TI 1 - Ergänzung 7

A1

1. $\text{push}_b(L) = \{b, ab, aab, abb, abab\}$

   $\text{pop}_a(L) = \{\varepsilon, a, ab\}$

2. Es gilt: $\text{push}_a(\text{pop}_a(L)) \overset{(1)}{\subseteq} L \overset{(2)}{=} \text{pop}_a(\text{push}_a(L))$.

   Beweis von (1):

   Sei $x \in \Sigma^*$ beliebig. Dann gilt:

   $$x \in \text{push}_a(\text{pop}_a(L)) \;\boxed{\Rightarrow}\; x = wa \text{ mit } w \in \text{pop}_a(L)$$
   $$\boxed{\Rightarrow}\; x = wa \text{ mit } wa \in L$$
   $$\boxed{\Rightarrow}\; x \in L. \qquad \square$$

   auch „$\Leftrightarrow$" möglich

   nur Implikation, keine Äquivalenz!

   Die Inklusion $\text{push}_a(\text{pop}_a(L)) \supseteq L$ ist im Allgemeinen falsch.
   Gegenbeispiel: $L = \{b\}$, denn:

   $$\text{push}_a(\underbrace{\text{pop}_a(\{b\})}_{=\emptyset}) = \text{push}_a(\emptyset) = \emptyset \not\supseteq \{b\}.$$

   Beweis von (2):

   Sei $x \in \Sigma^*$ beliebig. Dann gilt:

   $$x \in \text{pop}_a(\text{push}_a(L)) \Leftrightarrow xa \in \text{push}_a(L)$$
   $$\Leftrightarrow x \in L. \qquad \square$$

3.

(a) Angenommen, L ist regulär.

$\xRightarrow{\text{S.v. Kleene}}$ Es gibt einen regulären Ausdruck γ mit $L(\gamma) = L$.

$\Longrightarrow$ $\gamma' = \gamma a$ ist ein regulärer Ausdruck mit:

$$L(\gamma') = L(\gamma)L(a) = L\{a\} = push_a(L).$$

$\xRightarrow{\text{S.v. Kleene}}$ $push_a(L)$ ist regulär. $\square$

(b) Angenommen, L ist regulär.

$\xRightarrow{\text{F.11.1}}$ Es gibt einen DEA $M = (Z, \Sigma, \delta, z_0, E)$ mit $T(M) = L$.

$\Longrightarrow$ $M' = (Z, \Sigma, \delta, z_0, E')$ mit

$$E' = \{z \in Z \mid \delta(z,a) \in E\}$$

ist ein DEA mit:

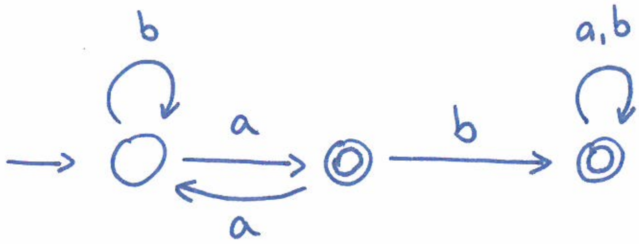
$$\begin{aligned} T(M') &= \{w \in \Sigma^* \mid \hat{\delta}(z_0, w) \in E'\} \\ &= \{w \in \Sigma^* \mid \delta(\hat{\delta}(z_0, w), a) \in E\} \\ &= \{w \in \Sigma^* \mid \hat{\delta}(z_0, wa) \in E\} \\ &= \{w \in \Sigma^* \mid wa \in \underbrace{T(M)}_{=L}\} \\ &= pop_a(L). \end{aligned}$$

$\xRightarrow{\text{F.11.1}}$ $pop_a(L)$ ist regulär. $\square$

hoffentlich!

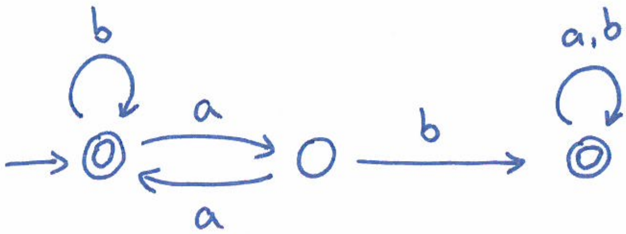
Verständnis förderndes Beispiel

M:



$\wr$

M':



Alternativer Beweis für (b)

Wir zeigen zuerst, dass R_L eine Verfeinerung von $R_{pop_a(L)}$ ist:

Seien $x, y \in \Sigma^*$ beliebig mit $x R_L y$, d.h.:

$$\underbrace{\forall w \in \Sigma^*: (xw \in L \iff yw \in L)}_{(*)}.$$

Z.z.: $x R_{pop_a(L)} y$, d.h.:

$$\forall w' \in \Sigma^*: (xw' \in pop_a(L) \iff yw' \in pop_a(L)).$$

Sei $w' \in \Sigma^*$ beliebig. Dann gilt:

$$\begin{aligned} xw' \in pop_a(L) &\iff xw'a \in L \\ &\overset{(*)}{\iff} yw'a \in L \\ &\iff yw' \in pop_a(L). \end{aligned}$$ $\square$

Die Aussage gilt für alle $w \in \Sigma^*$, also auch für $w = w'a$

Dann argumentieren wir mit dem Satz von Myhill und Nerode:

Angenommen, L ist regulär.

$\overset{\text{S.v. M\&N}}{\Longrightarrow} \quad |\Sigma^*/R_L| < \infty$

da R_L Verfeinerung von $R_{pop_a(L)}$

$\Longrightarrow \quad |\Sigma^*/R_{pop_a(L)}| \leq |\Sigma^*/R_L| < \infty$

$\overset{\text{S.v. M\&N}}{\Longrightarrow} \quad pop_a(L)$ ist regulär. $\square$

<u>Bemerkung</u>:

Bei dieser Teilaufgabe wurden folgende Charakterisierungen von regulären Sprachen verwendet:

(1) L regulär $\Leftrightarrow$ $\exists$ DEA M mit $T(M) = L$ (Folie 11.1)

(2) L regulär $\Leftrightarrow$ $\exists$ RA γ mit $L(\gamma) = L$ (Satz von Kleene)

(3) L regulär $\Leftrightarrow$ $|\Sigma^*/R_L| < \infty$ (Satz von Myhill und Nerode)

Obwohl die Definitionen von $push_a(L)$ und $pop_a(L)$ so ähnlich sind, sind die Lösungsansätze völlig unterschiedlich.

Aussage (a) konnte zwar sehr leicht mithilfe von (2) bewiesen werden, aber mit (1) oder (3) wäre es viel schwieriger gewesen. Beispielsweise ist R_L im Allgemeinen keine Verfeinerung von $R_{push_a(L)}$ (wähle z.B. $L = \{\varepsilon\}$).

Entsprechend konnte Aussage (b) sehr elegant mit (1) und (3), aber nicht mit (2) bewiesen werden.

A2

Wie sehen die Äquivalenzklassen von R_L aus?

$$[\varepsilon]_{R_L} = \{\varepsilon, ab, ba, aabb, abab, \ldots\} = \{w \in \Sigma^* \mid |w|_a = |w|_b\}$$

$$[a]_{R_L} = \{a, aab, aba, baa, \ldots\} = \{w \in \Sigma^* \mid |w|_a = |w|_b + 1\}$$

$$[aa]_{R_L} = \{aa, aaab, aaba, abaa, baaa, \ldots\} = \{w \in \Sigma^* \mid |w|_a = |w|_b + 2\}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$[b]_{R_L} = \{b, abb, bab, bba, \ldots\} = \{w \in \Sigma^* \mid |w|_a = |w|_b - 1\}$$

$$[bb]_{R_L} = \{bb, abbb, babb, bbab, bbba, \ldots\} = \{w \in \Sigma^* \mid |w|_a = |w|_b - 2\}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\Longrightarrow \Sigma^*/R_L = \{[x^k]_{R_L} \mid x \in \Sigma \wedge k \in \mathbb{N}\}.$$

Um zu zeigen, dass der Index $|\Sigma^*/R_L|$ tatsächlich unendlich ist, geben wir eine Folge von Äquivalenzklassen an und zeigen, dass sie paarweise unterschiedlich sind.

Jetzt kommt die eigentliche Lösung zur Aufgabe.

<u>Beweis</u>:

Betrachte die Folge von Äquivalenzklassen

$$S = \left([\varepsilon]_{R_L}, [a]_{R_L}, [aa]_{R_L}, [aaa]_{R_L}, \ldots \right) = \left([a^k] \right)_{k \in \mathbb{N}}.$$

Dann gilt für beliebige $k_1, k_2 \in \mathbb{N}$:

$$k_1 \neq k_2 \implies a^{k_1} \not R_L \, a^{k_2}, \text{ da } a^{k_1} b^{k_1} \in L, \text{ aber } a^{k_2} b^{k_1} \notin L$$

$$\implies [a^{k_1}]_{R_L} \neq [a^{k_2}].$$

Somit gibt es unendlich viele Äquivalenzklassen, also $|\Sigma^* / R_L| = \infty$, und L ist nicht regulär.

$\boxed{A3}$ $L = L(a^*b^*)$

1. <u>Quotientenmenge</u>: $\Sigma^*/_{\equiv_L} = \{[\varepsilon]_{\equiv_L}, [a]_{\equiv_L}, [b]_{\equiv_L}, [ab]_{\equiv_L}, [ba]_{\equiv_L}\}$

mit:

- $[\varepsilon]_{\equiv_L} = \{\varepsilon\}$,
- $[a]_{\equiv_L} = \{a, aa, aaa, \dots\} = \{a^k \mid k \geq 1\}$,
- $[b]_{\equiv_L} = \{b, bb, bbb, \dots\} = \{b^k \mid k \geq 1\}$,
- $[ab]_{\equiv_L} = \{ab, aab, abb, \dots\} = \{a^k b^\ell \mid k, \ell \geq 1\}$,
- $[ba]_{\equiv_L} = \{ba, aba, baa, bab, \dots\} = \{ubav \mid u,v \in \Sigma^*\}$.

<u>Index</u>: $|\Sigma^*/_{\equiv_L}| = 5$.

2.

$\cdot$	$[\varepsilon]$	$[a]$	$[b]$	$[ab]$	$[ba]$
$[\varepsilon]$	$[\varepsilon]$	$[a]$	$[b]$	$[ab]$	$[ba]$
$[a]$	$[a]$	$[a]$	$[ab]$	$[ab]$	$[ba]$
$[b]$	$[b]$	$[ba]$	$[b]$	$[ba]$	$[ba]$
$[ab]$	$[ab]$	$[ba]$	$[ab]$	$[ba]$	$[ba]$
$[ba]$	$[ba]$	$[ba]$	$\boxed{[ba]}$	$[ba]$	$[ba]$

Hier wurde vereinfacht $[w]$ statt $[w]_{\equiv_L}$ geschrieben.

<u>Bsp.</u>: $[ba]_{\equiv_L} \cdot [b]_{\equiv_L} = [bab]_{\equiv_L} = [ba]_{\equiv}$, da $bab \equiv_L ba$.

3. • $\varphi(\varepsilon) = [\varepsilon]_{\equiv_L}$, d.h. das neutrale Element von Σ^* wird auf das neutrale Element von $\Sigma^*/\equiv_L$.

• Für $x,y \in \Sigma^*$ gilt:

$$\varphi(xy) = [xy]_{\equiv_L} = [x]_{\equiv_L} \cdot [y]_{\equiv} = \varphi(x) \cdot \varphi(y).$$

da $\equiv_L$ eine Kongruenzrelation ist

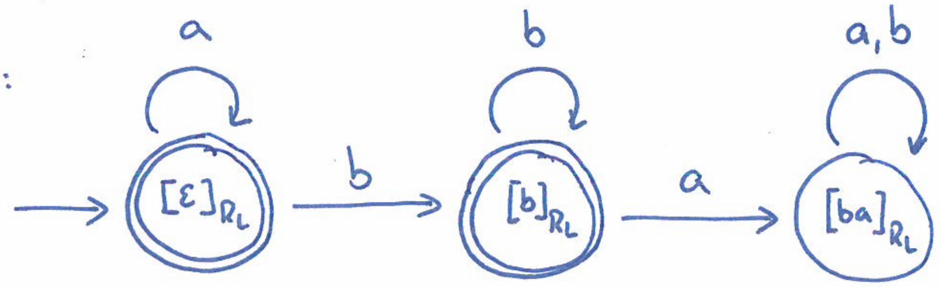
4. Für die Teilmenge $A = \{[\varepsilon]_{\equiv_L}, [a]_{\equiv_L}, [b]_{\equiv_L}, [ab]_{\equiv_L}\}$ von $\Sigma^*/\equiv_L$ gilt: $L = \varphi^{-1}(A)$.

5. Quotientenmenge: $\Sigma^*/R_L = \{[\varepsilon]_{R_L}, [b]_{R_L}, [ba]_{R_L}\}$ mit:

- $[\varepsilon]_{R_L} = \{\varepsilon, a, aa, aaa, \dots\} = \{a^k \mid k \geq 0\}$
- $[b]_{R_L} = \{b, ab, bb, aab, abb, \dots\} = \{a^k b^\ell \mid k \geq 0, \ell \geq 1\}$
- $[ba]_{R_L} = \{ba, aba, baa, bab, \dots\} = \{ubav \mid u,v \in \Sigma^*\}$

Index: $|\Sigma^*/R_L| = 3$.

6. M:



Bemerkung

Aus der Vorlesung wissen wir, dass $\equiv_L$ eine Verfeinerung von R_L ist, d.h.:

$$\forall x,y \in \Sigma^*: \left(x \equiv_L y \Rightarrow x R_L y \right)$$

Ist $\sim_1$ eine Verfeinerung von $\sim_2$, dann ist jede Äquivalenzklasse von $\sim_1$ vollständig in einer der Äquivalenzklassen von $\sim_2$ enthalten und der Index von $\sim_1$ ist mindestens so groß wie der von $\sim_2$.

Tatsächlich gilt für die Sprache L aus dieser Aufgabe:

- $[\varepsilon]_{R_L} = [\varepsilon]_{\equiv_L} \cup [a]_{\equiv_L}$,
- $[b]_{R_L} = [b]_{\equiv_L} \cup [ab]_{\equiv_L}$,
- $[ba]_{R_L} = [ba]_{\equiv_L}$

und $|\Sigma^*/R_L| = 3 \leq 5 = |\Sigma^*/\equiv_L|$ (s. Teilaufgaben 1. und 5.).

$\boxed{A4}$

1. Äquivalenz- und Kongruenzrelation.

Es gilt: $x \sim y \iff y-x$ ist ein Vielfaches von 3

$\iff \exists k \in \mathbb{Z}: \; y-x = 3k$

$\iff \exists k \in \mathbb{Z}: \; y = x + 3k$

$\iff x \equiv y \mod 3$

Rest: siehe Ergänzung 6, Aufgaben 3.3 und 6.5.

2. Weder Äquivalenz- noch Kongruenzrelation.

$\sim$ ist zwar reflexiv und symmetrisch, aber nicht transitiv.

Gegenbeispiel: Es gilt $0 \sim 2$ und $2 \sim 4$, aber $0 \nsim 4$.

Somit ist $\sim$ keine Äquivalenzrelation und folglich auch keine Kongruenzrelation.

3. Äquivalenzrelation, aber keine Kongruenzrelation.

Reflexivität: Wähle $m, n \in \mathbb{N} \setminus \{0\}$ beliebig, aber gleich. Dann gilt $x^m = x^n$. $\square$

Symmetrie: Seien $x, y, \in \mathbb{Z}$ mit $x \sim y$.

$\implies$ Es gibt $m, n \in \mathbb{N} \setminus \{0\}$ mit $x^m = y^n$.

Wähle $m' = n$ und $n' = m$.

$\Longrightarrow$ Es gibt $m', n' \in \mathbb{N} \setminus \{0\}$ mit $x^{m'} = y^{n'}$.

$\Longrightarrow$ $y \sim x$. $\square$

<u>Transitivität</u>: Seien $x, y, z \in \mathbb{Z}$ mit $x \sim y$ und $y \sim z$.

$\Longrightarrow$ Es gibt $m, n, m', n' \in \mathbb{N} \setminus \{0\}$ mit $\underbrace{x^m = y^n \text{ und } y^{m'} = z^{n'}}$.

$\Longleftrightarrow x^{mm'} = y^{nm'}$ und

$y^{nm'} = z^{nn'}$

Wähle $m'' = mm'$ und $n'' = nn'$.

$\Longrightarrow$ $x^{m''} = x^{mm'} = y^{nm'} = z^{nn'} = z^{n''}$.

$\Longrightarrow$ $x \sim z$. $\square$

$\sim$ ist jedoch keine Kongruenzrelation auf $(\mathbb{Z}, \cdot)$:

- $[0]_\sim = \{0\}$
- $[1]_\sim = \{-1, 1\}$
- $[2]_\sim = \{-2, 2, -4, 4, -8, 8, \ldots\}$
- $[3]_\sim = \{-3, 3, -9, 9, -27, 27, \ldots\}$
- $[5]_\sim = \{-5, 5, -25, 25, -125, 125, \ldots\}$

$\vdots$

<u>Gegenbeispiel</u>: Es gilt $2 \sim 2$ und $3 \sim 9$, aber

$2 \cdot 3 = 6 \not\sim 18 = 2 \cdot 9$.

$\boxed{A5}$

Dass $\equiv_L$ eine Äquivalenzrelation ist, ist leicht zu zeigen. Bitte selber ausprobieren!

<u>Beweis, dass $\equiv_L$ eine Kongruenzrelation ist</u>:

Seien $x, x', y, y' \in \Sigma^*$ mit $x \equiv_L x'$ und $y \equiv_L y'$.

$\Longrightarrow$ Für alle $u, v \in \Sigma^*$ gilt $\underbrace{uxv \in L \Leftrightarrow ux'v \in L}_{(1)}$ und $\underbrace{uyv \in L \Leftrightarrow uy'v \in L}_{(2)}$.

Zu zeigen ist: $xy \equiv_L x'y'$.

Seien $u', v' \in \Sigma^*$ beliebig. Dann gilt:

$$u'xyv' \in L \underset{(1)}{\Leftrightarrow} u'x'yv' \in L \underset{(2)}{\Leftrightarrow} u'x'y'v' \in L. \qquad \square$$

mit $v = yv'$, $u = u'$ mit $u = u'x'$, $v = v'$

Für $\mathrm{Synt}(L) = (\Sigma^*/\equiv_L, \cdot)$ heißt das, dass die Operation

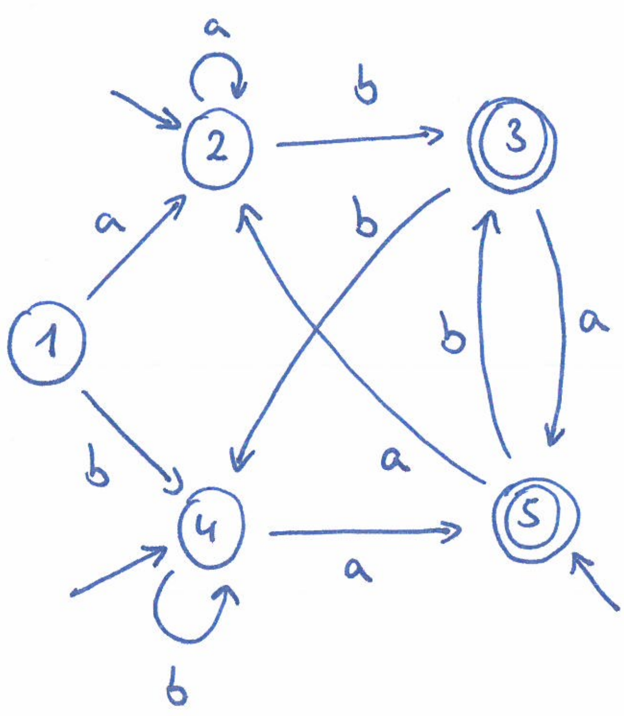
$$[x]_{\equiv_L} \cdot [y]_{\equiv_L} = [xy]_{\equiv_L}$$

auf Äquivalenzklassen wohldefiniert und somit tatsächlich eine Operation ist.

$\boxed{A6}$

1. $A^{-1}B = \{\underbrace{a, bb}_{u=aa}, \underbrace{\varepsilon, a, ba}_{u=ab}, \underbrace{a}_{u=abb}\} = \{\varepsilon, a, ba, bb\}$.

2.



3. Sei $M = (Z, \Sigma, \delta, z_0, E)$ ein DEA für B.

Definiere den NEA $M' = (Z, \Sigma, \delta', S, E)$ mit:

- $\delta'(z,a) = \{\delta(z,a)\}$ für $z \in Z, a \in \Sigma$ und
- $S = \{\hat{\delta}(z_0, u) \mid u \in A\}$.

Dann gilt $T(M') = A^{-1}B$.

Beweis:

Sei $v \in \Sigma^*$ beliebig. Dann gilt:

$$
\begin{aligned}
v \in T(M') &\overset{\text{F.09.2}}{\iff} \hat{\delta}'(S,v) \cap E \neq \emptyset \\
&\overset{\substack{\text{analog zu}\\ \text{F.09.7}}}{\iff} \bigcup_{z \in S} \{\hat{\delta}(z,v)\} \cap E \neq \emptyset \\
&\iff \exists z \in S: \hat{\delta}(z,v) \in E \\
&\iff \exists u \in A: \hat{\delta}(\hat{\delta}(z_0,u),v) \in E \\
&\overset{\text{F.07.7}}{\iff} \exists u \in A: \hat{\delta}(z_0,uv) \in E \\
&\overset{\text{F.07.8}}{\iff} \exists u \in A: uv \in B \\
&\iff v \in A^{-1}B. \qquad \square
\end{aligned}
$$

Bemerkung:

Hier wurde, im Gegensatz zur Lösung von Aufgabe 1.3, die Charakterisierung

$$L \text{ regulär} \iff \exists \text{ NEA } M \text{ mit } T(M) = L$$

aus Folie 11.1 verwendet.

$\boxed{A7}$

Wähle
$$s(m,n) = \begin{cases} 0 & \text{für } m=0 \text{ oder } n=0 \\ m+n-1 & \text{für } m,n>0 \,. \end{cases}$$

Beweis:

Der Fall $m=0$ oder $n=0$ folgt direkt aus $A\emptyset = \emptyset = \emptyset B$.

Für $m,n>0$ seien u ein Wort minimaler Länge aus A und v ein Wort maximaler Länge aus B. Dann gilt $\{u\}B, A\{v\} \subseteq AB$, also auch $\{u\}B \cup A\{v\} \subseteq AB$.

Daraus folgt:

$$|AB| \geq |\{u\}B \cup A\{v\}| = |A\{v\}| + |\{u\}B| - |\{u\}B \cap A\{v\}|$$
$$= |A| + |B| - |\{uv\}| = m+n-1 \,.$$

Somit ist $s(m,n)$ eine untere Schranke für $|AB|$.

Für $A = \{a^k \mid 1 \leq k \leq m\}$ und $B = \{a^k \mid 1 \leq k \leq n\}$ gilt $|A| = m$, $|B| = n$ und $AB = \{a^k \mid 2 \leq k \leq m+n\}$, d.h. $|AB| = m+n-1$.

Somit ist $s(m,n)$ eine scharfe untere Schranke für $|AB|$.