Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
Electronic Notes in Theoretical Computer Science 223 (2008) 187–200
www.elsevier.com/locate/entcs

The Length of Subset Reachability in Nondeterministic Automata

Pavel Martyugin[1]

Department of Mathematics and Mechanics
Ural State University
620083 Ekaterinburg, Russia

Abstract

We study subset reachability in nondeterministic finite automata and look for bounds of the length of the shortest reaching words for automata with a fixed number of states. We obtain such bounds for nondeterministic automata over 2-letter, 3-letter and arbitrary alphabets.

Keywords: Reachability, Synchronization, Nondeterministic Automata

1 Introduction

A ***nondeterministic finite automaton*** (***NFA***) is a triple $\mathscr{A} = (Q, \Sigma, \delta)$ such that Q is a finite set of states, Σ is a finite alphabet, and δ is a transition function. The function δ maps the set $Q \times \Sigma$ to the set 2^Q where 2^Q is a set of all subsets of the set Q. If $q \in Q$, $a \in \Sigma$, and $\delta(q, a) = P \subseteq Q$, we write $P = q.a$. Let Σ^* be the Σ-generated free monoid whose identity element (the empty word) is denoted by λ. The function δ can be naturally extended to the set $2^Q \times \Sigma^*$. Let $S \subseteq Q$, $a \in \Sigma$, then we put $S.a = \bigcup_{q \in S} q.a$. We also put $S.\lambda = S$. Let $S \subseteq Q$, $w \in \Sigma^*$, $w = ua$ and the set $S.u$ is defined, then we put $\delta(S, w) = S.w = S.u.a$.

Let $\mathscr{A} = (Q, \Sigma, \delta)$ be an NFA, $S, T \subseteq Q$, $w \in \Sigma^*$, and $S.w = T$. In this case we say that the set T is ***reachable*** from the set S in the automaton $\mathscr{A}$ and w is a ***reaching*** word.

If an NFA has only one letter, then it is just a directed graph. In this case reachability describes an 'infection' model in the graph. Let $\Gamma = (Q, E)$, where $E \subseteq Q \times Q$, be a directed graph. Suppose that at some initial moment $\tau = 0$

[1] martugin@mail.ru

doi:10.1016/j.entcs.2008.12.039

of discrete time τ some vertices $q \in Q$ get marked ('infected'). Now assume that marks propagate according to the following rule: a vertex $v \in Q$ gets a mark at the moment $\tau = i+1$ if and only if there exists an arrow $(u, v) \in E$ such that the vertex u was infected at the moment $\tau = i$. The following picture shows the evolution of 'infection' in a simple example. Initially only one vertex was marked but soon, more precisely, in three steps the whole graph has become infected. The process of the graph infection can be interpreted as a reachability of the set Q from one-element subset $S \subseteq Q$.

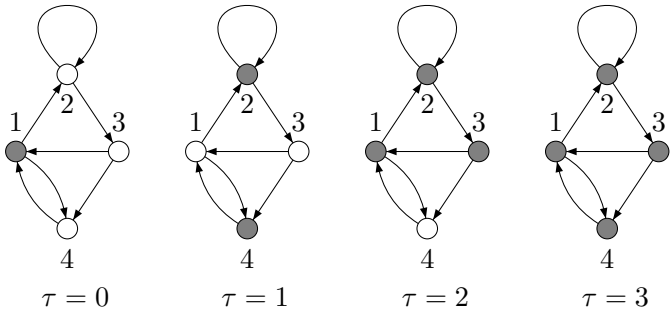

Fig. 1. Evolution of markings in a graph

One can think of the described model as of a version of Conway's Game of Life with rather simplified rules and a finite but arbitrarily complex gameboard. Our model also admits quite a natural interpretation in terms of the spread of e-mail viruses on networks, which is certainly a problem of both practical and theoretical interest. Indeed, imagine the directed graph whose vertices are, say, Microsoft Outlook Express users and whose arrows are pairs (B, C) of users such that the e-mail address of C is stored in the address book of B and also loops (B, B) for all users who do not use an appropriate anti-virus software. Many e-mail viruses propagate by using the following mechanism: when such a virus arrives at the computer of a user B, it immediately starts sending itself to all addresses that if finds in the infected computer. In this active phase, the virus can be detected and deleted by the corresponding anti-virus software provided the user B had installed some; if B had not taken care of protecting her or his computer, the latter stays infected forever and keeps infecting its 'neighbors' in the described graph. It is easy to see that the rule of our model formalizes exactly this propagation mechanism.

The natural question is the following one: how fast can such an 'epidemic' spread over a graph with a given number of vertices. The following theorem can be proved.

Theorem 1.1 *Let $\Gamma = (Q, E)$ be a directed graph with a marked vertex and $|Q| = n$. If marks can propagate over the whole set Q, then the propagation completes in at most $(n-1)^2 + 1$ steps. This bound is tight in the sense that for each $n > 1$ there exists a directed graph $\Gamma = (Q, E)$ with $|Q| = n$ such that marks can propagate from a certain vertex to Q and the propagation takes exactly $(n-1)^2 + 1$ steps.*

This theorem was discovered many times in different formulations. A proof can be found for instance in [7] or [2]. There the authors considered the following problems. Let M be a matrix of size $n \times n$ with nonnegative real elements. The

matrix M is called ***primitive*** if there exists an integer $p > 0$ such that all elements of M^p are positive. The question is: how large can be minimal $p > 0$ for primitive matrix M of size $n \times n$ such that all elements of matrix M^p are positive. The example of a primitive matrix is the adjacency matrix of a directed graph $G = (Q, E)$ such that the set Q is reachable from any one-element subset $q \subseteq Q$. The following theorem is equivalent to Theorem 1.1.

Theorem 1.2 *If M is a primitive matrix of size $n \times n$, then for $p \leq (n-1)^2 + 1$ all elements of M^p are positive. This bound is tight in the sense that for each $n > 1$ there exists a matrix M of size $n \times n$ such that $p = (n-1)^2 + 1$ is a smallest number with property that M^p contains only positive elements.*

The reachability in NFA containing more than one letter is thus a natural generalization of the reachability in directed graphs. We can also consider the infection of NFA. Let $\mathscr{A} = (Q, \Sigma, \delta)$ be a NFA and $q \in Q$. The question is how long can be the shortest word w such that $q.w = Q$. In this paper we consider not only reachability of the set Q from one-element subsets but also reachability of some subset $T \subseteq Q$ from some subset $S \subseteq Q$.

Even though the above interpretation may look quite attractive, it would be fair to say that our original motivation has come from a different source, namely, from the theory of synchronizing automata. Recall that a deterministic finite automaton (DFA) $A = \langle Q, \Sigma, \delta \rangle$ is said to be ***synchronizing*** (or ***directable***) if there exists a word $w \in \Sigma^+$ whose action resets A, that is, brings all states to a particular one: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. It is rather natural to ask how long such a ***reset*** (or ***directing***) word may be. Černý conjectured in [1] that for any synchronizing automaton A there exists a reset word of length $(|Q| - 1)^2$. Although being confirmed in some special cases, this simply looking conjecture still constitutes an open problem. Surveys of results concerning synchronizing words can be found in [5] or [6].

One can conveniently think of any DFA $A = \langle Q, \Sigma, \delta \rangle$ as a board for a solitaire-like game. Each letter $a \in \Sigma$ defines a move via the following rule: if tokens had covered certain subset S of the state set Q before the move corresponding to a then, after the move, tokens cover states from the set $\{\delta(q, a) \mid q \in S\}$. The initial position is such that every state in Q is covered by a token. Then synchronizing automata can be characterized as automata for which a sequence of moves collects all tokens on a single state, and the shortest reset word is nothing but the shortest sequence of moves with this property. This game viewpoint has proved to be useful, especially when constructing examples of 'slowly' synchronizing automata.

Now consider the ***reversal*** of A, that is, the non-deterministic automaton (NFA) $A^{rev} = \langle Q, \Sigma, \delta^{-1} \rangle$ where $\delta^{-1}(q, a) = \{q' \mid \delta(q', a) = q\}$. Clearly, the above solitaire game on A corresponds to an 'anti-solitaire' game on A^{rev} in which the move corresponding to a given letter a makes tokens propagate along the arrows labelled a (tokens may multiply if necessary). The reversals of synchronizing automata can be then characterized as automata for which a sequence of moves distributes tokens over the whole state set from a single state, and the shortest reset word for A co-

incides with the reversal of the shortest move sequence with the latter property for A^{rev}. Thus, studying the above anti-solitaire game on non-deterministic automata may be considered as an approach to the Černý conjecture and generalizations of the conjecture to the non-deterministic case (see [4] and [3, Chapter 8] for a discussion of such generalizations). At the same time the 'anti-solitaire' game is a model of reachability of the set Q from some one-element set.

The reachability in NFA can be described using a token model too. Let $\mathscr{A} = (Q, \Sigma, \delta)$ be an NFA, $S, T \subseteq Q$, and $w \in \Sigma^*$. Let at the start time there is a token on any state from the set S. We apply the letters of the word w step by step. The action of any letter $a \in \Sigma$ splits the token from the state q into $|\delta(q, a)|$ parts. After that, it moves these parts to the states of the set $\delta(q, a)$. If two tokens arrive to one state, then one of them removes. If a subset of states with tokens is equal to T after the action of the word w, then the set T is reachable from the set S.

We are ready to formulate the main problem discussed in the paper (an analogue of the Černý's problem). Let a finite set Q and its subsets $S, T \subseteq Q$ be fixed. Consider all NFAs $\mathscr{A} = (Q, \Sigma, \delta)$ such that the set T is reachable from the set S in $\mathscr{A}$. Denote by $d_{\mathscr{A}}(S, T)$ the length of the shortest word reaching the set T from the set S in the NFA $\mathscr{A}$. If there is no word u such that $S.u = T$, then we put $d_{\mathscr{A}}(S, T) = -\infty$. We study the maximal size of the value $d_{\mathscr{A}}(S, T)$ for fixed sets Q, fixed subsets $S, T \subseteq Q$, and an arbitrary NFA $\mathscr{A} = (Q, \Sigma, \delta)$. Define two values:

$$\omega(Q, S, T) = \max\{d_{\mathscr{A}}(S, T) | \mathscr{A} = (Q, \Sigma, \delta) \text{ is a NFA}\},$$

$$\omega^k(Q, S, T) = \max\{d_{\mathscr{A}}(S, T) | \mathscr{A} = (Q, \Sigma, \delta) \text{ is a NFA}, |\Sigma| = k\}.$$

We call these values the length of reachability and the length of k-reachability of the set T from the set S in the set Q. In this paper we obtain bounds for the values $\omega(Q, S, T)$ and $\omega^k(Q, S, T)$ for $k \geq 2$. Let $|Q| = n$. First we prove that $\omega(Q, S, T) = 2^n - 2$ for $T \notin \{\varnothing, Q, S\}$, and $\omega(Q, S, \varnothing) = 2^n - 1$ (Theorem 2.1). Then we show that $\omega(Q, S, Q) \geq 3^{\lfloor (n-1)/3 \rfloor}$ for $1 \leq |S| < n - 2$ (Theorem 2.2). We also prove that the minimum value of $\omega^3(Q, S, T)$ for fixed Q and arbitrary $S, T \subseteq Q, S \notin \{T, \varnothing\}$ as a function of $|Q| = n$ grows faster than any polynomial in n (Theorem 3.1). Moreover, we prove that the value $\omega^2(Q, S, T)$ for 'not very large' subsets T is greater than some function of $|Q| = n$ which grows faster than any polynomial in n (Theorem 3.2).

For the sequel, we need some notation. For a word $w \in \{a, b\}^*$, we denote by $|w|$ the length of w and by $w[i]$, where $1 \leq i \leq |w|$, the i^{th} letter in w from the left. If $1 \leq i \leq j \leq |w|$, we denote by $w[i, j]$ the word $w[i] \cdots w[j]$.

2 Automata over an arbitrary alphabet

Here we find the value $\omega(Q, S, T)$. The idea of the proof of the following theorem was used in [4] to prove a lower bound of the length of the shortest D_1-synchronizing words. We use it in a more general setting.

Theorem 2.1 *Let Q be a finite set, $|Q| = n$. Let S be a non-empty subset of Q and T a subset of Q such that $T \neq Q, \varnothing, S$. Then*

1) $\omega(Q, S, T) = 2^n - 2$;
2) $\omega(Q, S, \varnothing) = 2^n - 1$.

Proof. Let $\mathscr{A} = (Q, \Sigma, \delta)$ be a NFA. Recall that we denote by $d_{\mathscr{A}}(S, T)$ the length of the shortest word w such that $\delta(S, w) = T$. Let us first prove that $d_{\mathscr{A}}(S, T) \leq 2^n - 2$. Suppose by a contradiction that $d_{\mathscr{A}}(S, T) = m > 2^n - 2$. Let $w \in \Sigma$ be a word such that $S.w = T$ and $|w| = m > 2^n - 2$. Consider the sets $S.w[1, i]$, $i \in \{0, \ldots, m\}$. Each of them is not empty. The set Q contains only $2^n - 1$ distinct nonempty subsets. Therefore there exist numbers $i_1, i_2 \in \{0, \ldots, m\}, i_1 < i_2$ such that $S.w[1, i_1] = S.w[1, i_2]$. In this case $S.w[1, i_1][i_2 + 1, m] = T$ and $d_{\mathscr{A}}(S, T) \leq m - (i_2 - i_1) < m$. This is a contradiction. Thus $d_{\mathscr{A}}(S, T) \leq 2^n - 2$. The inequality $d_{\mathscr{A}}(S, \varnothing) \leq 2^n - 1$ can be proved by the same way.

Now we construct an NFA $\mathscr{A}_{nfa} = (Q, \Sigma, \delta)$ such that $d_{\mathscr{A}_{nfa}}(S, T) = 2^n - 2$. Let $P_0, \ldots, P_{2^n-2}$ be the distinct nonempty subsets of the set Q listed such that $P_0 = S$, $P_1 = Q$, $P_{2^n-2} = T$, and $|P_1| \geq |P_2| \geq \ldots \geq |P_{2^n-3}| = 1$. In the case of $S = Q$, we put $P_0 = Q$ and $|P_0| \geq |P_1| \geq \ldots \geq |P_{2^n-3}| = 1$. Now we take the alphabet $\Sigma = \{a_1, \ldots, a_{2^n-2}\}$ and, for each $i \in \{1, \ldots, 2^n - 2\}$, define

$$\delta(q, a_i) = \begin{cases} P_i \text{ if } q \in P_{i-1}, \\ Q \text{ if } q \notin P_{i-1}. \end{cases}$$

Let $w = a_1 \ldots a_{2^n-2}$. We have $S.a_1 \ldots a_i = P_i$ for $i \in \{1, \ldots, 2^n - 2\}$. Therefore $S.a_1 \ldots a_{2^n-2} = T$. We are going to prove that w is the shortest word such that $\delta(S, w) = T$. Let $u \in \Sigma^*$ be one of the shortest words such that $S.u = T$. Arguing by a contradiction, suppose $|u| < |w|$. Note that the word u can not be equal to $w[1, j]$ for some $j < |w|$ because $S.w[1, j] = P_j \neq T$. Let $k = \min\{j | w[j] \neq u[j]\}$. Consider the set $S.u[1, k]$. We have

$$S.u[1, k] = \begin{cases} P_i \text{ if } \exists i \in \{1, \ldots, 2^n - 2\},\ u[k] = a_i,\ S.u[1, k-1] \subseteq P_{i-1}, \\ Q \text{ otherwise.} \end{cases}$$

The set $S.u[1, k-1] = P_{k-1}$ can be a subset of P_{i-1} only if $k - 1 \geq i - 1$ (otherwise $|P_{k-1}| \geq |P_{i-1}|$). In this case $S.u[1, k-1].u[k] = S.u[1, k-1].a_i = P_i$. Therefore $S.u = S.u[1, i-1].u[k, |u|]$, and the word u is not the shortest reaching word. If $S.u[1, k] = Q$, then $S.u = S.u[1].u[k+1, |u|]$ (if $S = Q = P_0$, then $S.u = S.u[k+1, |u|]$). Again, in this case the word u is not the shortest reaching word. Hence $d_{\mathscr{A}_{nfa}}(S, T) \leq 2^n - 2$ and $\omega(Q, S, T) = 2^n - 2$.

It is enough to construct the automaton $\mathscr{A}_{nfa}$ and put $T = \varnothing$ for proving $\omega(Q, S, \varnothing) = 2^n - 1$. In this case the sequence of sets P_i contains all 2^n subsets of the set Q. Hence the shortest word reaching the empty set from the set S has length $2^n - 1$. The theorem is proved. □

Note that the case of $T = Q$ was not considered in Theorem 1. This case is more complicated, but we still can prove that the value $\omega(Q, S, Q)$ is exponential in $|Q|$ for any subset $S \subset Q$.

Theorem 2.2 *Let Q be a finite set, $|Q| = n$. If S is a subset of Q such that $1 \leq |S| < n-2$, then $\omega(Q, S, Q) \geq 3^{\lfloor (n-1)/3 \rfloor}$.*

Proof. Let n be equal to $3k+1$ for some integer k (one or two states can be added to obtain a similar construction for $n \neq 3k+1$). We put $k = (n-1)/3$. We are going to construct a NFA $\mathscr{B}_{nfa} = (Q, \Sigma, \delta)$. By definition, put

$$Q = \{q(m,i) | m \in \{0,1,2\}, i \in \{1,\ldots,k\}\} \cup \{start\}, \quad \Sigma = \{a_1, \ldots, a_k, b, c\}.$$

Let $i \in \{1,\ldots,k\}$, then by definition, put
$\delta(start, b) = \{q(0,j) \mid j \in \{1,\ldots,k\}\}$; for $q \neq start$, $\delta(q,b) = \varnothing$;
$\delta(start, c) = \varnothing$; for $\delta(q(0,i),c) = \delta(q(1,i),c) = \varnothing$;

$$\delta(q(2,i), c) = \{q(0,i), q(1,i), q(2,i), start\}.$$

Let $i, p \in \{1,\ldots,k\}$ and $m \in \{0,1,2\}$, then

$$\delta(q(m,i), a_p) = \begin{cases} \{q(m,i)\}, & p > i \\ \{q(m+1,i)\}, & p = i, m < 2 \\ \varnothing, & p = i, m = 2 \\ \varnothing, & p < i, m < 2 \\ \{q(0,i)\}, & p < i, m = 2 \end{cases}.$$

$$\delta(start, a_1) = \ldots = \delta(start, a_k) = start,$$

We have $1 \leq |S| < n-2$. Hence we can assume that $S \subseteq Q \backslash \{q(0,1), q(1,1), q(2,1)\}$ and $start \in S$. The automaton $\mathscr{B}_{nfa}$ for $k = 3$ is shown in Fig. 2. The action of the letters $a_1, \ldots, a_k$ in the automaton $\mathscr{B}_{nfa}$ can be thought of as the ternary counter of k-digit integers.

We construct a word w such that $S.w = Q$. First we define words $v_1, \ldots, v_k$. Let $v_1 = a_1^2$. Assume the word v_i is already defined, then by definition, put $v_{i+1} = v_i a_{i+1} v_i a_{i+1} v_i$. We prove that the word $w = b v_k c$ is the shortest word such that $S.w = Q$.

Let $i \in \{1,\ldots,k\}$. Notice that $S.b = \{q(0,1), \ldots, q(0,k)\}$. Inducting on i one can obtained $S.bv_i = \{q(2,1), \ldots, q(2,i)\} \cup \{q(0,i+1), \ldots, q(0,k)\}$. Therefore $Q.bv_kc = \{q(2,1), \ldots, q(2,k)\}.c = Q$. By the construction, $|v_1| = 2$, $|v_{i+1}| = 3 \cdot |v_i| + 2$. Hence $|v_k| = 3^k - 1$, $|w| = 3^k + 1 = 3^{n/3} + 1$.

We are going to prove that no word of length less then $|w|$ reaches the set Q from the set S. Denote by Q_i the set $\{q(0,i), q(1,i), q(2,i)\}$ for $i \in \{1,\ldots,k\}$. Let us define the weight $\mu(P)$ for any subset $P \subseteq Q$. Suppose $P_i \subseteq Q_i$ for some

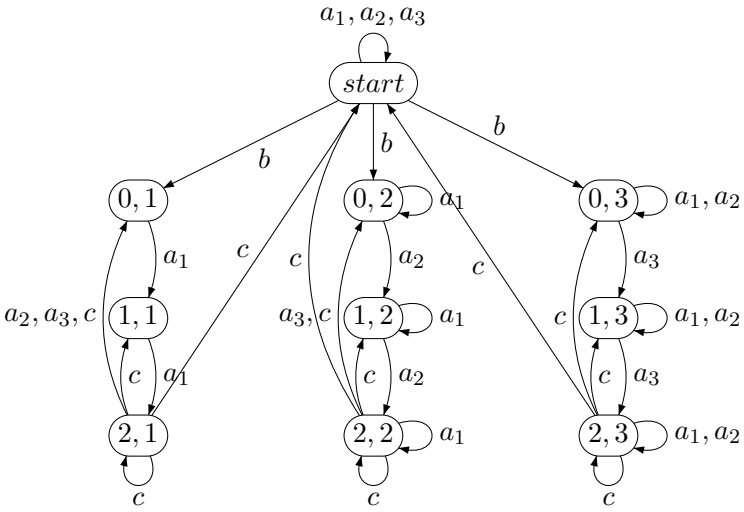

Fig. 2. The automaton $\mathscr{B}_{nfa}$ for $k = 3$

$i \in \{1, \ldots, k\}$. By definition, put

$$\mu(P_i) = \begin{cases} 2 \cdot 3^{i-1} & \text{if } q(2,i) \in P_i, \\ 3^{i-1} & \text{if } q(2,i) \notin P_i,\ q(1,i) \in P_i, \\ 0 & \text{if } q(2,i) \notin P_i,\ q(1,i) \notin P_i,\ q(0,i) \in P_i, \\ -\infty & \text{if } q(2,i) \notin P_i,\ q(1,i) \notin P_i,\ q(0,i) \notin P_i. \end{cases}$$

Let $Q_0 = \{start\}$ and $P_0 \subseteq Q_0$. By definition, put $\mu(P_0) = \begin{cases} 1 \text{ if } P_0 = \{start\}, \\ 0 \text{ if } P_0 = \varnothing. \end{cases}$
An arbitrary subset $P \subseteq Q$ is the union of the sets $P_i = P \cap Q_i$, $i \in \{0, \ldots, k\}$. We put $\mu(P) = \mu(P_0) + \ldots + \mu(P_k)$.

Suppose $\alpha \in \Sigma^*$ and $P \subseteq Q$. We prove that if $\mu(P) = -\infty$, then $\mu(P.\alpha) \leq 0$; if $\mu(P) \geq 0$, then $\mu(P.\alpha) \leq \mu(P) + 1$.

First suppose $\mu(P) = -\infty$. In this case there is $i \in \{1, \ldots, k\}$ such that $P_i = P \cap Q_i = \varnothing$.

- If $\alpha \in \{a_1, \ldots, a_k, c\}$, then $P.\alpha \cap Q_i = \varnothing$ and $\mu(P.\alpha) = -\infty$.
- Assume $\alpha = b$.
  · If $start \in P$, then $P.b = \{q(0,1), \ldots, q(0,k)\}$ and $\mu(P.b) = 0$,
  · If $start \notin P$, then $P.b = \varnothing$ and $\mu(P.b) = -\infty$.

Suppose $\mu(P) \geq 0$.

- Assume $\alpha = b$.
  · If $start \in P$, then $P.b = \{q(0,1), \ldots, q(0,k)\}$ and $\mu(P.b) = 0$,
  · If $start \notin P$, then $P.b = \varnothing$ and $\mu(P.b) = -\infty$.
- Assume $\alpha = c$.

- If $\{q(2,1),\dots,q(2,k)\} \subseteq P$, then
  if $start \notin P$, then $\mu(P) = 3^k - 1$ and $P.\alpha = Q$, therefore, $\mu(P.\alpha) = 3^k$;
  if $start \in P$, then $\mu(P) = 3^k$ and $P.\alpha = Q$, therefore, $\mu(P.\alpha) = 3^k$.
- If $\{q(2,1),\dots,q(2,k)\} \nsubseteq P$, then there exists $i \in \{1,\dots,k\}$ such that $q(2,i) \notin P$, in this case $P.\alpha \cap Q_i = \varnothing$ and $\mu(P.\alpha) = -\infty$.

• Assume $\alpha = a_i$ for some $i \in \{1,\dots,k\}$. In this case for $j \in \{i+1,\dots,k\}$, $P.\alpha \cap Q_j = P \cap Q_j$.
- Let $\{q(2,1),\dots,q(2,i-1)\} \subseteq P$, then for $j \in \{1,\dots,i-1\}$, $P.\alpha \cap Q_j = \{q(0,j)\}$.
- If $q(2,i) \notin P$, $q(1,i) \notin P$ and $q(0,i) \in P$, then $\{q(1,i)\} \subseteq P.\alpha \cap Q_i$ and $\mu(P.\alpha) = (\mu(P) - 2 - 2\cdot 3 - \ldots - 2\cdot 3^{i-2}) + 3^{i-1} = \mu(P) + 1$.
- If $q(2,i) \notin P$ and $q(1,i) \in P$, then $\{q(2,i)\} \subseteq P.\alpha \cap Q_i$ and $\mu(P.\alpha) = (\mu(P) - 2 - 2\cdot 3 - \ldots - 2\cdot 3^{i-2}) - 3^{i-1} + 2\cdot 3^{i-1} = \mu(P) + 1$.
- If $q(2,i) \in P$, then
  if $q(1,i) \notin P$ and $q(0,i) \notin P$, then $P.\alpha \cap Q_i = \varnothing$ and $\mu(P.\alpha) = -\infty$;
  if $q(1,i) \notin P$ and $q(0,i) \in P$, then $P.\alpha \cap Q_i = q(i,1)$ and $\mu(P.\alpha) = (\mu(P) - 2 - 2\cdot 3 - \ldots - 2\cdot 3^{i-2}) + 3^{i-1} - 2\cdot 3^{i-1} = \mu(P) - 2\cdot 3^{i-1} + 1$;
  if $q(1,i) \in P$, then $P.\alpha \cap Q_i = q(2,i)$ and $\mu(P.\alpha) = \mu(P) - 2 - 2\cdot 3 - \ldots - 2\cdot 3^{i-2} = \mu(P) - 3^{i-1} + 1$.
- Let there is $j \in \{1,\dots,i-1\}$ such that $q(2,j) \notin P$, then $P.\alpha \cap Q_i = \varnothing$ and $\mu(P.\alpha) = -\infty$.

Thus if $\mu(P) = -\infty$, then $\mu(P.\alpha) \le 0$; if $\mu(P) \ge 0$, then $\mu(P.\alpha) \le \mu(P) + 1$. Therefore for $P = S$ obtain $P \cap Q_1 = \varnothing$. Whence $\mu(S) = -\infty$. At the same time, $\mu(Q) = 1 + 2 + 2\cdot 3 + \ldots + 2\cdot 3^{k-1} = 3^k$. Therefore the set Q can not be reached from the set S under the action of a word of length less then $3^k + 1 = 3^{(n-1)/3} + 1$. Hence $\omega(Q,S,Q) \ge 3^{\lfloor (n-1)/3 \rfloor}$. □

The NFA $\mathscr{B}_{nfa}$ can be used to prove the bounds $\omega(Q,S,Q) \ge 2\cdot 3^{\lfloor (n-1)/3 \rfloor - 1}$ and $\omega(Q,S,Q) \ge 3^{\lfloor (n-1)/3 \rfloor - 1}$ for subsets $S \subseteq Q$ of cardinality $n-2$ and $n-1$ correspondingly. Therefore for any $S \subseteq Q$ the value $\omega(Q,S,Q)$ is exponential in $|Q|$.

3 Automata over a fixed alphabet

We showed in the previous section that for any subsets $S, T \subseteq Q$ the value $\omega(Q,S,T)$ is exponential in $|Q|$. What about the values $\omega^k(Q,S,T)$ for different k? Are they exponential or polynomial in $|Q|$?

Let us consider the minimal value of $\omega^k(Q,S,T)$ for fixed Q and arbitrary $S, T \subseteq Q$. Let $k \ge 2$ be an integer. Define

$$\omega^k_{\min}(n) = \min\{\omega^k(Q,S,T) | S,T \subseteq Q, S \notin \{T, \varnothing\}, |Q| = n\}.$$

We prove that for $k \ge 3$ the value $\omega^k_{\min}(n)$ grows faster than any polynomial in n.

Theorem 3.1 *If $k \ge 3$, then the value $\omega^k_{\min}(n)$ grows faster than any polynomial*

in n.

Proof. It is evident that $\omega^k_{\min}(n) \geq \omega^3_{\min}(n)$ for $k > 3$. Thus we consider the value $\omega^3_{\min}(n)$.We prove that for any subsets S, T of Q such that $S \neq T, \varnothing$, one has $\omega^3(Q, S, T) \geq 2\sqrt[3]{|Q|}$.

Case 1. $T \neq Q$, $|S| > 1$. We construct a NFA $\mathscr{A}_{nfa3} = (Q, \{a, b, c\}, \delta)$. Let p_j be the j-th prime number (i.e. $p_1 = 2$, $p_2 = 3$, and so on). Assume for simplicity that $|Q| = p_1 + \ldots + p_r$ for some r. By definition, put

$$Q = \{q(i, m) | i \in \{1, \ldots, r\}, m \in \{0, \ldots, p_i - 1\}\}.$$

Now we define the action of the letters a, b, c. Denote by R the set $\{q(j, 0) | j \in \{1, \ldots, r\}\}$. Let $i \in \{1, \ldots, r\}$, $m \in \{0, \ldots, p_i\}$, then

$$\delta(q(i, m), a) = R,$$

$$\delta(q(i, m), b) = \{q(i, (m + 1) \bmod p_i)\},$$

$$\delta(q(i, m), c) = \begin{cases} T \text{ if } m = p_i - 1, \\ Q \text{ otheswise.} \end{cases}$$

The NFA $\mathscr{A}_{nfa3}$ is shown in Fig. 3, where solid, dashed, and dotted lines stand for the action of respectively b, a, and c. It is easy to prove that, for any subset $S \subseteq Q$, one has $S.ab^{p_1 \cdot \ldots \cdot p_r - 1}c = T$.

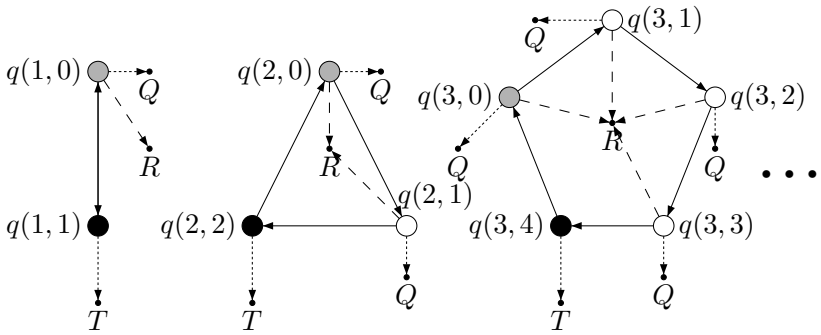

Fig. 3. Automaton $\mathscr{A}_{nfa3}$

Let $w \in \Sigma^*$ be the shortest word reaching the set T from the set S in $\mathscr{A}_{nfa3}$. Suppose $S \not\subset T$. We have $|S| > 1$ and $T \neq Q$. Therefore we can assume $\{q(1, 0), q(1, 1)\} \subseteq S$ and $q(1, 0) \notin T$. The word w contains the letter a because for any word $v \in \{b, c\}^*$ one has $\{q(1, 0), q(1, 1)\} \subseteq \{q(1, 0), q(1, 1)\}.v$. Suppose $S \subset T$; then we can assume $\{q(1, 0), q(1, 1)\} \subseteq S, T$. In this case for any word $v \in \{b, c\}^*$, $|S.v| \in \{|Q|, |S|\}$. This implies that $|S.v| \neq |T|$. Hence the word w contains the letter a.

It is easy to show that for any $v \in \Sigma^*, u \in \Sigma^*$ one has $S.vau = S.au$. Therefore $w[1] = a$ and $w[i] \neq a$ for any $i > 1$. We may assume that the automaton $\mathscr{A}_{nfa3}$ and the set T can be defined such that $T \neq R.b^t$ for any integer $t > 0$. Hence $w = ab^t c$

for some t. Notice that $S.ab^tc \in \{T, Q\}$. If $S.ab^tc = Q$, then the letter a should be applied again. Therefore $w = S.ab^tc$.

We have $S.a = R = \{q(i,0) | i \in \{1,\dots,r\}\}$. Note that for any $i \in \{1,\dots,r\}$, we have $q(i,0).a^x = q(i, p_i - 1)$ if and only if $x \equiv p_i - 1 (\mathrm{mod}\, p_i)$. We obtain a system of r linear congruences. The minimal positive solution of this system is $x = p_1p_2\dots p_r - 1$. Therefore $t = p_1p_2\dots p_r - 1$. This means that the word $w = ba^{p_1\cdot\dots\cdot p_r - 1}c$ is a shortest word reaching the set T from the set S in the automaton $\mathscr{A}_{nfa3}$.

Notice that $i < p_i$ for any $i \geq 1$. From the famous Tschebycheff theorem it follows that $\alpha \cdot i\ln(i) < p_i < \beta \cdot i\ln(i)$, where α and β are some constants. Hence for $1 < i \leq r$, $p_i < i^2 \leq r^2$. Therefore

$$|w| = \prod_{i=1}^{r} p_i + 1 > \prod_{i=1}^{r} i = r! > 2^r,\ n = \sum_{i=1}^{r} p_i \leq \sum_{i=1}^{r} r^2 = r^3.$$

Hence $\omega^3(Q,S,T) \geq 2^{\sqrt[3]{|Q|}}$.

If $\sum\limits_{i=1}^{r} p_i < |Q| < \sum\limits_{i=1}^{r+1} p_i$, then a similar construction proves the statement of the theorem. We just should add the states $q_1,\dots,q_\sigma$ to the automaton $\mathscr{A}_{nfa3}$ and put $q_i.a = \{q(j,0) | j \in \{1,\dots,r\}\}$, $q_i.b = \{q_i\}$, $q_i.c = T$ for $i \in \{1,\dots,\sigma\}$.

Case 2. $T \neq Q$, $|S| = 1$. The inequality $\omega^3(Q,S,T) \geq 2^{\sqrt[3]{|Q|}}$ can be proved similarly using the NFA $\mathscr{A}'_{nfa3} = (Q, \{a,b,c\}, \delta)$ such that $Q = \{q(i,m) \mid i \in \{1,\dots,r\}, m \in \{0,\dots,p_i - 1\}\} \cup \{start\}$, $S = \{start\}$, and for $i \in \{1,\dots,r\}$, $m \in \{0,\dots,p_i\}$

$$\delta(q(i,m),a) = Q,\ \delta(start,a) = \{q(j,0) | j \in \{1,\dots,r\}\},$$

$$\delta(q(i,m),b) = \{q(i,(m+1) \bmod p_i)\}, \delta(start,b) = Q,$$

$$\delta(q(i,m),c) = \begin{cases} T \text{ if } m = p_i - 1, \\ Q \text{ otherwise,} \end{cases} \quad \delta(start,c) = Q.$$

The proof of Case 2 is omitted due to the space constraints.

Case 3. $T = Q$. Let us construct a NFA $\mathscr{B}_{nfa3} = (Q, \{a,b,c\}, \delta)$. Let p_j be the j-th prime number. We put also $p_0 = 1$. For simplicity assume that $|Q| = p_0 + \dots + p_r + 2$ for some r. Let

$$Q = \{q(i,m) \mid i \in \{0,\dots,r\}, m \in \{0,\dots,p_i - 1\}\} \cup \{start\} \cup \{err\}.$$

In this case, $\varnothing \neq S \neq Q$. Whence we can assume $q(0,0) \notin S$ and $start \in S$. For $i \in \{0,\dots,r\}$ denote by K_i the set $\{q(i,m) \mid m \in \{0,\dots,p_i - 1\}\}$. Let $i \in \{0,\dots,r\}$, $m \in \{0,\dots,p_i - 1\}$. By the definition, we put

$$\delta(q(i,m),a) = \{err\}, \quad \delta(start,a) = \{q(j,0) | j \in \{1,\dots,r\}\} \cup \{err\},$$

$$\delta(q(i,m),b) = \{q(i,(m+1) \bmod p_i)\} \cup \{err\}, \quad \delta(start,b) = \{err\},$$

$$\delta(q(i,m),c) = \begin{cases} K_i \cup \{start\} \cup \{err\} & \text{if } m = p_i - 1, \\ \{err\}, & \text{otherwise,} \end{cases} \qquad \delta(start,c) = \{err\},$$

$$\delta(err,a) = \delta(err,b) = \delta(err,c) = \{err\}.$$

It can be proved that for any subset S, $S.ab^{p_1 \cdot \ldots \cdot p_r - 1}c = Q$. The NFA $\mathscr{B}_{nfa3}$ is represented in Fig. 4, where solid, dashed, and dotted lines stand for the action of respectively b, a, and c.

Let $w \in \Sigma^*$ be the shortest word such that $S.w = Q$. Suppose that at the beginning every state from the set S holds a token. There is no token on the state $q(0,0)$. After applying the word w one of the tokens should be on the state $q(0,0)$. It can appear there under the action of the letter a only. For any subset $P \subseteq Q$ we have either $P.a = \{q(j,0) | j \in \{1,\ldots,r\}\} \cup \{err\}$ (if $start \in P$), or $P.a = \{err\}$ (if $start \notin P$). Therefore for any word $v \in \Sigma^*$ we have either $S.va = S.a = \{q(j,0) | j \in \{1,\ldots,r\}\} \cup \{err\}$, or $S.va = \{err\}$. The word w can not be equal to vau for some $v \neq \lambda$ and $u \in \Sigma^*$. Indeed, if $S.va = S.a$, then $S.vau = S.au$ and the word w is not a shortest; if $S.va = \{err\}$, then $S.w \neq Q$. Therefore $w[1] = a$ and $w[\ell] \neq a$ for $\ell > 1$.

There is only one token in any set K_i at the moment when the letter $w[1] = a$ has been applied. The letter b does not change the number of tokens in the set K_i. Suppose $w[\ell] = c$. If $q(i, p_i - 1) \notin S.w[1, \ell - 1]$, then $S.w[1,\ell] \cap K_i = \varnothing$. In this case the word $w[\ell+1, |w|]$ should contain the letter a, and the word w is not the shortest. If $\{q(i, p_i - 1) | i \in \{1,\ldots,r\}\} \subseteq S.w[1, \ell - 1]$, then $S.w[1,\ell] = Q$. Therefore $\ell = |w|$. The set Q can not be obtained from the set S under the action of a word which consists of the letters a and b only. Therefore $w = ab^t c$ for some t. The minimal possible positive t is equal to $p_1 \cdot \ldots \cdot p_r - 1$. By the same argument as in the proof of Case 1, we obtain that $\omega^3(Q,S,T) \geq 2^{\sqrt[3]{|Q|}}$ for sufficiently large $|Q|$.

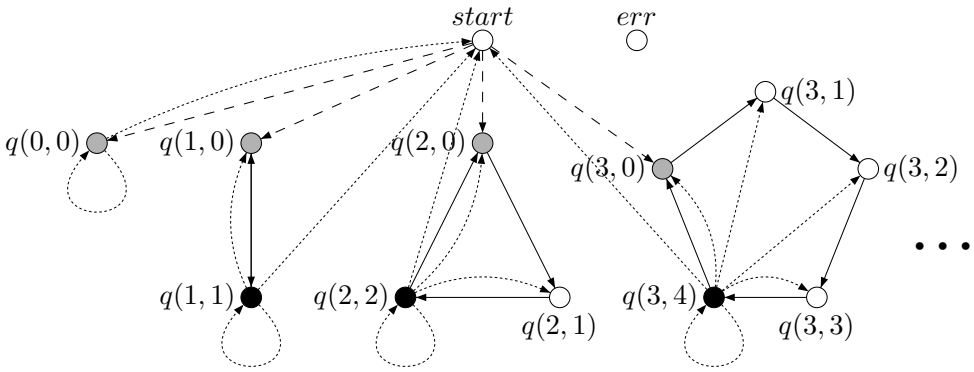

Fig. 4. Automaton B_{nfa3}

If $2 + \sum_{i=1}^{r} p_i < |Q| < 2 + \sum_{i=1}^{r+1} p_i$, then the same automaton can be constructed. We only should add some states $q_1, \ldots, q_\sigma$ and put $q_i.a = q_i.b = q_i.c = err$ for

$i \in \{1, \ldots, \sigma\}$.

Since in Cases 1-3 we have obtained that $\omega^3(Q, S, T) \geq 2^{\sqrt[3]{|Q|}}$ for $S, T \subseteq Q$ $S \neq T, \varnothing$, the value $\omega^3_{\min}(n)$ grows faster than any polynomial in n. The theorem is proved. □

Is the value $\omega^2_{\min}(n)$ a polynomial in n? This question is still open. We answer here to a weaker form of this question.

Let p_i be the i-th prime number (i.e. $p_1 = 2$, $p_2 = 3$, and so on). Let Q be a finite set, $|Q| = n$ and $\sum_{i=1}^{r} p_i \leq n < \sum_{i=1}^{r+1} p_i$ for some r. Let

$$\Psi = \{P \subseteq Q \mid |P| \leq \sum_{i=1}^{r} p_i - r - 2\},$$

i.e. Ψ consists of 'not very large' subsets of Q.

By the definition, put

$$\bar{\omega}^2_{\min}(n) = \min\{\omega^2(Q, S, T) | S \subseteq Q, T \in \Psi, S \notin \{T, \varnothing\}, |Q| = n\}.$$

Theorem 3.2 *The value $\bar{\omega}^2_{\min}(n)$ grows faster than any polynomial in n.*

Proof. We are going to prove that for sufficiently large $|Q|$ and $T \in \Psi$, $S \subseteq Q$ $S \neq T, \varnothing$ one has $\bar{\omega}^2(Q, S, T) \geq 2^{\sqrt[3]{|Q|}}$.

Case 1. $|S| > 1$. We define a NFA $\mathscr{A}_{nfa2} = (Q, \{a, b\}, \delta)$. Let p_j be the j-th prime number. Assume for simplicity that $|Q| = p_1 + \ldots + p_r$ for some r. We put

$$Q = \{q(i, m) \mid i \in \{1, \ldots, r\}, m \in \{0, \ldots, p_i - 1\}\}.$$

Denote by R the set $\{q(i, 0) | i \in \{1, \ldots, r\}\}$. Denote by F the set $\{q(i, p_i - 1) | i \in \{1, \ldots, r\}\}$. Notice that $|R| = |F| = k$. Let $i \in \{1, \ldots, r\}$, $m \in \{0, \ldots, p_i\}$. By definition put

$$\delta(q(i, m), a) = \begin{cases} T \text{ if } m = p_i - 1, \\ R \text{ if otherwise,} \end{cases}$$

$$\delta(q(i, m), b) = \{q(i, (m + 1) \bmod p_i)\}.$$

Since $T \in \Psi$, we have $|T| < |Q| - |F| - 1$. We may assume that $T \cap F \neq \varnothing$ and $R \subseteq T$ because we can take the set $Q \backslash (F \cup \{q(1, 0)\})$ containing in the set T.

The NFA $\mathscr{A}_{nfaA}$ is represented in Fig. 5, where solid and dotted lines stand for the action of respectively b and a.

Let $|S| > 1$. We prove that we may assume that $|S \cap K_2| \geq 2$. Indeed, if $|S \cap T| \geq 2$, then $|S| \geq 2$, and we may assume that $q(2, 1), q(2, 2) \in S$. If $S \cap T = \varnothing$, we may assume that $q(2, 1) \notin T$ because $|T| < |Q| - |F| - 1$. We have $q(2, 0) \in F$, whence $q(2, 0) \notin T$. Thus we may assume that $q(2, 0), q(2, 1) \in S$. If $|S \cap T| = 1$, then we may assume $q(2, 1) \in S \cap T$. We have $|S| > 1$, whence we may assume that $q(2, 0) \in S$. This implies that $|S \cap K_2| \geq 2$.

For any subset $S \subseteq Q$ one has $S.a^2 b^{p_1 \cdot \ldots \cdot p_r - 1} a = T$. Indeed, $S.a \subseteq T \cup R \subseteq Q \backslash F$. Hence $S.a^2 = R$. Further, $R.b^{p_1 \cdot \ldots \cdot p_r - 1} = F$. Therefore $F.a = T$.

Let $w \in \Sigma^*$ be such that $|w| = d_{\mathscr{A}_{nfa2}}(S, T)$. Suppose that at the beginning every state from the set S holds a token. We have $|S \cap K_2| \geq 2$, therefore there are at least two tokens on the set K_2. It can be proved that the automaton $\mathscr{A}_{nfa2}$ can be constructed such that $S.b^\ell \neq T$ for any integer ℓ. Hence the word w contains a letter a. Let j_1 be the position of the first occurrence of letter a in the word w. Let $S.w[1, j_1 - 1] = P_1$. Notice that $P_1.a \in \{T, R, T \cup R\}$.

Let $P_1.a = R \cup T$ and $T \neq \varnothing$. For any subset $P \subseteq Q$, $|P.b| = P$. Hence for any $t \geq 0$ it follows that $(R \cup T).b^t \neq T$. Therefore there is a second occurrence of the letter a in the word w. Let j_2 be the number of this occurrence. If $S.w[1, j_2] = R \cup T$, then $S.w = S.w[1, j_1]w[j_2 + 1, |w|] = T$. This means that $S.w[1, j_2] \neq R \cup T$. We have $P_1.a = R \cup T$ and $T \neq \varnothing$. Therefore there exists $i \in \{1, \ldots, r\}$ such that $|K_i \cap P_1.a| = 2$. Hence for any t we have $|P_1.ab^t \cap K_i| \geq 2$. Therefore $S.w[1, j_2] \neq T$. Thus $S.w[1, j_2] = R$.

Let $m = \min\{j | S.w[1, j] = R\}$. We have just proved that $m = j_1$ or $m = j_2$. For any $i \in \{1, \ldots, r\}$, $|S.w[1, m] \cap K_i| = 1$. Either the set T is empty, or $|T| = 1$, or for some $i \in \{1, \ldots, r\}$, $|T \cap K_i| \geq 2$. Hence for any integer $t > 0$ it follows that $T \neq R.b^t$. The set F cannot be reached from the set R under the action of any word of length less than $b^{p_1 \cdot \ldots \cdot p_r - 1}$. At the same time for $t < p_1 \cdot \ldots \cdot p_r - 1$ we have $R.b^t a = T \cup R$. Therefore $|w| \geq m + p_1 \cdot \ldots \cdot p_r$. Hence if $S \subseteq T$ or $T = \varnothing$, then $|w| \geq 1 + p_1 \cdot \ldots \cdot p_r$, else $|w| \geq 2 + p_1 \cdot \ldots \cdot p_r$. In any case, for sufficiently large $|Q|$, we have $\omega^2(Q, S, T) \geq 2^{\sqrt[3]{|Q|}}$.

For $\sum_{i=1}^{r} p_i < |Q| < \sum_{i=1}^{r+1} p_i$, the construction is similar. To obtain it we should add states $q_1, \ldots, q_\sigma$ to the automaton $\mathscr{A}_{nfa2}$ and define $q_i.a = R, q_i.b = \{q_i\}$ for $i \in \{1, \ldots, \sigma\}$. We should also assume that $q_1, \ldots, q_\sigma \notin T$, because $|T| \leq (\sum_{i=1}^{r} p_i) - r - 2$. The proof for this case is similar.

Case 2. $|S| = 1$. The inequality $\omega^3(Q, S, T) \geq 2^{\sqrt[3]{|Q|}}$ can be proved similarly using the NFA $\mathscr{A}'_{nfa2} = (Q, \{a, b\}, \delta)$ such that $Q = \{q(i, m) \mid i \in \{1, \ldots, r\}, m \in \{0, \ldots, p_i - 1\}\} \cup \{start\}$, $S = \{start\}$, $R = \{q(i, 0) \mid i \in \{1, \ldots, r\}\}$, and for

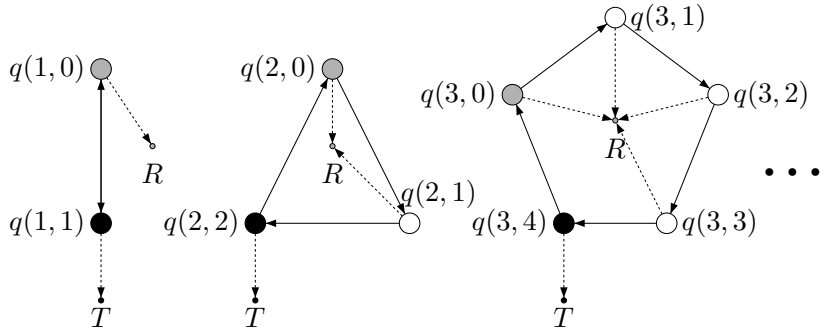

Fig. 5. Automaton A_{nfa2}

$i \in \{1, \ldots, r\}$, $m \in \{0, \ldots, p_i\}$,

$$\delta(q(i,m),a) = \begin{cases} T \text{ if } m = p_i - 1, \\ Q \text{ if otherwise,} \end{cases} \qquad \delta(start, a) = R,$$

$$\delta(q(i,m),b) = \{q(i,(m+1) \bmod p_i)\}, \quad \delta(start, b) = Q.$$

The proof of Case 2 is omitted. □

Thus we proved that the values $\omega(Q,S,T)$ and $\omega^k(Q,S,T)$ for $k \geq 2$ are not polynomials in $|Q|$ in most cases. It is an open question whether the values $\omega^2(Q,S,T)$ for large sets T are polynomials or not.

Acknowledgement

The author is grateful to his supervisor Dr. D. S. Ananichev and to Prof. M. V. Volkov for their valuable help.

References

[1] Černý, J. Poznámka k homogénnym eksperimentom s konecnými automatami, Mat.-Fyz. Čas. Slovensk. Akad. Vied. 14 (1964) 208–216 [in Slovak].

[2] Holladay, I.; Varga, R. On powers of non negative matrices, Proc. Amer. Math. Soc. 9 (1958) 631–634.

[3] Ito, M. Algebraic Theory of Automata and Languages, World Scientific, Singapore, 2004.

[4] Ito, M.; Shikishima-Tsuji, K. Some results on directable automata, in J. Karhumäki, H. Mauer, Gh. Păun, and G. Rozenberg (eds.), Theory Is Forever. Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday. [Lect. Notes Comp. Sci. 3113] Springer, Berlin, 2004, 125–133.

[5] Mateescu, A.; Salomaa, A. Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68 (1999) 134–150.

[6] Sandberg, S. Homing and synchronizing sequences, in M. Broy et al (eds.), Model-Based Testing of Reactive Systems [Lect. Notes Comp. Sci., 3472], Springer, Berlin, 2005, 5–33.

[7] Wielandt, H. On eigenvalues of sums of normal matrices, Pacif. J. Math. 5(4) (1955) 633–638.