Acta Informatica (2009) 46:591–607
DOI 10.1007/s00236-009-0106-7

ORIGINAL ARTICLE

Strongly transitive automata and the Černý conjecture

Arturo Carpi · Flavio D'Alessandro

Received: 2 December 2008 / Accepted: 21 September 2009 / Published online: 10 October 2009

Abstract The synchronization problem is investigated for a new class of deterministic automata called strongly transitive. An extension to unambiguous automata is also considered.

1 Introduction

The *synchronization problem* for a deterministic n-state automaton consists in the search of an input-sequence, called a *synchronizing word*, such that the state attained by the automaton, when this sequence is read, does not depend on the initial state of the automaton itself. If such a sequence exists, the automaton is called *synchronizing*. If a synchronizing automaton is deterministic and complete, a well-known conjecture by Černý [7] claims that it has a synchronizing word of length not larger than $(n-1)^2$. This conjecture has been shown to be true for several classes of automata (cf. [1,2,7,9,11,12,14,16,18,19]). Complexity issues for this problem have been studied in [11]. The interested reader is referred to [20] for a historical survey of the problem. Two of the quoted references deserve a special mention: in [14], Kari proved the Černý conjecture for Eulerian automata, that is, for automata whose underlying graph is Eulerian. Dubuc [9] proved the conjecture for circular automata, that is, for automata possessing a letter that acts as a circular permutation over the set of states of the automaton. In [2], Béal proposed a unified algebraic approach, based upon rational series, that allows one to

This work was partially supported by MIUR project "Linguaggi formali e automi: teoria e applicazioni" and by fundings "Facoltà di Scienze MM. FF. NN. 2006" of the University of Rome "La Sapienza".

A. Carpi
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia,
via Vanvitelli 1, 06123 Perugia, Italy
e-mail: carpi@dipmat.unipg.it

F. D'Alessandro (✉)
Dipartimento di Matematica, Università di Roma "La Sapienza",
Piazzale Aldo Moro 2, 00185 Rome, Italy
e-mail: dalessan@mat.uniroma1.it

obtain upper bounds $2n^2 - 6n + 5$ and $n^2 - 3n + 3$ for the length of the shortest synchronizing word in an n-state synchronizing automaton which is, respectively, circular or Eulerian. In the first part of this paper (see Sect. 3), the synchronization problem for deterministic and complete automata is studied. This study is based upon a new notion, called *strongly transitivity* introduced in this paper. An n-state automaton is said to be strongly transitive if it is equipped by a set of n words $\{w_1, \ldots, w_n\}$, called *independent*, such that, for any two given states s and t, there exists a (unique) word w_i such that $sw_i = t$. This notion naturally extends that of transitivity, that is the property of being strongly connected for the underlying graph of the automaton. Some combinatorial properties of strongly transitive automata are investigated and, in particular, it is shown that several well-studied classes of automata are contained in the class of strongly transitive automata. A remarkable family of automata that satisfy the above mentioned property is that of transitive synchronizing automata. This result together with the fact that the study of the Černý conjecture can be always reduced, without loss of generality, to this class of automata should make this concept highly non trivial in this theoretical setting.

The main result of this section is that any synchronizing strongly transitive n-state automaton has a synchronizing word of length not larger than

$$(n-2)(n+L-1)+1,$$

where L denotes the length of the longest word of an independent set of words of the automaton. This result is proved by developing the theoretical approach of [2]. As a straightforward corollary of this result, one can obtain the bound $2(n-2)(n-1)+1$ for the shortest synchronizing word of any n-state synchronizing circular automaton. As we previously pointed out, together with this result, some basic properties of such automata are investigated. It is shown that circular automata and transitive synchronizing automata are strongly transitive. In particular, it is proved that if a transitive n-state automaton has a synchronizing word u, then it has an independent set of words of length not larger than $|u| + n - 1$. It is also proved that the previous upper bound is tight. More precisely, we construct an infinite family of synchronizing strongly transitive automata such that any independent set of the automaton contains a word whose length is not smaller than $|u| + n - 1$ where u is the shortest synchronizing word. Moreover we give examples of strongly transitive automata which are neither circular nor synchronizing.

In Sect. 4, we focus our attention on the class of unambiguous automata. We recall that the synchronization problem is closely related to that of finding short words of minimal rank in an automaton. Here, the rank of a word is the linear rank of the associated transition relation and thus a synchronizing word is a word of rank 1. In general, the length of the shortest word of minimal rank in a nondeterministic automaton is not polynomially upperbounded by the number of states of the automaton [13]. However in the case of unambiguous automata, such a bound exists: in [5] it is shown that for an n-state complete unambiguous and transitive automaton, there exists a word of minimal rank r of length less than $\frac{1}{2}rn^3$. Some interesting results on such class of automata have been recently proven in [3].

In this paper, we consider unambiguous and transitive automata on an alphabet A satisfying the following combinatorial property: there exist two sets of words V and W such that $A \subseteq V$, W and, for any state s, one has

$$\sum_{v \in V} \mathrm{Card}(sv) \geq \mathrm{Card}(V) \quad \text{and} \quad \sum_{w \in W} \mathrm{Card}(sw^{-1}) \geq \mathrm{Card}(W).$$

For instance, Eulerian automata satisfy the previous conditions with $V = W = A$. The main result of this section is that a synchronizing unambiguous n-state automaton satisfying the previous conditions has a synchronizing word of length not larger than

$$(n-2)(n+L-1)+1,$$

where L is the maximal length of the words of the set $V \cup W$. In particular, we derive that any transitive synchronizing unambiguous Eulerian n-state automaton has a synchronizing word of length not larger than $(n-1)^2$.

Some of the results of this paper were presented in undetailed form at DLT 2008 [6].

2 Preliminaries

We assume that the reader is familiar with the theory of automata and rational series. In this section we shortly recall a vocabulary of few terms and we fix the corresponding notation used in the paper.

Let A be a finite alphabet and let A^* be the free monoid of words over the alphabet A. The identity of A^* is called the *empty word* and is denoted by ϵ. The *length* of a word of A^* is the integer $|w|$ inductively defined by $|\epsilon| = 0$, $|wa| = |w| + 1$, $w \in A^*$, $a \in A$. If n is a positive integer, A^n denotes the set of all words of A^* of length equal to n. For any $u \in A^*$ and $a \in A$, $|u|_a$ denotes the number of occurrences of the letter a in u. For any finite set W of words of A^*, we denote by L_W the length of the longest word in W.

A finite automaton is a triple $\mathcal{A} = (S, A, \delta)$ where S is a finite set of elements called *states* and δ is a map

$$\delta : S \times A \longrightarrow \Pi(S)$$

from $S \times A$ into the family $\Pi(S)$ of all subsets of S. The map δ is called the *transition function* of $\mathcal{A}$. The canonical extension of the map δ to the set $S \times A^*$ is still denoted by δ. For any $u \in A^*$ and $s \in S$, the set of states $\delta(s, u)$ will be also denoted su. If P is a subset of S and u is a word of A^*, we denote by Pu and Pu^{-1} the sets:

$$Pu = \bigcup_{s \in P} su, \quad Pu^{-1} = \{s \in S \mid su \cap P \neq \emptyset\}.$$

If $\mathrm{Card}(sa) \leq 1$ for all $s \in S$, $a \in A$, the automaton $\mathcal{A}$ is *deterministic*; if $Sw \neq \emptyset$ for all $w \in A^*$, $\mathcal{A}$ is *complete*; if $\bigcup_{w \in A^*} sw = S$ for all $s \in S$, $\mathcal{A}$ is *transitive*. If $n = \mathrm{Card}(S)$, we will say that $\mathcal{A}$ is an n-state automaton. Let $\mathcal{A}$ be a deterministic automaton. A *synchronizing* or *reset* word is a word $u \in A^*$ such that $\mathrm{Card}(Su) = 1$. The state q such that $Su = \{q\}$ is called the *reset state* of u. A *synchronizing* deterministic automaton is an automaton that has a reset word. The following conjecture has been raised in [7].

Černý conjecture *Each synchronizing complete deterministic n-state automaton has a reset word of length not larger than $(n-1)^2$.*

We recall that a *formal power series* with rational coefficients and non-commuting variables in A is a mapping of the free monoid A^* into $\mathbb{Q}$. A series $\mathcal{S} : A^* \to \mathbb{Q}$ is *rational* if there exists a triple (α, μ, β) where

- $\alpha \in \mathbb{Q}^{1\times n}$, $\beta \in \mathbb{Q}^{n\times 1}$ are a horizontal and a vertical vector, respectively,
- $\mu : A^* \to \mathbb{Q}^{n\times n}$ is a morphism of the free monoid A^* in the multiplicative monoid $\mathbb{Q}^{n\times n}$ of matrices with coefficients in $\mathbb{Q}$,
- for every $u \in A^*$, $\mathcal{S}(u) = \alpha\mu(u)\beta$.

The triple (α, μ, β) is called *a representation* of $\mathcal{S}$ and the integer n is called its *dimension*. With a minor abuse of language, if no ambiguity arises, the number n will be also called the dimension of $\mathcal{S}$. Let $\mathcal{A} = (S, A, \delta)$ be any n-state automaton. One can associate with $\mathcal{A}$ a morphism

$$\varphi_{\mathcal{A}} : A^* \to \mathbb{Q}^{S\times S},$$

of the free monoid A^* in the multiplicative monoid $\mathbb{Q}^{S\times S}$ of matrices over the set of rational numbers, defined as: for any $a \in A$ and for any $s, t \in S$,

$$\varphi_{\mathcal{A}}(a)_{st} = \begin{cases} 1 & \text{if } t \in sa \\ 0 & \text{otherwise.} \end{cases}$$

It is worth to recall some well-known properties of the map $\varphi_{\mathcal{A}}$. For every $u \in A^*$ and for every $s, t \in S$, the coefficient $\varphi_{\mathcal{A}}(u)_{st}$ is the number of all distinct computations of $\mathcal{A}$ from s to t labelled by u.

If every matrix of the monoid $\varphi_{\mathcal{A}}(A^*)$ is such that every row does not contain more than one non-null entry, then $\mathcal{A}$ is deterministic.

If $\varphi_{\mathcal{A}}(A^*)$ does not contain the null matrix then $\mathcal{A}$ is complete. The following result is important [4, Corollary 3.6].

Proposition 1 *Let $\mathcal{S} : A^* \to \mathbb{Q}$ be a rational series of dimension n with coefficients in $\mathbb{Q}$. If, for every $u \in A^*$ such that $|u| \leq n-1$, $\mathcal{S}(u) = 0$ the series $\mathcal{S}$ is null.*

As a corollary we obtain the following well-known result (see [4,10]).

Theorem 1 (Moore, Conway) *Let $\mathcal{S}_1,\ \mathcal{S}_2 : A^* \to \mathbb{Q}$ be two rational series with coefficients in $\mathbb{Q}$ of dimension n_1 and n_2, respectively. If, for every $u \in A^*$ such that $|u| \leq n_1 + n_2 - 1$, $\mathcal{S}_1(u) = \mathcal{S}_2(u)$, the series $\mathcal{S}_1$ and $\mathcal{S}_2$ are equal.*

Let P be a subset of S. We associate with P a series $\mathcal{S}$ with coefficients in $\mathbb{Q}$ defined as: for every $u \in A^*$,

$$\mathcal{S}(u) = \mathrm{Card}(Pu^{-1}) - \mathrm{Card}(P). \tag{1}$$

The following result was proven in [2, Lemma 2]

Lemma 1 *Let $\mathcal{A} = (S, A, \delta)$ be a deterministic n-state automaton and let P be a subset of S. The series $\mathcal{S}$ defined by Eq. (1) is rational of dimension n.*

The following result is a consequence of Proposition 1.

Corollary 1 *Let $\mathcal{A} = (S, A, \delta)$ be a deterministic n-state automaton and let P be a subset of S. Suppose that there exists a word u such that*

$$\mathrm{Card}(Pu^{-1}) \neq \mathrm{Card}(P).$$

Then there exists a word satisfying the previous condition whose length is not larger than $n-1$.

Proof By Lemma 1, $\mathcal{S}$ is a rational series of dimension n. By hypotheses, $\mathcal{S}$ is not null. The claim follows from the latter condition by applying Proposition 1. □

Remark 1 It is useful to remark that if $\mathcal{A} = (S, A, \delta)$ is a deterministic transitive synchronizing automaton, then every proper and nonempty subset P of S satisfies the hypotheses of Corollary 1. Indeed, if P is such a set, for any state p of P, one can find a reset word w such that $Sw = \{p\}$. This gives $S = Pw^{-1}$ and thus $\mathrm{Card}(Pw^{-1}) > \mathrm{Card}(P)$.

3 Strongly transitive automata

All the automata considered in this section are deterministic and complete, unless differently stated.

As is well-known, the study of the Černý conjecture can be always reduced to the case of transitive automata (*cf.* [15]). For the sake of completeness we report a proof of this reduction.

Proposition 2 *Let $\mathcal{A}$ be a synchronizing n-state automaton. Then there exist a synchronizing transitive m-state automaton $\mathcal{A}'$, with $m \leq n$, and a word v such that*

- $|v| \leq (n-m)^2$,
- *for every reset word w of $\mathcal{A}'$, vw is a reset word of $\mathcal{A}$.*

Proof Let $\mathcal{A} = (S, A, \delta)$ and let R be the set of the reset states of $\mathcal{A}$. Set $m = \mathrm{Card}(R)$. First note that

$$\forall a \in A, \quad Ra \subseteq R. \tag{2}$$

Let $S' \subseteq S$ and $s \in S' \backslash R$. Since R is the set of the reset states of $\mathcal{A}$, there exists $u \in A^*$ such that $su \in R$. Moreover we may assume that $|u| \leq \mathrm{Card}(S \backslash R) = n - m$. By Eq. (2), one has $Ru \subseteq R$. Thus $\mathrm{Card}(S'u \backslash R) < \mathrm{Card}(S' \backslash R)$. By applying $n - m$ times at most the previous argument starting from $S' = S$, one constructs a word $v \in A^*$ such that

$$|v| \leq (n-m)^2, \quad Sv \subseteq R.$$

Consider the triple $\mathcal{A}' = (R, A, \delta')$ where δ' is the restriction of the map δ to the set $R \times A$. By Eq. (2), it is easily checked that $\mathcal{A}'$ is a transitive synchronizing automaton. Since R is the set of the reset states of the automaton $\mathcal{A}'$, v is the desired word and this concludes the proof. □

Remark 2 By Proposition 2, if w is a reset word of $\mathcal{A}'$, then the word vw is a reset word of $\mathcal{A}$. Assuming that the Černý conjecture is true for transitive automata, we may take $|w| \leq (m-1)^2$ so that

$$|vw| = |v| + |w| \leq (n-m)^2 + (m-1)^2 \leq (n-1)^2.$$

In this section, we shall introduce a special class of transitive automata called strongly transitive and we shall study the synchronization problem for this class of automata. Let us first introduce the following definition.

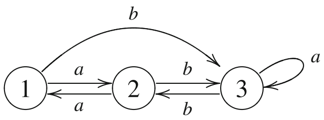
Definition 1 Let $\mathcal{A} = (S, A, \delta)$ be an n-state automaton. Then $\mathcal{A}$ is called *strongly transitive* if there exist n words $w_0, \ldots, w_{n-1} \in A^*$ such that

$$\forall s, t \in S, \quad \exists\, i = 0, \ldots, n-1, \; sw_i = t. \tag{3}$$

The set $\{w_0, \ldots, w_{n-1}\}$ is called *independent*.

We observe that a set $\{w_0, \ldots, w_{n-1}\}$ is independent if and only if, for any state s of S, the states $sw_i, \; i = 0, \ldots, n-1$, are pairwise distinct. The following example shows that transitivity does not imply strongly transitivity.

Example 1 Consider the 3-state automaton $\mathcal{A}$ over the alphabet $A = \{a, b\}$ defined by the following graph:



The automaton $\mathcal{A}$ is transitive. Let us prove that it is not strongly transitive. Indeed, by contradiction, let W be an independent set. Then there are words $u, v \in W$ such that $3u = 1, 3v = 2$. One easily derives that $|u|_b$ and $|v|_b$ are odd so that $1u = 1v = 3$. Therefore we have a contradiction because the states $1u$ and $1v$ must be distinct. Hence W cannot be independent.

Now we show that any transitive synchronizing automaton has an independent set.

Proposition 3 *Let $\mathcal{A}$ be a transitive n-state automaton. If $\mathcal{A}$ has a reset word of length ℓ, then there exists an independent set W for $\mathcal{A}$ such that $L_W < \ell + n$.*

Proof Let u be a reset word of $\mathcal{A}$ and q be its reset state. Since $\mathcal{A}$ is transitive, there exist words $u_0, u_1, \ldots, u_{n-1}$ that label computations from q to all the states of $\mathcal{A}$, with $|u_i| < n$, $i = 0, \ldots, n-1$. Therefore the set of n words

$$W = \{uu_0,\ uu_1, \ldots,\ uu_{n-1}\}$$

is independent for $\mathcal{A}$ and $L_W < \ell + n$. □

The previous proposition allows us to state the following corollary.

Corollary 2 *Any transitive synchronizing automaton is strongly transitive.*

By a well-known result [12,17], any synchronizing automaton has a reset word of length not larger than $(n^3 - n)/6$. Thus it has an independent set W such that L_W is not larger than

$$\frac{n^3 - n}{6} + n - 1.$$

Moreover if the Černý conjecture is true, the previous bound can be lowered to

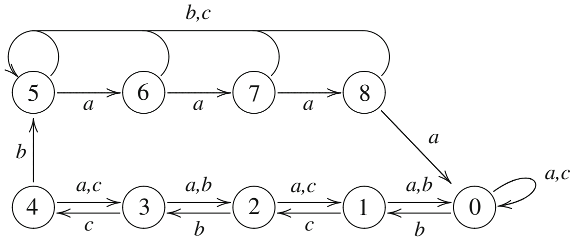
$$n(n-1).$$

Now we prove that there exist automata for which the upper bound stated in Proposition 3 is tight. More precisely, we will construct, for any positive integer n, a synchronizing $(2n+1)$-state automaton $\mathcal{A}$ such that, for any independent set W of $\mathcal{A}$, $L_W \geq \ell + 2n$, where ℓ is the length of the shortest reset word of $\mathcal{A}$.

Example 2 Let n be a positive integer. Consider the automaton $\mathcal{A}_n = (S_n, A, \delta_n)$ where $A = \{a, b, c\}$, $S_n = \{0, 1, 2, \ldots, 2n\}$ and the transition map δ_n is defined as follows:

- $0a = 0c = 0, 0b = 1,$
- for $i = 1, 2, \ldots, n$, $ia = i - 1$, $ib = i + (-1)^i$, $ic = i - (-1)^i$,
- for $i = n+1, n+2, \ldots, 2n$, $ia = i + 1 \bmod (2n+1)$, $ib = ic = n + 1$.

For instance, the graph of the automaton $\mathcal{A}_4$ is drawn in the following picture:



One can easily check that the word a^4 is a reset word of minimal length while the set

$$\{a^4, a^4b, a^4bc, a^4bcb, a^4bcbc, a^4bcbcb, a^4bcbcba, a^4bcbcba^2, a^4bcbcba^3\},$$

is an independent set of words of the automaton $\mathcal{A}_4$.

One can easily verify that $S_n a^n = \{0\}$. Thus $\mathcal{A}_n$ is a synchronizing automaton and, by Corollary 2, it is strongly transitive. We shall prove that, for any independent set W, $L_W \geq \mathrm{Card}(S_n) + |a^n| - 1$.

Lemma 2 *Let W be an independent set of $\mathcal{A}_n$. Then every word of W is a reset word.*

Proof Let $W = \{w_0, \ldots, w_{2n}\}$ be an independent set of words of $\mathcal{A}_n$. By possibly rearranging the words of W, we can suppose that, for $i = 0, 1, \ldots, 2n$, $(n+1)w_i = i$. In view of the definition of the map δ_n, one can easily check that, for $i = 0, 1, \ldots, n$,

$$w_i \in A^* a^n A^*.$$

Since a^n is a reset word for $\mathcal{A}_n$, one has that, for $i = 0, 1, \ldots, n$, w_i is a reset word of $\mathcal{A}_n$ and, moreover,

$$S_n w_i = \{i\}. \tag{4}$$

By Eq. (4), one has, for $i = n+1, \ldots, 2n$,

$$S_n w_i \subseteq \{n+1, n+2, \ldots, 2n\}. \tag{5}$$

We now prove that Eq. (4) holds also for $i = n+1, n+2, \ldots, 2n$. Let us first consider the state $i = 2n$. One can easily remark that every word that labels a computation from $n+1$ to $2n$ must end with the word a^{n-1}. On the other hand, for $i = n+1, \ldots, 2n-1$, every word that labels a computation from $n+1$ to i cannot end with a^{n-1}. In view of Eq. (5), this implies that $S_n w_{2n} = \{2n\}$ and, for $i = n, n+1, \ldots, 2n-1$,

$$S_n w_i \subseteq \{n+1, \ldots, 2n-1\}.$$

By iterating this combinatorial argument one can prove that Eq. (4) holds for $i = 2n-1, 2n-2, \ldots, n+1$. Thus all elements of W are reset words and the statement is proved. □

The following proposition allows us to obtain the quoted claim.

Proposition 4 *For any independent set W of $\mathcal{A}_n$ one has $L_W \geq 3n$.*

Proof By Lemma 2, any independent set contains a word w such that $S_n w = \{2n\}$. Thus the main task amounts to prove that $|w| \geq 3n$. For this purpose, one can observe that, for $i = 0, \ldots, n$ and $\sigma \in A$,

$$\{0, 1, \ldots, i\}\sigma \supseteq \{0, 1, \ldots, i-1\}.$$

This implies that, for every $u \in A^n$,

$$0 \in \{0, 1, \ldots, n\}u. \tag{6}$$

Since the minimal length of a path from 0 to $2n$ in the graph of $\mathcal{A}_n$ is $2n$, one has $|w| \geq 2n$, so that one can factorize $w = uv$ with $u, v \in A^*$ and $|u| = n$. Equation (6) implies that $0 \in S_n u$ and therefore, $0v \in S_n w = \{2n\}$. By the previous remark, this implies $|v| \geq 2n$, so that $|w| \geq 3n$ and the proof is complete. □

The following useful property easily follows from Definition 1.

Lemma 3 *Let $\mathcal{A}$ be a strongly transitive automaton and let W be an independent set of $\mathcal{A}$. Then, for every $u \in A^*$, the set uW is an independent set of $\mathcal{A}$.*

Proposition 5 *Let $\mathcal{A} = (S, A, \delta)$ be a strongly transitive n-state automaton and let W be an independent set of $\mathcal{A}$. Then for every subset P of S:*

$$\sum_{w \in W} \mathrm{Card}(Pw^{-1}) = n\,\mathrm{Card}(P). \tag{7}$$

Proof Let $W = \{w_0, \ldots, w_{n-1}\}$ and let $p \in S$. Because of Eq. (3), one has

$$S = \bigcup_{i=0}^{n-1} \{p\}w_i^{-1},$$

and the sets $\{p\}w_i^{-1}$ are pairwise disjoint. This immediately gives:

$$\sum_{i=0}^{n-1} \mathrm{Card}(\{p\}w_i^{-1}) = n. \tag{8}$$

Let $P = \{p_1, \ldots, p_m\}$ be a subset of m states. Since $\mathcal{A}$ is deterministic, for any pair p_i, p_j of distinct states of P and for every $u \in A^*$, one has:

$$\{p_i\}u^{-1} \cap \{p_j\}u^{-1} = \emptyset,$$

and, along with Eq. (8), this yields:

$$\sum_{i=0}^{n-1} \mathrm{Card}(Pw_i^{-1}) = \sum_{i=0}^{n-1} \sum_{j=1}^{m} \mathrm{Card}(\{p_j\}w_i^{-1}) = mn. \tag{9}$$

□

Corollary 3 *Let $\mathcal{A} = (S, A, \delta)$ be a synchronizing transitive n-state automaton and let W be an independent set of $\mathcal{A}$. Let P be a proper and non empty subset of S. Then there exists a word $v \in A^*$ such that*

$$|v| \leq n + L_W - 1, \quad \mathrm{Card}(Pv^{-1}) > \mathrm{Card}(P).$$

Proof Let $W = \{w_0, \ldots, w_{n-1}\}$. We first prove that there exist a word $v \in A^*$ with $|v| \leq n-1$ and $i = 0, \ldots, n-1$ such that

$$\mathrm{Card}(P(vw_i)^{-1}) \neq \mathrm{Card}(P). \tag{10}$$

If there exists $i = 0, \ldots, n-1$ such that $\mathrm{Card}(Pw_i^{-1}) \neq \mathrm{Card}(P)$, take $v = \epsilon$. Now suppose that the latter condition does not hold so that

$$\mathrm{Card}(Pw_0^{-1}) = \mathrm{Card}(P).$$

Since P is a proper subset of S, by Remark 1 and by applying Corollary 1 to the set Pw_0^{-1}, one has that there exists a word $v \in A^*$ such that $|v| \leq n-1$ and $\mathrm{Card}(P(vw_0)^{-1}) \neq \mathrm{Card}(P)$.

Thus take words v and w_i that satisfy Eq. (10). If $\mathrm{Card}(P(vw_i)^{-1}) > \mathrm{Card}(P)$, since $|vw_i^{-1}| \leq n-1+L_W$, we are done. Finally suppose that

$$\mathrm{Card}(P(vw_i)^{-1}) < \mathrm{Card}(P).$$

By Lemma 3, the set $vW = \{vw_0, \ldots, vw_{n-1}\}$ is independent for $\mathcal{A}$. Therefore, by Proposition 5,

$$\sum_{i=0}^{n-1} \mathrm{Card}(P(vw_i)^{-1}) = n\,\mathrm{Card}(P),$$

so that Eq. (10) implies the existence of an index j such that $\mathrm{Card}(P(vw_j)^{-1}) > \mathrm{Card}(P)$. Since, as before, $|vw_j^{-1}| \leq n-1+L_W$, the claim is proved. □

As a consequence of Corollary 3, the following theorem holds.

Theorem 2 *Let $\mathcal{A} = (S, A, \delta)$ be a synchronizing transitive n-state automaton and let W be an independent set of $\mathcal{A}$. Then there exists a reset word for $\mathcal{A}$ of length not larger than*

$$(n-2)(n+L_W-1)+1. \tag{11}$$

Proof Let P be a non-empty subset of S with $\mathrm{Card}(P) < n$. Since $\mathcal{A}$ is synchronizing, there exists some word u such that

$$\mathrm{Card}(Pu^{-1}) \neq \mathrm{Card}(P).$$

By Corollary 3, we can assume that $|u| \leq n+L_W-1$ and $\mathrm{Card}(Pu^{-1}) > \mathrm{Card}(P)$. Therefore from any subset P of at least 2 states, by applying the previous argument $(n-2)$ times at most, we can construct a word u such that $Su \subseteq P$ and $|u| \leq (n-2)(n+L_W-1)$. The claim finally follows from the fact that, in a synchronizing automaton, there always exist a letter $a \in A$ and a set P of two states such that $\mathrm{Card}(Pa) = 1$. □

Remark 3 In [9], Dubuc showed that the Černý conjecture is true for circular automata. An n-state automaton is called *circular* if its underlying graph has a Hamiltonian cycle labelled by a power of a letter. This is equivalent to say that such a letter, say a, acts as a circular permutation on the set of states of the automaton. This implies that the words $\epsilon, a, a^2, \ldots, a^{n-1}$ form an independent set of the automaton. Thus, from Theorem 2, one derives that any circular n-state automaton has a reset word of length not larger than

$$2(n-2)(n-1)+1.$$

We remark that a similar bound was established in [18] for the larger class of regular automata.

We have seen that circular automata are strongly transitive. However this notion is more general than that of circular automaton as shown in the following three examples.

Example 3 Let $\mathbb{Z}_k \times \mathbb{Z}_\ell$ be the direct product of the cyclic groups $\mathbb{Z}_k$ and $\mathbb{Z}_\ell$ of orders k and ℓ, respectively. Consider the automaton $\mathcal{A} = (S, A, \delta)$ where $A = \{a, b\}$, $S = \mathbb{Z}_k \times \mathbb{Z}_\ell$ and the transition map δ is defined as: for any $(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_\ell$,

$$\delta((i, j), a) = (i + 1, j), \quad \delta((i, j), b) = (i, j + 1).$$

If $k, \ell \geq 2$, then it is easily checked that the automaton is not circular and that the set W of words

$$\epsilon, a, \ldots, a^{k-1}, \quad b, ba, \ldots, ba^{k-1}, \quad \ldots, \quad b^{\ell-1}, b^{\ell-1}a, \ldots, b^{\ell-1}a^{k-1}$$

is an independent set of $\mathcal{A}$ with $L_W = k + \ell - 2$.

The next example can be viewed as a generalization of the previous one.

Example 4 Let $\mathcal{A}_i = (S_i, \{a, c\}, \delta_i)$, $i = 0, \ldots, k - 1$, be circular ℓ-state automata whose underlying graph has a Hamiltonian cycle labeled by a^ℓ. We assume that the sets S_i are pairwise disjoint and, moreover, that the automaton $\mathcal{A}_0$ is a synchronizing automaton such as, for instance, the Černý automaton [7]. We define the automaton $\mathcal{A} = (S, A, \delta)$ where the set of states is $S = \bigcup_{i=0}^{k-1} S_i$, the alphabet is $A = \{a, b, c\}$ and the transition function δ satisfies the following conditions:

1. for $q \in S_i$, $i = 0, \ldots, k - 2$,

$$\delta(q, a) = \delta_i(q, a), \quad \delta(q, c) = \delta_i(q, c), \quad \delta(q, b) \in S_{i+1},$$

2. for $q \in S_{k-1}$,

$$\delta(q, a) = \delta_{k-1}(q, a), \quad \delta(q, b),\ \delta(q, c) \in S_0,$$

It is easily checked that the automaton is not circular and that the set W of words

$$\epsilon, a, \ldots, a^{\ell-1}, \quad b, ba, \ldots, ba^{\ell-1}, \quad \ldots, \quad b^{k-1}, b^{k-1}a, \ldots, b^{k-1}a^{\ell-1}$$

is an independent set of $\mathcal{A}$ with $L_W = k + \ell - 2$.

We now check that $\mathcal{A}$ is synchronizing. Set $\alpha = \alpha_0\alpha_1$, where

$$\alpha_0 = (cb^{k-1})^{k-2}c,$$

and α_1 is a reset word of $\mathcal{A}_0$ (in the case that $\mathcal{A}_0$ is a Černý automaton, just take $\alpha_1 = (ca^{\ell-1})^{\ell-2}c$). Indeed, the symbols b and c act on the subsets $\{S_i\}_{i=0,\ldots,k-1}$ as in the Černý k-state automaton. This implies that, for any $i = 0, \ldots, k - 1$,

$$S_i\alpha_0 \subseteq S_0.$$

Again, by the fact that $\mathcal{A}_0$ is the Černý ℓ-state automaton on the alphabet $\{a, c\}$, one has that

$$S_0\alpha_1 = \{s_0\}, s_0 \in S_0.$$

Therefore we have

$$S\alpha = S\alpha_0\alpha_1 = S_0\alpha_1 = \{s_0\},$$

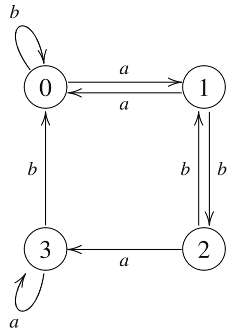
thus showing that $\mathcal{A}$ is synchronizing.

Example 5 Let $\mathcal{A}$ be an n-state automaton whose underlying graph G has a Hamiltonian cycle $\mathcal{C} = (0, 1, \ldots, n-1, 0)$ labelled by a power u of a primitive word $v \in A^*$, that is $u = v^\ell, \ell \geq 2$. Consider the partition of S given by the family of cosets of the arithmetic congruence modulo $|v|$. Denote $\mathcal{C}_i$ the coset of an element i in S. Moreover suppose that there exists a word w such that $Sw \subseteq \mathcal{C}_0$. Let W be the set of n words

$$wp_0, wp_1, \ldots, wp_{n-1},$$

where, for every $i = 0, \ldots, n-1$, p_i is the prefix of u of length i. It is easily checked that W is an independent set for the automaton and that $L_W = |w| + n - 1$. We finally remark that, in general, this automaton is not circular.

For instance, in the following automaton there is a Hamiltonian cycle labelled by $(ab)^2$ and the word $w = ab$ maps every state of the automaton in the set $\mathcal{C}_0 = \{0, 2\}$. Thus $W = \{ab, aba, abab, ababa\}$ is an independent set.



4 Unambiguous automata

In this section, we study the synchronization problem for unambiguous automata. First, we need to recall some basic notions and results concerning monoids of (0, 1)-matrices.

4.1 Monoids of (0, 1)-matrices

Let S be a finite set of indices and let $\mathbb{Q}^{S\times S}$ be the monoid of $S \times S$ matrices with the usual row-column product. For any $m \in \mathbb{Q}^{S\times S}$ and for any $s \in S$, the symbols m_{s*} and m_{*s} will denote, respectively, the row and the column of m of index s.

We will denote by $\{0, 1\}^{S\times S}$ the set of the matrices of $\mathbb{Q}^{S\times S}$ whose entries are all 0 and 1. Any submonoid M of $\mathbb{Q}^{S\times S}$ such that $M \subseteq \{0, 1\}^{S\times S}$ will be called a *monoid of* (0, 1)*-matrices* (or *monoid of unambiguous relations*).

A monoid of (0, 1)-matrices is *transitive* if, for any $s, t \in S$, there exists $m \in M$ such that $m_{st} = 1$.

Let M be a monoid of (0, 1)-matrices. Any row (resp., column) of a matrix of M will be called a *row* (resp., *column*) of M. The sets of the rows and columns of M are ordered in the usual way:

$$\mathbf{a} \leq \mathbf{b} \quad \text{if} \quad \mathrm{a}_s \leq \mathrm{b}_s \quad \text{for all} \quad s \in S.$$

The *weight* of a row or column $\mathbf{a}$ of M is the integer $\|\mathbf{a}\| = \sum_{s\in S} \mathrm{a}_s$. The following two lemmas will be useful in the sequel.

Lemma 4 *Let M be a transitive monoid of $(0, 1)$-matrices. If $\mathbf{a} \neq \mathbf{0}$ is a row (resp., column) of M which is not maximal, then one has $\|\mathbf{a}m\| > \|\mathbf{a}\|$ (resp., $\|m\mathbf{a}\| > \|\mathbf{a}\|$) for some $m \in M$.*

Proof We assume that $\mathbf{a}$ is a row of M. The case where $\mathbf{a}$ is a column can be dealt with symmetrically. Since $\mathbf{a}$ is not maximal, one has $\mathbf{a} < m'_{s*}$ for some $m' \in M$, $s \in S$. Let $r \in S$ be such that $\mathrm{a}_r = 1$. By transitivity, there exists $m'' \in M$ such that $m''_{rs} = 1$. Setting $m = m''m'$, one derives $\mathbf{a}m \geq m'_{s*} > \mathbf{a}$ and, consequently, $\|\mathbf{a}m\| > \|\mathbf{a}\|$. □

Lemma 5 *Let M be a monoid of $(0, 1)$-matrices of dimension n. For any row $\mathbf{a}$ and any column $\mathbf{b}$ of M, one has $\|\mathbf{a}\| + \|\mathbf{b}\| \leq n + 1$.*

Proof One has $\mathbf{a} = m_{r*}$ and $\mathbf{b} = m'_{*s}$ for suitable $m, m' \in M$, $r, s \in S$. Consequently, $\mathbf{ab} = (mm')_{rs} \leq 1$. Hence, there is at most one index $p \in S$ such that $\mathrm{a}_p = \mathrm{b}_p = 1$. The conclusion follows. □

The minimal ideal of a transitive monoid of (0, 1)-matrices has been characterized by Césari [8]. We summarize in the following statement some of the results of [8].

Proposition 6 *Let M be a transitive monoid of $(0, 1)$-matrices that does not contain the null matrix and let D be its minimal ideal. Then there exists an integer p such that*

1. *the elements of D are the matrices of M of the form*

$$m = \mathbf{b}_1\mathbf{a}_1 + \mathbf{b}_2\mathbf{a}_2 + \cdots + \mathbf{b}_p\mathbf{a}_p\,,$$

   with $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p$ maximal rows of M and $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_p$ maximal columns of M,
2. *for any matrix $m \in M$ of the form*

$$m = \mathbf{b}_1\mathbf{a}_1 + \mathbf{b}_2\mathbf{a}_2 + \cdots + \mathbf{b}_p\mathbf{a}_p + \mu\,,$$

   with $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p$ maximal rows of M, $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_p$ maximal columns of M, and $\mu \in \{0, 1\}^{S \times S}$, one has $\mu = 0$, and consequently m belongs to D,
3. *the integer p is the minimal linear rank of the matrices of M.*

4.2 Synchronizing unambiguous automata

An automaton $\mathcal{A} = (S, A, \delta)$ is said to be *unambiguous* if and only if $M = \varphi_{\mathcal{A}}(A^*)$ is a monoid of (0, 1)-matrices. This is equivalent to say that, for any pair of states s, t and any word u, there exists at most one computation of $\mathcal{A}$ from s to t labelled by u.

Let $\mathcal{A}$ be a non-deterministic automaton. A *reset word* of $\mathcal{A}$ is any word w such that $\varphi_{\mathcal{A}}(w)$ has linear rank 1.

In the sequel we will suppose that $\mathcal{A}$ is a transitive unambiguous n-state automaton. Moreover, we assume that there exists a finite set $V \subseteq A^*$ such that $A \subseteq V$ and

$$\forall p \in S, \quad \sum_{v \in V} \mathrm{Card}(pv) \geq \mathrm{Card}(V). \tag{12}$$

Notice that if $\mathcal{A}$ is deterministic and complete, then any finite set V satisfies Eq. (12).

Under our hypotheses, the following holds.

Lemma 6 *For all $\mathbf{a} \in \mathbb{N}^S$,*

$$\sum_{v \in V} \|\mathbf{a}\varphi_{\mathcal{A}}(v)\| \geq \|\mathbf{a}\|\,\mathrm{Card}(V).$$

Proof One has

$$\sum_{v\in V}\|\mathbf{a}\varphi_{\mathcal{A}}(v)\| = \sum_{v\in V}\sum_{p,r\in S}\mathrm{a}_p(\varphi_{\mathcal{A}}(v))_{pr} = \sum_{p\in S}\mathrm{a}_p\sum_{v\in V}\sum_{r\in S}(\varphi_{\mathcal{A}}(v))_{pr}.$$

Since for any $v \in A^*$, $r \in S$ one has $\sum_{r\in S}(\varphi_{\mathcal{A}}(v))_{pr} = \mathrm{Card}(pv)$, from Eq. (12)

$$\sum_{v\in V}\|\mathbf{a}\varphi_{\mathcal{A}}(v)\| \geq \sum_{p\in S}\mathrm{a}_p\,\mathrm{Card}(V) = \|\mathbf{a}\|\,\mathrm{Card}(V).$$

□

In view of Proposition 6, in order to find a reset word of $\mathcal{A}$, it would be useful to find a word w of short length such that $\varphi_{\mathcal{A}}(w)$ has a maximal row or column. The next propositions furnish a tool to produce rows of increasing weight.

Proposition 7 *Let* $\mathbf{a}$ *be a row of* $\varphi_{\mathcal{A}}(A^*)$ *such that* $\|\mathbf{a}\varphi_{\mathcal{A}}(u)\| \neq \|\mathbf{a}\|$ *for some* $u \in A^*$. *Then there exists a word* w *such that*

$$\|\mathbf{a}\varphi_{\mathcal{A}}(w)\| > \|\mathbf{a}\|\,, \quad |w| \leq L_V + n - 1.$$

Proof We notice that the series $\mathcal{S}$ defined by $\mathcal{S}(u) = \|\mathbf{a}\varphi_{\mathcal{A}}(u)\|$, $u \in A^*$, is a rational series of dimension n. Indeed, $\mathcal{S}$ has the linear representation $(\mathbf{a}, \varphi_{\mathcal{A}}, \Lambda)$ where $\Lambda = {}^{\mathrm{t}}(1, 1, \ldots, 1)$. On the other side, the series $\mathcal{S}_0$ defined by $\mathcal{S}_0(u) = \|\mathbf{a}\|$ for all $u \in A^*$, is a rational series of dimension 1.

Let u be the shortest word such that $\|\mathbf{a}\varphi_{\mathcal{A}}(u)\| \neq \|\mathbf{a}\|$. By Theorem 1, one has $|u| \leq n$. If $\|\mathbf{a}\varphi_{\mathcal{A}}(u)\| > \|\mathbf{a}\|$, then the statement is verified for $w = u$. Thus we assume $\|\mathbf{a}\varphi_{\mathcal{A}}(u)\| < \|\mathbf{a}\|$.

Write $u = u'x$ with $u' \in A^*$ and $x \in A$, and set $\mathbf{b} = \mathbf{a}\varphi_{\mathcal{A}}(u')$. Since $x \in V$, by Lemma 6 one has

$$\sum_{v\in V\backslash\{x\}}\|\mathbf{b}\varphi_{\mathcal{A}}(v)\| \geq \|\mathbf{b}\|\,\mathrm{Card}(V) - \|\mathbf{b}\varphi_{\mathcal{A}}(x)\|.$$

By the minimality of u, one has $\|\mathbf{b}\| = \|\mathbf{a}\|$ while $\|\mathbf{b}\varphi_{\mathcal{A}}(x)\| = \|\mathbf{a}\varphi_{\mathcal{A}}(u)\| < \|\mathbf{a}\|$. Thus, from the previous equation one obtains

$$\sum_{v\in V\backslash\{x\}}\|\mathbf{b}\varphi_{\mathcal{A}}(v)\| > \|\mathbf{a}\|\,\mathrm{Card}(V\backslash\{x\}).$$

Consequently, there is $v \in V\backslash\{x\}$ such that $\|\mathbf{b}\varphi_{\mathcal{A}}(v)\| > \|\mathbf{a}\|$. Taking $w = u'v$, one has $\|\mathbf{a}\varphi_{\mathcal{A}}(w)\| = \|\mathbf{b}\varphi_{\mathcal{A}}(v)\| > \|\mathbf{a}\|$. Since, moreover, $|w| = |u| - 1 + |v| \leq |u| + L_V - 1$, the proof is achieved. □

Lemma 7 *The automaton* $\mathcal{A}$ *is complete.*

Proof Let $\mathbf{a}$ be a row of $\varphi_{\mathcal{A}}(A^*)$ with $\|\mathbf{a}\|$ maximal. By Proposition 7, it follows that $\|\mathbf{a}\varphi_{\mathcal{A}}(u)\| = \|\mathbf{a}\| > 0$ for all $u \in A^*$. Consequently, $\varphi_{\mathcal{A}}(u) \neq 0$ for all $u \in A^*$. □

Proposition 8 *Set* $m_1 = \max\{\|\mathbf{a}\| \mid \mathbf{a}$ *row of* $\varphi_{\mathcal{A}}(A^*)\}$. *There exists a word* w *such that* $\varphi_{\mathcal{A}}(w)$ *has a maximal row and*

$$|w| \leq \max\{0,\ 1 + (m_1 - 2)(L_V + n - 1)\}. \tag{13}$$

Proof If the automaton $\mathcal{A}$ is deterministic, then any row of $\varphi_{\mathcal{A}}(\varepsilon)$ is maximal and the statement is trivially verified. Thus we assume that $\mathcal{A}$ is not deterministic. Hence, there is a letter $x \in A$ and a row $\mathbf{a}_0$ of $\varphi_{\mathcal{A}}(x)$ such that $\|\mathbf{a}_0\| \geq 2$.

In view of Proposition 7 and Lemma 4 one can find words w_i and vectors $\mathbf{a}_i$, $1 \leq i \leq k$ such that

$$\mathbf{a}_i = \mathbf{a}_{i-1}\varphi_{\mathcal{A}}(w_i)\,, \quad \|\mathbf{a}_i\| > \|\mathbf{a}_{i-1}\|\,, \quad |w_i| \leq L_V + n - 1\,, \tag{14}$$

and $\mathbf{a}_k$ is a maximal row of $\varphi_{\mathcal{A}}(A^*)$. Set $w = xw_1w_2\cdots w_k$. Since $\mathbf{a}_0$ is a row of $\varphi_{\mathcal{A}}(x)$, the vector $\mathbf{a}_k = \mathbf{a}_0\varphi_{\mathcal{A}}(w_1w_2\cdots w_k)$ is a row of $\varphi_{\mathcal{A}}(w)$. Moreover, from (14) one has

$$m_1 \geq \|\mathbf{a}_k\| \geq k + \|\mathbf{a}_0\| \geq k + 2\,, \quad |w| \leq 1 + k(L_V + n - 1).$$

From these inequalities, one easily derives Eq. (13), concluding the proof. □

In the sequel we will further suppose that there exists also a finite set $W \subseteq A^*$ such that $A \subseteq W$ and

$$\forall p \in S, \quad \sum_{w \in W} \mathrm{Card}(pw^{-1}) \geq \mathrm{Card}(W). \tag{15}$$

In such a case, with an argument symmetrical to that used in the proof of Proposition 8 one can prove the following

Proposition 9 *Set* $m_2 = \max\{\|\mathbf{b}\| \mid \mathbf{b}$*column of* $\varphi_{\mathcal{A}}(A^*)\}$. *There exists a word* v *such that* $\varphi_{\mathcal{A}}(v)$ *has a maximal column and*

$$|v| \leq \max\{0,\ 1 + (m_2 - 2)(L_W + n - 1)\}.$$

Now we state the main result of this section.

Proposition 10 *Let* $\mathcal{A}$ *be a synchronizing unambiguous transitive* n*-state automaton, with* $n \geq 2$. *Let* $V, W \subseteq A^*$ *be two finite sets of words satisfying Eq.* (12) *and Eq.* (15), *respectively, with* $A \subseteq V, W$. *Then* $\mathcal{A}$ *has a reset word* u *such that*

$$|u| \leq (n-2)L_{V\cup W} + n^2 - 3n + 3.$$

Proof First, we consider the case that the parameters m_1, m_2 introduced in Propositions 8 and 9 verify the conditions $m_i \geq 2$, $i = 1, 2$.

By Propositions 8 and 9, there are words w and v and states $p, q \in S$ such that $(\varphi_{\mathcal{A}}(v))_{p*} = \mathbf{a}$ is a maximal row of $\varphi_{\mathcal{A}}(A^*)$, $(\varphi_{\mathcal{A}}(w))_{*q} = \mathbf{b}$ is a maximal column of $\varphi_{\mathcal{A}}(A^*)$, and

$$|v| \leq 1 + (m_1 - 2)(L_V + n - 1)\,, \quad |w| \leq 1 + (m_2 - 2)(L_W + n - 1). \tag{16}$$

Since $\mathcal{A}$ is transitive, there exists a word z such that $p \in qz$ and $|z| \leq n - 1$. One has then $(\varphi_{\mathcal{A}}(z))_{qp} = 1$ and consequently

$$\varphi_{\mathcal{A}}(wzv) = (\varphi_{\mathcal{A}}(w))_{*q}(\varphi_{\mathcal{A}}(z))_{qp}(\varphi_{\mathcal{A}}(v))_{p*} + \mu = \mathbf{ba} + \mu\,,$$

for some $\mu \in \{0,1\}^{S\times S}$. By Lemma 7, $\varphi_{\mathcal{A}}(A^*)$ is a transitive monoid of (0, 1)-matrices without 0, and, by hypothesis, its minimal rank is 1. By Proposition 6 one derives that $\mu = 0$ and $u = wzv$ is a reset word.

Now we evaluate $|u|$. From (16) one has

$$|u| = |v| + |w| + |z| \leq n + 1 + (m_1 + m_2 - 4)(L_{V\cup W} + n - 1).$$

Since by Lemma 5, $m_1 + m_2 \leq n + 1$, one derives

$$|u| \leq (n-3)L_{V \cup W} + n^2 - 3n + 4\,,$$

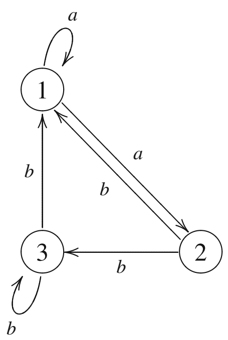
so that the statement holds true.

Now we consider the case $m_2 = 1$ (the case $m_1 = 1$ is symmetrically dealt with). We can still find a word v and a state $p \in S$ such that $\mathbf{a} = (\varphi_{\mathcal{A}}(v))_{p*}$ is a maximal row of $\varphi_{\mathcal{A}}(A^*)$ and $|v| \leq 1 + (m_1 - 2)(L_V + n - 1)$. Since $m_1 \leq n$ and $L_V \leq L_{V \cup W}$, one obtains

$$|w| \leq (n-2)L_{V \cup W} + n^2 - 3n + 3.$$

Now, to complete the proof, it is sufficient to verify that v is a reset word. Since $m_2 = 1$, the vector $\mathbf{b} = (\varphi_{\mathcal{A}}(\epsilon))_{*p}$ is a maximal column of $\varphi_{\mathcal{A}}(A^*)$. Moreover, $\varphi_{\mathcal{A}}(v) = \mathbf{ba} + \mu$ for some $\mu \in \{0, 1\}^{S \times S}$. By Proposition 6 one derives that v is a reset word. This concludes the proof. $\square$

Example 6 Consider the following unambiguous transitive complete automaton.



Let us verify that there does not exist a finite set $W \subseteq A^*$ such that $A \subseteq W$ and satisfying Eq. (15). Indeed, one easily verifies that, for any $v \in A^*$,

$$(1, 1, 1)\varphi_{\mathcal{A}}(v) = (\mathrm{Card}(1v^{-1}), \mathrm{Card}(2v^{-1}), \mathrm{Card}(3v^{-1})).$$

One easily checks that the vectors of the form $(1, 1, 1)\varphi_{\mathcal{A}}(v)$ with $v \in A^*$ are:

$$\mathbf{x}_0 = (1, 1, 1),\ \ \mathbf{x}_1 = (1, 1, 0),\ \ \mathbf{x}_2 = (2, 0, 2),\ \ \mathbf{x}_3 = (1, 0, 1),\ \ \mathbf{x}_4 = (2, 2, 0).$$

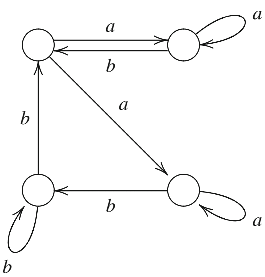
Thus if a set W satisfying Eq. (15) exists there is a linear combination of $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ and $\mathbf{x}_4$ with non negative coefficients k_0, k_1, k_2, k_3 and k_4 such that

$$\sum_{i=0}^{4} k_i \mathbf{x}_i \geq \sum_{i=0}^{4} k_i\ \mathbf{x}_0.$$

Moreover, if $A \subseteq W$ then the coefficients k_1 and k_2 of $\mathbf{x}_1 = (1, 1, 1)\varphi_{\mathcal{A}}(a)$ and $\mathbf{x}_2 = (1, 1, 1)\varphi_{\mathcal{A}}(b)$ have to be positive. It is easily seen that this is impossible.

An automaton $\mathcal{A}$ on a k-letter alphabet is *Eulerian* if for any vertex of its graph, there are exactly k in-coming and k out-coming arrows.

Example 7 The following automaton is unambiguous and Eulerian. We remark that it is neither deterministic nor co-deterministic.



The word ba is a reset word for the automaton.

In [14], Kari showed that the Černý conjecture is true for Eulerian deterministic automata. As an application of Proposition 10, we may extend this result to unambiguous Eulerian automata.

Corollary 4 *Any transitive, synchronizing, and unambiguous Eulerian n-state automaton has a reset word of length not larger than* $(n-1)^2$.

Proof Let $\mathcal{A}$ be an Eulerian automaton. From the definition, for any state p of $\mathcal{A}$, one has

$$\sum_{a\in A}\mathrm{Card}(pa)=\sum_{a\in A}\mathrm{Card}(pa^{-1})=\mathrm{Card}(A).$$

Thus, the hypotheses of Proposition 10 are satisfied for $V=W=A$. The conclusion follows. □

5 Concluding remarks

In this paper we introduced the notion of strongly transitive automaton. We showed that any synchronizing deterministic complete transitive automaton $\mathcal{A}$ is strongly transitive. Moreover, denoted by ℓ the length of the shortest synchronizing word and by L the minimal value of L_W with W an independent set of $\mathcal{A}$, the quantities ℓ and L are bounded by the following inequalities:

$$L-n+1\le\ell\le(n-2)(n+L-1)+1\,,$$

where n is the number of states of $\mathcal{A}$.

A naturally arising question asks for bounds of L when $\mathcal{A}$ varies in the class of synchronizing deterministic complete transitive automata or, more generally, in the class of strongly transitive deterministic complete automata.

As we have seen in Sect. 3, if $\mathcal{A}$ is a synchronizing deterministic complete transitive n-state automaton, then $L\le(n^3-n)/6+n-1$ and this bound can be lowered to $n(n-1)$ if the Černý conjecture is true. On the other side, by Proposition 4 for any odd n there is a synchronizing deterministic complete n-state automaton such that $L=3(n-1)/2$.

We propose the following

Conjecture 1 *There exists a positive number k such that for any synchronizing deterministic complete n-state automaton, $L<kn$.*

If this conjecture were true, one would derive that, for any synchronizing deterministic complete transitive n-state automaton, $\ell<(k+1)n^2-(3+2k)n+3$.

References

1. Ananichev, D.S., Volkov, M.V.: Synchronizing generalized monotonic automata. Theoret. Comput. Sci. **330**, 3–13 (2005)
2. Béal, M.P.: A note on Černý's Conjecture and rational series, technical report, Institut Gaspard Monge, Université de Marne-la-Vallée (2003)
3. Béal, M.P., Czeizler, E., Kari, J., Perrin, D.: Unambiguous automata. Math. Comput. Sci. **1**, 625–638 (2008)
4. Berstel, J., Reutenauer, C.: Rational Series and Their Languages. Springer, Berlin (1988)
5. Carpi, A.: On synchronizing unambiguous automata. Theoret. Comput. Sci. **60**, 285–296 (1988)
6. Carpi, A., D'Alessandro, F.: The synchronization problem for strongly transitive automata. In: Ito, M., Toyama, M. (eds.) Developments in Language Theory, DLT 2008, Lecture Notes in Computer Science, vol. 5257, Springer, Berlin (2008)
7. Černý, J., Poznámka, K.: Homogénnym experimenton s konečnými automatmi. Mat. Fyz. Cas SAV **14**, 208–215 (1964)
8. Césari, Y.: Sur l'application du théorème de Suschkewitsch à l'étude des codes rationnels complets. In: Loeckx, J. (ed.) Automata, Languages and Programming, Lecture Notes in Computer Science, vol. 14, pp. 342–350. Springer, Berlin (1974)
9. Dubuc, L.: Sur les automates circulaires et la conjecture de Cerny, RAIRO Inform. Théor. Appl. **32**, 21–34 (1998)
10. Eilenberg, S.: Automata, Languages and Machines, vol. A. Academic Press, New York (1974)
11. Eppstein, D.: Reset sequences for monotonic automata. SIAM J. Comput. **19**, 500–510 (1990)
12. Frankl, P.: An extremal problem for two families of sets. Eur. J. Comb. **3**, 125–127 (1982)
13. Goralčík, P., Hedrlín, Z., Koubek, V., Ryšlinková, J.: A game of composing binary relations. RAIRO Inform. Théor. **16**, 365–369 (1982)
14. Kari, J.: Synchronizing finite automata on Eulerian digraphs. Theoret. Comput. Sci. **295**, 223–232 (2003)
15. Pin, J.E.: Le problème de la synchronization et la conjecture de Cerny, Thèse de 3ème cycle. Université de Paris 6 (1978)
16. Pin, J.E.: Sur un cas particulier de la conjecture de Cerny, In: Proceedings of the 5th ICALP. Lecture Notes in Computer Science, vol. 62, pp. 345–352. Springer, Berlin (1978)
17. Pin, J.E.: On two combinatorial problems arising from automata theory. Ann. Discrete Math. **17**, 535–548 (1983)
18. Rystov, I.: Almost optimal bound of recurrent word length for regular automata. Cybern. Syst. Anal. **31**(5), 669–674 (1995)
19. Trahtman, A.N.: The Cerny conjecture for aperiodic automata. Discrete Math. Theor. Comput. Sci. **9**, 3–10 (2007)
20. Volkov, M.V.: Synchronizing automata and the Černý conjecture. In: Martín-Vide, C., Otto, F., Fernau, H. (eds.) LATA 2008, Lecture Notes in Computer Science, vol. 5196, pp. 11–27. Springer, Berlin (2008)