Automata and Formal Languages — Exercise Sheet 3

Exercise 3.1
Determine the residuals of the following languages:

(a) $(ab + ba)^*$ over $\Sigma = \{a, b\}$,

(b) $(aa)^*$ over $\Sigma = \{a, b\}$,

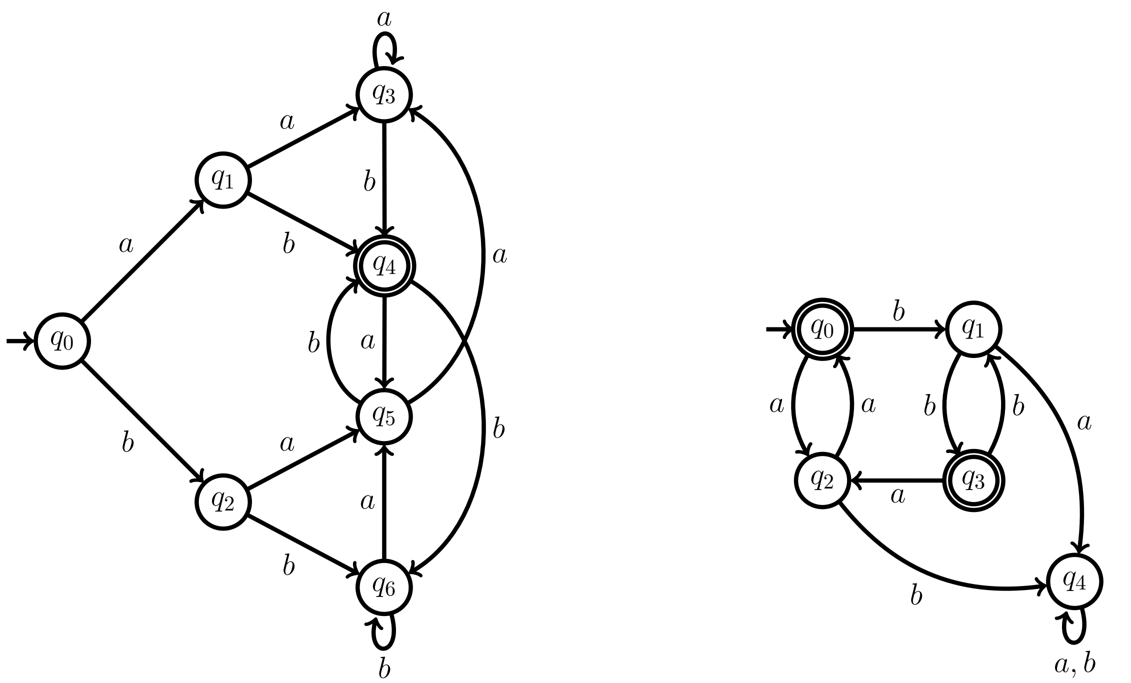
(c) $\{a^n b^n c^n \mid n \geq 0\}$ over $\Sigma = \{a, b, c\}$.

Exercise 3.2

(a) Let $\Sigma = \{0, 1\}$ be an alphabet.
Find a language $L \subseteq \Sigma^*$ that has infinitely many residuals and $|L^w| > 0$ for all $w \in \Sigma^*$.

(b) Let $\Sigma = \{a\}$ be an alphabet.
Find a language $L \subseteq \Sigma^*$, such that $L^w = L^{w'} \implies w = w'$ for all words $w, w' \in \Sigma^*$.
What can you say about the residuals for such a language L? Is such a language regular?

Exercise 3.3
Let A and B be respectively the following DFAs:

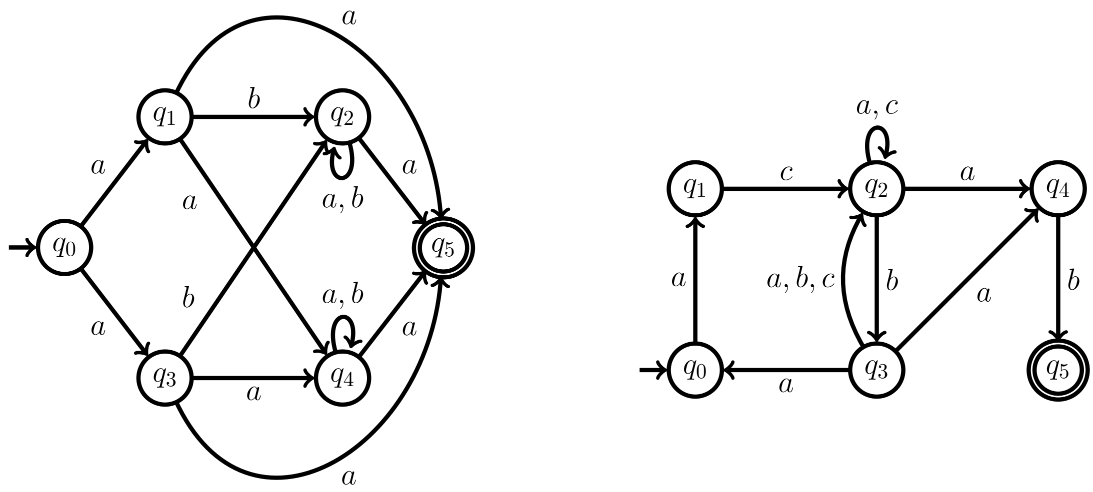


(a) Compute the language partitions of A and B.

(b) Construct the quotients of A and B with respect to their language partitions.

(c) Give regular expressions for $L(A)$ and $L(B)$.

Exercise 3.4
Let A and B be respectively the following NFAs:



(a) Compute the coarsest stable refinements (CSR) of A and B.

(b) Construct the quotients of A and B with respect to their CSRs.

(c) Show that

$$L(A) = \{w \in \{a,b\}^* : w \text{ starts and ends with } a\}$$
$$L(B) = \{w \in \{a,b,c\}^* : w \text{ starts with } ac \text{ and ends with } ab\}$$

(d) Are the automata obtained in (b) minimal?

Exercise 3.5
★ Let msbf: $\{0,1\}^* \to \mathbb{N}$ be such that $\text{msbf}(w)$ is the number represented by w in the "most significant bit first" encoding. For example,

$$\text{msbf}(1010) = 10,\ \text{msbf}(100) = 4,\ \text{msbf}(0011) = 3.$$

For every $n \geq 2$, let us define the following language:

$$M_n = \{w \in \{0,1\}^* :\ \text{msbf}(w) \text{ is a multiple of } n\}.$$

(a) Show that M_3 has (exactly) three residuals, i.e. show that $|\{(M_3)^w : w \in \{0,1\}^*\}| = 3$.

(b) Show that M_4 has less than four residuals.

(c) Show that M_p has (exactly) p residuals for every prime number p. You may use the fact that, by Fermat's little theorem, $2^{p-1} \equiv 1 \pmod{p}$. [Hint: For every $0 \leq i < p$, consider the word u_i such that $|u_i| = p - 1$ and $\text{msbf}(u_i) = i$.]

Solution 3.1

- For $(ab+ba)^*$. We give the residuals as regular expressions: $(ab+ba)^*$ (residual with respect to ε); $b(ab+ba)^*$ (residual with respect to a); $a(ab+ba)^*$ (residual with respect to b); $\emptyset$ (residual with respect to aa). All other residuals are equal to one of these four.
- For $(aa)^*$. We give the residuals as regular expressions: $(aa)^*$ (residual of ε); $a(aa)^*$ (residual of a); $\emptyset$ (residual of b). All other residuals are equal to one of these three.
- For $\{a^nb^nc^n \mid n \geq 0\}$: Every prefix of a word of the form $a^nb^nc^n$ has a different residual. For all other words the residual is the empty set. There are infinitely many residuals.

Solution 3.2

(a) $L = \{ww \mid w \in \Sigma^*\}$. First we prove that L has infinitely many residuals by showing that for each pair of words of the infinite set $\{0^i1 \mid i \geq 0\}$ the corresponding residuals are not equal. Let $u = 0^i1, v = 0^j1 \in \Sigma^*$ two words with $i < j$. Then $L^u \neq L^v$ since $u \in L^u$, but $u \not\in L^v$. For the second half consider some arbitrary word w. Then $w \in L^w$, which shows the statement.

(b) We observe that for all languages satisfying that property L^w has to be non-empty for all w and thus also infinite. Furthermore all these languages are not regular, since there are infinitely many residuals.

$L = \{a^{2^n} \mid n \geq 0\}$. Let a^i and a^j two distinct words. W.l.o.g. we assume $i < j$. Let now d_i and d_j denote the distance from i and j to resp. closest larger square number. If $d_i < d_j$ holds, we are immediately done since $a^{d_i} \in L^{a^i}$ and $a^{d_i} \notin L^{a^j}$. $d_i > d_j$ is analogous. Thus assume $d_i = d_j$. Let us then define d'_i and d'_j denote the distance from i and j to resp. second closest larger square number. These have to be unequal, since the gaps between the square numbers are strictly increasing and we can repeat the argument from before.

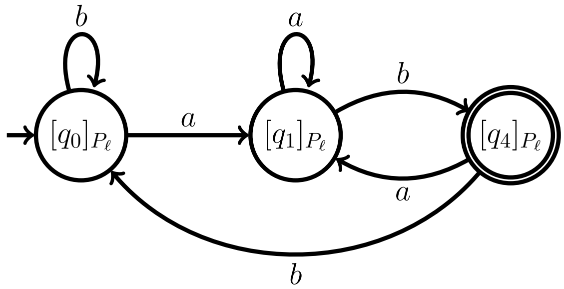
Solution 3.3

A) (a)

Iter.	Block to split	Splitter	New partition
0	—	—	$\{q_0,q_1,q_2,q_3,q_5,q_6\},\{q_4\}$
1	$\{q_0,q_1,q_2,q_3,q_5,q_6\}$	$(b,\{q_4\})$	$\{q_0,q_2,q_6\},\{q_1,q_3,q_5\},\{q_4\}$
2	none, partition is stable	—	—

The language partition is $P_\ell = \{\{q_0,q_2,q_6\},\{q_1,q_3,q_5\},\{q_4\}\}$.

(b)



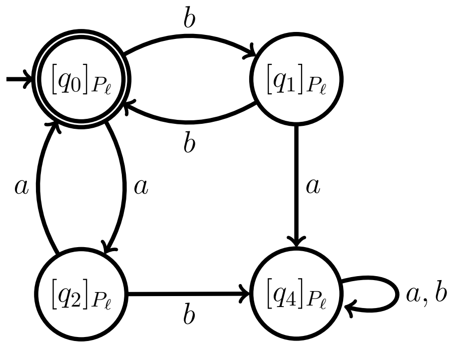
(c) $(a + b)^* ab$.

B) (a)

Iter.	Block to split	Splitter	New partition
0	—	—	$\{q_0, q_3\}, \{q_1, q_2, q_4\}$
1	$\{q_1, q_2, q_4\}$	$(b, \{q_1, q_2, q_4\})$	$\{q_0, q_3\}, \{q_1\}, \{q_2, q_4\}$
2	$\{q_2, q_4\}$	$(a, \{q_0, q_3\})$	$\{q_0, q_3\}, \{q_1\}, \{q_2\}, \{q_4\}$
3	none, partition is stable	—	—

The language partition is $P_\ell = \{\{q_0, q_3\}, \{q_1\}, \{q_2\}, \{q_4\}\}$.

(b)



(c) $(aa + bb)^*$ or $((aa)^*(bb)^*)^*$.

Solution 3.4

This exercise will appear in next week's tutorial.

Solution 3.5

Solutions will be given next week.