Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 327 (2004) 225–239
Theoretical Computer Science
www.elsevier.com/locate/tcs

Synchronizing monotonic automata

D.S. Ananichev, M.V. Volkov*

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

Received 1 October 2003; received in revised form 30 March 2004; accepted 31 March 2004

Abstract

We show that if the state set Q of a synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ admits a linear order such that for each letter $a \in \Sigma$ the transformation $\delta(\_, a)$ of Q preserves this order, then $\mathscr{A}$ possesses a reset word of length $|Q| - 1$. We also consider two natural generalizations of the notion of a reset word and provide for them results of a similar flavour.

Keywords: Synchronizing automata; Order preserving transformation; Monotonic automata; Rank of a word; Interval rank of a word

1. Motivation and overview

Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a DFA (deterministic finite automaton), where Q denotes the state set, Σ stands for the input alphabet, and $\delta : Q \times \Sigma \to Q$ is the transition function defining an action of the letters in Σ on Q. The action extends in a unique way to an action $Q \times \Sigma^* \to Q$ of the free monoid Σ^* over Σ; the latter action is still denoted by δ. The automaton $\mathscr{A}$ is called *synchronizing* if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. Any word w with this property is said to be a *reset* word for the automaton.

Fig. 1 shows an example of a synchronizing automaton with 4 states. The reader can easily verify that the word ab^3ab^3a resets the automaton leaving it in the state 2. With somewhat more effort one can also check that ab^3ab^3a is the shortest reset word for this automaton.

* Corresponding author.
E-mail addresses: dmitry.ananichev@usu.ru (D.S. Ananichev), mikhail.volkov@usu.ru (M.V. Volkov).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2004.03.068

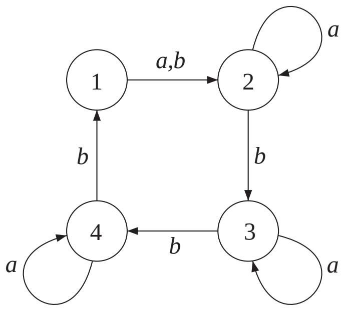

Fig. 1. A synchronizing automaton.

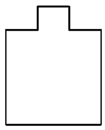

Fig. 2. A polygonal detail.

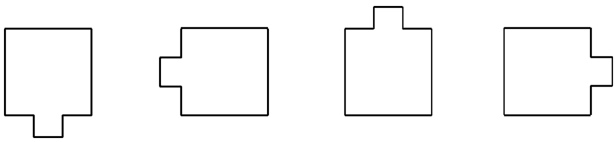

Fig. 3. Four possible orientations.

For a mathematician, the notion of a synchronizing automaton is pretty natural by itself but we would like to mention here that it is also of interest for various applications, for instance, for *robotics* or, more precisely, *robotic manipulation* which deals with part handling problems in industrial automation such as part feeding, fixturing, loading, assembly and packing (and which is therefore of utmost and direct practical importance). Of course, there exists vast literature about the role that synchronizing automata play in these matters (tracing back to Natarajan's pioneering papers [10,11]) but we prefer to explain the idea of using such automata on the following simple example.

Suppose that one of the parts of a certain device has the shape shown on Fig. 2. Such parts arrive at manufacturing sites in boxes and they need to be sorted and oriented before assembly. For simplicity, assume that only four initial orientations of the part are possible, namely, the ones shown on Fig. 3.

Further, suppose that prior the assembly the detail should take the "bump-left" orientation (the second one in Fig. 3). Thus, one needs a device that puts the detail in the prescribed position independently of its initial orientation.

Of course, there are many ways to design such an orienter but practical considerations favour methods which require little or no sensing, employ simple devices, and are as robust

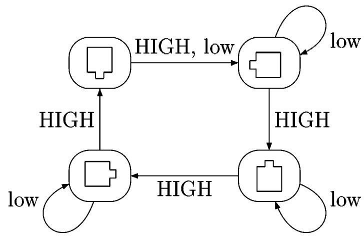

Fig. 4. The action of the obstacles.

as possible. For our particular case, these goals can be achieved as follows. We put details to be oriented on a conveyer belt which takes them to the assembly point and let the stream of the details encounter a series of passive obstacles placed along the belt. We need two type of obstacles: high and low. A high obstacle should be high enough in order that any detail on the belt encounters this obstacle by its rightmost low angle (we assume that the belt is moving from left to right). Being curried by the belt, the detail then is forced to turn 90° clockwise. A low obstacle has the same effect whenever the detail is in the "bump-down" orientation (the first one in Fig. 3); otherwise it does not touch the detail which therefore passes by without changing the orientation.

The scheme on Fig. 4 summarizes how the aforementioned obstacles effect the orientation of the detail. The reader immediately recognizes the synchronizing automaton from Fig. 1. Remembering that its shortest reset word is the word ab^3ab^3a, we conclude that the series of obstacles

$$\text{low} - \text{HIGH} - \text{HIGH} - \text{HIGH} - \text{low} - \text{HIGH} - \text{HIGH} - \text{HIGH} - \text{low}$$

yields the desired sensorless orienter.

Another, perhaps, even more striking application of synchronizing automata is connected with *biocomputing*. Mastering a simple illustrating example from this area is not that easy (one need to be acquainted at least with some rudiments of molecular biology) so we just refer to recent experiments (see [2,3]) in which DNA molecules have been used as both hardware and software for constructing finite automata of nanoscaling size. For instance, the authors of [3] have produced a "soup of automata", that is, a solution containing 3×10^{12} identical automata/μl. All these molecular automata can work in parallel on different inputs, thus ending up in different and unpredictable states. In contrast to an electronic computer, one cannot reset such a system by just pressing a button; instead, in order to synchronously bring each automaton to its "ready-to-restart" state, one should spice the soup with (sufficiently many copies of) a DNA molecule whose nucleotide sequence encodes a reset word.

Clearly, from the viewpoint of the above applications (as well as from mathematical point of view) it is rather natural to ask how long a reset word for a given synchronizing automaton may be. This question is very intriguing as it remains open for 40 years. In 1964, Černý [4] produced for each n a synchronizing automaton with n states whose shortest reset word has length $(n-1)^2$ (the automaton on Fig. 1 is Černý's example for $n = 4$) and conjectured that these automata represent the worst possible case, that is, every synchronizing automaton with n states can be reset by a word of length $(n-1)^2$. By now this simply looking conjecture is arguably the most longstanding open problem in the theory of finite automata. It is however confirmed for several special types of automata. Instead of an attempt to overview and to analyze all related results, we refer to the recent survey [9] and mention here only three typical examples involving restrictions of rather different sorts.

In Kari's elegant paper [8] the restriction has been imposed on the underlying digraphs of automata in question, namely, Černý's conjecture has been verified for automata with Eulerian digraphs. In contrast, Dubuc [5] has proved the conjecture under the assumption that there is a letter that acts on the state set Q as a cyclic permutation of order $|Q|$. A condition of yet another type has been used by Eppstein [6] who has confirmed Černý's conjecture for automata whose states can be arranged in some cyclic order which is preserved by the action of each letter in Σ. Eppstein (whose interest in synchronizing automata was motivated by their robotics applications) has called those automata *monotonic*; we will refer to them as to *oriented* automata since we prefer to save the term 'monotonic' for a somewhat stronger notion which is in fact the object of the present paper.

We call a DFA $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ *monotonic* if its state set Q admits a linear order $\leqslant$ such that for each letter $a \in \Sigma$ the transformation $\delta(\_, a)$ of Q preserves $\leqslant$ in the sense that $\delta(q, a) \leqslant \delta(q', a)$ whenever $q \leqslant q'$. It is clear that monotonic automata form a (proper) subclass of the class of oriented automata, and therefore, by Eppstein's result any synchronizing monotonic automaton with n states possesses a reset word of length $(n-1)^2$. We will radically improve this upper bound by showing that such an automaton can be in fact reset by a word of length $n-1$. It is easy to see that the latter bound is already exact. (Observe that for general oriented automata the bound $(n-1)^2$ is exact: for each $n \geqslant 3$ Černý has constructed in [4] an n-state synchronizing automaton whose shortest reset word is of length $(n-1)^2$, and one can easily check that all these automata are oriented.)

In fact, we will prove a much stronger result in the flavour of Pin's generalization [12,13] of Černý's conjecture. Given a DFA $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, we define the *rank* of a word $w \in \Sigma^*$ as the cardinality of the image of the transformation $\delta(\_, w)$ of the set Q. (Thus, in this terminology reset words are precisely words of rank 1.) In 1978 Pin conjectured that for every k, if an n-state automaton admits a word of rank at most k, then it has also a word with rank at most k and of length $(n-k)^2$. Pin [12,13] has proved the conjecture for $n-k = 1, 2, 3$ but Kari [7] has found a remarkable counter example in the case $n-k = 4$. It is not yet clear if the conjecture holds true for some restricted classes of automata such as, say, the class of oriented automata. For monotonic automata, however, the situation is completely clarified by the following

Theorem 1. *Let $\mathscr{A}$ be a monotonic DFA with n states and let k satisfy $1 \leqslant k \leqslant n$. If there is a word of rank at most k with respect to $\mathscr{A}$, then some word of length at most $n-k$ also has rank at most k with respect to $\mathscr{A}$.*

The proof (which, being elementary in its essence, is not easy) is presented in Section 2. In Section 3 we discuss a related problem arising when one replaces the above notion of the rank by a similar notion of the interval rank. Given a monotonic DFA $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, we define the *interval rank* of a word $w \in \Sigma^*$ as the cardinality of the least interval of the chain $\langle Q, \leqslant\rangle$ containing the image of the transformation $\delta(\_, w)$. Thus, when looking for a word of low interval rank, we aim at compressing the state set of an automaton into a certain small interval; in other words, if we have several copies of the automaton, each being in a distinct initial state, then applying such a word we can make the behaviour of all the copies be 'almost the same'.

It is to be expected that compressing to small intervals would require more effort than compressing to just small subsets that can be scattered over the state set in an arbitrary way. We provide a series of examples showing that no linear function of the size n of the state set can serve as an upper bound for the length of a word of interval rank 2 (Propositions 1 and 2). This strongly contrasts with Theorem 1. On the other hand, we give a quadratic upper bound for the length of a word of interval rank k for any k with $2 \leqslant k \leqslant n$:

Theorem 2. *Let $\mathscr{A}$ be a monotonic DFA with n states and let k satisfy $2 \leqslant k \leqslant n$. If there is a word of interval rank at most k with respect to $\mathscr{A}$, then some word of length at most $(n-k)(n-k-1)/2+1$ also has interval rank at most k with respect to $\mathscr{A}$.*

A further series of examples (Propositions 3 and 4) serves to show that this upper bound is exact for all 'sufficiently large' k, that is, for all $k \geqslant \lfloor n/2 \rfloor$.

We mention that the results of Section 3 essentially improve the bounds published in the proceedings version [1] of the present paper.

2. Proof of Theorem 1

Of course, without any loss we may assume that the state set Q of our monotonic automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is the set $\{1, 2, \ldots, n\}$ of the first n positive integers and that the linear order $\leqslant$ on Q is the usual order $1 < 2 < \cdots < n$. For $x, y \in Q$ with $x \leqslant y$ we denote by $[x, y]$ the interval $\{x, x+1, x+2, \ldots, y\}$. Then for any non-empty subset $X \subseteq Q$ we have $X \subseteq [\min(X), \max(X)]$ where $\max(X)$ and $\min(X)$ stand respectively for the maximal and the minimal elements of X. Given a word $w \in \Sigma^*$ and non-empty subset $X \subseteq Q$, we write $X.w$ for the set $\{\delta(x, w) \mid x \in X\}$. Also observe that since the composition of order preserving transformations is order preserving, all transformations $\delta(\_, w)$ where $w \in \Sigma^*$ are order preserving. We say that a subset $X \subseteq Q$ is *invariant* with respect to a transformation φ of the set Q if $X\varphi \subseteq X$.

Lemma 1. *Let X be a non-empty subset of Q such that* $\max(X.w) \leqslant \max(X)$ *for some* $w \in \Sigma^*$. *Then for each* $p \in [\max(X.w), \max(X)]$ *there exists a word* $\mathcal{D}(X, w, p)$ *of length at most* $\max(X) - p$ *such that* $\max(X.\mathcal{D}(X, w, p)) \leqslant p$.

Proof. If $p = \max(X)$, then the empty word satisfies all the properties to be fulfilled by the word $\mathcal{D}(X, w, p)$. Therefore for the rest of the proof we may assume that $p < \max(X)$ and, therefore, $\max(X.w) < \max(X)$. Take an arbitrary q in the interval $[\max(X.w)+1, \max(X)]$. We want to show that there is a letter $\alpha(q) \in \Sigma$ such that $\delta(q, \alpha(q)) < q$. Arguing by contradiction, suppose that for some $q \in [\max(X.w)+1, \max(X)]$ we have $\delta(q, a) \geqslant q$ for all letters $a \in \Sigma$. Since all transformations $\delta(\_, a)$ are order preserving, this would mean that the interval $Y = [q, n]$ is invariant with respect to all these transformations whence it is also invariant with respect to all transformations $\delta(\_, w)$ with $w \in \Sigma^*$. But $\max(X) \in Y$ while $\delta(\max(X), w) = \max(X.w) \notin Y$, a contradiction.

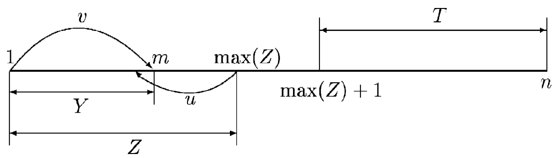

Fig. 5. Intervals in the proof of Theorem 1.

Now we construct a sequence of words as follows: let $u_1 = \alpha(\max(X))$ and, as long as $\delta(\max(X), u_i) > p$, let $u_{i+1} = u_i\alpha(\delta(\max(X), u_i))$. Observe that by the construction the length of the word u_i equals i and the last word u_s in the sequence must satisfy $\delta(\max(X), u_s) \leqslant p$. Besides that we have $s \leqslant \max(X) - p$ because by the construction

$$\max(X) > \delta(\max(X), u_1) > \delta(\max(X), u_2) > \cdots > \delta(\max(X), u_{s-1}) > p.$$

Thus, the word u_s can be chosen to play the role of $\mathcal{D}(X, w, p)$ from the formulation of the lemma. $\square$

By symmetry, we also have the following dual statement:

Lemma 2. *Let X be a non-empty subset of Q such that* $\min(X.w) \geqslant \min(X)$ *for some* $w \in \Sigma^*$. *Then for each* $p \in [\min(X), \min(X.w)]$ *there exists a word* $\mathscr{U}(X, w, p)$ *of length at most* $p - \min(X)$ *such that* $\min(X.\mathscr{U}(X, w, p)) \geqslant p$.

Now we can begin with the proof of Theorem 1. We induct on n with the induction base $n = 1$ being obvious. Thus, suppose that $n > 1$ and consider the set $X = \{\min(Q.w) \mid w \in \Sigma^*,\ |Q.w| \leqslant k\}$. (This set is not empty because by the condition of the theorem there exists a word of rank $\leqslant k$ with respect to $\mathscr{A}$.) Let $m = \max(X)$ and let $v \in \Sigma^*$ be such that $\min(Q.v) = m$ and $|Q.v| \leqslant k$.

Consider the interval $Y = [1, m]$. It is invariant with respect to all transformations $\delta(\_, w)$, $w \in \Sigma^*$. Indeed, arguing by contradiction, suppose that there are $q \in Y$ and $w \in \Sigma^*$ such that $\delta(q, w) > m$. Since the transformation $\delta(\_, w)$ is order preserving, $\min(Q.vw) = \delta(m, w) \geqslant \delta(q, w) > m$. At the same time, $|Q.vw| \leqslant |Q.v| \leqslant k$ whence $\min(Q.vw)$ belongs to the set X. This contradicts the choice of m.

Now consider the set $Z = \{q \in Q \mid \delta(q, w) \leqslant m$ for some $w \in \Sigma^*\}$. Observe that Z is an interval and that $Y \subseteq Z$ since for $q \in Y$ the empty word can serve as w with $\delta(q, w) \leqslant m$. Therefore $\max(Z) \geqslant m$. Fix a word $u \in \Sigma^*$ such that $\delta(\max(Z), u) \leqslant m$. Then $\delta(q, u) \leqslant m$ for each $q \in Z$ as the transformation $\delta(\_, u)$ is order preserving.

Finally, consider the interval $T = [\max(Z) + 1, n] = Q \setminus Z$. It is invariant with respect to all transformations $\delta(\_, w)$, $w \in \Sigma^*$. Indeed, suppose that there exist $q \in T$ and $w \in \Sigma^*$ such that $\delta(q, w) \leqslant \max(Z)$. This means that $\delta(q, wu) \leqslant m$ whence $q \in Z$, in a contradiction to the choice of q.

Fig. 5 should help the reader to keep track of the relative location of the intervals introduced so far. We have also depicted the actions of the words u and v introduced above on the states $\max(Z)$ and 1, respectively.

Now consider the state $p \in Q$ defined as follows:

$$p = \begin{cases} k - |T| & \text{if } |T| + m \leqslant k, \\ m & \text{if } |T| + m > k. \end{cases} \tag{1}$$

Observe that $m \leqslant p \leqslant n - |T| = \max(Z)$. Therefore we can apply Lemma 1 to the set Z, the state p and the word $u \in \Sigma^*$. Let $w_1 = \mathcal{D}(Z, u, p)$; then the length of w_1 is at most $\max(Z) - p$ and $\max(Z.w_1) \leqslant p$. Therefore $Z.w_1 = (Q \setminus T).w_1 \subseteq [1, p]$. Since the interval T is invariant with respect to $\delta(\_, w_1)$, we conclude that $Q.w_1 \subseteq [1, p] \cup T$. From (1) we see that in the case when $|T| + m \leqslant k$ the length of word w_1 does not exceed $\max(Z) - k + |T| = n - k$ and $|Q.w_1| \leqslant q + |T| = k$. We have thus found a word of length at most $n - k$ and rank at most k with respect to $\mathscr{A}$. This means that for the rest of the proof we may assume that $|T| + m > k$ and $p = m$. In particular, the length of w_1 is at most $\max(Z) - m$ and $Q.w_1 \subseteq Y \cup T$.

Consider the following state $r \in Q$:

$$r = \begin{cases} m + 1 + |T| - k & \text{if } |T| + 1 \leqslant k, \\ m & \text{if } |T| + 1 > k. \end{cases} \tag{2}$$

Clearly, $1 \leqslant r \leqslant m$, and we can apply Lemma 2 to the set Q, the state r and the word v. Let $w_2 = \mathscr{U}(Q, v, r)$. The length of w is at most $r - \min(Q) = r - 1$ and $\delta(1, w_2) \geqslant r$. Since the interval $Y = [1, m]$ is invariant with respect to $\delta(\_, w_2)$, we conclude that $Y.w_2 \subseteq [r, m]$. From (2) we see that in the case when $|T| + 1 \leqslant k$ the length of the word w_1w_2 does not exceed $\max(Z) - m + r - 1 = \max(Z) + |T| - k = n - k$ and $|Q.w_1w_2| \leqslant m - r + 1 + |T| = k$. Again we have found a word of length at most $n - k$ and rank at most k. Thus, from now on we assume that $|T| + 1 > k$ and $r = m$. This means that $Q.w_1w_2 \subseteq \{m\} \cup T$ and the length of the word w_1w_2 is at most $(\max(Z) - m) + (m - 1) = \max(Z) - 1$.

Consider now the automaton $\mathscr{A}_T = \langle T, \Sigma, \delta_T \rangle$ where δ_T is δ restricted to the set $T \times \Sigma$. We have observed that the set T is invariant with respect to all transformations $\delta(\_, w)$, $w \in \Sigma^*$, whence $\mathscr{A}_T$ is a DFA, which obviously is monotonic. We claim that there is a word of rank at most $k - 1$ with respect to $\mathscr{A}_T$. Indeed, suppose that $|T.w| \geqslant k$ for each word $w \in \Sigma^*$. Since $T \cap Y = \emptyset$ and both T and Y are invariant, we obtain $T.w \cap Y.w = \emptyset$ for every $w \in \Sigma^*$. Therefore

$$|Q.w| \geqslant |Y.w| + |T.w| \geqslant 1 + k > k.$$

This contradicts to the condition that there exists a word of rank at most k with respect to the automaton $\mathscr{A}$.

We see that we are in a position to apply the induction assumption to the automaton $\mathscr{A}_T$. Hence there exists a word $w_3 \in \Sigma^*$ of length at most

$$|T| - (k - 1) = n - \max(Z) - k + 1$$

such that $|T.w_3| \leqslant k - 1$. Then the word $w_1w_2w_3$ has the length at most $(\max(Z) - 1) + (n - \max(Z) - k + 1) = n - k$ and $Q.w_1w_2w_3 \subseteq \{\delta(m, w_3)\} \cup T.w_3$ whence $|Q.w_1w_2w_3| \leqslant 1 + |T.w_3| = k$. □

For the sake of completeness we mention that it is pretty easy to find examples showing that the upper bound $n - k$ for the length of a word of rank $\leqslant k$ with respect to a monotonic automaton is tight. Given n and k with $1 \leqslant k \leqslant n$, one can consider, for instance, the automaton on the set $\{1, 2, \ldots, n\}$ with the input alphabet $\{a\}$ and the transition function

$$\delta(i, a) = \begin{cases} i-1 & \text{if } i > k, \\ i & \text{if } i \leqslant k. \end{cases}$$

Clearly, the word a^{n-k} is the shortest word of rank $\leqslant k$ with respect to this automaton.

3. Compressing to intervals

We start with presenting a series of examples of monotonic automata $\mathscr{A}_\ell$, where $\ell = 2, 3, \ldots$, that cannot be efficiently compressed to a 2-element interval. The state set Q_ℓ of the automaton $\mathscr{A}_\ell$ consists of $2\ell + 1$ elements and can be conveniently identified with the chain

$$-\ell < 1-\ell < \cdots < -1 < 0 < 1 < \cdots < \ell. \tag{3}$$

The input alphabet Σ of $\mathscr{A}_\ell$ contains three letters A, B and C. The action of the letter A on the set Q_ℓ is defined as follows:

$$\delta(j, A) = \begin{cases} \ell-1 & \text{if } j \geqslant 0, \\ -\ell & \text{if } j < 0. \end{cases} \tag{4}$$

The action of the letter B is defined as follows:

$$\delta(j, B) = \begin{cases} j-1 & \text{if } 0 < j < \ell, \\ j & \text{in all other cases.} \end{cases} \tag{5}$$

The action of the letter C is defined as follows:

$$\delta(j, C) = \begin{cases} \ell & \text{if } 0 < j \leqslant \ell, \\ \ell-1 & \text{if } j = 0, \\ -1 & \text{if } j = -1, \\ j+1 & \text{if } -\ell \leqslant j < -1. \end{cases} \tag{6}$$

Fig. 6 shows the action of Σ on Q_ℓ for $\ell = 4$.

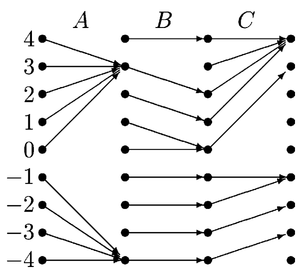

Fig. 6. The automaton $\mathscr{A}_4$.

It is easy to see that the actions (4)–(6) preserve the ordering (3) of the set Q_ℓ, and therefore, $\mathscr{A}_\ell = \langle Q_\ell, \Sigma, \delta\rangle$ is a monotonic DFA. The intervals $[-\ell, -1]$ and $[0, \ell]$ are invariant with respect to the action of Σ. Therefore, for any word $w \in \Sigma^*$, the set $Q_\ell.w$ contains at least two states: a negative state and a non-negative one, whence the rank of w is at least 2. Clearly, words of rank 2 exist: for instance, the word A is such. The interval rank of the word is however 2ℓ because $\delta(\_, A) = \{-\ell, \ell - 1\}$. Still we have the following.

Proposition 1. *There exists a word over Σ whose interval rank with respect to the automaton $\mathscr{A}_\ell$ is equal to* 2.

Proof. For each m such that $1 \leqslant m \leqslant \ell$ consider the interval $I_m = [-m, 0]$. By the definition of the actions of B and C we have

$$I_m . CB^{\ell-1} \subseteq [1 - m, 0] = I_{m-1},$$

for each $m = 2, \ldots, \ell$. On the other hand, we see that

$$Q.AB^{\ell-1} \subseteq [-\ell, 0] = I_\ell,$$

and therefore,

$$Q.AB^{\ell-1}(CB^{\ell-1})^{\ell-1} \subseteq I_1 = [-1, 0].$$

Thus, the interval rank of the word $W_\ell = AB^{\ell-1}(CB^{\ell-1})^{\ell-1}$ is at most 2. As we observed above, the rank of any word with respect to the automaton $\mathscr{A}_\ell$ is at least 2 whence the interval rank of W_ℓ is precisely 2. $\square$

The length of the word W_ℓ is equal to ℓ^2. This is in fact the best possible result as our next proposition shows.

Proposition 2. *The length of any word $v \in \Sigma^*$ whose interval rank with respect to the automaton $\mathscr{A}_\ell$ is* 2 *is at least ℓ^2.*

Proof. As already mentioned, the intervals $[-\ell, -1]$ and $[0, \ell]$ are invariant with respect to the action of Σ. Therefore the only interval of size 2 to which the set Q_ℓ can be compressed is the interval $[-1, 0]$ and we must have $[-\ell, -1].v = \{-1\}$ and $[0, \ell].v = \{0\}$. Another consequence of this observation is that $Q.uA = \{-\ell, \ell - 1\}$ for any word $u \in \Sigma^*$.

Any word v of interval rank 2 with respect to the automaton $\mathscr{A}_\ell$ must contain at least one occurrence of the letter A because A is the only letter that moves the state ℓ. We find the last occurrence of the letter A in v and represent this word in the form

$$v = u_1 A u_2,$$

where the suffix u_2 does not contain A. The last observation from the previous paragraph means that the word $w = Au_2$ also has interval rank 2.

One readily calculates the actions of the following words on the state 0:

$$\delta(0, AB^k) = \delta(0, CB^k) = \begin{cases} \ell - k - 1 & \text{if } k < \ell - 1, \\ 0 & \text{if } k \geqslant \ell - 1, \end{cases}$$

$$\delta(0, AB^kC) = \delta(0, CB^kC) = \begin{cases} \ell & \text{if } k < \ell - 1, \\ \ell - 1 & \text{if } k \geqslant \ell - 1. \end{cases}$$

Since the word u_2 does not move the state ℓ, we conclude from these formulas that the word w contains no factors of the kind AB^kC and CB^kC where $0 \leqslant k < \ell - 1$. (We notice that if $\delta(0, u) = \ell$ for some word $u \in \Sigma^*$ then $\delta(q, u) = \ell$ for any $q \geqslant 0$.) Therefore, this word has the form:

$$w = AB^{k_1}CB^{k_2} \cdots CB^{k_s} \quad \text{ where } k_1, \ldots k_{s-1} \geqslant \ell - 1.$$

In addition, $\delta(0, w) = 0$ whence $\delta(0, CB^{k_s}) = 0$, and therefore, we must also have $k_s \geqslant \ell - 1$.

Now we observe that the only letter that moves the negative states up is C and an application of C moves each negative state up at most by 1. This means that in order to move the state $-\ell$ to the state -1 the word w must have at least $\ell - 1$ occurrences of the letter C, that is, $s \geqslant \ell$. Hence the length of w is at least ℓ^2 and, of course, the length of the word v we started with is at least ℓ^2 as well. □

Recall that the number of states of the automaton $\mathscr{A}_\ell$ is equal to $2\ell + 1$. Thus, Propositions 1 and 2 show that for any odd $n \geqslant 5$ there exists a monotonic DFA with n states for which the shortest word of interval rank 2 is of length $(n-1)^2/4$. On the other hand, Theorem 2 (formulated in Section 1) gives the upper bound $(n-k)(n-k-1)/2+1$ for the lengths of words of interval rank $k \geqslant 2$ in monotonic automata. We proceed with the proof of this theorem.

Thus, let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a monotonic DFA with n states. Consider the automaton $\mathscr{I}$ whose states are the intervals of the chain $\langle Q, \leqslant \rangle$. The automaton $\mathscr{I}$ has the same input alphabet Σ and the transition function δ' defined by the rule: for each I being an interval of $\langle Q, \leqslant \rangle$ and for each letter $a \in \Sigma$

$$\delta'(I, a) = [\min(I.a), \max(I.a)].$$

It is easy to see that the existence of a word of interval rank at most k with respect to $\mathscr{A}$ implies that there is a path in $\mathscr{I}$ from the interval Q to an interval of size at most k. Conversely, if we read the consecutive labels of a minimum length path from Q to an interval of size at most k in the automaton $\mathscr{I}$ then we get a word of minimum length with interval rank at most k with respect to $\mathscr{A}$. Thus, it remains to estimate the length of such a path. Clearly, a minimum length path from Q to an interval of size at most k passes only through intervals of size $k+1, \ldots, n-1$ between its extreme points and visit each of these intermediate intervals at most once. Therefore the length of such a path exceeds the number of the intervals of size $k+1, \ldots, n-1$ at most by one, and this gives us the upper bound $(n-k)(n-k+1)/2$.

Now we are going to slightly improve this upper bound. We say that an interval $I \subseteq Q$ is *extreme* if it contains one of the two extreme states of the chain $\langle Q, \leqslant \rangle$. It is easy to calculate that there are $2(n-k)-1$ extreme intervals of size at least $k+1$ and $(n-k-1)(n-k-2)/2$

non-extreme intervals of this size. Take the last extreme interval Y in the shortest path from Q to an interval of size at most k in the automaton $\mathscr{I}$. The rest of the path after Y passes through non-extreme intervals only whence its length does not exceed $(n-k-1)(n-k-2)/2+1$. Therefore we can represent the shortest word of rank at most k as a product of two words w_1w_2, where $\delta'(Q, w_1) = Y$ and the length of w_2 is at most $(n-k-1)(n-k-2)/2+1$.

Let m denote the size of the interval Y. First assume that $m \geqslant k+1$ and Y contains the minimum of Q. Apply Lemma 1 to the set Q and the word w_1 (in the symmetric case when Y contains the maximum of Q we use Lemma 2). It gives us a word $w_1' = \mathcal{D}(Q, w_1, \max(Y))$ of length at most $n-m$ such that $\max(Q.w_1') \leqslant \max(Y)$. Since the interval Y is extreme, the last inequality implies that $Q.w_1' \subseteq Y$. Therefore the product $w_1'w_2$ also has rank at most k and the length of this word is at most

$$\begin{aligned}\frac{(n-k-1)(n-k-2)}{2}+1+n-m &\leqslant \frac{(n-k-1)(n-k-2)}{2}+n-k\\ &= \frac{(n-k)(n-k-1)}{2}+1.\end{aligned}$$

Finally, if $m = k$ then already the word w_1' is of rank at most k and its length does not exceed $n-k \leqslant (n-k)(n-k-1)/2+1$. □

For $k = 2$ there is a significant gap between the lower bound provided by Propositions 1 and 2 and the upper bound of Theorem 2. We use the next series of examples in order to show that for $k \geqslant \lfloor n/2 \rfloor$ the bound of Theorem 2 is tight. The series consists of the automata $\mathscr{B}_\ell$, $\ell = 3, 4, \ldots$. The state set Q_ℓ of the automaton $\mathscr{B}_\ell$ is the chain (3). The input alphabet Σ_ℓ of $\mathscr{B}_\ell$ contains three groups of letters. The first group consists of $\ell-1$ 'non-increasing' letters $B_1, \ldots, B_{\ell-1}$ whose action on the set Q_ℓ is defined as follows:

$$\delta(j, B_i) = \begin{cases} j-1 & \text{if } j = \ell - i,\\ -i-1 & \text{if } -i-1 < j < 0 \text{ and } i \neq 1,\\ j & \text{in all other cases.}\end{cases} \tag{7}$$

The second group consists of $\ell-1$ 'non-decreasing' letters $C_1, \ldots, C_{\ell-1}$ that act on the state set by the rule

$$\delta(j, C_i) = \begin{cases} j+1 & \text{if } j = i-\ell-1\\ \ell-1 & \text{if } 0 \leqslant j < i\\ \ell & \text{if } i \leqslant j < \ell\\ j & \text{in all other cases.}\end{cases} \tag{8}$$

Finally, we need a 'special' letter A whose action is described by the rule

$$\delta(j, A) = \begin{cases} \ell-1 & \text{if } j \geqslant 0,\\ -\ell & \text{if } j < 0\end{cases} \tag{9}$$

(the same as the rule (4) in the definition of the automaton $\mathscr{A}_\ell$). Fig. 7 shows the action of Σ_ℓ on Q_ℓ for $\ell = 4$.

It is clear that actions (7)–(9) preserve the ordering (3) of the set Q_ℓ whence $\mathscr{B}_\ell = \langle Q_\ell, \Sigma_\ell, \delta \rangle$ is a monotonic DFA.

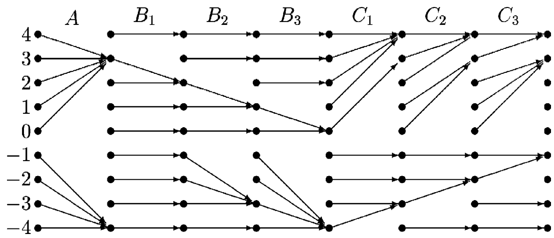

Fig. 7. The automaton $\mathscr{B}_4$.

Proposition 3. *There exists a word over Σ_ℓ whose interval rank with respect to the automaton $\mathscr{B}_\ell$ is at most ℓ.*

Proof. Consider the word

$$w_m = B_1 B_2 \cdots B_m C_{\ell-m}$$

for $m = 1, \ldots, \ell - 1$. It is straightforward to verify that

$$\delta(\ell - 1, w_m) = \ell - 1 \text{ and } \delta(-m - 1, w_m) = -m.$$

Denote the product $w_{\ell-1} w_{\ell-2} \cdots w_1$ by w. Then we see that

$$\delta(\ell - 1, w) = \ell - 1 \text{ and } \delta(-\ell, w) = -1,$$

and therefore,

$$\delta(\ell, AwB_1) = \ell - 2 \text{ and } \delta(-\ell, AwB_1) = -1.$$

This means that

$$Q.AwB_1 \subseteq [-1, \ell - 2], \quad Q.AwB_1 \nsubseteq [0, \ell - 2], \quad Q.AwB_1 \nsubseteq [-1, \ell - 3].$$

Thus, the interval rank of the word $W = AwB_1$ with respect to the automaton $\mathscr{B}_\ell$ is equal to ℓ. □

Since the length of the word w_m is equal to $m + 1$, it is easy to calculate that the length of the word

$$W = Aw_{\ell-1} w_{\ell-2} \cdots w_1 B_1$$

is equal to $(\ell + 1)\ell/2 + 1$. Our next proposition shows that W is in fact a word of interval rank ℓ with the minimum possible length.

Proposition 4. *The length of any word $w \in \Sigma_\ell^*$ whose interval rank with respect to the automaton $\mathscr{B}_\ell$ is at most ℓ is at least $(\ell + 1)\ell/2 + 1$.*

Proof. The intervals $[-\ell, -1]$ and $[0, \ell]$ are invariant with respect to the action of Σ_ℓ. Therefore, for any word $u \in \Sigma_\ell^*$, the set $Q_\ell.u$ contains a negative state and a non-negative one. This implies that $Q.uA = \{-\ell, \ell - 1\}$ for any word $u \in \Sigma_\ell^*$.

Another consequence of the above observation is that for any word w with interval rank at most ℓ the states ℓ, $\ell-1$ and $-\ell$ do not belong to the set $Q_\ell.w$. Since A is the only letter that moves the state ℓ, it must occur in the word w. We find the last occurrence of A in w and represent w as

$$w = u_1 A u_2,$$

where the suffix u_2 does not contain A. The observation from the previous paragraph implies that the interval rank of the word $v = Au_2$ does not exceed ℓ. Therefore if $v = a_1 a_2 \dots a_m$ ($a_1, a_2, \dots, a_m \in \Sigma_\ell$) is a shortest word of interval rank $\leqslant \ell$ with respect to the automaton $\mathscr{B}_\ell$, then $a_1 = A$ and $a_j \neq A$ for all $j = 2, \dots, m$. Let $v_i = a_1 \cdots a_i$ be the prefix of length i of the word v, $i = 1, \dots, m$. We denote the set $Q.v_i$ by I_i. Observe that $I_i \subseteq [-\ell, \ell-1]$ for all i because $a_1 = A$, A does not occur in $a_2 \dots a_m$, and $\ell \notin Q.v$.

Now we notice that the last letter of the word v is B_1. Indeed, C_i cannot be the last letter because $[0, \ell].C_i = \{\ell-1, \ell\}$ but neither $\ell - 1$ nor ℓ are in $Q.v$. Let $a_m = B_i$. The word v_{m-1} has interval rank at least $\ell + 1$, therefore the letter B_i must move the state $\max(Q.v_{m-1})$ down. Since the only positive state moved by B_i is $\ell - i$, we have $\max(Q.v) = \ell - i - 1$. Then from the fact that the interval rank of v does not exceed ℓ we conclude that $\min(Q.v) \geqslant -i$. This is only possible if $i = 1$ because each letter B_i with $i > 1$ sends every negative state below $-i$.

Thus, $v = Aa_2 \dots a_{m-1}B_1$. Therefore $Q.v = \{-1, \ell-2\}$ and $Q.v_{m-1} = \{-1, \ell-1\}$.

For each $k \in [1, \ell-1]$, let $\sigma(k)$ be the least number such that the sets I_i for all $i \geqslant \sigma(k)$ are contained in the interval $[-k, \ell-1]$. From the fact stated in the previous paragraph it follows that the numbers $\sigma(k)$ are indeed well defined. Clearly, we have

$$\sigma(\ell-1) \leqslant \sigma(\ell-2) \leqslant \cdots \leqslant \sigma(2) \leqslant \sigma(1).$$

Observe that if $\sigma(k) = s$ then $a_s = C_{\ell-k}$. Indeed, by the choice of s we must have

$$I_{s-1} \nsubseteq [-k, \ell-1] \quad \text{and} \quad I_{s-1}.a_s = I_s \subseteq [-k, \ell-1].$$

The first condition shows that $\min(I_{s-1}) < -k$ whence $\min(I_{s-1}) \leqslant -k-1$ while the second one implies that $\delta(\min(I_{s-1}), a_s) = \min(I_s) \geqslant -k$. Since the transformation $\delta(\_, a_s)$ is order preserving, we have that $\delta(-k-1, a_s) \geqslant -k$. The only letter in Σ_ℓ satisfying this property is $C_{\ell-k}$. In particular,

$$\sigma(\ell-1) < \sigma(\ell-2) < \cdots < \sigma(2) < \sigma(1).$$

Now we estimate the difference $\sigma(k-1) - \sigma(k)$ for each $k \in [2, \ell-1]$. Let $\sigma(k) = s$ and $\sigma(k-1) = t$. By the previous observation $a_s = C_{\ell-k}$ and $a_t = C_{\ell-k+1}$. Since $\ell \notin Q.v_t$, from the definition of the action of $C_{\ell-k+1}$ we see that $\max(Q.v_{t-1}) \leqslant \ell - k$. On the other hand, $\max(Q.v_s) = \ell - 1$. This means that the word $a_{s+1}a_{s+2} \dots a_{t-1}$ moves the state $\ell - 1$ at least $k - 1$ position down, but any letter from Σ_ℓ moves any positive state at most one step down. Hence $\sigma(k-1) - \sigma(k) \geqslant k$.

Let $\sigma(\ell) = 1$. A similar argument (that uses the fact that $a_1 = A$) shows that $\sigma(\ell-1) - \sigma(\ell) \geqslant \ell$.

Now we estimate $\sigma(1)$:

$$\sigma(1)=\sigma(\ell)+\sum_{k=2}^{\ell}(\sigma(k-1)-\sigma(k))\geqslant 1+\sum_{k=2}^{\ell}k=\frac{(\ell+1)\ell}{2}.$$

We already know that the last letter of v is not $C_{\ell-1}$ but B_1. This means that the length of the word v is at least $(\ell+1)\ell/2+1$. □

Now if we take an odd n and let $k=(n-1)/2$, then we conclude from Proposition 4 that the shortest word of interval rank k with respect to monotonic automata $\mathscr{B}_k$ has the length

$$\frac{(k+1)k}{2}+1=\frac{(2k+1-k)(2k+1-k-1)}{2}+1=\frac{(n-k)(n-k-1)}{2}+1.$$

We see that this lower bound coincides with the upper bound from Theorem 2.

In order to show that the upper bound of Theorem 2 is tight for an arbitrary $n\geqslant 5$ and for any $k\geqslant\lfloor n/2\rfloor$, we can proceed as follows. Let $s=k-\lfloor n/2\rfloor$. Now if n is odd, let $\ell=(n-1)/2-s$ and consider the automaton $\mathscr{B}_\ell$. It has $2\ell+1=n-2s$ states. We insert $2s$ new states between the states -1 and 0 of the automaton $\mathscr{B}_\ell$ and let all letters from Σ_ℓ fix these new states. Then the proofs of Propositions 3 and 4 apply showing that the modified automaton with n states admits a word of interval rank $\ell+2s=k$ and that the minimum length of such a word is equal to

$$\frac{(\ell+1)\ell}{2}+1=\frac{(n-k)(n-k-1)}{2}+1.$$

If n is even, consider the automaton $\mathscr{B}_\ell$ for $\ell=n/2-s-1$. This automaton has $2\ell+1=n-2s-1$ states, and we get an automaton with n states by inserting $2s+1$ new states between the states -1 and 0 and letting all letters from Σ_ℓ fix these new states. Again it is easy to see that the minimum length of any word of interval rank $\ell+2s+1=k$ with respect to the modified automaton is equal to $(n-k)(n-k-1)/2+1$.

Acknowledgements

Several useful comments of the anonymous referees of the proceedings version [1] of this paper are gratefully acknowledged. The authors acknowledge support from the Education Ministry of Russian Federation, Grants E02-1.0-143 and 04.01.059, the Russian Foundation for Basic Research, Grant 01-01-00258, the President Program of Leading Scientific Schools, Grant 2227.2003.1, and the INTAS (through Network Project 99-1224 “Combinatorial and Geometric Theory of Groups and Semigroups and its Applications to Computer Science”).

References

[1] D.S. Ananichev, M.V. Volkov, Synchronizing monotonic automata, Developments in language theory, 7th Internat. Conf., Szeged, 2003, Lect. Notes Comput. Sci. 2710 (2003) 111–121.

[2] Y. Benenson, R. Adar, T. Paz-Elizur, Z. Livneh, E. Shapiro, DNA molecule provides a computing machine with both data and fuel, Proc. Nat. Acad. Sci. USA 100 (2003) 2191–2196.
[3] Y. Benenson, T. Paz-Elizur, R. Adar, E. Keinan, Z. Livneh, E. Shapiro, Programmable and autonomous computing machine made of biomolecules, Nature 414 (1) (2001) 430–434.
[4] J. Černý, Poznámka k homogénnym eksperimentom s konecnými automatami, Mat.-Fyz. Cas. Slovensk. Akad. Vied. 14 (1964) 208–216 (in Slovak).
[5] L. Dubuc, Sur les automates circulaires et la conjecture de Černý, Rairo Inform. Theor. Appl. 32 (1998) 21–34 (in French).
[6] D. Eppstein, Reset sequences for monotonic automata, SIAM J. Comput. 19 (1990) 500–510.
[7] J. Kari, A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull. 73 (2001) 146.
[8] J. Kari, Synchronizing finite automata on Eulerian digraphs, Math. Foundations Comput. Sci., 26th Internat. Symp., Marianske Lazne, Lect. Notes Comput. Sci. 2136 (2001) 432–438.
[9] A. Mateescu, A. Salomaa, Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68 (1999) 134–150.
[10] B.K. Natarajan, An algorithmic approach to the automated design of parts orienters, Proc. 27th Annu. Symp. Foundations Comput. Sci., IEEE, 1986, pp. 132–142.
[11] B.K. Natarajan, Some paradigms for the automated design of parts feeders, Internat. J. Robot. Res. 8 (6) (1989) 89–109.
[12] J.-E. Pin, Le problème de la Synchronisation, Contribution à l'Étude de la Conjecture de Černý, Thèse de 3éme cycle, Paris, 1978 (in French).
[13] J.-E. Pin, Sur les mots synchronisants dans un automate fini, Elektronische Informationverarbeitung und Kybernetik 14 (1978) 283–289 (in French).