in \Sigma, 1 \le i < |f(q, a)|\} \\ q'_0 &= (q_0, q_{0,L}) \\ Q'_{\text{acc}} &= \{(q, q_L) \mid q \in Q_{\text{acc}}, q_L \in Q_{acc,L}\} \end{aligned}$$

und

$$\begin{aligned} \delta' = &\{((q, q_L), f(q, a)_1, (q, q_L)_{f(q,a)_1}) \mid (q, a, q') \in \delta, (q_L, a, q'_L) \in \delta_L, |f(q, a)| > 1\} \\ &\cup \{((q, q_L)_{f(q,a)_{|f(q,a)|-1}}, f(q, a)_{|f(q,a)|}, (q', q'_L) \mid (q, a, q') \in \delta, (q_L, a, q'_L) \in \delta_L, |f(q, a)| > 1\} \\ &\cup \{((q, q_L), f(q, a), (q', q'_L)) \mid (q, a, q') \in \delta, (q_L, a, q'_L) \in \delta_L, |f(q, a)| \le 1\} \\ &\cup \{((q, q_L)_{f(q,a)_i}, f(q, a)_{i+1}, (q, q_L)_{f(q,a)_{i+1}}) \mid q \in Q, q_L \in Q_L, a \in \Sigma, 1 \le i \le |f(q, a)| - 2\}. \end{aligned}$$

wobei wir hier die Transitionsfunktionen in Relationenschreibweise verwenden, also $(q, a, q') \in \delta \Leftrightarrow q' \in \delta(q, a)$.

Nun erkennt M' die Sprache $L(M') = f_M(L)$.

$\supseteq$: Sei $x \in f_M(L)$. Dann existiert ein $y \in L$ mit $f_M(y) = x$ und somit eine Folge von Zuständen $q_{0,L}, q_{1,L}, \ldots, q_{|y|,L} \in Q_L$, wobei $\delta_L(q_{i-1,L}, y_i) = q_{i,L}$ und $q_{|y|,L} \in Q_{acc,L}$.

Ebenso gibt es eine Folge von Zuständen $q_0, q_1, \ldots, q_{|y|} \in Q$ mit $\delta(q_{i-1}, y_i) = q_i$ und $q_{|y|} \in Q_{\text{acc}}$.

Nun hat die Folge von Zuständen $(q_0, q_{0,L}), (q_1, q_{1,L}), \ldots, (q_{|y|}, q_{|y|,L}) \in Q'$ die Eigenschaft $(q_i, q_{i,L}) \in \delta'^{\star}((q_{i-1}, q_{i-1,L}), f(q_{i-1}, y_i))$ für alle i und $(q_{|y|}, q_{|y|,L}) \in Q'_{\text{acc}}$. Diese wird durchlaufen bei der Berechnung des Wortes

$$f(q_0, y_1) f(q_1, y_2) \cdots f(q_{|y|-1}, y_{|y|}) = f_M(y) = x\,.$$

Somit akzeptiert M' das Wort x.

$\subseteq$: Sei $x \in L(M')$. Wir betrachten die Zustände in $(Q \times Q_L) \cap Q'$, die von M' bei der Berechnung von x durchlaufen werden.
Diese bilden eine Folge $(q_0, q_{0,L}), (q_1, q_{1,L}), \ldots, (q_\ell, q_{\ell,L}) \in Q'$ mit $(q_\ell, q_{\ell,L}) \in Q'_{\text{acc}}$. Nach Konstruktion erkennen die einzigen Pfade von $(q_{i-1}, q_{i-1,L})$ nach $(q_i, q_{i,L})$ Worte der Form $f(q_{i-1}, a_i)$ für Zeichen $a_i \in \Sigma$ mit $\delta_L(q_{i-1,L}, a_i) = q_{i,L}$ und $\delta(q_{i-1}, a_i) = q_i$. Damit ist aber $a = a_1 a_2 \cdots a_\ell \in L$ und

$$x = f(q_0, a_1) f(q_1, a_2) \cdots f(q_{\ell-1}, a_\ell) = f_M(a)\,.$$

Somit ist $x \in f_M(L)$.

(b) Sei $M_L = (Q_L, \Gamma, \delta_L, q_{0,L}, Q_{acc,L})$ ein DEA mit $L(M_L) = L$. Wir konstruieren einen DEA $M' = (Q', \Sigma, q'_0, \delta', Q'_{\text{acc}})$ mit

$$\begin{aligned} Q' &= Q \times Q_L \\ q'_0 &= (q_0, q_{0,L}) \\ Q'_{\text{acc}} &= \{(q, q_L) \mid q \in Q_{\text{acc}}, q_L \in Q_{acc,L}\} \end{aligned}$$

und

$$\delta'((q, q_L), a) = \begin{cases} (\delta(q,a), \delta_L^\star(q_L, f(q,a))) & \text{falls } \delta(q,a), f(q,a) \text{ und } \delta_L^\star(q_L, f(q,a))) \text{ definiert sind} \\ \text{undefiniert} & \text{sonst} \end{cases}$$

Damit ist

$$\begin{aligned} & x = x_1 \ldots x_\ell \in L(M') \\ & \quad \Leftrightarrow \exists q_1, q_2, \ldots, q_\ell \in Q : (\forall i \in \{1, 2, \ldots, \ell\} : \delta(q_{i-1}, x_i) = q_i) \\ & \qquad \wedge q_\ell \in Q_{\text{acc}} \\ & \qquad \wedge \delta_L^\star(\delta_L^\star(\ldots \delta_L^\star(\delta_L^\star(q_{0,L}, f(q_0, x_1)), f(q_1, x_2)) \ldots, f(q_{\ell-2}, x_{\ell-1})), f(q_{\ell-1}, x_\ell)) \in Q_{acc,L} \\ & \quad \Leftrightarrow f_M(x) \in L. \end{aligned}$$

(c) Sei $h : \Sigma^\star \to \Gamma^\star$ ein Homomorphismus.

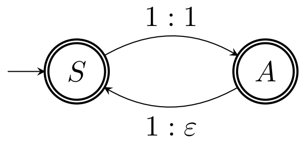
Nun konstruieren wir den Transduktor $M = (\{q_0\}, \Sigma, \Gamma, \delta, f, q_0, \{q_0\})$, wobei $\delta(q_0, a) = q_0$ für alle Zeichen $a \in \Sigma$ und $f(q_0, a) = h(a)$.

Wir behaupten nun $f^\star(q_0, x) = h(x)$ für alle $x \in \Sigma^\star$ und beweisen dies per Induktion über $|x|$. Für $|x| = 0$ gilt $f^\star(q_0, \varepsilon) = \varepsilon = h(\varepsilon)$. Gelte nun also $f^\star(q_0, y) = h(y)$ für alle $y \in \Sigma^\star$ mit Länge $|y| < |x|$. Dann gilt für $x = ay$

$$f^\star(q_0, ay) = f(q_0, a) f^\star(q_0, y) = h(a)h(y) = h(ay)$$

Schließlich gilt $f_M(x) = f^\star(q_0, x) = h(x)$ für alle $x \in \Sigma^\star$.

(d) Betrachten wir den Automaten M mit $\Sigma = \Gamma = \{1\}$ gegeben durch



Dann gilt $f_M(11) = 1 \neq 11 = f_M(1) f_M(1)$. Somit ist f_M kein Homomorphismus.

Weiterführende Hinweise[3]: Diese Konstruktionen würde ebenfalls funktionieren für eine nicht-deterministische Variante der endlichen Transduktoren.

Formal ist dann:

$$M = (Q, \Sigma, \Gamma, \Delta, q_0, Q_{\text{acc}})$$

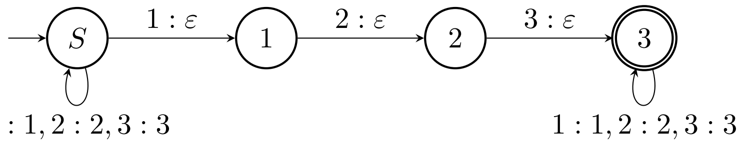
wobei $Q, \Sigma, \Gamma, q_0, Q_{\text{acc}}$ wie gewohnt zu interpretieren sind. Es gibt nun eine kombinierte Transitions-und Ausgaberelation $\Delta \subseteq Q \times \Sigma_\varepsilon \times \Gamma^\star \times Q$, wobei Δ endlich ist.

$q_0, q_1, \ldots, q_m$ ist nun analog zu NEAs eine Berechnung von M auf x mit Ausgabe y, wenn $x = u_1, u_2, \ldots u_m$ mit $u_\mu \in \Sigma_\varepsilon$ und $y = v_1, v_2, \ldots, v_m$ mit $v_\mu \in \Gamma^\star$ existieren und für alle $0 \le \mu < m$ gilt $(q_\mu, u_{\mu+1}, v_{\mu+1}, q_{\mu+1}) \in \Delta$. Eine Berechnung heißt akzeptierend, wenn $q_m \in Q_{\text{acc}}$, ansonsten heißt diese verwerfend.

Nun berechnet M die Funktion $f_M : \Sigma^\star \to \mathcal{P}(\Gamma^\star)$ definiert durch

$f_M(x) = \{y \in \Gamma^\star \mid \text{Es gibt eine akzeptierende Berechnung von } M \text{ auf } x \text{ mit Ausgabe } y\}$

Zum Beispiel ist der folgende Automat ein nicht-deterministischer Transduktor mit $\Sigma = \Gamma = \{1, 2, 3\}$, der nur Wörter akzeptiert, die 123 enthalten und dabei eines dieser Vorkommen entfernt.



[3] Sie dürfen die Aussagen dieser Aufgabe für diese Variation für kommende Übungsblätter und Klausuren als bewiesen annehmen und dann dort ohne Beweis verwenden.

Aufgabe A3.5 (Teilwortsuche) *(4 Bonuspunkte)*
Wir betrachten in dieser Aufgabe das Teilwortproblem: Für $x \in \Sigma^\star$ definieren wir die Sprache

$$L_x = \{y \in \Sigma^\star \mid \exists u, w \in \Sigma^\star : y = uxw\}\,.$$

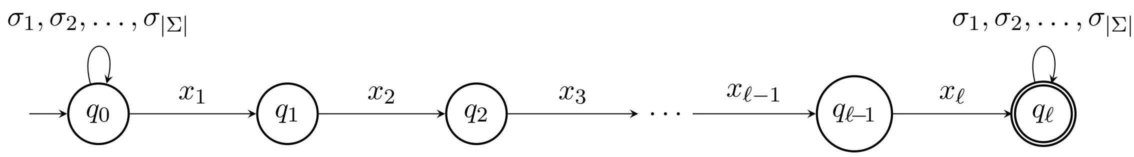
als die Sprache aller Wörter y, die das Teilwort x enthalten.

(a) Zeigen Sie, dass L_x für alle $x \in \Sigma^\star$ von einem NEA N mit $|x|+1$ Zuständen erkannt wird. Verwenden Sie hierzu nicht den DEA aus Teilaufgabe (b).

(b) Zeigen Sie, dass L_x für alle $x \in \Sigma^\star$ ebenfalls von einem DEA M mit $|x|+1$ Zuständen erkannt wird. *Hinweis: M sollte für jedes Präfix von x genau einen Zustand haben. Weiterhin könnte eine Funktion $P(y, x)$ die das längste Suffix von y beschreibt, das ebenfalls ein Präfix von x ist, hilfreich sein.*

Lösung A3.5 (Teilwortsuche)

(a) Sei $x \in \Sigma^\star$ beliebig und $\Sigma = \{\sigma_1, \dots, \sigma_{|\Sigma|}\}$. Wenn x Länge ℓ hat, dann können wir folgenden NEA $N = (Q, \Sigma, \delta, q_0, \{q_\ell\})$ mit $\ell + 1$ Zuständen konstruieren, der L_x erkennt:



Sei $y \in L_x$, dann gibt es $u, w \in \Sigma^\star$ mit $y = uxw$. Nun gilt aber $q_0 \in \delta^\star(q_0, u)$, $q_\ell \in \delta^\star(q_0, x)$, $q_\ell \in\in \delta^\star(q_\ell, w)$ und $q_\ell \in Q_{\text{acc}}$, also insgesamt $\delta^\star(q_0, uxw) \cap Q_{\text{acc}} \neq \emptyset$. Es gilt also $y \in L(N)$.

Sei nun $y \in L(N)$. Dann gibt es eine akzeptierende Berechnung $s_0, \dots, s_n$ mit $s_0 = q_0$ und $s_n = q_\ell$. Sei nun i maximal, so dass $s_i = q_0$ und j minimal, so dass $s_j = q_\ell$. Nun gibt es eine Aufteilung $y = uvw$, so dass $s_i \in \delta^\star(s_0, u)$, $s_j \in \delta^\star(s_i, v)$ und $s_n \in \delta^\star(s_i, w)$. Durch die Wahl von i und j gilt nun aber nach Konstruktion $v = x$, es gilt also $y \in L_x$.

(b) Der hier konstruierte DEA unterliegt dem Knuth-Morris-Pratt-Algorithmus zum Suchen von Teilwörtern.

Wir konstruieren den DEA $M = (Q, \Sigma, \delta, q_0, Q_{\text{acc}})$ wie folgt:

$$\begin{aligned}
Q &= \{q_u \mid u \in \Sigma^\star \text{ und } \exists v \in \Sigma^\star uv = x\} \\
q_0 &= q_\varepsilon \\
Q_{\text{acc}} &= \{q_x\} \\
\delta(q_u, \sigma) &= q_{P(u\sigma, x)} && \text{für } q_u \in Q \setminus \{q_x\}, \sigma \in \Sigma \\
\delta(q_x, \sigma) &= q_x && \text{für } \sigma \in \Sigma
\end{aligned}$$

Hierbei ist $P(y,x)$ das längste Suffix von y, das ebenfalls ein Präfix von x ist, also das längste $v \in \Sigma^\star$, so dass $u, w \in \Sigma^\star$ existieren, mit $uv = y$ und $vw = x$. Da $P(y,x)$ immer ein Präfix von x ist, ist $q_{P(u\sigma,x)}$ insbesondere wohldefiniert.

Wir behaupten nun, dass

$$\delta^\star(q_0, y) = \begin{cases} q_x & \text{falls } x \text{ ein Teilwort von } y \text{ ist} \\ q_{P(y,x)} & \text{sonst} \end{cases}$$

Beweis per Induktion:
Für $y = \varepsilon$ gilt die Behauptung direkt.
Gelte die Behauptung nun für ein beliebiges $y \in \Sigma^\star$ und sei $\sigma \in \Sigma$. Falls $y\sigma$ das Teilwort x nicht enthält, kann auch y das Teilwort x nicht enthalten haben, es gilt also $\delta^\star(q_0, y) = q_{P(y,x)}$. Daraus folgt

$$\delta^\star(q_0, y\sigma) = \delta(\delta^\star(q_0, y), \sigma) = \delta(q_{P(y,x)}, \sigma) = q_{P(P(y,x)\sigma,x)} \, .$$

Bleibt zu zeigen $P(P(y,x)\sigma, x) = P(y\sigma, x)$.

Wir bemerken zuerst, dass jedes Suffix von y, das ein Präfix von x ist, ebenfalls ein Suffix von $P(y,x)$ ist durch die Maximalitätsbedingung in der Definition von P. Weiterhin ist, wenn v ein Suffix von y ist, $v\sigma$ ein Suffix von $y\sigma$. Bleibt also nur zu zeigen, dass das längste Suffix v von $y\sigma$, das auch ein Präfix von x ist, ebenfalls ein Suffix von $P(y,x)\sigma$ ist. Falls $v = \varepsilon$, gilt dies direkt. Ansonsten gilt $v = v'\sigma$, da das letzte Zeichen von $y\sigma$ ein σ ist. Nun ist aber v' ein Suffix von y und ein Präfix von x, v' ist also ein Suffix von $P(y,x)$ und somit ist v ein Suffix von $P(y,x)\sigma$.

Falls aber $y\sigma$ das Teilwort x enthält, so gibt es zwei Möglichkeiten:

y enthält schon das Teilwort x: Nun gilt

$$\delta^\star(q_0, y\sigma) = \delta(\delta^\star(q_0, y), \sigma) = \delta(q_x, \sigma) = q_x$$

y enthält das Teilwort x nicht.: Dann muss $y\sigma$ das Teilwort x als Suffix enthalten. Wir bemerken $P(y\sigma, x) = x$, die Behauptung folgt also mit gleicher Begründung wie im Fall, dass $y\sigma$ das Teilwort x nicht enthält.

Wir verwenden nun die Behauptung um $L_x = L(M)$ zu beweisen:
Sei $y \in L_x$, dann enthält y das Teilwort x und $\delta^\star(q_0, y) = q_x \in Q_{\text{acc}}$ und $y \in L(M)$. Sei umgekehrt $y \notin L_x$, dann enthält y das Teilwort x nicht, es gilt also $\delta^\star(q_0, y) = P(y,x) \neq q_x$, da y insbesondere x nicht als Suffix enthält. Somit verwirft M und es gilt $y \notin L(M)$.