Lösungsblatt 4

Vorbereitungsaufgaben

Vorbereitungsaufgabe 1

Studieren Sie die Definition der Kongruenz modulo n aus Ergänzungsblatt 3, Präsenzaufgabe 2.

Lösung

Bitte machen! Dieser Begriff wird nicht nur in dieser Ergänzung wichtig sein, sondern auch später in dieser sowie in anderen Vorlesungen.

Die Intuition, dass $x \equiv y \mod n$ genau dann gilt, wenn x und y den gleichen Rest bei Division durch n haben, ist zwar hilfreich, aber keineswegs ausreichend. Die formale Definition mit Quantoren sollte ebenso verstanden und verinnerlicht werden.

Auch die Aussagen aus Ergänzungsblatt 3, Knobelaufgabe 1 können das Verständnis fördern. Dazu muss die Knobelaufgabe nicht unbedingt gelöst werden.

Vorbereitungsaufgabe 2

Seien $Q = \{0, 1, 2\}$, $\Sigma = \{a, b\}$ und $F = \{1, 2\}$ drei Mengen und $\delta \colon Q \times \Sigma \to Q$ eine Funktion mit

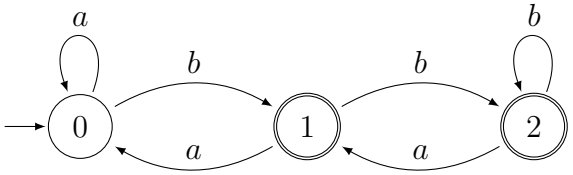
$$(0, a) \mapsto 0,\ (0, b) \mapsto 1,\ (1, a) \mapsto 0,\ (1, b) \mapsto 2,\ (2, a) \mapsto 1 \text{ und } (2, b) \mapsto 2.$$

Als Tabelle:

δ	a	b
0	0	1
1	0	2
2	1	2

1. Überprüfen Sie, dass $M = (Q, \Sigma, \delta, 0, F)$ ein (formal korrekter) DFA ist.
2. Zeigen Sie $\hat{\delta}(1, abbab) = 2$ durch wiederholtes Anwenden der Definition von $\hat{\delta}$.
3. Geben Sie M grafisch an.
4. Welche grafische Bedeutung hat die Gleichung aus Teilaufgabe 2?
5. Verwenden Sie die in der Vorlesung beschriebene Methode, um eine reguläre Grammatik G mit $L(G) = T(M)$ zu konstruieren.

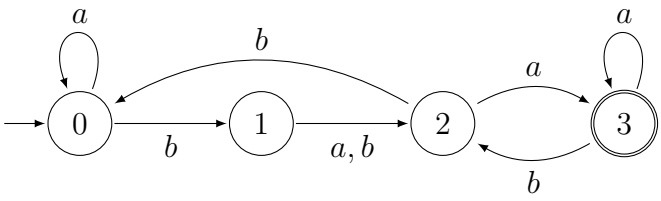
Lösung

1. Q und Σ sind nichtleer, endlich und disjunkt und es gilt $0 \in Q$, $F \subseteq Q$ und $\delta\colon Q \times \Sigma \to Q$.
2. $\hat{\delta}(1, abbab) = \hat{\delta}(0, bbab) = \hat{\delta}(1, bab) = \hat{\delta}(2, ab) = \hat{\delta}(1, b) = 2$.
3. 

4. Falls sich M vor dem Lesen des Wortes *abbab* im Zustand 1 befindet, geht er danach in den Zustand 2 über.
5. $G = (\{0, 1, 2\}, \{a, b\}, P, 0)$ mit
$$P = \{0 \to a0 \mid b1 \mid b, 1 \to a0 \mid b2 \mid b, 2 \to a1 \mid b2 \mid a \mid b\}.$$

Vorbereitungsaufgabe 3

Geben Sie den folgenden DFA M als 5-Tupel an:



Analog zu Vorbereitungsaufgabe 2 kann die Überführungsfunktion auch als Tabelle angegeben werden.

Lösung

$M = (Q, \Sigma, \delta, 0, F)$ für $Q = \{0, 1, 2, 3\}$, $\Sigma = \{a, b\}$, $F = \{3\}$ und $\delta\colon Q \times \Sigma \to Q$ mit:

δ	a	b
0	0	1
1	2	2
2	3	0
3	3	2

Vorbereitungsaufgabe 4

Sei $\Sigma = \{a, b\}$ ein Alphabet. Geben Sie für jede der folgenden Sprachen L über Σ grafisch einen minimalen DFA an, der die jeweilige Sprache akzeptiert.

Ein DFA heißt *minimal*, wenn kein DFA mit weniger Zuständen existiert, der dieselbe Sprache akzeptiert.

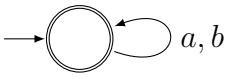
1. $L = \Sigma^*$
2. $L = \emptyset$
3. $L = \{\varepsilon\}$
4. $L = \Sigma$
5. $L = \{w \in \Sigma^* \mid |w|_a \equiv 1 \mod 3\}$
6. $L = \{w \in \Sigma^* \mid aba \text{ ist Präfix von } w\}$

Lösung

Wenn man Automaten grafisch angibt, müssen die Zustände nicht notwendigerweise beschriftet werden. Lässt man die Zustände der DFA unbeschriftet, dann ist die Lösung jeder Teilaufgabe eindeutig, da zu einer gegebenen Sprache bis auf die Benennung der Zustände immer genau ein minimaler DFA existiert.

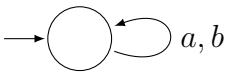
1. L enthält alle Wörter über Σ.

   Minimaler DFA

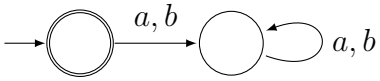
2. L enthält gar kein Wort.

   Minimaler DFA

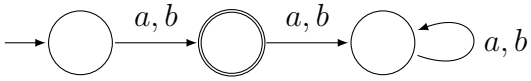
3. L enthält nur das leere Wort ε.

   Minimaler DFA

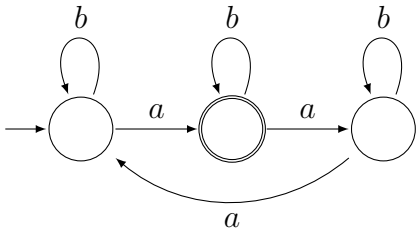
4. L enthält genau die Wörter a und b.

   Minimaler DFA

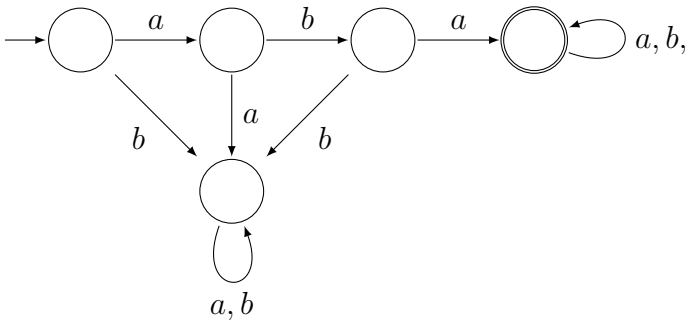
5. L enthält genau die Wörter über Σ mit $|w|_a \in \{1, 4, 7, 10, 13, 16, \dots\}$.

   Minimaler DFA

6. L enthält genau die Wörter über Σ, die mit aba beginnen.

Minimaler DFA



Präsenzaufgaben

Präsenzaufgabe 1

Sei $\Sigma = \{a, b\}$ ein Alphabet. Zeigen Sie, dass die Grammatik $G = (\{S\}, \Sigma, P, S)$ mit

$$P = \{S \to aSb \mid \varepsilon\}$$

die Sprache $L = \{a^m b^m \mid m \geq 0\}$ erzeugt.

Lösung

Zu zeigen ist die Mengengleichheit $L(G) = L$. Wie üblich zeigen wir beide Inklusionen getrennt voneinander.

Beweis der Inklusion $L(G) \subseteq L$

Zu zeigen ist, dass jedes von G erzeugte Wort die Form $a^m b^m$ für ein $m \geq 0$ hat, d. h.:

$$\forall w \in \Sigma^* \colon (w \in L(G) \implies \exists m \geq 0 \colon w = a^m b^m).$$

Wegen

$$\begin{aligned}
&\forall w \in \Sigma^* \colon (w \in L(G) \implies \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall w \in \Sigma^* \colon (\exists n \geq 1 \colon S \Rightarrow_G^n w \implies \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall w \in \Sigma^* \colon (\neg \exists n \geq 1 \colon S \Rightarrow_G^n w \vee \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall w \in \Sigma^* \colon (\forall n \geq 1 \colon \neg (S \Rightarrow_G^n w) \vee \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall w \in \Sigma^* \colon \forall n \geq 1 \colon (\neg (S \Rightarrow_G^n w) \vee \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall w \in \Sigma^* \colon \forall n \geq 1 \colon (S \Rightarrow_G^n w \implies \exists m \geq 0 \colon w = a^m b^m) \\
&\iff \forall n \geq 1 \colon \underbrace{\forall w \in \Sigma^* \colon (S \Rightarrow_G^n w \implies \exists m \geq 0 \colon w = a^m b^m)}_{A(n)}
\end{aligned}$$

verwenden wir vollständige Induktion, um die Aussage $\forall n \geq 1 \colon A(n)$ zu zeigen. Wir sagen in solchen Fällen, dass die Induktion *über die Ableitungslänge n geht.*

Bemerkung: In der Ergänzung wurde $A(n)$ für alle $n \geq 0$ gezeigt. Weil kein $w \in \Sigma^*$ mit $S \Rightarrow_G^0 w$ existiert sind die Aussagen $\exists n \geq 0 \colon S \Rightarrow_G^n w$ und $\exists n \geq 1 \colon S \Rightarrow_G^n w$ für jede Grammatik G äquivalent.

Induktionsanfang

Zu zeigen ist $A(1)$. Sei hierzu $w \in \Sigma^*$ beliebig mit $S \Rightarrow_G^1 w$. Da ε das einzige Wort ist, das in einem Schritt von S abgeleitet werden kann, folgt $w = \varepsilon = a^0 b^0$.

Induktionsschritt

Zu zeigen ist

$$\forall n \geq 1 \colon (A(n) \implies A(n+1)).$$

Sei hierzu $n \geq 1$ beliebig. Angenommen, für jedes $w \in \Sigma^*$ mit $S \Rightarrow_G^n w$ existiert ein $m \geq 0$ mit $w = a^m b^m$ (Induktionsvoraussetzung). Sei nun $w' \in \Sigma^*$ beliebig mit $S \Rightarrow_G^{n+1} w$. Wegen $n \geq 1$ gilt $S \Rightarrow_G aSb \Rightarrow_G^n w'$, also hat w' die Form $w' = awb$ für ein Wort w mit $S \Rightarrow_G^n w$. Nach Induktionsvoraussetzung existiert ein $m \geq 0$ mit $w = a^m b^m$. Wähle $m' = m + 1$. Dann ist $m' \geq 0$ mit

$$w' = awb = aa^m b^m b = a^{m+1} b^{m+1} = a^{m'} b^{m'}.$$

Beweis der Inklusion $L \subseteq L(G)$

Analog zur ersten Beweisrichtung ist die zu beweisende Aussage äquivalent ist zu

$$\forall m \geq 0 \colon \forall w \in \Sigma^* \colon (w = a^m b^m \implies S \Rightarrow_G^n w)$$

bzw. $\forall m \geq 0 \colon \underbrace{S \Rightarrow_G^* a^m b^m}_{A(m)}$. Diese zeigen wir mit vollständiger Induktion nach m.

Induktionsanfang

Zu zeigen ist $A(0)$, d. h. $S \Rightarrow_G^* a^0 b^0 = \varepsilon$. Aus $S \to \varepsilon \in P$ folgt $S \Rightarrow_G^1 \varepsilon$ und somit $S \Rightarrow_G^* \varepsilon$.

Induktionsschritt

Zu zeigen ist

$$\forall m \geq 0 \colon (A(m) \implies A(m+1)).$$

Sei hierzu $m \geq 0$ beliebig. Angenommen, es gilt $S \Rightarrow_G^* a^m b^m$ (Induktionsvoraussetzung). Dann gilt

$$S \Rightarrow_G aSb \overset{\text{IV}}{\Rightarrow}_G^* aa^m b^m b = a^{m+1} b^{m+1}$$

und somit $S \Rightarrow_G^* a^{m+1} b^{m+1}$.

Präsenzaufgabe 2

Sei $\Sigma = \{a, b\}$ ein Alphabet. Zeigen Sie, dass die Grammatik $G = (\{S\}, \Sigma, P, S)$ mit

$$P = \{S \to aSb \mid bSa \mid SS \mid \varepsilon\}$$

die Sprache $L = \{w \in \Sigma^* \mid |w|_a = |w|_b\}$ erzeugt.

Lösung

Auch in dieser Aufgabe zeigen wir beide Inklusionen getrennt voneinander. Wenn die Grammatik Regeln mit mehr als eine Variable auf der rechten Seite enthält (in diesem Fall $S \to SS$), ist vollständige Induktion nicht direkt anwendbar. Wir verwenden daher in dieser Aufgabe starke Induktion. Statt $\forall n \geq n_0 \colon A(n)$ zu zeigen, zeigen wir zuerst den Induktionsanfang $A(n_0)$ und danach den Induktionsschritt

$$\forall n \geq n_0 \colon \left(\bigwedge_{k=n_0}^{n} A(k) \right) \implies A(n+1).$$

Beweis der Inklusion $L(G) \subseteq L$

Wir zeigen die dazu äquivalente Aussage

$$\forall n \geq 1 \colon \underbrace{\forall w \in \Sigma^* \colon (S \Rightarrow_G^n w \implies |w|_a = |w|_b)}_{A(n)}$$

mit starker Induktion nach der Ableitungslänge n.

Induktionsanfang

Für $n = 1$ folgt aus $S \Rightarrow_G^n w$ und $w \in \Sigma^*$ sofort $w = \varepsilon$ und somit $|w|_a = 0 = |w|_b$.

Induktionsschritt

Sei $n \geq 1$ beliebig. Für jedes $k \leq n$ erfüllt nach Induktionsvoraussetzung jedes $w \in \Sigma^*$ mit $S \Rightarrow_G^k w$ die Gleichung $|w|_a = |w|_b$. Sei nun $w' \in \Sigma^*$ mit $S \Rightarrow_G^{n+1} w'$ beliebig. Wir unterscheiden drei Fälle.

Fall 1: $S \Rightarrow_G aSb \Rightarrow_G^n w'$

Dann existiert ein $w \in \Sigma^*$ mit $w' = awb$ und $S \Rightarrow_G^n w$. Es folgt:

$$|w'|_a = |awb|_a = 1 + |w|_a \overset{\text{IV}}{=} 1 + |w|_b = |awb|_b = |w'|_b.$$

Fall 2: $S \Rightarrow_G bSa \Rightarrow_G^n w'$

Analog zu Fall 1.

Fall 3: $S \Rightarrow_G SS \Rightarrow_G^n w'$

Dann existieren $w_1, w_2 \in \Sigma^*$ mit $w' = w_1 w_2$, $S \Rightarrow_G^{k_1} w_1$ und $S \Rightarrow_G^{k_2} w_2$ für $k_1, k_2 \leq n$. Es folgt:

$$|w'|_a = |w_1 w_2|_a = |w_1|_a + |w_2|_a \overset{\text{IV}}{=} |w_1|_b + |w_2|_b = |w_1 w_2|_b = |w'|_b.$$

In allen drei Fällen gilt $|w'|_a = |w'|_b$.

Beweis der Inklusion $L \subseteq L(G)$

Um die Beweismethode der Inklusion $L \subseteq L(G)$ von Präsenzaufgabe 1 verwenden zu können, benötigen wir wie bei $\exists m \geq 0 \colon w = a^m b^m$ eine mit existentiell quantifizierte natürliche Zahl m. Hier kann man die Äquivalenzen

$$w \in L \iff |w|_a = |w|_b \iff \exists m \geq 0 \colon |w|_a = m = |w|_b$$

verwenden, um auf die zu $L \subseteq L(G)$ äquivalente Aussage

$$\forall m \geq 0 \colon \underbrace{\forall w \in \Sigma^* \colon (|w|_a = m = |w|_b \implies S \Rightarrow_G^* w)}_{A(m)}$$

zu kommen. Diese zeigen wir mit starker induktion nach m.

Induktionsanfang

Für $m = 0$ folgt aus $|w|_a = 0 = |w|_b$ sofort $w = \varepsilon$. Wegen $S \Rightarrow_G \varepsilon$ gilt auch $S \Rightarrow_G^* w$.

Induktionsschritt

Sei $m \geq 0$ beliebig. Für jedes $k \leq n$ ist nach Induktionsvoraussetzung jedes $w \in \Sigma^*$ mit $|w|_a = k = |w|_b$ von S ableitbar, d. h. $S \Rightarrow_G^* w$. Sei nun $w' \in \Sigma^*$ mit $|w'|_a = |w'|_b = n + 1$. Wir unterscheiden drei Fälle.

Fall 1: w' beginnt mit a und endet mit b

Dann existiert ein $w \in \Sigma^*$ mit $w' = awb$. Für dieses w gilt $|w|_a = m = |w|_b$. Dann folgt für w':

$$S \Rightarrow_G aSb \overset{\text{IV}}{\Rightarrow}_G^* awb = w'.$$

Fall 2: w' beginnt mit b und endet mit a

Analog zu Fall 1.

Fall 3: w' beginnt und endet mit a

Dann existiert ein $w \in \Sigma^*$ mit $w' = awa$. Für dieses w gilt zwar $|w|_b = m$, aber $|w|_a = m - 2$. Aus $|a|_a = |a|_b + 1$ und $|aw|_a = |aw|_b - 1$ folgt, dass $w_1, w_2 \in \Sigma^*$ existieren müssen mit $w = w_1 w_2$ und $|aw_1|_a = |aw_1|_b$. Dann gilt auch $|aw_2|_a = |aw_2|_b$ und für w' folgt:

$$S \Rightarrow_G SS \overset{\text{IV}}{\Rightarrow}_G^* aw_1w_2a = w'.$$

Fall 4: w' beginnt und endet mit b

Analog zu Fall 3.

In allen drei Fällen gilt $S \Rightarrow_G^* w'$.

Präsenzaufgabe 3

Sei $\Sigma = \{a, b\}$ ein Alphabet. Geben Sie für jede der folgenden Sprachen L über Σ grafisch einen minimalen DFA an, der die jeweilige Sprache akzeptiert.

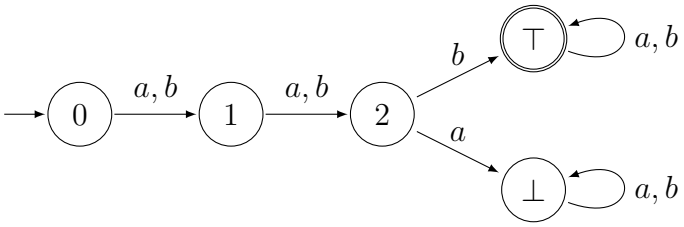
1. $L = \{ubv \mid u, v \in \Sigma^* \wedge |u| = 2\}$
2. $L = \{w \in \Sigma^* \mid |w|_a$ ist gerade und $|w|_b$ ungerade$\}$
3. $L = \{w \in \Sigma^* \mid abba$ ist ein Suffix von $w\}$
4. $L = \{w \in \Sigma^* \mid abab$ ist ein Infix von $w\}$
5. $L = \{a^m b^n \mid m \equiv 2 \mod 3 \wedge n \equiv 0 \mod 2\}$
6. $L = \{w \in \Sigma^* \mid ab$ ist ein Präfix und ba ein Suffix von $w\}$

Lösung

Obwohl bei grafischen DFAs auf die Beschriftung der Zustände verzichtet werden kann, wurden die Namen der Zustände hier so gewählt, dass man ihnen entnehmen kann, welche Eigenschaft des bisher gelesenen Wortes im Automat gespeichert werden soll. Absorbierende Zustände (solche, die nicht mehr verlassen werden können) werden manchmal mit einem *Top-Symbol* $\top$ notiert, falls sie Endzustände sind und mit einem *Bottom-Symbol* $\bot$ sonst. Im zweiten Fall nennt man solche Zustände *Fang-* bzw. *Fehlerzustände*.

1. L enthält genau die Wörter über Σ, die an der dritten Stelle ein b haben.

   Minimaler DFA

   Bedeutung der Zustände

   0: Das bisher gelesene Wort hat Länge 0.

   1: Das bisher gelesene Wort hat Länge 1.

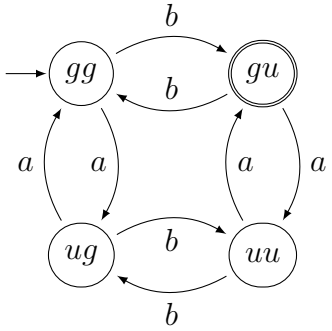
   2: Das bisher gelesene Wort hat Länge 2.

   $\top$: Das bisher gelesene Wort hat an der 3. Selle ein b.

   $\bot$: Das bisher gelesene Wort hat an der 3. Selle ein a.

2. L enthält genau die Wörter über Σ, die gerade viele as und ungerade viele bs haben.

   Minimaler DFA

   Bedeutung der Zustände

   gg: Das bisher gelesene Wort hat gerade viele as und gerade viele bs.

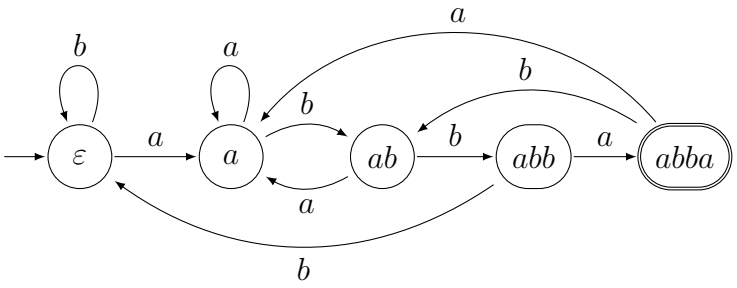
   ug: Das bisher gelesene Wort hat ungerade viele as und gerade viele bs.

   gu: Das bisher gelesene Wort hat gerade viele as und ungerade viele bs.

   uu: Das bisher gelesene Wort hat ungerade viele as und ungerade viele bs.

3. L enthält genau die Wörter über Σ, die mit $abba$ enden.

   Minimaler DFA



   Bedeutung der Zustände

   ε: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist ε.

   a: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist a.

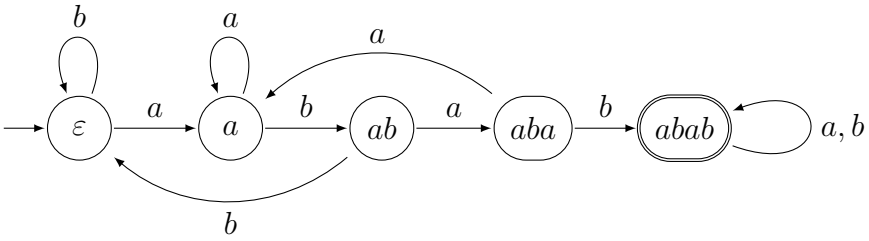
   ab: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist ab.

   abb: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist abb.

   $abba$: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist $abba$.

4. L enthält genau die Wörter über Σ, in denen das Wort $abba$ irgendwo vorkommt.

   Minimaler DFA



   Bedeutung der Zustände

   ε: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist ε.

   a: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist a.

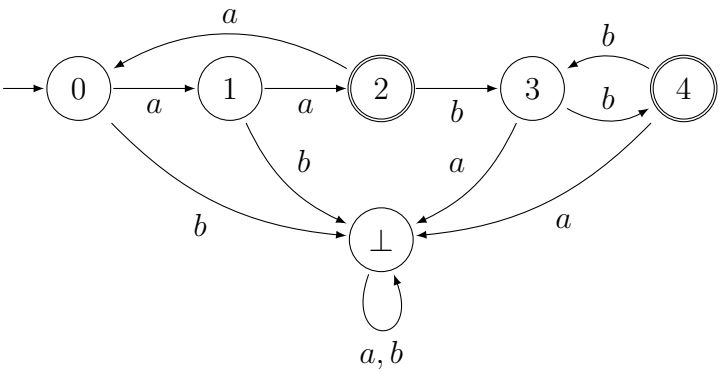
   ab: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist ab.

   aba: Das längste Suffix des bisher gelesenen Wortes, das Präfix von $abba$ ist, ist aba.

   $abab$: Das bisher gelesene Wort enthält $abab$ als Infix.

5. L enthält genau die Wörter über Σ der Form $a^m b^n$ mit $m \in \{2, 5, 8, 11, \dots\}$ und n gerade.

   Minimaler DFA

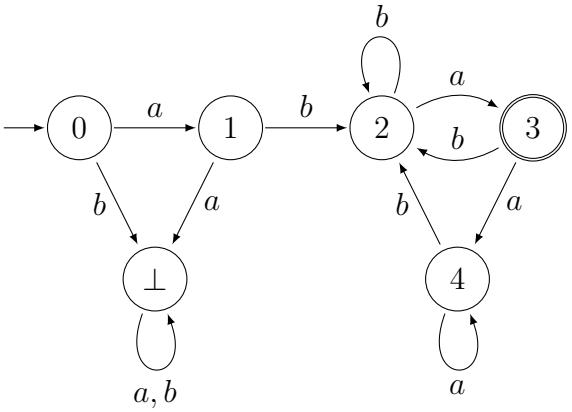


Bedeutung der Zustände

- 0: Das bisher gelesene Wort hat die Form a^m für ein $m \in \{0, 3, 6, 9, \dots\}$.
- 1: Das bisher gelesene Wort hat die Form a^m für ein $m \in \{1, 4, 7, 10, \dots\}$.
- 2: Das bisher gelesene Wort hat die Form a^m für ein $m \in \{2, 5, 8, 11, \dots\}$.
- 3: Das bisher gelesene Wort hat die Form $a^m b^n$ für ein $m \in \{2, 5, 8, 11, \dots\}$ und n ungerade.
- 4: Das bisher gelesene Wort hat die Form $a^m b^n$ für ein $m \in \{2, 5, 8, 11, \dots\}$ und n ungerade.
- $\perp$: Das bisher gelesene Wort hat $a^m b$ für ein $m \notin \{2, 5, 8, 11, \dots\}$ als Präfix oder ba als Infix.

6. L enthält genau die Wörter über Σ, die mit ab beginnen und mit ba enden.

Minimaler DFA



Bedeutung der Zustände

- 0: Das bisher gelesene Wort ist ε.
- 1: Das bisher gelesene Wort ist a.
- 2: Das bisher gelesene Wort beginnt mit ab und sein längstes Suffix, das Präfix von ba ist, ist b.

3: Das bisher gelesene Wort beginnt mit ab und sein längstes Suffix, das Präfix von ba ist, ist ba.

4: Das bisher gelesene Wort beginnt mit ab und sein längstes Suffix, das Präfix von ba ist, ist ε.

$\perp$: Das bisher gelesene Wort beginnt entweder mit b oder mit aa.

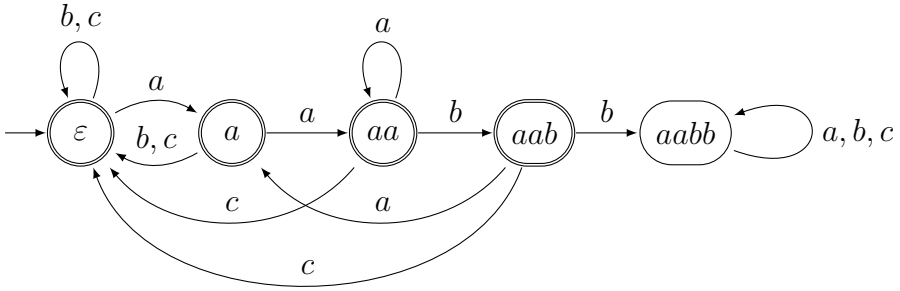
Präsenzaufgabe 4

Sei $\Sigma = \{a, b, c\}$ ein Alphabet. Geben Sie für jede der folgenden Sprachen L über Σ grafisch einen minimalen DFA an, der die jeweilige Sprache akzeptiert.

1. $L = \{w \in \Sigma^* \mid aabb \text{ ist } \underline{\text{kein}} \text{ Infix von } w\}$
2. $L = \{w \in \Sigma^* \mid |w|_a = 2 \wedge |w|_b = 1\}$
3. $L = \{w \in \Sigma^* \mid |w|_a \geq 1 \vee |w|_b \geq 2 \vee |w|_c \geq 3\}$

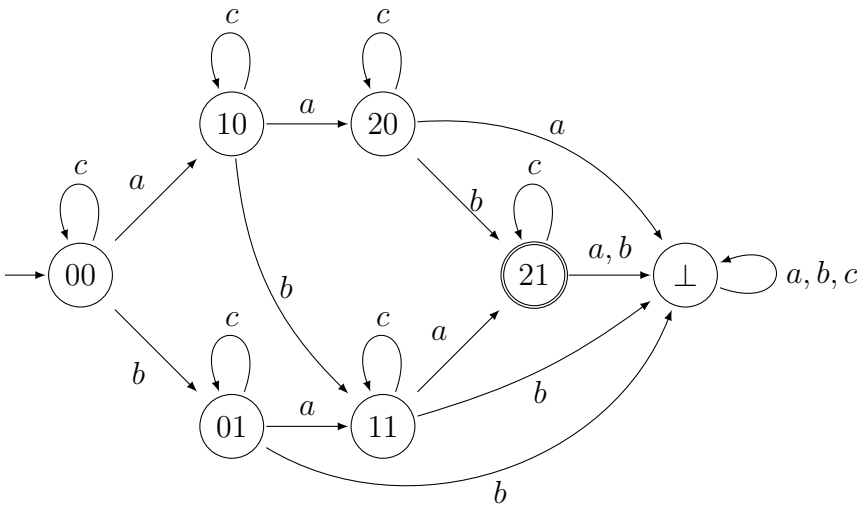
Lösung

1. Minimaler DFA



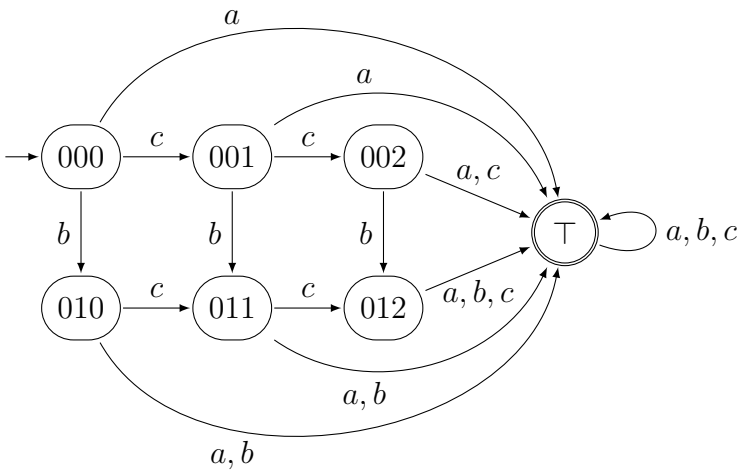
Lösungsansatz analog zu Präsenzaufgabe 3.4, aber mit vertauschten Endzuständen.

2. Minimaler DFA



Jeder Zustand xy hat als Bedeutung, dass das bisher gelesene Wort genau x as und genau y bs enthält. Sind es mehr als zwe as oder mehr als ein b, so führt das Wort zum Fangzustand $\bot$.

3. Minimaler DFA



Jeder Zustand xyz hat als Bedeutung, dass das bisher gelesene Wort genau x as, genau y bs und genau z cs enthält. Enthält es ein a, zwei bs oder drei cs, so führt das Wort zum absorbierenden Endzustand $\top$.

Knobelaufgaben

Knobelaufgabe 1

Seien $m \geq 1$ eine natürliche Zahl und Σ ein m-elementiges Alphabet. Geben Sie einen DFA an, der die Sprache

$$L = \{w \in \Sigma^* \mid \text{ in } w \text{ kommt jedes Element von } \Sigma \text{ vor}\}$$

über Σ akzeptiert und beweisen Sie die Korrektheit Ihrer Konstruktion.

Knobelaufgabe 2

Seien $a, b, n \in \mathbb{Z}$ mit $n \geq 1$ beliebig.

1. Zeigen Sie:

   (1) $(a + b) \bmod n = ((a \bmod n) + b) \bmod n$

   (2) $(a \cdot b) \bmod n = ((a \bmod n) \cdot b) \bmod n$

2. Welche der folgenden Gleichungen gelten für beliebige $a, b, n \in \mathbb{Z}$ mit $n \geq 1$ und welche nicht? Beweisen Sie Ihre Antworten.

   (3) $(a + b) \bmod n = (a \bmod n) + (b \bmod n)$

(4) $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

(5) $(a \cdot b) \bmod n = (a \bmod n) \cdot (b \bmod n)$

(6) $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$