International Journal of Foundations of Computer Science
Vol. 24, No. 2 (2013) 251–262

DOI: 10.1142/S0129054113400108

World Scientific
www.worldscientific.com

LOWER BOUNDS FOR THE LENGTH OF RESET WORDS IN EULERIAN AUTOMATA*

VLADIMIR V. GUSEV
Institute of Mathematics and Computer Science
Ural Federal University, Lenina 51
Ekaterinburg, 620083, Russia
vl.gusev@gmail.com

Received 30 November 2011
Accepted 13 July 2012
Communicated by Giorgio Delzanno and Igor Potapov

For each odd $n \geq 5$ we present a synchronizing Eulerian automaton with n states for which the minimum length of reset words is equal to $\frac{n^2-3n+4}{2}$. We also discuss various connections between the reset threshold of a synchronizing automaton and a sequence of reachability properties in its underlying graph.

Keywords: Synchronizing automata; exponent of digraph; Černý conjecture.

1. Background and Overview

A complete deterministic finite automaton $\mathscr{A}$ is called *synchronizing* if the action of some word w resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter at which state it is applied. Any such word w is said to be a *reset word* for the automaton. The minimum length of reset words for $\mathscr{A}$ is called the *reset threshold* of $\mathscr{A}$ and denoted by $\mathrm{rt}(\mathscr{A})$. Synchronizing automata constitute an interesting combinatorial object and naturally appear in many applications such as coding theory, robotics and testing of reactive systems. For a brief introduction to the theory of synchronizing automata we refer the reader to the recent surveys [11, 16]. The interest to the field is also heated by the famous Černý conjecture.

In 1964 Jan Černý [3] constructed for each $n > 1$ a synchronizing automaton $\mathscr{C}_n$ with n states whose reset threshold is $(n-1)^2$. Soon after that he 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 $(n-1)^2$. Despite intensive research, the best upper bound on the reset threshold of synchronizing automata with n states achieved so far is $\frac{n(7n^2+6n-16)}{48}$, see [15], so it is much larger

*Supported by the Russian Foundation for Basic Research, grant 10-01-00524, and by the Federal Education Agency of Russia, grant 2.1.1/13995.

than the conjectured value. Though the Černý conjecture is open in general, it has been confirmed for various restricted classes of synchronizing automata, see, e.g., [4, 6, 7, 14, 17]. We recall here a result by Jarkko Kari from [7] as it has served as a departure point for the present paper.

Kari [7] has shown that every synchronizing Eulerian automaton with n states possesses a reset word of length at most n^2-3n+3. Even though this result confirms the Černý conjecture for Eulerian automata, it does not close the synchronizability question for this class of automata since no matching lower bound for the reset threshold of Eulerian automata has been found so far. In order to find such a matching bound, we need a series of Eulerian automata with large reset threshold, which is the main problem that we address in the present paper.

Our first attempt was following an approach from [1]. In that paper, several examples of slowly synchronizing automata, which had been discovered in the course of a massive computational experiment, have been related to known examples of primitive graphs with large exponent from [5] and then have been expanded to infinite series. The idea was to apply a similar analysis to Eulerian graphs with large exponent that have been characterized in [13]. However, it turns out that in this way we cannot achieve results close to what we can get by computational experiments. Thus, a refinement of the approach from [1] appears to be necessary. Here we suggest such a refinement, and this is the main novelty of the present paper. As a concrete demonstration of our modified approach, we exhibit a series of slowly synchronizing Eulerian automata whose reset threshold is twice as large as the reset threshold of automata that can be obtained by a direct application of techniques from [1]. We believe that the method suggested in this paper can find a number of other applications and its further development may shed a new light on the properties of synchronizing automata.

2. Preliminaries

A *complete deterministic finite automaton* (DFA) is a couple $\mathscr{A} = \langle Q, \Sigma \rangle$, where Q stands for the *state set* and Σ for the *input alphabet* whose letters act on Q by totally defined transformations. The action of Σ on Q extends in natural way to an action of the set Σ^* of all words over Σ. The result of the action of a word $w \in \Sigma^*$ on the state $q \in Q$ is denoted by $q \cdot w$. Triples of the form $(q, a, q \cdot a)$ where $q \in Q$ and $a \in \Sigma$ are called *transitions* of the DFA; q, a and $q \cdot a$ are referred to as, respectively, the *source*, the *label* and the *target* of the transition $(q, a, q \cdot a)$.

By a *graph* we mean a tuple of sets and maps: the set of *vertices* V, the set of *edges* E, a map $t : E \to V$ that maps every edge to its *tail* vertex, and a map $h : E \to V$ that maps every edge to its *head* vertex. Notice that in a graph, there may be several edges with the same tail and head.[a] We assume the reader's acquaintance with basic notions of the theory of graphs such as path, cycle, isomorphism etc.

[a]Our graphs are in fact directed multigraphs with loops. But we use a short name, since no other graph species will show up in this paper.

Given a DFA $\mathscr{A} = \langle Q, \Sigma \rangle$, its *underlying graph* $D(\mathscr{A})$ has Q as the vertex set and has an edge e_τ with $t(e_\tau) = q$, $h(e_\tau) = q \cdot a$ for each transition $\tau = (q, a, q \cdot a)$ of $\mathscr{A}$. We stress that if two transitions have a common source and a common target (but different labels), then they give rise to different edges (with a common tail and a common head). It is easy to see that a graph D is isomorphic to the underlying graph of some DFA if and only if each vertex of D serves as the tail for the same number of edges (the number is called the *outdegree* of D). In the sequel, we always consider only graphs satisfying this property. Every DFA $\mathscr{A}$ such that $D \cong D(\mathscr{A})$ is called a *coloring* of D. Thus, every coloring of D is a labeling of its edges by letters from some alphabet and such that edges with a common tail get different colors. Figure 1 shows a graph and two of its colorings by $\Sigma = \{a, b\}$.

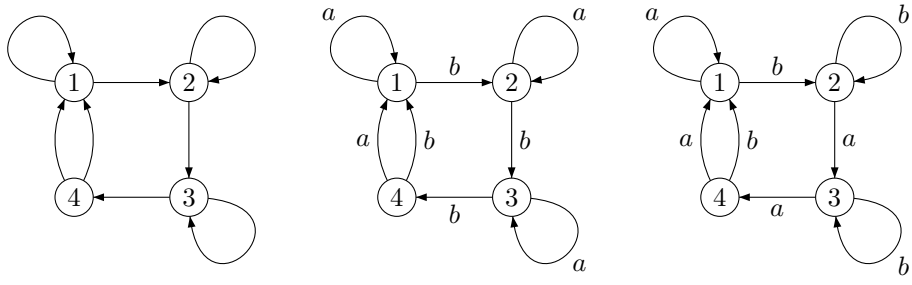

Fig. 1. A graph and two of its colorings.

A graph $D = \langle V, E \rangle$ is said to be *strongly connected* if for every pair $(v, v') \in V \times V$, there exists a path from v to v'. A graph is *Eulerian* if it is strongly connected and each of its vertices serves as the tail and as the head for the same number of edges. A DFA is said to be *Eulerian* if so is its underlying graph. More generally, we will freely transfer graph notions (such as path, cycle, etc) from graphs to automata they underlie.

A graph $D = \langle V, E \rangle$ is called *primitive* if there exists a positive integer t such that for every pair $(v, v') \in V \times V$, there exists a path from v to v' of length precisely t. The least t with this property is called the *exponent* of the graph D and is denoted by $\exp(D)$. Various facts concerning these classical notions can be found in [2].

Let w be a word over the alphabet $\Sigma = \{a_1, a_2, \ldots, a_k\}$. We say that a word $u \in \Sigma^*$ *occurs ℓ times as a factor of w* if there are exactly ℓ different words $x_1, \ldots, x_\ell \in \Sigma^*$ such that for each i, $1 \leq i \leq \ell$, there is a word $y_i \in \Sigma^*$ for which w has a decomposition $w = x_i u y_i$. The number ℓ is called the *number of occurrences of u in w* and is denoted by $|w|_u$. The vector $(|w|_{a_1}, |w|_{a_2}, \ldots, |w|_{a_k}) \in \mathbb{N}_0^k$ is called the *Parikh vector* of the word w; here $\mathbb{N}_0$ stands for the set of non-negative integers.

Now suppose that $\mathscr{A} = \langle Q, \Sigma \rangle$ is a DFA and α is a path in $\mathscr{A}$ labelled by a word $w \in \Sigma^*$. If a vector $\mathsf{v} \in \mathbb{N}_0^k$ is equal to the Parikh vector of w, then we say that v is the *Parikh vector* of the path α. We refer to any path that has v as its Parikh vector as a v-*path*.

3. Main Results

We start with revisiting the technique used in [1] to obtain lower bounds for the reset threshold of certain synchronizing automata.

Consider an arbitrary synchronizing automaton $\mathscr{A} = \langle Q, \Sigma\rangle$. Let w be a reset word for $\mathscr{A}$ that leaves the automaton in some state $r \in Q$, that is, $p \cdot w = r$ for every $p \in Q$. Then, for every state $p \in Q$, the word w labels a path from p to r. Therefore, for every state $p \in Q$ there is a path of length $|w|$ from p to r in the underlying graph $D(\mathscr{A})$. This leads us to the following notion. We say that a strongly connected graph $D = (V, E)$ is 0-*primitive* if there exists an integer $k > 0$ and a vertex $r \in V$ such that for every vertex $p \in V$ there is a path of length exactly k from p to r. The minimal integer k with this property (over all possible choices of r) is called the 0-*exponent* of D and is denoted by $\exp_0(D)$. We write $\exp_0(\mathscr{A})$ instead of $\exp_0(D(\mathscr{A}))$. Then we have that every synchronizing automaton $\mathscr{A}$ is 0-primitive and

$$\mathrm{rt}(\mathscr{A}) \geq \exp_0(\mathscr{A}). \tag{1}$$

It is not hard to see that the notions of 0-primitivity and primitivity are equivalent. Indeed, every primitive digraph is obviously 0-primitive. Conversely, let D be a 0-primitive digraph with n vertices. By the definition there are paths of length exactly $\exp_0(D)$ from every vertex to some fixed vertex r. Consider two arbitrary vertices p and q of D. Since D is strongly connected, there is a path α of length at most $n-1$ from r to q. Now take any path β of length $n-1-|\alpha|$ starting at p and let s be the endpoint of β. There is a path γ of length $\exp_0(D)$ from s to r. Now the path $\beta\gamma\alpha$ leads from p to q (through s and r) and $|\beta\gamma\alpha| = n - 1 + \exp_0(D)$. Thus, the digraph D is primitive, and moreover, we have the following inequality:

$$\exp_0(D) + n - 1 \geq \exp(D). \tag{2}$$

Obviously, we also have $\exp(D) \geq \exp_0(D)$. Thus, there is only linear difference between $\exp(D)$ and $\exp_0(D)$ in terms of n. The reader who may wonder why we need such a slight variation of the standard notion will see that this variation fits better into a more general framework that we will present below.

First, however, we demonstrate how to construct Eulerian automata with a relatively large reset threshold on the basis of the notion of 0-primitivity. For this, we need Eulerian digraphs with the largest possible exponent (or 0-exponent) among all primitive Eulerian digraphs with n vertices. Such digraphs have been classified by Shen [13].

For every odd $n \geq 5$, consider the automaton $\mathscr{D}_n$ with the state set $Q = \{1, 2, \ldots, n\}$ and the input letters a and b acting on Q as follows:

$1 \cdot a = 2$, $1 \cdot b = 3$; $(n-1) \cdot a = 2$, $(n-1) \cdot b = 1$; $n \cdot a = 1$, $n \cdot b = 3$; and for every $1 < k < n-1$

$$k \cdot a = \begin{cases} k+2 & \text{if } k \text{ is even,} \\ k+1 & \text{if } k \text{ is odd;} \end{cases} \qquad k \cdot b = \begin{cases} k+3 & \text{if } k \text{ is even,} \\ k+2 & \text{if } k \text{ is odd.} \end{cases}$$

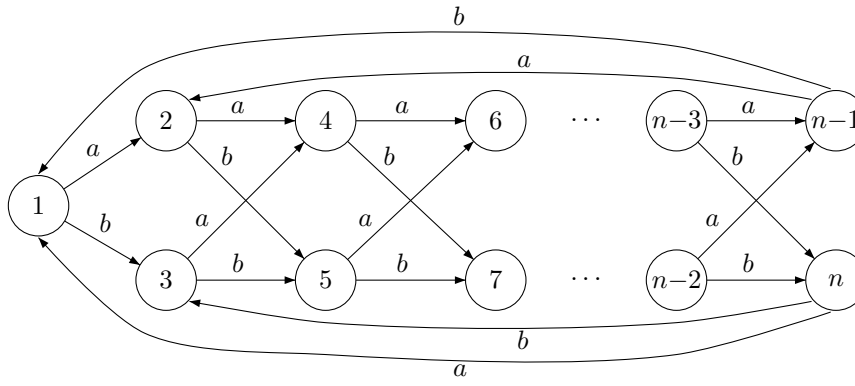

Fig. 2. The automaton $\mathscr{D}_n$.

The automaton $\mathscr{D}_n$ is shown in Fig. 2. We denote the underlying graph of $\mathscr{D}_n$ by $\mathcal{D}_n$.

Proposition 1 ([13, Theorem 1]**).** *If $\mathcal{G}$ is a primitive Eulerian graph with outdegree 2 and n vertices, $n \geq 8$, then* $\exp(\mathcal{G}) \leq \frac{(n-1)^2}{4} + 1$. *The equality holds only for the graph $\mathcal{D}_n$.*

Proposition 1 and the inequalities (1) and (2) guarantee that every synchronizing coloring of the graph $\mathcal{D}_n$ has reset threshold of magnitude $\frac{n^2}{4} + o(n^2)$. In particular, we can prove the following result using the technique developed in [1].

Proposition 2. *The reset threshold of the automaton $\mathscr{D}_n$ is equal to* $\frac{n^2-4n+11}{4}$.

Proof. We start with estimating $\exp_0(\mathscr{D}_n)$. Observe that for every $\ell \geq \exp_0(\mathscr{D}_n)$ there is a cycle of length ℓ in $\mathscr{D}_n$. Indeed, let r be a state such that for every $p \in Q$ there is a path of length $\exp_0(\mathscr{D}_n)$ from p to r. Now take an arbitrary path α of length $\ell - \exp_0(\mathscr{D}_n)$ starting at r and let s be the endpoint of α. By the choice of r, there is a path β of length $\exp_0(\mathscr{D}_n)$ from s to r. Thus, the path $\alpha\beta$ is a cycle of length exactly ℓ.

Now consider the partition π of the set Q into $\frac{n+1}{2}$ classes V_i, $0 \leq i \leq \frac{n-1}{2}$, where $V_0 = 1$ and $V_i = \{2i, 2i+1\}$ for every $0 < i \leq \frac{n-1}{2}$. We define a graph $\mathcal{G}_n$ with the quotient set Q/π as the vertex set and with the edges induced by the edges of $\mathcal{D}_n$ as follows: there is an edge e' in $\mathcal{G}_n$ with $t(e') = V_i$ and $h(e) = V_j$ if and only if there is an edge e in $\mathcal{D}_n$ with $t(e) \in V_i$ and $h(e) \in V_j$. Then every cycle in $\mathcal{D}_n$ induces a cycle of the same length in $\mathcal{G}_n$. In particular, for every $\ell \geq \exp_0(\mathscr{D}_n)$ there is a cycle of length ℓ in $\mathcal{G}_n$. It is easy to see that the graph $\mathcal{G}_n$ has precisely two simple cycles: one of length $\frac{n-1}{2}$ and one of length $\frac{n+1}{2}$. We conclude that every $\ell \geq \exp_0(\mathscr{D}_n)$ is expressible as a non-negative integer combination of $\frac{n-1}{2}$ and $\frac{n+1}{2}$.

Here we invoke well-known and elementary result from arithmetic. It was obtained by James Joseph Sylvester in 1884:

Lemma 3 ([10, Theorem 2.1.1]**).** *If k_1, k_2 are relatively prime positive integers, then $k_1k_2 - k_1 - k_2$ is the largest integer that is not expressible as a non-negative integer combination of k_1 and k_2.*

Applying Lemma 3 we conclude that $\exp_0(\mathscr{D}_n) \geq \frac{n^2-4n+3}{4}$ and there is no cycle of length $\frac{n^2-4n-1}{4}$ in $\mathcal{G}_n$. The inequality 1 implies that $\mathrm{rt}(\mathscr{D}_n) \geq \frac{n^2-4n+3}{4}$, and it remains to exclude two cases: $\mathrm{rt}(\mathscr{D}_n) = \frac{n^2-4n+3}{4}$ and $\mathrm{rt}(\mathscr{D}_n) = \frac{n^2-4n+7}{4}$. This is easy.

Suppose that w is a shortest reset word for $\mathscr{D}_n$ which leaves $\mathscr{D}_n$ in some state $r \in V_i$. Note that $i \neq 0$ (otherwise the word obtained by removing the last letter from w would be a shorter reset word, and this is impossible).

If $|w| = \frac{n^2-4n+3}{4}$, we write $w = xw'$ for some letter x and apply the word w to some state from V_{i-1}. We conclude that w' induces a cycle from V_i to V_i in $\mathcal{G}_n$. This cycle would be of length $\frac{n^2-4n-1}{4}$, which is impossible.

Finally suppose that the length of w is $\frac{n^2-4n+7}{4}$. If $i \neq 1$, then the same argument as in the previous paragraph leads to a contradiction. (We just apply w to a state from V_{i-2}.) If $i = 1$, let $w = xyw'$ for some letters x and y. Depending on x, either $n \cdot xy \in V_1$ or $(n-1) \cdot xy \in V_1$. In both cases w' induces a cycle from V_1 to V_1 in $\mathcal{G}_n$ of length $\frac{n^2-4n-1}{4}$, which is impossible.

We thus see that the reset threshold of the automaton $\mathscr{D}_n$ is at least $\frac{n^2-4n+11}{4}$. Since the word $aa(ba^{\frac{n-1}{2}})^{\frac{n-5}{2}}bb$ resets $\mathscr{D}_n$, we conclude that this bound is tight. □

Our computational experiments suggest that the largest reset threshold among all synchronizing colorings of $\mathcal{D}_n$ is equal to $\frac{(n-1)^2}{4} + 1$. Therefore, it seems that $\frac{n^2}{4} + o(n^2)$ is the best lower bound on the reset threshold of synchronizing Eulerian automata with n states that can be obtained by a direct encoding of Eulerian graphs with large exponent. However, our main result (see Theorem 6 below) shows that for every odd n there is a synchronizing Eulerian automaton with n states and reset threshold $\frac{n^2-3n+4}{2}$. This lead us to idea that the notion of 0-exponent is too weak to be useful for isolating synchronizing Eulerian automata with maximal reset threshold (although, we can not prove it rigorously). The reason for this is that we have discarded too much information when passing from synchronizability to 0-primitivity — we forget everything about paths labelled by reset words except their length. Thus, we use another notion in which more information is preserved, namely, the Parikh vectors of the paths leading to the same state are taken into account.

Consider a DFA $\mathscr{A} = \langle Q, \Sigma \rangle$ with $|\Sigma| = k$ and fix some ordering of the letters in Σ. We define a subset $\mathrm{E}_1(\mathscr{A})$ of $\mathbb{N}_0^k$ as follows: a vector $\mathsf{v} \in \mathbb{N}_0^k$ belongs to $\mathrm{E}_1(\mathscr{A})$ if and only if there is state $r \in Q$ such that for every $p \in Q$, there exists a v-path from p to r. If the set $\mathrm{E}_1(\mathscr{A})$ is non-empty, then the automaton $\mathscr{A}$ is called 1-*primitive*. The minimum value of the sum $i_1 + i_2 + \cdots + i_k$ over all k-tuples $(i_1, i_2, \ldots, i_k)$ from $\mathrm{E}_1(\mathscr{A})$ is called the 1-*exponent* of $\mathscr{A}$ and denoted by $\exp_1(\mathscr{A})$. We would like to

note that a very close concept for colored multigraphs has been studied in [8, 12]. Clearly, every synchronizing automaton $\mathscr{A}$ is 1-primitive and

$$\mathrm{rt}(\mathscr{A}) \geq \exp_1(\mathscr{A}). \tag{3}$$

In order to illustrate how the notion of 1-exponent may be utilized, we prove a statement concerning the Černý automata $\mathscr{C}_n$ (this statement will be used in the proof of our main result). Recall the definition of $\mathscr{C}_n$. The state set of $\mathscr{C}_n$ is $Q = \{1, 2, \ldots, n\}$ and the letters a and b act on Q as follows:

$$i \cdot a = \begin{cases} 2 & \text{if } i = 1, \\ i & \text{if } 1 < i; \end{cases} \qquad i \cdot b = \begin{cases} i+1 & \text{if } i < n, \\ 1 & \text{if } i = n. \end{cases}$$

The automaton $\mathscr{C}_n$ for $n = 7$ is shown in Fig. 3. Here and below we adopt the convention that edges bearing multiple labels represent bunches of edges sharing tails and heads. In particular, the edge $1 \xrightarrow{a,b} 2$ in Fig. 3 represents the two parallel edges $1 \xrightarrow{a} 2$ and $1 \xrightarrow{b} 2$.

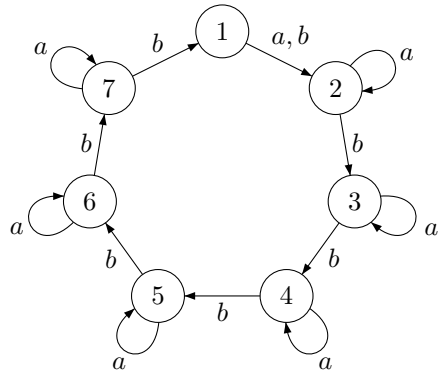

Fig. 3. The automaton $\mathscr{C}_n$ for $n = 7$.

Proposition 4. *Every reset word of the automaton $\mathscr{C}_n$ contains at least $n^2 - 3n + 2$ occurrences of the letter b and at least $n - 1$ occurrences of the letter a.*

Proof. Since the automaton $\mathscr{C}_n$ is synchronizing, the set $\mathrm{E}_1(\mathscr{C}_n)$ is non-empty. We make use of the following simple property of $\mathrm{E}_1(\mathscr{C}_n)$: if $\mathsf{v} = (\alpha, \beta) \in \mathrm{E}_1(\mathscr{C}_n)$, then for every $t \in \mathbb{N}$ we have $(\alpha, \beta + t) \in \mathrm{E}_1(\mathscr{C}_n)$. Indeed, let r be a state such that for every $p \in Q$ there is a v-path from p to r. We aim to show that there is also an $(\alpha, \beta + t)$-path from an arbitrary state p to r. Let $q = p \cdot b^t$, then by definition of r there is a v-path from q to r. Augmenting this path in the beginning by the path starting at p and labeled b^t, we obtain an $(\alpha, \beta + t)$-path from p to r.

Now observe that there is a v-path from r to r. This path is a cycle and it can be decomposed into simple cycles of the automaton $\mathscr{C}_n$. The simple paths in $\mathscr{C}_n$ are

loops labeled a with the Parikh vector $(1,0)$, the cycle

$$1 \xrightarrow{a} 2 \xrightarrow{b} 3 \xrightarrow{b} \ldots \xrightarrow{b} n-1 \xrightarrow{b} n \xrightarrow{b} 1$$

with the Parikh vector $(1,n-1)$ and the cycle

$$1 \xrightarrow{b} 2 \xrightarrow{b} 3 \xrightarrow{b} \ldots \xrightarrow{b} n-1 \xrightarrow{b} n \xrightarrow{b} 1$$

with the Parikh vector $(0,n)$. Thus, there are some $x,y,z \in \mathbb{N}_0$ such that the following equality holds true:

$$(\alpha,\beta) = x(1,0) + y(1,n-1) + z(0,n).$$

It readily implies that $\beta = y(n-1)+zn$. Since for every $t \in \mathbb{N}$ the vector $(\alpha,\beta+t)$ also belongs to $\mathrm{E}_1(\mathscr{C}_n)$, we conclude that $\beta+t$ is also expressible as a non-negative integer combination of n and $n-1$. Lemma 3 implies that $\beta \geq n(n-1)-n-(n-1)+1 = n^2-3n+2$. If w is a reset word of the automaton $\mathscr{C}_n$, then the Parikh vector of w belongs to $\mathrm{E}_1(\mathscr{C}_n)$, whence w contains at least n^2-3n+2 occurrences of the letter b.

It remains to prove that w contains at least $n-1$ occurrences of the letter a. Note that for every set S of states, we have $|S\cdot b| = |S|$ and $|S\cdot a| \geq |S|-1$. Hence, to decrease the cardinality from n to 1, one has to apply a at least $n-1$ times, and any word w such that $|Q\cdot w| = 1$ must contain at least $n-1$ occurrences of a. □

As a corollary we immediately obtain Černý's result [3, Lemma 1] that $\mathrm{rt}(\mathscr{C}_n) = (n-1)^2$. Indeed, Proposition 4 implies that the reset threshold is at least $(n-1)^2$, and it is easy to check that the word $(ab^{n-1})^{n-2}a$ of length $(n-1)^2$ resets $\mathscr{C}_n$. Also we see that a reset word w of minimal length for $\mathscr{C}_n$ is unique. Indeed, w cannot start or end with b because b acts as a cyclic permutation. Thus, $w = aua$ and the word u has n^2-3n+2 occurrences of b and $n-3$ occurrences of a. Note that b^n cannot occur as a factor of u since b^n acts is an identity mapping. Clearly, there is only one way to insert $n-3$ letters a in the word b^{n^2-3n+2} such that the resulting word contains no factor b^n. Though the series $\mathscr{C}_n$ is very well studied, to the best of our knowledge the uniqueness of the shortest reset word for $\mathscr{C}_n$ has not been explicitly stated in the literature.

Observe that $\exp_0(\mathscr{C}_n) = n-1$ and we could not extract any strong lower bound for $\mathrm{rt}(\mathscr{C}_n)$ from the inequality (2). In [1] a tight lower bound for $\mathrm{rt}(\mathscr{C}_n)$ has been obtained in an indirect way, via relating $\mathscr{C}_n$ to graphs with largest possible 0-exponent from [18]. In contrast, Proposition 4 implies that $\exp_1(\mathscr{C}_n)$ is close to $(n-1)^2$, so the inequality (3) gives a stronger lower bound. In fact, $\exp_1(\mathscr{C}_n) = \mathrm{rt}(\mathscr{C}_n)$. Thus, the inequality (3) gives tight lower bound. But we need additional efforts to prove it.

Proposition 5. *For every $n \geq 2$, the 1-exponent of $\mathscr{C}_n$ is equal to $(n-1)^2$.*

Proof. Consider words $u_1, u_2, \ldots, u_n$ with the same Parikh vector (α,β), such that $i\cdot u_i = 1$. We will see later that such words do exist. The path marked by u_i can

be naturally divided in two parts: a path from the state i till the first occurrence of the state 1, and a cycle containing state 1. Parikh vector of the first part of the path is equal to $(s_i, n-i+1)$ for some non-negative integer s_i, since it must contain exactly $n-i+1$ occurrences of letter b. If we represent the second part of the path in the same way as we did in Proposition 4 we obtain the following equality:

$$(\alpha, \beta) = (s_i, n-i+1) + x_i(1,0) + y_i(1, n-1) + z_i(0, n),$$

where x_i, y_i, z_i are non-negative integers. We are going to show that for some i we have $y_i \geq n-1$. Let us focus on the number of letters b modulo n. For every i we have $\beta \equiv n - i + 1 + y_i(n-1) + z_i n \ (mod\ n)$. Trivially, we obtain an equality:

$$y_i \equiv 1 - i - \beta \ (mod\ n).$$

Since it is true for every $i \in \{1, 2, \ldots, n\}$ we conclude that there is j such that $y_j \equiv n-1 \ (mod\ n)$. Inequality $y_j \geq 0$ easily implies $y_j \geq n-1$. Thus, we have $|u_j| \geq n y_j \geq n(n-1)$.

Let $v_1, v_2, \ldots, v_n$ be the words that witness 1-exponent of $\mathscr{C}_n$, and r be the state in which we end up after applying them to their corresponding states. Let w be the shortest path from r to 1. Note, that $|w| \leq n-1$. Then the words $v_1 w, v_2 w, \ldots, v_n w$ have common Parikh vector and lead corresponding states to the state 1. By the first part of the proof we have $\exp_1(\mathscr{C}_n) + n - 1 \geq n(n-1)$. Therefore, $\exp_1(\mathscr{C}_n) \geq (n-1)^2$. The inequality 3 and the fact $\mathrm{rt}(\mathscr{C}_n) = (n-1)^2$ ensure that this bound is tight. □

Now we are ready to present the main result of this paper. We define the automaton $\mathscr{M}_n$ (from Matricaria) on the state set $Q = \{1, 2, \ldots, n\}$, where $n \geq 5$ is odd, in which the letters a and b act as follows:

$$k \cdot a = \begin{cases} k & \text{if } k \text{ is odd,} \\ k+1 & \text{if } k \text{ is even;} \end{cases} \qquad k \cdot b = \begin{cases} k+1 & \text{if } k \neq n \text{ is odd,} \\ k & \text{if } k \text{ is even,} \\ 1 & \text{if } k = n. \end{cases}$$

Observe that $\mathscr{M}_n$ is Eulerian. The automaton $\mathscr{M}_n$ for $n = 7$ is shown in Fig. 4 on the left.

Theorem 6. *If $n \geq 5$ is odd, then the automaton $\mathscr{M}_n$ is synchronizing and its reset threshold is equal to $\frac{n^2-3n+4}{2}$.*

Proof. Let w be a reset word of minimum length for $\mathscr{M}_n$. Note that the action of aa is the same as the action of a. Therefore aa could not be a factor of w. (Otherwise reducing this factor to just a results in a shorter reset word.) So every occurrence of a, maybe except the last one, is followed by b. If we let $c = ab$, then either w or wb (if w ends with a) could be rewritten into a word u over the alphabet $\{b, c\}$. The actions of b and c induce a new automaton on the state set of $\mathscr{M}_n$ (this induced automaton is shown in Fig. 4 on the right). It is not hard to see that in both cases u is a reset word for the induced automaton. After applying the first letter of u it remains to

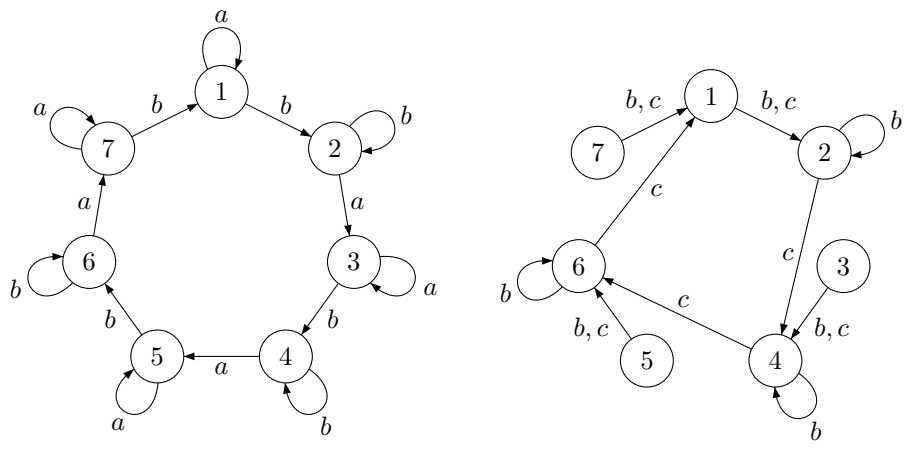

Fig. 4. The automaton $\mathscr{M}_n$ for $n = 7$ and the automaton induced by the actions of b and $c = ab$.

synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$.

Suppose $u = u'c$ for some word u' over $\{b, c\}$. Since the action of c on any subset of S cannot decrease its cardinality, we conclude that u' is also a reset word for the induced automaton. But c is the last letter of u only if $w = w'a$ and w' was rewritten into u'. Thus, w' also is a reset word for $\mathscr{M}_n$, which is a contradiction. So, w was rewritten into u, not wb.

If $u = xu'$ for some letter x, then by Proposition 4 we conclude that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b. Since each occurrence of c in u' corresponds to an occurrence of the factor ab in w, we conclude that the length of w is at least $1 + 2\frac{n^2-4n+3}{4} + \frac{n-1}{2} = \frac{n^2-3n+4}{2}$.

One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ is a reset word for $\mathscr{M}_n$ whence the above bound is tight. □

It is not hard to see that $\exp_0(\mathscr{M}_n) = n - 1$ and also $\exp_1(\mathscr{M}_n)$ is linear in n. Thus, both the 0-exponent and the 1-exponent are far too weak to give a good lower bound for the reset threshold of $\mathscr{M}_n$. That is why we have obtained a tight lower bound for $\mathrm{rt}(\mathscr{M}_n)$ in an indirect way, via relating $\mathscr{M}_n$ to an automaton with a large 1-exponent (namely, to $\mathscr{C}_{\frac{n+1}{2}}$). Now we are going to develop a notion that can give a good bound in a more direct way.

Observe that the most important part of the proof of Theorem 6 deals with estimating the number of occurrences of the factor ab in a reset word. In fact, a rough estimation can be done directly. Let w be a reset word that leaves $\mathscr{M}_n$ in the state 2 and $k = |w|_{ab}$. Consider a path from 2 to 2 in which the state 2 does not occur in the middle. Words labeling such paths come from the language $L = b^*(a^+b^+)^{\frac{n-1}{2}}ba^*b$. Thus, w can be divided into several blocks from L. Since every block has either $\frac{n-1}{2}$ or $\frac{n+1}{2}$ occurrences of the factor ab, we conclude that k

is expressible as a non-negative integer combination of the numbers $\frac{n-1}{2}$ and $\frac{n+1}{2}$. Note that $(ab)^t w$, where $t \in \mathbb{N}$, is a reset word that leaves $\mathscr{M}_n$ in the state 2. Since ab occurs $k+t$ times as a factor in $(ab)^t w$, we see that $k+t$ also is expressible as a non-negative integer combination of $\frac{n-1}{2}$ and $\frac{n+1}{2}$. Applying Lemma 3 we conclude that $k \geq \frac{n^2-4n+3}{4}$. Thus, the length of w is at least $\frac{n^2-4n+3}{2}$.

The above reasoning suggests the following generalization. Let $\mathscr{A} = \langle Q, \Sigma \rangle$ be a DFA with $Q = \{1, 2, \ldots, n\}$ and let k be a non-negative integer. We say that the automaton $\mathscr{A}$ is *k-primitive* if there exist words $u_1, u_2, \ldots, u_n$ such that $1 \cdot u_1 = 2 \cdot u_2 = \cdots = n \cdot u_n$ and for every word v of length at most k we have $|u_1|_v = |u_2|_v = \ldots = |u_n|_v$. Note that the last condition implies that all words $u_1, u_2, \ldots, u_n$ have the same length. The minimal length of words that witness k-primitivity of $\mathscr{A}$ is called the *k-exponent* of $\mathscr{A}$ and is denoted by $\exp_k(\mathscr{A})$. Observe that the rough estimation in the previous paragraph shows that $\exp_2(\mathscr{M}_n)$ is close to $\mathrm{rt}(\mathscr{M}_n)$.

Consider now an arbitrary synchronizing automaton $\mathscr{A}$. It is clear that $\mathscr{A}$ is k-primitive for every k and $\mathrm{rt}(\mathscr{A}) \geq \exp_k(\mathscr{A})$. Thus, we have the following non-decreasing sequence:

$$\exp_0(\mathscr{A}) \leq \exp_1(\mathscr{A}) \leq \cdots \leq \exp_k(\mathscr{A}) \leq \exp_{k+1}(\mathscr{A}) \leq \ldots . \tag{4}$$

At every next step we require that the words $u_1, u_2, \ldots, u_n$ get more similar to each other than they were in previous step. Thus, eventually these words converge to a reset word and the sequence stabilizes at $\mathrm{rt}(\mathscr{A})$. So we hope that studying the sequence (4) may lead to a new approach to the Černý conjecture.

References

[1] Ananichev, D.S., Gusev, V.V., Volkov, M.V.: Slowly synchronizing automata and digraphs. MFCS 2010, LNCS 6281, 55–65 (2010)

[2] Brualdi R., Ryser H.: Combinatorial Matrix Theory. Cambridge University Press (1991).

[3] Černý, J.: Poznámka k homogénnym eksperimentom s konečnými automatami. Matem.-fyzikalny Časopis Slovensk. Akad. Vied 14(3), 208–216 (1964) (in Slovak)

[4] Dubuc, L.: Sur les automates circulaires et la conjecture de Černý. RAIRO Inform. Théor. Appl. 32, 21–34 (1998) (in French)

[5] Dulmage, A.L., Mendelsohn, N.S.: Gaps in the exponent set of primitive matrices. Ill. J. Math. 8, 642–656 (1964)

[6] Eppstein, D.: Reset sequences for monotonic automata. SIAM J. Comput. 19, 500–510 (1990)

[7] Kari, J.: Synchronizing finite automata on Eulerian digraphs. Theoret. Comput. Sci. 295, 223–232 (2003)

[8] Olesky, D.D., Shader, B., van den Driessche, P.: Exponents of tuples of nonnegative matrices. Linear Algebra Appl. 356, 123–134 (2002)

[9] Pin, J.-E.: On two combinatorial problems arising from automata theory. Ann. Discrete Math. 17, 535–548 (1983)

[10] Ramírez Alfonsín, J.L.: The diophantine Frobenius problem. Oxford University Press (2005)

[11] Sandberg, S.: Homing and synchronizing sequences, Model-Based Testing of Reactive Systems 2004, LNCS 3472, 5–33 (2005)
[12] Shader, B.L., Suwilo, S.: Exponents of nonnegative matrix pairs, Linear Algebra Appl. 363, 275–293 (2003)
[13] Shen, J.: Exponents of 2-regular digraphs, Discrete Math. 214, 211–219 (2000)
[14] Trahtman, A.N.: The Černý conjecture for aperiodic automata. Discrete Math. Theor. Comput. Sci. 9(2), 3–10 (2007)
[15] Trahtman A.N.: Modifying the Upper Bound on the Length of Minimal Synchronizing Word. Lect. Notes in Comp. Sci, 173–180, 6914 (2011)
[16] Volkov, M.V.: Synchronizing automata and the Černý conjecture, LATA 2008, LNCS 5196, 11–27 (2008)
[17] Volkov, M.V.: Synchronizing automata preserving a chain of partial orders, Theoret. Comput. Sci. 410, 2992–2998 (2009)
[18] Wielandt, H.: Unzerlegbare, nicht negative Matrizen. Math. Z. 52, 642–648 (1950) (in German)