ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 330 (2005) 3–13

Theoretical Computer Science

www.elsevier.com/locate/tcs

Synchronizing generalized monotonic automata

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

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

Dedicated to Academician Arto Salomaa on the occasian of his 70th birthday

Abstract

In an earlier paper, we have studied reset words for synchronizing automata whose states admit a stable linear order. Here we show that the same bound on the length of the shortest reset word persists for synchronizing automata satisfying much weaker stability restriction. This result supports our conjecture concerning the length of reset words for synchronizing automata accepting only star-free languages.

Keywords: Synchronizing automata; Order-preserving transformation; Monotonic automata; Congruence on an automaton; Generalized monotonic automata; Rank of a word with respect to an automaton; Rank of an automaton

1. Background and motivation

Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a 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: $\delta(q_1, w) = \delta(q_2, w)$ for all $q_1, q_2 \in Q$. Any word w with this property is said to be a *reset word* for the automaton.

It is rather natural to ask how long a reset word for a given synchronizing automaton may be. The problem is known to be NP-complete (see, e.g. [14, Section 6]), but on the other hand, there are some upper bounds on the minimum length of reset words for synchronizing

* Corresponding author.
E-mail addresses: Dmitry.Ananichev@usu.ru (D.S. Ananichev), Mikhail.Volkov@usu.ru (M.V. Volkov).

0304-3975/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2004.09.006

automata with a given number of states. The best such bound known so far is due to Pin [11] (it is based on a combinatorial theorem conjectured by Pin and then proved by Frankl [5]): for each synchronizing automaton with n states, there exists a reset word of length at most $(n^3 - n)/6$. In 1964 Černý [3] produced for each n a synchronizing automaton with n states whose shortest reset word has length $(n-1)^2$ 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 combinatorial theory of finite automata (and one of the favorite topics of Arto Salomaa's research, see his recent publications [12–14]). The reader is referred to the survey paper [8] for an interesting overview of the area and its relations to multiple-valued logic and symbolic dynamics; applications of synchronizing automata to robotics are discussed in [4].

In [2] we have studied a special kind of automata which we called monotonic. (This term was also used in [4] but in a different sense.) Namely, an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is said to be *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 $\delta(q_1, a) \leqslant \delta(q_2, a)$ whenever $q_1 \leqslant q_2$. We have observed that every monotonic synchronizing automaton with n states has a reset word of length at most $n-1$ and this upper bound is tight. In the present paper, we prove that the same upper bound persists within a much wider class of automata which are in a certain sense representative for the class of automata accepting only star-free languages.

In order to define our generalized monotonic automata, we recall the notion of a congruence on an automaton. An equivalence relation ρ on the state set Q of an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is said to be a *congruence* on $\mathscr{A}$ if $(q_1, q_2) \in \rho$ implies $\big(\delta(q_1, a), \delta(q_2, a)\big) \in \rho$ for all states $q_1, q_2 \in Q$ and all letters $a \in \Sigma$. For $q \in Q$, we denote by $[q]_\rho$ the ρ-class containing the state q. The *quotient* $\mathscr{A}/\rho$ is the automaton $\langle Q/\rho, \Sigma, \delta_\rho\rangle$ where $Q/\rho = \{[q]_\rho \mid q \in Q\}$ and the transition function δ_ρ is defined by the rule $\delta_\rho([q]_\rho, a) = [\delta(q, a)]_\rho$ for all $q \in Q$ and $a \in \Sigma$.

Now let ρ be a congruence on an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$. The automaton is said to be *ρ-monotonic* if there exists a (partial) order $\leqslant$ on the set Q such that

(1) two states are $\leqslant$-comparable if and only if they belong to the same ρ-class; in other words, the order $\leqslant$ is contained in ρ (as a subset of $Q \times Q$) and its restriction to any ρ-class is a linear order;
(2) for each letter $a \in \Sigma$, the transformation $\delta(\_, a) : Q \to Q$ preserves $\leqslant$.

Clearly, for ρ being the universal congruence, ρ-monotonic automata are precisely monotonic automata as defined above. On the other hand, for ρ being the equality relation, every automaton is ρ-monotonic.

We call an automaton $\mathscr{A}$ *generalized monotonic of level ℓ* if it has a strictly increasing chain of congruences

$$\rho_0 \subset \rho_1 \subset \cdots \subset \rho_\ell \tag{1}$$

in which ρ_0 is the equality relation, ρ_ℓ is the universal relation, and the quotient $\mathscr{A}/\rho_{i-1}$ is ρ_i/ρ_{i-1}-monotonic for each $i = 1, \ldots, \ell$. Thus, monotonic automata of [2] are precisely generalized monotonic automata of level 1. Here is a simple example of a generalized monotonic automaton of level 2 which is not monotonic.

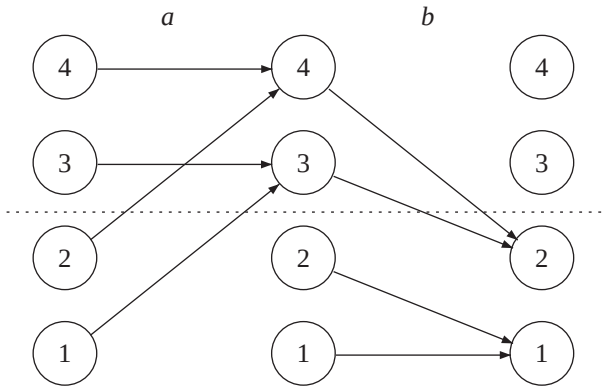

Fig. 1. The automaton $\mathscr{E}$.

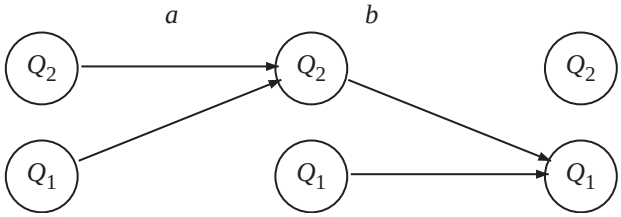

Fig. 2. The quotient automaton $\mathscr{E}/\rho_1$.

Example 1.1. The automaton $\mathscr{E}$ with the state set $Q = \{1, 2, 3, 4\}$ and the input letters a, b whose action is shown on Fig. 1 is generalized monotonic of level 2 but not monotonic.

Proof. Consider the chain of relations

$$\rho_0 \subset \rho_1 \subset \rho_2$$

in which ρ_0 is the equality relation, ρ_2 is the universal relation, and ρ_1 is the partition of Q into 2 classes $Q_1 = \{1, 2\}$ and $Q_2 = \{3, 4\}$ (the partition is shown in Fig. 1 by the dotted line). Obviously, ρ_1 is a congruence on $\mathscr{E}$. Endowing Q with the partial order $\leqslant_1$ such that $1 <_1 2$ and $3 <_1 4$, we immediately see that the automaton $\mathscr{E} = \mathscr{E}/\rho_0$ is ρ_1-monotonic.

The quotient automaton $\mathscr{E}/\rho_1$ is shown in Fig. 2. If we order the set Q/ρ_1 by letting $Q_1 <_2 Q_2$, the transformations induced by the letters a and b become order preserving. We see that $\mathscr{E}/\rho_1$ is a monotonic, that is, ρ_2/ρ_1-monotonic automaton. Thus, we have verified that $\mathscr{E}$ is a generalized monotonic automaton of level 2.

In order to show that $\mathscr{E}$ is not monotonic, one can directly check that the action of the letters a and b violates each of 24 linear orders on the set $Q = \{1, 2, 3, 4\}$. Alternatively, one can refer to a (much stronger) result proved in [17]: the transition monoid of $\mathscr{E}$ does not divide the transition monoid of any monotonic automaton. (In automata-theoretic terms this result means that no monotonic automaton can emulate $\mathscr{E}$.) □

The reader acquainted with paper [1] will see a strong analogy between our notion of a generalized monotonic automaton of level ℓ and the concept of a transformation monoid preserving an ℓ-chain of interval partitions developed in [1]. In fact, our notion is nothing but an automata-theoretic reformulation of this important concept. Since no result from [1] is needed for the proof of our main theorem, we postpone a discussion of relationships between [1] and the present paper till Section 3. Here we only mention that from [1] it follows that the hierarchy of generalized monotonic automata based on their level is strict: for each ℓ there exists a generalized monotonic automaton whose level is precisely ℓ.

We will show that every generalized monotonic synchronizing automaton with n states can be reset by a word of length $n-1$. In fact, we will prove a much stronger result in the flavor of Pin's generalization [9,10] of Černý's conjecture. Given an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, we define the *rank* of a word $w \in \Sigma^*$ with respect to $\mathscr{A}$ 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 $(n-k)^2$. He [9,10] has proved the conjecture for $n-k = 1, 2, 3$ but Kari [6] has found a remarkable counter example in the case $n-k = 4$.

The following modification of Pin's conjecture has been recently suggested (in particular, in [7]). Define the *rank* $r(\mathscr{A})$ of an automaton $\mathscr{A}$ as the minimum rank of words with respect to $\mathscr{A}$. (Thus, synchronizing automata are precisely automata of rank 1.) Then the modified conjecture is that for every automaton with n states and rank k there exists a word with rank k and of length at most $(n-k)^2$. Kari's automaton does not refute this conjecture: the automaton has 6 states and rank 1 (so it is synchronizing) and indeed admits a reset word of length 25. In [2] we have proved that for every monotonic automaton with n states and rank k, there is a word with rank k and of length at most $n-k$. Here we will prove that the same result holds true for generalized monotonic automata:

Theorem 1.2. *Let $\mathscr{A}$ be a generalized monotonic automaton with n states and rank k, $1 \leqslant k \leqslant n$. Then there exists a word of length at most $n-k$ which has rank k with respect to $\mathscr{A}$.*

The proof of the theorem—which uses only fairly elementary tools but is by no means easy—is presented in the next section.

2. Proof of the main result

A subset X of a set Q is said to be *invariant with respect to a transformation* $\varphi : Q \to Q$ if $X\varphi \subseteq X$. A subset of the state set of an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is called *invariant* if it is invariant with respect to all the transformations $\delta(\_, a)$ with $a \in \Sigma$. If X is an invariant subset, we define the *restriction* of $\mathscr{A}$ to X as the automaton $\mathscr{A}_X = \langle X, \Sigma, \delta_X\rangle$, where δ_X is the restriction of the transition function δ to the set $X \times \Sigma$.

If $X \subseteq Q$ and $w \in \Sigma^*$, then in order to simplify the notation we will write $X.w$ for the set $\{\delta(q, w) \mid q \in X\}$. We need a simple lemma relating rank of an automaton with ranks of its suitable restrictions.

Lemma 2.1. *Let X and Z be two disjoint invariant subsets of the state set of an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$. If there exists a word $w \in \Sigma^*$ such that $Q.w \subseteq X \cup Z$, then $r(\mathscr{A}_X) + r(\mathscr{A}_Z) = r(\mathscr{A})$.*

Proof. Let v be a word of minimum rank with respect to $\mathscr{A}$. Then

$$r(\mathscr{A}_X) + r(\mathscr{A}_Z) \leqslant |X.v| + |Z.v| = |(X \cup Z).v| \leqslant Q.v = r(\mathscr{A}).$$

On the other hand, let v_X and v_Z be words of minimum rank with respect to the automata $\mathscr{A}_X$ and $\mathscr{A}_Z$. Then the product $v_X v_Z$ is a word of minimum rank with respect to both the automata. Therefore,

$$\begin{aligned} r(\mathscr{A}) &\leqslant |Q.wv_Xv_Z| \leqslant |(X \cup Z).v_Xv_Z| \\ &= |X.v_Xv_Z \cup Z.v_Xv_Z| = r(\mathscr{A}_X) + r(\mathscr{A}_Z). \qquad \square \end{aligned}$$

We say that an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ can be *reset to each state* if for each $q \in Q$ there is a word $w \in \Sigma^*$ such that $Q.w = \{q\}$.

Lemma 2.2. *Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a ρ-monotonic automaton for a congruence ρ, and suppose that the quotient automaton $\mathscr{A}/\rho$ can be reset to each state. Then for each ρ-class C there exists an invariant subset $Z \subseteq Q$ such that $r(\mathscr{A}_Z) = r(\mathscr{A}) - 1$ and $|C.w_C \setminus Z| = 1$ for a suitable word $w_C \in \Sigma^*$ of length at most $|Q| - |Z| - |Q/\rho|$.*

Before proceeding with the proof of the lemma, we would like to mention that the invariant subset Z may be empty. In fact, this happens precisely when $\mathscr{A}$ is a synchronizing automaton. The lemma then means that there is a word w_C of length at most $|Q| - |Q/\rho|$ which compresses the class C to a singleton. There is no need in isolating this special case because our proof works fine under the natural agreement that rank of the empty automaton is 0.

Proof. Let $\leqslant$ be the order from the definition of a ρ-monotonic automaton. Recall that every ρ-class is a chain with respect to $\leqslant$, and therefore, every non-empty subset S of such a ρ-class contains a unique minimal element which we denote by $\min(S)$.

Let $k = r(\mathscr{A})$. From the fact that the quotient automaton $\mathscr{A}/\rho$ can be reset to each of its states it is easy to deduce that for every ρ-class R there exists a word v of rank k with respect to $\mathscr{A}$ such that $Q.v \subseteq R$. Let $M(R)$ be the maximal element of the set

$$\{\min(Q.v) \mid v \text{ is a word of rank } k \text{ such that } \ Q.v \subseteq R\}$$

and let v_R be a word of rank k such that $Q.v_R \subseteq R$ and $\min(Q.v_R) = M(R)$. Denote by M the set of elements $M(R)$ for all ρ-classes $R \in Q/\rho$. Clearly, $|M| = |Q/\rho|$.

For brevity, we will write $[q]$ instead of $[q]_\rho$ for the ρ-class containing $q \in Q$. Consider the set

$$X = \{q \in Q \mid q \leqslant M([q])\}.$$

Observe that $M \subseteq X$ so that, in particular, the set X is non-empty. We aim to prove that X is invariant. Indeed, arguing by contradiction, suppose that $\delta(q, a) > M([\delta(q, a)])$ for some

$q \in X$ and $a \in \Sigma$. Since the transformation $\delta(\_, a)$ preserves $\leqslant$ and $M([q]) \geqslant q$, we see that $\delta(M([q]), a) > M([\delta(q, a)])$. Since $M([q]) = \min(Q.v_{[q]})$, we have

$$\delta(M([q]), a) = \delta(\min(Q.v_{[q]}), a) = \min(Q.v_{[q]}a),$$

whence $\min(Q.v_{[q]}a) > M([\delta(q, a)])$. This contradicts the choice of $M([\delta(q, a)])$ if one takes into account that the word $v_{[q]}a$ has rank k.

Next, we verify that the restriction $\mathscr{A}_X$ is a synchronizing automaton. Moreover, we can show that $X.v_R = \{M(R)\}$ for every ρ-class $R \in Q/\rho$ so that each word v_R is a reset word for $\mathscr{A}_X$. Indeed, take an arbitrary state $q \in X$. Then $\delta(q, v_R) \in R$ because $Q.v_R \subseteq R$, and we get the following inequality in the chain $\langle R, \leqslant\rangle$:

$$\delta(q, v_R) \geqslant \min(Q.v_R) = M(R).$$

On the other hand, $\delta(q, v_R) \in X$ because X is invariant, and from the definition of X we obtain the opposite inequality:

$$\delta(q, v_R) \leqslant M([\delta(q, v_R)]) = M(R).$$

Thus, $\delta(q, v_R) = M(R)$.

Now consider the set

$$Y = \{q \in Q \mid \delta(q, w) \in X \quad \text{for some } w \in \Sigma^*\}.$$

Observe that $X \subseteq Y$ since for $q \in X$ the empty word can be chosen as w satisfying $\delta(q, w) \in X$. Observe also that the set $Z = Q \setminus Y$ is invariant. (This is the invariant subset from the conclusion of the lemma.) Indeed, suppose that $\delta(q, a) \in Y$ for some $q \in Z$ and $a \in \Sigma$. Then there is a word $w \in \Sigma^*$ such that $\delta(\delta(q, a), w) \in X$. However, $\delta(\delta(q, a), w) = \delta(q, aw)$ whence $q \in Y$, in a contradiction to the choice of q.

Next we show that there is a word $w \in \Sigma^*$ such that $Q.w \subseteq X \cup Z$. Arguing by contradiction, suppose that for every word $w \in \Sigma^*$ the difference $Q.w \setminus (X \cup Z)$ is non-empty. Let u be a word such that the difference $D = Q.u \setminus (X \cup Z)$ has minimum possible size. Now take a state $q \in D$. Since $D \subseteq Y$, there is a word $w \in \Sigma^*$ such that $\delta(q, w) \in X$. Since the union $X \cup Z$ is invariant, this implies that the difference $Q.uw \setminus (X \cup Z)$ has strictly less elements than D, a contradiction.

Now we see that we are in the conditions of Lemma 2.1: we have got two disjoint invariant subsets X and Z in Q and there exists a word $w \in \Sigma^*$ such that $Q.w \subseteq X \cup Z$. From Lemma 2.1, we conclude that $r(\mathscr{A}_X) + r(\mathscr{A}_Z) = r(\mathscr{A})$. However, we have already proved that $\mathscr{A}_X$ is a synchronizing automaton, that is, $r(\mathscr{A}_X) = 1$, whence $r(\mathscr{A}_Z) = r(\mathscr{A}) - 1$.

Now we take an arbitrary ρ-class $C \in Q/\rho$. The intersection $C \cap Y$ is non-empty because $Y \supseteq X \supseteq M \ni M(C)$. Let x be the maximal element of this intersection. Since $x \in Y$, there is a word $v \in \Sigma^*$ such that $\delta(x, v) \in X$. We choose $w_1 = a_1a_2 \cdots a_s$ with $a_1, a_2, \ldots, a_s \in \Sigma$ to be a word of minimum length with this property. Consider the path

$$x \xrightarrow{a_1} \delta(x, a_1) \xrightarrow{a_2} \delta(x, a_1a_2) \xrightarrow{a_3} \ldots \xrightarrow{a_s} \delta(x, w_1)$$

in the transition graph of the automaton $\mathscr{A}$. This path cannot visit any state twice and only its last state lies in X. The path also cannot leave Y because $Z = Q \setminus Y$ is an invariant set

and, having once entered Z, the path would never be able to return to X. Therefore, all states of this path except the last one are in $Y \setminus X$. Hence, the length of the word w_1 is at most $|Y| - |X|$.

Consider the minimal state y in the ρ-class $\delta_\rho(C, w_1)$. Then $y \leqslant M([y])$ whence $y \in X$. We have shown that the set X can be compressed by a suitable word to each state in the set M. Therefore, there exists a word of minimum length in the set of all words v with the property $\delta(y, v) \in M$. We represent this word as $w_2 = b_1 b_2 \cdots b_t$ with $b_1, b_2, \ldots, b_t \in \Sigma$ and consider the path

$$y \xrightarrow{b_1} \delta(y, b_1) \xrightarrow{b_2} \delta(y, b_1 b_2) \xrightarrow{b_3} \ldots \xrightarrow{b_t} \delta(y, w_2)$$

in the transition graph of our automaton. Again the path cannot visit any state more than once and only its last state lies in M. Since $y \in X$ and X is an invariant set, all states of this path except the last one are in $X \setminus M$. Hence, length of the word w_2 is at most $|X| - |M|$.

We let w_C be the product $w_1 w_2$. Then the length of w_C does not exceed

$$(|Y| - |X|) + (|X| - |M|) = |Y| - |M| = |Q| - |Z| - |Q/\rho|$$

as required. To complete the proof of the lemma, it remains to verify that the image of C under the transformation $\delta(\_, w_C)$ up to exactly one state is contained in the set Z, that is, $|C.w_C \setminus Z| = 1$.

To this aim, we first observe that by the choice of y as the minimum state in the ρ-class $\delta_\rho(C, w_1)$, we have $y \leqslant \delta(q, w_1)$ for all $q \in C$. Applying the order preserving transformation $\delta(\_, w_2)$ to this inequality yields

$$\delta(y, w_2) \leqslant \delta(\delta(q, w_1), w_2) = \delta(q, w_C).$$

Since the word w_2 has been chosen to ensure the containment $\delta(y, w_2) \in M$, we conclude that $\delta(y, w_2) = M(B)$ where B stands for the ρ-class $\delta_\rho(C, w_C)$. Hence $M(B) \leqslant \delta(q, w_C)$ for all $q \in C$.

By the choice of the word w_1 we have $\delta(x, w_1) \in X$. Since the set X is invariant, $\delta(x, w_C) = \delta(\delta(x, w_1), w_2) \in X$, that is, $\delta(x, w_C) \leqslant M(B)$. Hence for all $q \in C$ with $q \leqslant x$ we have $\delta(q, w_C) \leqslant M(B)$ as the transformation $\delta(\_, w_C)$ preserves the order $\leqslant$. Taking into account the inequality proved in the previous paragraph, we conclude that all states $q \in C$ with $q \leqslant x$ are mapped by $\delta(\_, w_C)$ to the single state $M(B)$.

Finally, recall that the state x has been chosen to be the maximal element of the intersection $C \cap Y$. This means that any state $q \in C$ with $q > x$ must belong to $Q \setminus Y = Z$. Since Z is an invariant set, $\delta(q, w_C) \in Z$ for all such states q.

We see that for every $q \in C$ either $\delta(q, w_C) \in Z$ or $\delta(q, w_C) = M(B) \notin Z$. Thus, $|C.w_C \setminus Z| = 1$, as required. □

We say that the automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *reducible* if there is an invariant subset $P \subset Q$ such that $r(\mathscr{A}_P) = r(\mathscr{A}) - 1$ and $|Q.v_P \setminus P| = 1$ for some word v_P of length at most $|Q| - |P| - 1$. This property may seem somewhat exotic but, as the next proposition shows, it always occurs in the situation which we are focused on. This fact is crucial for the proof of our main result.

Proposition 2.3. *Every generalized monotonic automaton is reducible.*

Proof. Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a generalized monotonic automaton and (1) the corresponding chain of congruences. We induct on the number n of the states of $\mathscr{A}$.

The case $n = 1$ is obvious because we can let P and v be empty. Thus, let $n > 1$. In order to simplify the notation, we write ρ for ρ_1 and $[q]$ for $[q]_\rho$. The automaton $\mathscr{A}$ is ρ-monotonic; let $\leqslant$ be the corresponding partial order.

Since ρ strictly contains the equality relation, the automaton $\mathscr{A}/\rho$ has less than n states and hence is reducible by the induction assumption. Thus, we can fix an invariant subset X of Q/ρ such that $r((\mathscr{A}/\rho)_X) = r(\mathscr{A}/\rho) - 1$ and a word v_1 of length $|Q/\rho| - |X| - 1$ such that $|(Q/\rho).v_1 \setminus X| = 1$. (The set X may be empty but this does not affect the reasoning below.) Consider the set $Y = \{q \in Q \mid [q] \in X\}$. Since X is invariant, Y is easily seen to be invariant as well.

Consider the union R of all singleton sets of the form $(Q/\rho).w \setminus X$ where $w \in \Sigma^*$. This union is non-empty because $(Q/\rho).v_1 \setminus X$ is a singleton whence $(Q/\rho).v_1 \setminus X \subseteq R$. Now consider the pullback $S = \{q \in Q \mid [q] \in R\}$ of R in Q. Since by the definition $R \cap X = \emptyset$, we have $S \cap Y = \emptyset$.

We aim to show that R is an invariant set, and hence S is also invariant. For every $r \in R$ there is a word $w \in \Sigma^*$ such that $(Q/\rho.w) \setminus X = \{r\}$. Suppose that $\delta_\rho(r, a) \in X$ for some letter $a \in \Sigma$. Since X is invariant, we then have $(Q/\rho).wa \subseteq X$. We know that $r((\mathscr{A}/\rho)_X) = r(\mathscr{A}/\rho) - 1$ whence there exists a word u of rank $r(\mathscr{A}/\rho) - 1$ with respect to $(\mathscr{A}/\rho)_X$. Then the words wau has rank $r(\mathscr{A}/\rho) - 1$ with respect to $\mathscr{A}/\rho$, and this is clearly impossible. Thus, $\delta_\rho(r, a) \notin X$. Since the set X is invariant, this implies that $(Q/\rho).wa \setminus X = \{\delta_\rho(r, a)\}$. Therefore $\delta_\rho(r, a) \in R$ for each letter $a \in \Sigma$, and therefore, R and S are invariant.

Since $(Q/\rho).v_1 \setminus X \subseteq R$, we have $Q.v_1 \setminus Y \subseteq S$. Hence $Q.v_1 \subseteq Y \cup S$. We are in the conditions of Lemma 2.1. Applying it, we obtain

$$r(\mathscr{A}_Y) + r(\mathscr{A}_S) = r(\mathscr{A}). \tag{2}$$

Observe that the automaton $(\mathscr{A}/\rho)_R$ can be reset to each state. Indeed, for every state $r \in R$ there is a word $w \in \Sigma^*$ such that

$$\{r\} = (Q/\rho).w \setminus X = (Q/\rho).w \cap R,$$

but since R is an invariant set, we must have $R.w = \{r\}$. Further, we can identify this automaton with the automaton $(\mathscr{A}_S)/\rho$ because both the automata have the same state set R and the same transition function δ_ρ restricted to R. We are in a position to apply Lemma 2.2 to the automaton $\mathscr{A}_S$ and its ρ-class containing $Q.v_1$. The lemma gives us an invariant subset $T \subset S$ such that $r(\mathscr{A}_T) = r(\mathscr{A}_S) - 1$ and a word v_2 of length at most $|S| - |T| - |R|$ such that $(Q.v_1).v_2 \setminus T$ is a singleton. Now we can complete the proof by letting $P = Y \cup T$ and $v_P = v_1 v_2$. Let us check that these P and v_P satisfy all requirements in the definition of a reducible automaton.

The length of the word v_P is at most

$$(|Q/\rho| - |X| - 1) + (|S| - |T| - |R|) = (|Q/\rho| - |X| - |R|) + (|S| - |T| - 1).$$

The first summand in the right-hand side is the number of ρ-classes in the set $Q/\rho \setminus (X \cup R)$. It does not exceed the number of elements in these classes (because each ρ-class contains

at least one element) and the latter is equal to $|Q| - |Y| - |S|$. Thus, the length of v_P does not exceed

$$(|Q| - |Y| - |S|) + (|S| - |T| - 1) = |Q| - |T| - |Y| - 1 = |Q| - |P| - 1$$

as required. Finally, from (2) we obtain,

$$r(\mathscr{A}_P) = r(\mathscr{A}_Y) + r(\mathscr{A}_T) = r(\mathscr{A}_Y) + r(\mathscr{A}_S) - 1 = r(\mathscr{A}) - 1. \quad \square$$

Now we can prove Theorem 1.2 inducting on the rank k of our generalized monotonic automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$. By Proposition 2.3, there exists an invariant subset $P \subset Q$ such that $r(\mathscr{A}_P) = r(\mathscr{A}) - 1 = k - 1$ and $|Q.v_P \setminus P| = 1$ for some word v_P of length at most $|Q| - |P| - 1$.

First consider the case $k = 1$. Then we have $r(\mathscr{A}_P) = 0$ which means that the set P is empty. Therefore, $|Q.v_P| = 1$ whence v_P is a reset word (that is, a word of rank 1) of length at most $|Q| - 1$. Since $|Q| = n$ and $k = 1$, this yields the desired bound $n - k$.

Now let $k > 1$. The equality $|Q.v_P \setminus P| = 1$ means that $Q.v_P \subseteq P \cup \{q\}$ for some $q \in Q \setminus P$. Applying the induction assumption to the restriction $\mathscr{A}_P$, we obtain a word w of length at most $|P| - (k - 1)$ such that $|P.w| = k - 1$. Hence

$$|Q.v_P w| = |P.w \cup \{\delta(q, w)\}| \leqslant q(k - 1) + 1 = k.$$

But $r(\mathscr{A}) = k$, therefore $v_P w$ is a word of rank k and of length at most

$$(|Q| - |P| - 1) + (|P| - (k - 1)) = n - k. \qquad \square$$

For the sake of completeness we mention that the upper bound of Theorem 1.2 is tight because it is tight already for monotonic automata.

3. Discussion

In the introduction, we have mentioned in passing that our notion of a generalized monotonic automaton is a precise automata-theoretic counterpart for the concept of a transformation monoid preserving a chain of interval partitions introduced and studied by Almeida and Higgins [1]. The importance of the latter concept lies in the fact that, as shown in [1], that this class of transformation monoids is representative for the class of all finite aperiodic [1] monoids in the sense:

(i) every transformation monoid preserving a chain of interval partitions is aperiodic, and conversely,
(ii) every finite aperiodic monoid divides a transformation monoid preserving a chain of interval partitions.

We recall that finite aperiodic monoids play a distinguished role in the formal language theory via celebrated Schützenberger's theorem [15] stating that a language is star-free if and only if it can be recognized by a finite aperiodic monoid. In view of this fact, the representative property of Almeida–Higgins monoids can be reformulated as yet another

[1] Recall that a monoid is said to be *aperiodic* if all its subgroups are singletons.

characterization of the class of star-free languages: a language is star-free if and only if it can be recognized by a transformation monoid preserving a chain of interval partitions. Translating the latter characterization into automata-theoretic terms reveals the role of generalized monotonic automata: a language is star-free if and only if it can be recognized by a generalized monotonic automaton.

Let us call a deterministic finite automaton $\mathscr{A}$ *aperiodic* if the transition monoid of $\mathscr{A}$ is aperiodic, or in other words, if $\mathscr{A}$ can recognize only star-free languages. Since generalized monotonic automata are representative for the class of aperiodic automata, our Theorem 1.2 provides some evidence for the conjecture that the same statement may extend to all aperiodic automata. In particular, we conjecture that for every aperiodic synchronizing automaton with n states there exists a reset word of length at most $n-1$. An extensive computer search performed by Raskovalov, a student of the second-named author, also supports this conjecture. It should be mentioned that a quadratic upper bound for the length of reset words for aperiodic synchronizing automata has been recently established by Trahtman [16].

On the other hand, it is not very likely that a proof of the conjecture (if it is true) can be found by using the fact that every aperiodic automaton $\mathscr{A}$ can be emulated by a suitable generalized monotonic automaton $\mathscr{B}$. First of all, the property of being synchronizing does not, generally speaking, transfer from $\mathscr{A}$ to $\mathscr{B}$, and also the size of $\mathscr{B}$ normally exceeds the size of $\mathscr{A}$ by far so that an upper bound in terms of the size of $\mathscr{B}$ may make no sense for $\mathscr{A}$.

Added in proof. Recently the authors have found a series of aperiodic synchronizing automata $\mathscr{A}_n$ $(n = 5, 6, 7, \ldots)$ with n states such that the shortest reset word for the automaton $\mathscr{A}_n$ has length n. This refutes the conjecture discussed in Section 3.

Acknowledgements

The authors acknowledge support from the Science and Education Ministry of Russian Federation, Grants E02-1.0-143 and 04.01.059, and the President Program of Leading Scientific Schools, Grant 2227.2003.1. The paper was completed when the second-named author was visiting Laboratoire d'Informatique Algorithmique: Fondements et Applications at Université Paris 7 – Denis Diderot with support of Ministere de Education nationale de France.

References

[1] J. Almeida, P.M. Higgins, Monoids respecting n-chains of intervals, J. Algebra 187 (1997) 183–202.
[2] D.S. Ananichev, M. V. Volkov, Synchronizing monotonic automata, Theoret. Comput. Sci., accepted; A preliminary version has appeared, in: Z. Fülop, Z. Ézik (Eds.), Developments in Language Theory; 7th Internat. Conf., Szeged, 2003, Lecture Notes in Computer Science, Vol. 2710, 2003, pp. 111–121.
[3] J. Černý, Poznámka k homogénnym eksperimentom s konecnými automatami, Mat. -Fyz. Cas. Slovensk, Akad. Vied. 14 (1964) 208–216 [in Slovak].
[4] D. Eppstein, Reset sequences for monotonic automata, SIAM J. Comput. 19 (1990) 500–510.
[5] P. Frankl, An extremal problem for two families of sets, European J. Combin. 3 (1982) 125–127.

[6] J. Kari, A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull. 73 (2001) 146.
[7] S. Margolis, J.-E. Pin, M.V. Volkov, Words guaranteeing minimum image, Int. J. Foundations Comput. Sci. 15 (2004) 259–276.
[8] A. Mateescu, A. Salomaa, Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68 (1999) 134–150.
[9] 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).
[10] J.-E. Pin, Sur les mots synchronisants dans un automate fini, Elektronische Informationverarbeitung und Kybernetik 14 (1978) 283–289 (in French).
[11] J.-E. Pin, On two combinatorial problems arising from automata theory, Ann. Discrete Math. 17 (1983) 535–548.
[12] A. Salomaa, Generation of constants and synchronization of finite automata, J. Universal Comput. Sci. 8 (2002) 332–347.
[13] A. Salomaa, Synchronization of finite automata. Contributions to an old problem, in: T. Æ. Mogensen, D. A. Schmidt, I. H. Sudborough (Eds.), The Essence of Computation, Lecture Notes in Computer Science, Vol. 2566, 2002, pp. 37–59.
[14] A. Salomaa, Composition sequences for functions over a finite domain, Theoret. Comput. Sci. 292 (2003) 263–281.
[15] M.P. Schützenberger, On finite monoids having only trivial subgroups, Inform. Control 8 (1965) 190–194.
[16] A.N. Trahtman, Černý conjecture for DFA accepting star-free languages, submitted for publication .
[17] A.S. Vernitskiĭ, M.V. Volkov, A proof and a generalization of Higgins' division theorem for semigroups of order-preserving mappings, Russian Math. (Iz. VUZ) 39 (1995) 34–39.