Lösungsblatt 9

Vorbereitungsaufgaben

Vorbereitungsaufgabe 1

Sei $\Sigma = \{a, b, c\}$ ein Alphabet. Geben Sie für jede der folgenden Sprachen L über Σ an, welche der darunter stehenden Aussagen wahr und welche falsch sind.

Erinnerung: Mit R_L bezeichnen wir die Myhill-Nerode-Äquivalenz bezüglich L.

1. $L = \left\{a^k b^\ell c^m \,\middle|\, k, \ell, m \in \mathbb{N}\right\}$

   (a) $abb\ R_L\ b$ (b) $aab\ R_L\ aac$ (c) $abc\ R_L\ \varepsilon$ (d) $ba\ R_L\ cb$

2. $L = \{w \in \Sigma^* \mid abc \text{ ist Präfix von } w\} = \{abcu \mid u \in \Sigma^*\}$

   (a) $ab\ R_L\ \varepsilon$ (b) $aaa\ R_L\ a$ (c) $abcaa\ R_L\ abc$ (d) $abbc\ R_L\ aabc$

3. $L = \{w \in \Sigma^* \mid abc \text{ ist Suffix von } w\} = \{uabc \mid u \in \Sigma^*\}$

   (a) $aab\ R_L\ ab$ (b) $baab\ R_L\ abba$ (c) $bbb\ R_L\ ccc$ (d) $ac\ R_L\ a$

4. $L = \{w \in \Sigma^* \mid |w|_a \leq 1 \wedge |w|_b = 1 \wedge |w|_c \geq 1\}$

   (a) $bca\ R_L\ cab$ (b) $acb\ R_L\ bc$ (c) $bcc\ R_L\ cb$ (d) $bc\ R_L\ ab$

5. $L = \{w \in \Sigma^* \mid |w|_a = |w|_b = |w|_c\}$

   (a) $abc\ R_L\ cba$ (b) $aac\ R_L\ abcc$ (c) $\varepsilon\ R_L\ aa$ (d) $bbc\ R_L\ abbbcc$

Lösung

1. (a) Wahr.

   Für alle $w \in \Sigma^*$ gilt: $abbw \in L \iff w \in \{b\}^*\{c\}^* \iff bw \in L$.

   (b) Falsch.

   Für $w = b$ gilt: $aabw \in L$, aber $aacw \notin L$.

   (c) Falsch.

   Für $w = a$ gilt: $abcw \notin L$, aber $w \in L$.

   (d) Wahr.

   Für alle $w \in \Sigma^*$ sind die Aussagen $baw \in L$ und $cbw \in L$ beide falsch und somit äquivalent.

2. (a) Falsch.

   Für $w = c$ gilt: $abw \in L$, aber $w \notin L$.

   (b) Falsch.

   Für $w = bc$ gilt: $aaaw \notin L$, aber $aw \in L$.

   (c) Wahr.

   Für alle $w \in \Sigma^*$ sind die Aussagen $abcaaw \in L$ und $abcw \in L$ beide wahr und somit äquivalent.

   (d) Wahr.

   Für alle $w \in \Sigma^*$ sind die Aussagen $abbcw \in L$ und $aabcw \in L$ beide falsch und somit äquivalent.

3. (a) Wahr.

   Für alle $w \in \Sigma^*$ gilt: $aabw \in L \iff w = c \vee w \in L \iff abw \in L$.

   (b) Falsch.

   Für $w = c$ gilt: $baabw \in L$, aber $abbaw \notin L$.

   (c) Wahr.

   Für alle $w \in \Sigma^*$ gilt: $bbbw \in L \iff w \in L \iff cccw \in L$.

   (d) Falsch.

   Für $w = bc$ gilt: $acw \notin L$, aber $aw \in L$.

4. (a) Wahr.

   Für alle $w \in \Sigma^*$ gilt: $bcaw \in L \iff |w|_a = |w|_b = 0 \iff cabw \in L$.

   (b) Falsch.

   Für $w = a$ gilt: $acbw \notin L$, aber $bcw \in L$.

(c) Wahr.

Für alle $w \in \Sigma^*$ gilt: $bccw \in L \iff |w|_a \leq 1 \wedge |w|_b = 0 \iff cbw \in L$.

(d) Falsch.

Für $w = \varepsilon$ gilt: $bcw \in L$, aber $abw \notin L$.

5. (a) Wahr.

Für alle $w \in \Sigma^*$ gilt: $abcw \in L \iff |w|_a = |w|_b = |w|_c \iff cbaw \in L$.

(b) Falsch.

Für $w = ab$ gilt: $aabw \notin L$, aber $abccw \in L$.

(c) Falsch.

Für $w = abc$ gilt: $w \in L$, aber $aaw \notin L$.

(d) Wahr.

Für alle $w \in \Sigma^*$ gilt: $bbcw \in L \iff |w|_a = |w|_b + 2 = |w|_c + 1 \iff abbbccw \in L$.

Vorbereitungsaufgabe 2

Seien $\sim, \approx$ Äquivalenzrelationen auf einer Menge S. $\approx$ heißt *Verfeinerung* von $\sim$, falls:

$$\forall x, y \in S\colon (x \approx y \implies x \sim y).$$

In diesem Fall ist jede Äquivalenzklasse bezüglich $\approx$ vollständig in einer Äquivalenzklasse bezüglich $\sim$ enthalten und es gilt folglich $|S/{\sim}| \leq |S/{\approx}|$.

Seien $\Sigma = \{a, b\}$ ein Alphabet und $\sim, \approx$ Äquivalenzrelationen auf Σ^* mit

$$\begin{aligned} x \sim y &\iff |x| = |y| \\ x \approx y &\iff (|x|_a = |y|_a \wedge |x|_b = |y|_b). \end{aligned}$$

1. Zeigen Sie, das $\approx$ eine Verfeinerung von $\sim$ ist.
2. Listen Sie alle Elemente von $[aab]_\sim$ auf.
3. Welche Äquivalenzklassen bezüglich $\approx$ enthält $[aab]_\sim$?

Lösung

1. Seien $x, y \in \Sigma^*$ beliebig mit $x \approx y$, d. h. $|x|_a = |y|_a$ und $|x|_b = |y|_b$. Dann gilt $|x| = |x|_a + |x|_b = |y|_a + |y|_b = |y|$, d. h. $x \sim y$.
2. $[aab]_\sim = \Sigma^3$
3. $[aab]_\sim$ enthält die Klassen
   - $[aaa]_\approx = \{aaa\}$,
   - $[aab]_\approx = \{aab, aba, baa\}$,

- $[abb]_\approx = \{abb, bab, bba\}$ und
- $[bbb]_\approx = \{bbb\}$.

Vorbereitungsaufgabe 3

Ein Tupel $(S, \circ)$ bestehend aus einer Menge S und einer binären Verknüpfung $\circ\colon S \times S \to S$ nennen wir *Magma*. Ein Magma $(S, \circ)$ heißt

- *Halbgruppe*, falls $(S, \circ)$ ein Magma ist und $\circ$ assoziativ ist, d. h.:
$$\forall x, y, z \in S\colon (x \circ y) \circ z = x \circ (y \circ z).$$
- *Monoid*, falls $(S, \circ)$ eine Halbgruppe ist und ein neutrales Element existiert, d. h.:
$$\exists e \in S\colon \forall x \in S\colon x \circ e = x = e \circ x.$$
Das neutrale Element e ist dann eindeutig und wird oft mit 1 notiert.
- *Gruppe*, falls $(S, \circ)$ ein Monoid ist und jedes Element ein Inverses hat, d. h.:
$$\forall x \in S\colon \exists y \in S\colon x \circ y = 1 = y \circ x.$$
Das Inverse y zu x ist dann eindeutig und wird oft mit x^{-1} notiert.

Ein Tupel $(S, \circ)$ heißt *kommutativ*, falls gilt:
$$\forall x, y \in S\colon x \circ y = y \circ x.$$

Wie so oft in der Mathematik verwenden wir häufig ein einziges Symbol für verschiedene Verknüpfungen. Beispielsweise wird $\cdot$ für die Multiplikation auf den natürlichen, ganzen, rationalen, reellen oder komplexen Zahlen, aber auch die Konkatenation von Wörtern ($u \cdot v = uv$) verwendet.

Falls klar ist, um welche Verknüpfung $\circ$ es geht, identifizieren wir ein Magma $(S, \circ)$ mit seiner Trägermenge S. Man schreibt dann S und meint dabei $(S, \circ)$. In der Vorlesung wurde beispielsweise Σ^* als das freie Monoid vorgestellt, obwohl eigentlich $(\Sigma^*, \cdot)$ gemeint war. Des Weiteren schreibt man oft xy statt $x \circ y$.

1. Welche der folgenden Tupel sind Magmen/Halbgruppen/Monoide/Gruppen? Welche davon sind kommutativ?

   (a) $(\mathbb{N}, +)$ (b) $(\mathbb{N}, -)$ (c) $(\mathbb{N}, \max)$ (d) $(\mathbb{N}, \min)$ (e) $(\mathbb{Z}, +)$ (f) $(\mathbb{Z}, -)$ (g) $(\mathbb{Q}, \cdot)$ (h) $(\mathbb{Q} \setminus \{0\}, \cdot)$ (i) $(\{a, b\}^*, \cdot)$ (j) $(\mathcal{P}(\mathbb{N}), \cap)$ (k) $(\mathcal{P}(\mathbb{N}), \cup)$ (l) $(\mathcal{P}(\mathbb{N}), \setminus)$

2. Sei $(S, \circ)$ eine endliche Halbgruppe mit $S = \{a, b, c, d, e, f\}$ als Trägermenge und der rechtsstehenden Verknüpfungstafel für $\circ$.
   (a) Ist $(S, \circ)$ ein Monoid?
   (b) Ist $(S, \circ)$ eine Gruppe?
   (c) Ist $(S, \circ)$ kommutativ?
   Begründen Sie Ihre Antworten kurz.

$\circ$	a	b	c	d	e	f
a	d	e	f	a	b	c
b	f	d	e	b	c	a
c	e	f	d	c	a	b
d	a	b	c	d	e	f
e	c	a	b	e	f	d
f	b	c	a	f	d	e

Lösung

1. (a) $(\mathbb{N}, +)$ ist ein kommutatives Monoid, aber keine Gruppe.
   (b) $(\mathbb{N}, -)$ ist weder ein Magma noch kommutativ.
   (c) $(\mathbb{N}, \max)$ ist ein kommutatives Monoid, aber keine Gruppe.
   (d) $(\mathbb{N}, \min)$ ist eine kommutative Halbgruppe, aber kein Monoid.
   (e) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe.
   (f) $(\mathbb{Z}, -)$ ist ein Magma, aber weder eine Halbgruppe noch kommutativ.
   (g) $(\mathbb{Q}, \cdot)$ ist ein kommutatives Monoid, aber keine Gruppe.
   (h) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.
   (i) $(\{a, b\}^*, \cdot)$ ist ein Monoid, aber weder eine Gruppe noch kommutativ.
   (j) $(\mathcal{P}(\mathbb{N}), \cap)$ ist ein kommutatives Monoid, aber keine Gruppe.
   (k) $(\mathcal{P}(\mathbb{N}), \cup)$ ist ein kommutatives Monoid, aber keine Gruppe.
   (l) $(\mathcal{P}(\mathbb{N}), \setminus)$ ist ein Magma, aber weder eine Halbgruppe noch kommutativ.
2. (a) Ja. Das neutrale Element ist d.
   (b) Ja. Die Inversen sind: $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$, $e^{-1} = f$ und $f^{-1} = e$.
   (c) Nein. Es gilt beispielsweise $a \circ b = e \neq f = b \circ a$.

Vorbereitungsaufgabe 4

Eine Äquivalenzrelation $\sim$ heißt *Kongruenzrelation* auf ein Monoid $(S, \circ)$, wenn gilt:

$$\forall x, x', y, y' \in S\colon (x \sim x' \land y \sim y') \implies x \circ y \sim x' \circ y'.$$

Ist $\sim$ eine Kongruenzrelation auf $(S, \circ)$, dann ist $\bullet$ mit

$$[x]_\sim \bullet [y]_\sim = [x \circ y]_\sim$$

eine wohldefinierte Verknüpfung, die zusammen mit $S/{\sim}$ ein Monoid bildet, das sogenannte *Quotientenmonoid* $(S/{\sim}, \bullet)$. Wohldefiniert heißt in diesem Fall, dass das Ergebnis der Verknüpfung $[x]_\sim \bullet [y]_\sim$ nicht von der konkreten Wahl der Repräsentanten x und y abhängt.

Sei $\sim$ eine Relation auf $\mathbb{Z}$ mit $x \sim y$ genau dann, wenn $x^2 = y^2$.

1. Zeigen Sie, dass $\sim$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist.
2. Zeigen Sie, dass $\sim$ eine Kongruenzrelation auf $(\mathbb{Z}, \cdot)$ ist.
3. Zeigen Sie, dass $\sim$ keine Kongruenzrelation auf $(\mathbb{Z}, +)$ ist.

Bemerkungen:

- Oft verwendet man dasselbe Symbol für $\circ$ und $\bullet$, obwohl das formal zwei verschiedene Verknüpfungen sind.

- Kongruenzrelationen können auch für Magmen, Halbgruppen und Gruppen definiert werden. Die entstehende Struktur $(S/{\sim}, \bullet)$ wird dann entsprechend *Quotientenmagma*, *-halbgruppe* oder *-gruppe* genannt.

Lösung

1. Reflexivität

   Für jedes $x \in \mathbb{Z}$ gilt $x^2 = x^2$. Somit ist $x \sim x$.

   Symmetrie

   Seien $x, y \in \mathbb{Z}$ beliebig mit $x \sim y$. Dann gilt $x^2 = y^2$ und folglich auch $y^2 = x^2$. Somit ist $y \sim x$.

   Transitivität

   Seien $x, y, z \in \mathbb{Z}$ beliebig mit $x \sim y$ und $y \sim z$. Dann gilt $x^2 = y^2$ und $y^2 = z^2$ und folglich auch $x^2 = y^2 = z^2$. Somit ist $x \sim z$.

   Bemerkung: Man erkennt, dass dieser Beweis völlig analog zu dem Beweis aus Aufgabe 2, Teil 1 (b) auf Ergänzungsblatt 6 funktioniert. Tatsächlich ist eine Relation $\sim$ auf einer Menge S mit

   $$x \sim y \iff f(x) = f(y)$$

   für jede Funktion f mit Definitionsbereich S eine Äquivalenzrelation. Die Äquivalenzklassen sind dann genau die Urbilder.

2. Seien $x, x', y, y' \in \mathbb{Z}$ mit $x \sim x'$ und $y \sim y'$, d. h. $x^2 = x'^2$ und $y^2 = y'^2$. Dann gilt:

   $$(x \cdot y)^2 = x^2 \cdot y^2 = x'^2 \cdot y'^2 = (x' \cdot y')^2.$$

   Somit ist $x \cdot y \sim x' \cdot y'$.

3. Man sieht, dass der Beweis aus Teilaufgabe 2 mit $+$ statt $\cdot$ nicht funktioniert, da die Gleichung $(a+b)^2 = a^2 + b^2$ im Allgemeinen falsch ist. Dies ist jedoch noch kein Beweis dafür, dass $\sim$ keine Kongruenzrelation auf $(\mathbb{Z}, +)$ ist. Es zeigt jediglich, dass dieser eine Ansatz fehlschlägt.

   Wir zeigen, dass $\sim$ keine Kongruenzrelation auf $(\mathbb{Z}, +)$ ist, indem wir Elemente $x, x', y, y' \in \mathbb{Z}$ mit $x \sim x'$, $y \sim y'$ und $x \cdot x' \not\sim y \cdot y'$ angeben.

   Beweis

   Seien $x = x' = y = 1$ und $y' = -1$. Dann gilt $x, x', y, y' \in \mathbb{Z}$, $x \sim x'$ und $y \sim y'$. Wegen

   $$(x + x')^2 = 4 \neq 0 = (y + y')^2$$

   gilt jedoch $x \cdot x' \not\sim y \cdot y'$. □

   An diesem Beispiel erkennt man den Sinn der obigen Definition einer Kongruenzrelation. Man kann keine Verknüpfung der Art

   $$[x]_\sim + [y]_\sim = [x + y]_\sim$$

auf der Quotientenmenge $\mathbb{Z}/\sim$ definieren. Diese wäre nämlich nicht wohldefiniert, da das Ergebnis $[x+y]_\sim$ der Verknüpfung abhängig von der Wahl der Repräsentanten x und y wäre.

Präsenzaufgaben

Präsenzaufgabe 1

Zeigen Sie mithilfe des Satzes von Myhill-Nerode, dass keine der folgenden Sprachen L über dem entsprechenden Alphabet Σ regulär ist.

1. $L = \{w \in \Sigma^* \mid |w|_a = |w|_b\}$, $\Sigma = \{a, b\}$
2. $L = a^{3^k} k \in \mathbb{N}$, $\Sigma = \{a\}$
3. $L = \left\{a^{\lfloor\sqrt{k}\rfloor} b^\ell c^k \,\middle|\, k, \ell \in \mathbb{N}\right\}$, $\Sigma = \{a, b, c\}$

Lösung

Zu zeigen ist, dass es die Myhill-Nerode-Äquivalenz R_L unendlichen Index hat, d. h. $|\Sigma^*/R_L| = \infty$. Dies kann ereicht werden, indem man die Existenz einer unendlichen Menge $M \subseteq \Sigma^*$ mit

$$\forall x, y \in M\colon x \neq y \implies x \not R_L\, y$$

zeigt. Dann folgt daraus, dass die Elemente von M paarweise nicht R_L-äquivalent sind, also in unterschiedlichen Klassen enthalten sind. Dann ist $\{[z]_{R_L} \mid z \in M\}$ eine unendliche Teilmenge von Σ^*/R_L, was $|\Sigma^*/R_L| = \infty$ impliziert.

1. Betrachte die Menge $M = \{a^n \mid n \in \mathbb{N}\}$. Dann ist $M \subseteq \Sigma^*$ mit $|M| = \infty$.

   Seien $x, y \in M$ beliebig mit $x \neq y$. Dann existieren $i, j \in \mathbb{N}$ mit $i \neq j$, $x = a^i$ und $y = a^j$. Für $w = b^i$ ist $xw \in L$, aber $yw \notin L$.

2. Betrachte die Menge $M = \left\{a^{3^n} \,\middle|\, n \in \mathbb{N}\right\}$. Dann ist $M \subseteq \Sigma^*$ mit $|M| = \infty$.

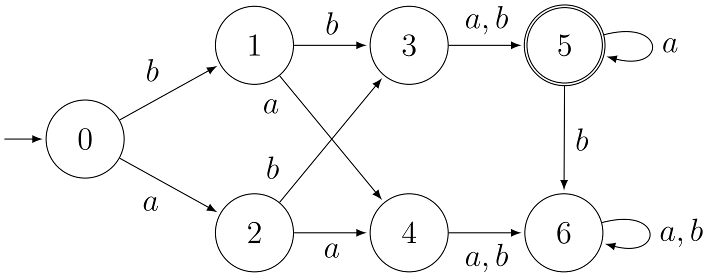
   Seien $x, y \in M$ beliebig mit $x \neq y$. Dann existieren $i, j \in \mathbb{N}$ mit $i \neq j$, $x = a^{3^i}$ und $y = a^{3^j}$. O. B. d. A. sei $i < j$. Für $w = a^{2\cdot 3^i}$ ist $xw = a^{3^i + 2\cdot 3^i} = a^{3\cdot 3^i} = a^{3^{i+1}} \in L$, aber $yw = a^{3^j + 2\cdot 3^i} = a^{3^i(3^{j-i}+2)} \notin L$, da $3^{j-i} + 2$ nicht durch 3 teilbar und somit $3^i(3^{j-i} + 2)$ keine Dreierpotenz ist.

3. Betrachte die Menge $M = \{a^n \mid n \in \mathbb{N}\}$. Dann ist $M \subseteq \Sigma^*$ mit $|M| = \infty$.

   Seien $x, y \in M$ beliebig mit $x \neq y$. Dann existieren $i, j \in \mathbb{N}$ mit $i \neq j$, $x = a^i$ und $y = a^j$. Für $w = c^{i^2}$ ist $xw \in L$, aber $yw \notin L$.

Präsenzaufgabe 2

Sei M der folgende DFA:



1. Führen Sie Minimierungsalgorithmus aus der Vorlesung durch.

   Anstatt nicht äquivalente Zustände (bezüglich der Myhill-Nerode-Äquivalenz R_L) zu markieren, soll ein Zeuge eingetragen werden, der die Inäquivalenz der Zustände belegt.

   Ein Wort $w \in \Sigma^*$ heißt *Zeuge* für die Inäquivalenz von p und q, falls gilt:

   $$\hat{\delta}(p, w) \in F \iff \hat{\delta}(q, w) \notin F.$$

   Tragen Sie in jedes Feld einen Zeugen minimaler Länge ein oder schreiben Sie „R_L“, falls die Zustände äquivalent sind.

2. Wie sieht der resultierende minimale DFA aus?

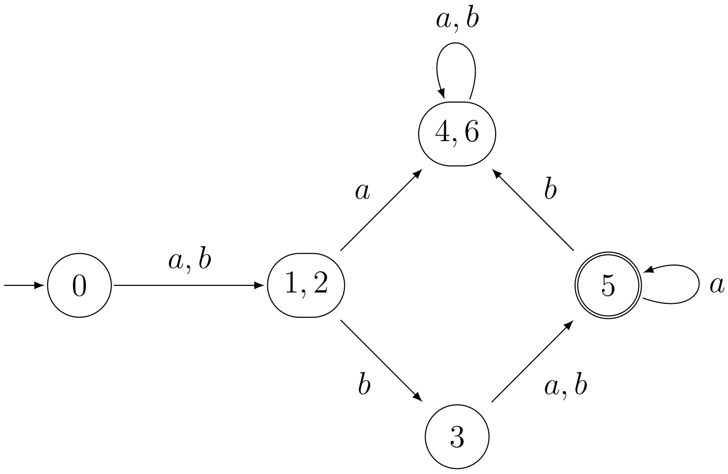
3. Geben Sie einen regulären Audruck γ mit $L(\gamma) = T(M)$ an.

Lösung

1.

	0	1	2	3	4	5
1	ba					
2	ba	R_L				
3	a	a	a			
4	aba	ba	ba	a		
5	ε	ε	ε	ε	ε	
6	aba	ba	ba	a	R_L	ε

2.



3. $\gamma = (a|b)b(a|b)a^*$

Knobelaufgaben

Knobelaufgabe 1

Zeigen Sie mit dem Satz von Myhill-Nerode, dass die Sprache

$$L = a^k b^\ell \, \mathrm{ggT}(k, \ell) = 1$$

über dem Alphabet $\Sigma = \{a, b\}$ nicht regulär ist.

Hinweis: $\mathrm{ggT}(k, \ell)$ ist der *größte gemeinsame Teiler* von k und ℓ mit $\mathrm{ggT}(k, 0) = k$ und $\mathrm{ggT}(k, 1) = 1$ für alle $k \in \mathbb{N}$. $\mathrm{ggT}(k, \ell) = 1$ besagt also, dass k und ℓ *teilerfremd* sind.

Knobelaufgabe 2

Sei Σ ein Alphabet. In früheren Knobelaufgaben (Ergänzungblätter 3 und 8) sollten Sie zeigen, dass folgende Relationen Äquivalenzrelationen auf Σ^* sind:

1. $x \sim y :\Longleftrightarrow \exists u \in \Sigma^* \colon xu = uy$
2. $x \sim y :\Longleftrightarrow \exists u, v \in \Sigma^* \colon x = uv \land y = vu$

Welche davon sind Kongruenzrelationen auf $(\Sigma^*, \cdot)$?

Beweisen Sie Ihre Antworten.