Technische Universität München **Winter term 21/22**
I7
Prof. J. Esparza / A. R. Balasubramanian / C. Weil-Kennedy

Automata and Formal Languages — Exercise Sheet 3

Exercise 3.1
For each of the following languages, determine if the number of its residuals is finite or not. If they are finite, state all of the residuals; Otherwise, give a proof that the number of residuals is infinite.

(a) $\{w \mid w$ does not have any two consecutive occurrences of $a\}$ over $\Sigma = \{a, b\}$

(b) $\{w \mid w \neq uu$ for any word $u\}$ over $\Sigma = \{a, b\}$

(c) $\{a^{2n} \mid n \geq 0\}$ over $\Sigma = \{a, b\}$

(d) $\{a^{n^2} \mid n \geq 0\}$ over $\Sigma = \{a\}$

Exercise 3.2
For any natural number $n \geq 2$, let $M_n = \{w \in \{0,1\}^* \mid w \in \text{MSBF}(k)$ and k is a multiple of $n\}$. (For the definition of the MSBF notation, see Tutorial sheet 1).

(a) Show that M_3 and M_5 have exactly 3 and 5 residuals respectively.

(b) Show that M_4 has strictly less than 4 residuals.

(c) What is the number of residuals that M_p has when p is a prime number? Can you assign an intuitive meaning behind each residual?

Exercise 3.3
Let $\Sigma = \{a, b\}$. Let L_k be the language $\{w\#w^R : w \in \Sigma^k\}$, where w^R is the reverse of w, e.g. $(abc)^R = cba$.

(a) Construct A_2, the minimal DFA such that $\mathcal{L}(A_2) = L_2$.

(b) What are the residuals of L_2? Assign them to the states of the DFA you gave for (a).

(c) Give a construction for a DFA that accepts L_k.

(d) How many states does the minimal DFA for L_k contain, for $k \geq 2$?

Exercise 3.4
★ We introduce a new notion of automata called *alternating automata*. An alternating automaton is a tuple $(Q, \Sigma, \delta, q_0, F)$ which is similar to the definition of a non-deterministic automaton, except now the finite set of states Q is partitioned into *existential* and *universal* states. We say that an existential state q accepts a word w (i.e., $w \in L(q)$) if $w = \varepsilon$ and $q \in F$ or $w = aw'$ and *there exists* a transition (q, a, q') such that q' accepts w'. Similarly, we say that a universal state q accepts a word w if $w = \varepsilon$ and $q \in F$ or $w = aw'$ and *for every* transition (q, a, q') the state q' accepts w'. The language recognized by an alternating automaton is the set of words accepted by its initial state.

Give an algorithm that transforms an alternating automaton into a DFA recognizing the same language.

Solution 3.1

- For $\{w \mid w$ does not have any two consecutive occurrences of $a\}$: Notice that this is the same as the language given by the regular expression $(ab+b)^*$. We give the residuals as regular expressions: $(ab+b)^*$ (residual of ε); $b(ab+b)^*$ (residual of a); $\emptyset$ (residual of aa). All other residuals are equal to one of these three.

- For $L = \{w \mid w \neq uu$ for any word $u\}$ over $\Sigma = \{a, b\}$: The number of residuals is infinite. To prove this, notice that if $m < n$, then the words $a^m b$ and $a^n b$ have different residues over M, because $a^m b a^m b \notin L$ but $a^n b a^m b \in L$.

- For $\{a^{2n} \mid n \geq 0\}$: 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 $\{a^{n^2} \mid n \geq 0\}$: Each word has a distinct residual. Indeed, let a^i and a^j be two words with $i < j$. Let d_i (resp. d_j) be the smallest number such that $i + d_i$ (resp. $j + d_j$) is a perfect square. If $d_i < d_j$ then $a^{i+d_i} \in L$, but $a^{j+d_i} \notin L$. Similarly for the case of $d_i > d_j$. Suppose $d_i = d_j$. Then let e_i (resp. e_j) be the *second* smallest number such that $i + e_i$ (resp. $j + e_j$) is a perfect square. We claim that $e_i \neq e_j$.

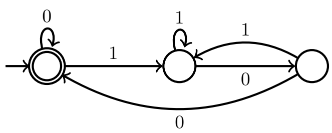
  Indeed, by assumption $i + d_i$ and $j + d_i$ are both perfect squares which we shall denote respectively by n^2 and m^2. Since $i < j$, $n \neq m$. Then, notice that $(n+1)^2 - n^2 = 2n + 1$ and $(m+1)^2 - m^2 = 2m + 1$. Hence e_i must be $d_i + 2n + 1$ and e_j must be $d_i + 2m + 1$. It then follows that $e_i \neq e_j$ and so we can use the same argument as for the case of $d_i \neq d_j$ to conclude that a^i and a^j have different residuals.

Solution 3.2

- We have already seen in the first tutorial sheet that there is a DFA for M_3 with 3 states. The same DFA can be generalized to get a DFA with 5 states for M_5. (See the solution for the last subproblem of this problem for an explicit construction of such a DFA). This shows that M_3 and M_5 can have at most 3 and 5 residuals respectively.

  Notice that M_3 has different residuals with respect to 0, 1 and 10. Indeed, $0\varepsilon \in M_3$ while $1\varepsilon, 10\varepsilon \notin M_3$ and $11 \in M_3$ while $101 \notin M_3$. Similarly, we can show that M_5 has different residuals with respect to 0, 1, 10, 11 and 100. This shows that M_3 and M_5 have exactly 3 and 5 residuals respectively.

- Here is a DFA for M_4 with 3 states. This is the same DFA as given in the first tutorial sheet except both the final states are merged into a single state.

  This shows that the number of residuals for M_4 must be at most 3.

- If p is a prime number, then the number of residuals of M_p must be p. Indeed, we can generalize the DFA given in the first tutorial sheet for M_3 to get a DFA with p states for M_p. This DFA is given by $A_p = (Q_p, \{0,1\}, \delta_p, 0, \{0\})$ where

$$Q_p = \{0, 1, \ldots, p-1\},$$
$$\delta_p(q, b) = (2q + b) \bmod p \quad \text{for every } q \in Q_p \text{ and } b \in \{0, 1\}.$$

  Hence, M_p has at most p residuals. We now show that M_p has at least p residuals. For a word $w \in \{0,1\}^*$, let $\text{msbf}(w)$ denote the number n such that $w \in \text{MSBF}(n)$.

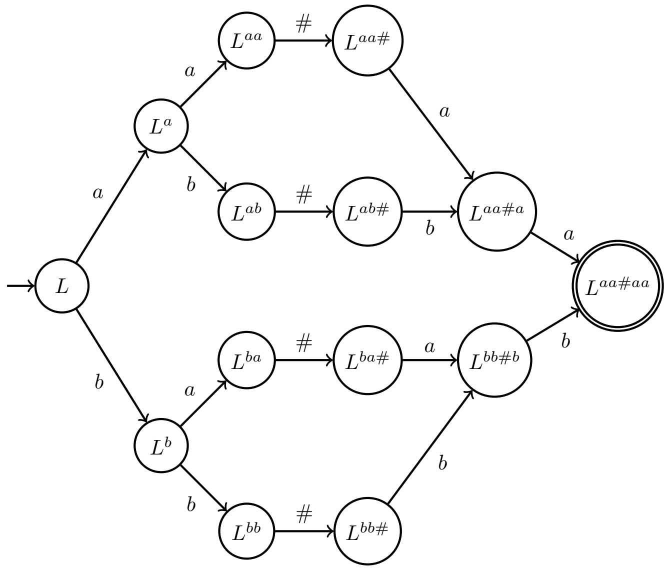
  For every $0 \leq i < p$, let u_i be a word such that $\text{msbf}(w) = i$ and $|u_i| = p - 1$. Note that such an u_i exists since the smallest encoding of i has at most $p - 1$ bits, and it can be extended to length $p - 1$ by padding with zeros on the left. Let us show that the u_i-residual and u_j-residual of M_p are distinct for every $0 \leq i, j < p$ such that $i \neq j$. Let $0 \leq k < p$, and let $\ell = (p - i) \bmod p$. We have:

$$\begin{aligned}
\text{msbf}(u_k u_\ell) &= 2^{|u_\ell|} \cdot \text{msbf}(u_k) + \text{msbf}(u_\ell) \\
&= 2^{p-1} \cdot k + ((p-i) \bmod p) \\
&\equiv k + ((p-i) \bmod p) && \text{(by Fermat's little theorem)} \\
&\equiv k + p - i \\
&\equiv k - i
\end{aligned}$$

Let $0 \leq i, j < p$ be such that $i \neq j$. We have $u_i u_\ell \in M_p$ since $\text{msbf}(u_i u_\ell) \equiv i - i \equiv 0$, but we have $u_j u_\ell \notin M_p$ since $\text{msbf}(u_j u_\ell) \equiv j - i \not\equiv 0$. Therefore, the u_i-residual and u_j-residual of M_p are distinct.

Solution 3.3

(a) The trap state is omitted for the sake of readability:



(b) We have $L_2 = \{aa\#aa, ab\#ba, ba\#ab, bb\#bb\}$. We compute the residuals L^w for all words w by increasing length of w.

- $|w| = 0$: $L^\varepsilon = \{aa\#aa, ab\#ba, ba\#ab, bb\#bb\}$.
- $|w| = 1$: $L^a = \{a\#aa, b\#ba\}$ and $L^b = \{a\#ab, b\#bb\}$.
- $|w| = 2$: $L^{aa} = \{\#aa\}$, $L^{ab} = \{\#ba\}$, $L^{ba} = \{\#ab\}$ and $L^{bb} = \{\#bb\}$.
- $|w| = 3$: $L^{aa\#} = \{aa\}$, $L^{ab\#} = \{ba\}$, $L^{ba\#} = \{ab\}$ and $L^{bb\#} = \{bb\}$.
- $|w| = 4$: $L^{aa\#a} = \{a\} = L^{ab\#b}$, and $L^{ba\#a} = \{b\} = L^{bb\#b}$.
- $|w| \geq 5$: $L^w = \begin{cases} \{\varepsilon\} & \text{if } w \in L_k, \\ \emptyset & \text{otherwise.} \end{cases}$

(c) Notice that L_{k+1} is simply $aL_k a + bL_k b$ for any $k \geq 2$. Using this observation, we generalize the construction given in (a) for $k = 2$, by induction on k. The base case of $k = 2$ has been done already. Suppose we have already constructed $A_k = (Q_k, \{a, b, \#\}, \delta_k, q_0^k, q_f^k)$ with the property that it has exactly one initial state and one final state and one trap state $trap_k$ (Note that A_2 satisfies this property). We now construct $A_{k+1} = (Q_{k+1}, \{a, b, \#\}, \delta_{k+1}, q_0^{k+1}, q_f^{k+1})$ as follows:

The set of states Q_{k+1} is taken to be $\{q_0^{k+1}, q_f^{k+1}, trap_{k+1}\} \cup ((Q_k \setminus \{trap_k\}) \times \{1, 2\})$, where $q_0^{k+1}, q_f^{k+1}, trap_{k+1}$ are three fresh states. Intuitively we add a fresh initial state, a fresh final state, a fresh trap state and take two *copies* of the states of A_k while removing $trap_k$.

The transition function δ_{k+1} is defined as follows:

- $\delta_{k+1}(q_0^{k+1}, a) = (q_0^k, 1)$ and $\delta_{k+1}(q_0^{k+1}, b) = (q_0^k, 2)$. Intuitively, upon reading an a (resp. b) from the initial state of A_{k+1}, we move to the initial state of the first (resp. second) copy of A_k.
- $\delta_{k+1}(q_f^k, a) = q_f^{k+1}$ and $\delta_{k+1}(q_f^k, b) = q_f^{k+1}$. Intuitively, upon reading an a (resp. b) from the final state of the first (resp. second) copy of A_{k+1}, we move to the final state of of A_{k+1}.
- $\delta_{k+1}((q, i), a) = p$ where $p = (\delta_k(q, a), i)$ if $\delta_k(q, a) \neq trap_k$ and otherwise $p = trap_{k+1}$. Intuitively, within a copy of A_k, we follow the transitions of A_k and stay within that copy itself if the state that we are supposed to go to is not the trap state of A_k. Otherwise, instead of going to the trap state of A_k, we go to the trap state of A_{k+1}.

We can now prove by induction on the length of the word that A_{k+1} is a DFA for L_{k+1}.

(d) Note that if $f(k)$ is the number of states that A_k has, (where A_k is the DFA defined in the previous subproblem), then $f(2) = 15$ and $f(k+1) = 2(f(k)-1)+3 = 2f(k)+1$. Solving this, we get $f(k) = 2^{k+2}-1$. We claim that A_k is a minimal DFA, by induction on k. The base case of $k = 2$ is already done. For the induction step, suppse p, q are two distinct states of A_{k+1}. We will show that $L_{A_{k+1}}(p) \neq L_{A_{k+1}}(q)$.

Notice that the initial state q_0^{k+1} recognizes only strings of length $2k+3$ and the final state q_f^{k+1} recognizes only ϵ, whereas the other states of A_{k+1} do not recognize any of these strings. This implies that the languages of the initial and the final states are different from the rest. Similarly, the language of the trap state is also different from the rest.

Hence, we can assume that $p = (p', i)$ and $q = (q', j)$ for some $p', q' \in Q_k$ and some $i, j \in \{1, 2\}$. If $i \neq j$, then p and q belong to different copies of A_k. Let $i = 1$ and $j = 2$. Notice that $L_{A_{k+1}}(p) = L_{A_k}(p')a$ and $L_{A_{k+1}}(q) = L_{A_k}(q')b$. Hence $L_{A_{k+1}}(p) \neq L_{A_{k+1}}(q)$.

The only case left is when $i = j$. In this case notice that $L_{A_{k+1}}(p) = L_{A_k}(p')c$ and $L_{A_{k+1}}(q) = L_{A_k}(q')c$ where c is either a or b, depending on whether i is 1 or 2. By induction hypothesis, A_k is the minimal DFA for L_k and so $L_{A_k}(p')$ and $L_{A_k}(q')$ are different. Hence $L_{A_{k+1}}(p) \neq L_{A_{k+1}}(q)$, thereby concluding the proof.

Solution 3.4

Let $A = (Q, \Sigma, \delta, q_0, F)$ be the given alternating finite-state automaton (AFA) and let $Q = Q_\exists \cup Q_\forall$ be a partition of Q into existential and universal states.

Notice that when $Q_\forall$ is empty, this AFA is just an NFA and so we can use the powerset construction to get a corresponding DFA. Further, notice that when $Q_\exists$ is empty, we can still perform the powerset construction except we now set the set of final states to be $\{T : T \subseteq F\}$, instead of the usual $\{T : T \cap F \neq \emptyset\}$ as in the case of NFA.

Now we consider the general case. From the given AFA A, we will construct an NFA recognizing the same language. This suffices, because we know how to translate an NFA into a DFA. To construct an equivalent NFA, we once again do a powerset construction $A' = (2^Q, \Sigma, \delta', \{q_0\}, F')$, except now the transition function $\delta' : 2^Q \times \Sigma \to 2^{2^Q}$ is slightly more complex: We let $T \in \delta'(S, a)$ iff $T \subseteq \cup_{s \in S} \delta(s, a)$ and T satisfies the following two constraints:

- For every existential state p of S, there is exactly one state q of $\delta(p, a)$ such that $q \in T$
- For every universal state p of S, for every state q of $\delta(p, a)$, we have $q \in T$

Intuitively, for the universal states, the transition relation is defined in a manner which is similar to the usual powerset construction, because we want to take into account all possible transitions from that state. But for the existential states, we allow exactly one successor in the transition relation, because we only want to check if there is a transition from this state which can lead to a final state.

We finally set F' to be $F' := \{T : T \subseteq F\}$. We can now argue by induction on the length of a word w to show that for any subset S of Q, the word w is accepted by all the states of S in the automaton A iff the word w is accepted by the state S in the automaton A'. This then finishes the proof.