SEMISIMPLE SYNCHRONIZING AUTOMATA AND THE WEDDERBURN-ARTIN THEORY

JORGE ALMEIDA AND EMANUELE RODARO

Abstract. We present a ring theoretic approach to Černý's conjecture via the Wedderburn-Artin theory. We first introduce the radical ideal of a synchronizing automaton, and then the natural notion of semisimple synchronizing automata. This is a rather broad class since it contains simple synchronizing automata like those in Černý's series. Semisimplicity gives also the advantage of "factorizing" the problem of finding a synchronizing word into the sub-problems of finding "short" words that are zeros into the projection of the simple components in the Wedderburn-Artin decomposition. In the general case this last problem is related to the search of radical words of length at most $(n-1)^2$ where n is the number of states of the automaton. We show that the solution of this "Radical Conjecture" would give an upper bound $2(n-1)^2$ for the shortest reset word in a strongly connected synchronizing automaton. Finally, we use this approach to prove the Radical Conjecture in some particular cases and Černý's conjecture for the class of strongly semisimple synchronizing automata. These are automata whose sets of synchronizing words are cyclic ideals, or equivalently, ideal regular languages that are closed under taking roots.

1. Introduction

A deterministic finite automaton (DFA) $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is called synchronizing if there exists a word $w \in \Sigma^*$ "sending" all the states into a single state, i.e. $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. Any such word is said to be synchronizing (or reset) for the DFA $\mathscr{A}$. These automata have been widely studied since the work of Černý in 1964 [8] and his well known conjecture regarding an upper bound for the length of the shortest reset word. This conjecture states that any synchronizing automaton $\mathscr{A}$ with n states admits at least a reset word w with $|w| \leq (n-1)^2$. In [8] it is shown that this bound is tight by exhibiting an infinite series of synchronizing automata $\mathscr{C}_n$ having a shortest synchronizing word of length $(n-1)^2$. For more information on synchronizing automata we refer the reader to Volkov's survey [21]. In this paper we follow a representation theoretic approach to the Černý conjecture and synchronizing automata initially pursued in [1, 3, 5, 19]. However, our approach has a more ring theoretic flavor making use of the well-known Wedderburn-Artin theory for semisimple rings.

The paper is organized as follows. In Section 2 we introduce the notion of radical of a synchronizing automaton. In Section 3 we characterize this ideal and we introduce the natural notion of semisimple synchronizing automaton. Then, we exhibit some classes of semisimple and simple synchronizing automata. Finally, we formally state a weak version of Černý's conjecture

(the Radical Conjecture) whose solution would solve this conjecture for the class of semisimple automata, and we show that its solution would also imply a quadratic upper bound $2(n-1)^2$ for the shortest reset word in a strongly connected synchronizing automaton with n states. In Section 4 we show how the Wedderburn-Artin Theory may be used to factorize the problem of finding "short" radical words into the sub-problem of finding "short" words that are zero in the projections into the simple components. This approach works for instance in case the 0-minimal ideals in the factor monoids do not contain zero $\mathcal{H}$-classes similarly to [1, 3]. In Section 5 we introduce cyclic ideal languages and we characterize them. Finally, using the results of Section 4, we show that Černý's conjecture holds for a particular class of semisimple synchronizing automata: the strongly semisimple automata. This is the class of synchronizing automata whose set of reset words is a cyclic ideal language. Finally, in Section 6 we present some cases in which the Radical Conjecture may be solved. In particular, we consider the following two cases: the set of radical words forms a cyclic ideal, and the case where set of the idempotents in the associated 0-minimal ideals are semilattices.

2. The radical of a synchronizing automaton

In this section we fix notation used throughout the paper, and we introduce the central notion of radical of a synchronizing automaton. Henceforth, we consider a synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ with set of states $Q = \{q_1, \ldots, q_n\}$, and by $\mathcal{S}$ we denote the set of the synchronizing (reset) words of $\mathscr{A}$. It is an easy exercise to check that the set $\mathcal{S}$ is a regular language which is a two-sided ideal of Σ^*, i.e. $\Sigma^*\mathcal{S}\Sigma^* \subseteq \mathcal{S}$. Let $\mathrm{M}(\mathscr{A})$ be the transition monoid of $\mathscr{A}$ and let $\pi : \Sigma^* \to \mathrm{M}(\mathscr{A})$ be the natural epimorphism and put $\mathscr{A}^* = \mathrm{M}(\mathscr{A})/\pi(\mathcal{S})$. There is a natural action of $\mathrm{M}(\mathscr{A})$ on the set Q given by $q \cdot \pi(u) = \delta(q, u)$; we often omit the map π and we use the simpler notation $q \cdot u$. This action is extended to subsets of Q in the obvious way. It is a well known fact that $\mathrm{M}(\mathscr{A})$ embeds into the ring $\mathbb{M}_n(\mathbb{C})$ of $n \times n$ matrices with entries in $\mathbb{C}$ and with a slight abuse of notation we still denote by $\pi : \Sigma^* \to \mathbb{M}_n(\mathbb{C})$ the representation induced by this embedding. This representation determines an action of Σ^* on the vector space $\mathbb{C}Q$ defined by $v \cdot u = v\pi(u)$. Consider the vector $w = q_1 + \cdots + q_n$ formed by summing all the elements of the canonical basis. Using the fact that the $\pi(a)$, $a \in \Sigma$, are functions it is not difficult to see that Σ^* acts on the orthogonal space $w^\perp = \{u \in \mathbb{C}Q : \langle u|w\rangle = 0\}$ where $\langle\cdot|\cdot\rangle$ is the usual scalar product (see for instance [5]). This may be easily verified by checking that Σ^* maps the basis of $w^\perp$ formed by the vectors $q_1 - q_i$ for $i = 2, \ldots, n$ into $w^\perp$. Furthermore, it is an easy exercise to check that $u \in \mathcal{S}$ if and only if for every $v \in w^\perp$ we get $v \cdot u = 0$. This induces a representation $\varphi : \Sigma^*/\mathcal{S} \to \mathrm{End}(w^\perp) \simeq \mathbb{M}_{n-1}(\mathbb{C})$ with $\varphi(\Sigma^*/\mathcal{S}) \simeq \mathscr{A}^*$. Therefore, we see $\mathscr{A}^*$ as a finite multiplicative submonoid of $\mathbb{M}_{n-1}(\mathbb{C})$. Let $\mathcal{R}$ be the $\mathbb{C}$-subalgebra of $\mathbb{M}_{n-1}(\mathbb{C})$ generated by $\mathscr{A}^*$. Clearly $\mathcal{R}$ is a finitely generated $\mathbb{C}$-algebra called the *synchronized* $\mathbb{C}$-*algebra associated to* the synchronizing DFA $\mathscr{A}$ where $\mathscr{A}^*$ embeds into $\mathcal{R}$, and with a slight abuse of notation we identify $\mathscr{A}^*$ with the image of this embedding $\mathscr{A}^* \hookrightarrow \mathcal{R}$. Therefore, we define the *radical* $\mathrm{Rad}(\mathscr{A}^*)$ of $\mathscr{A}^*$ as

$\mathrm{Rad}(\mathscr{A}^*) = \mathrm{Rad}(\mathcal{R}) \cap \mathscr{A}^*$, where $\mathrm{Rad}(\mathcal{R})$ is the radical (see [11]) of the $\mathbb{C}$-subalgebra $\mathcal{R}$.

Let $\theta : \Sigma^* \to \Sigma^*/\mathcal{S}$ be the Rees morphism. Throughout the paper we consider the morphism $\rho : \Sigma^* \to \mathscr{A}^*$ defined by $\rho = \varphi \circ \theta$. Since $\mathrm{Rad}(\mathcal{R})$ is an ideal of $\mathcal{R}$, the radical $\mathrm{Rad}(\mathscr{A}^*)$ is also an ideal of the (finite) monoid $\mathscr{A}^*$. We have the following definition of radical of a synchronizing automaton.

Definition 1. The set $\mathrm{Rad}(\mathscr{A}) = \rho^{-1}(\mathrm{Rad}(\mathscr{A}^*)) \subseteq \Sigma^*$ is a two-sided ideal which is clearly a regular language called the radical of the synchronizing automaton $\mathscr{A}$.

Note that $\mathcal{S} \subseteq \mathrm{Rad}(\mathscr{A})$. The elements of $\mathrm{Rad}(\mathscr{A})$ are called the *radical words* of $\mathscr{A}$.

3. Semisimple synchronizing automata and radical words

In view of Definition 1, it is natural to call a synchronizing DFA $\mathscr{A}$ *semisimple* whenever $\mathrm{Rad}(\mathscr{A}^*) = \{0\}$. Note that $\mathscr{A}$ is semisimple if and only if $\mathrm{Rad}(\mathscr{A}) = \mathcal{S}$. This last fact shows that the search for synchronizing words in a semisimple synchronizing automaton is reduced to the search of words $u \in \Sigma^*$ for which $\psi(\rho(u)) = 0$, where $\psi : \mathcal{R} \to \overline{\mathcal{R}} := \mathcal{R}/\mathrm{Rad}(\mathcal{R})$ is the canonical epimorphism. We now make some general considerations on $\mathrm{Rad}(\mathscr{A})$. We recall that an ideal I in a monoid with zero (or in a ring) is *nilpotent* whenever there is an integer m such that $I^m = 0$. The following proposition characterizes the radical words of a synchronizing automaton.

Proposition 2. $\mathrm{Rad}(\mathscr{A})$ *is an ideal containing* $\mathcal{S}$*, moreover* $\mathrm{Rad}(\mathscr{A})/\mathcal{S}$ *is the largest nilpotent left (right) ideal of* $\Sigma^*/\mathcal{S}$*.*

Proof. Since $\mathcal{R}$ is both noetherian and artinian, by Theorem 4.12 of [11] $\mathrm{Rad}(\mathcal{R})$ is the largest nilpotent left (right) ideal of $\mathcal{R}$. We claim that $\mathrm{Rad}(\mathscr{A}^*)$ is the largest nilpotent left (right) ideal of $\mathscr{A}^*$. Indeed, assume that H is a nilpotent left ideal of $\mathscr{A}^*$, and let $\mathcal{H}$ be the $\mathbb{C}$-algebra generated by H. Since $\mathcal{R}$ is generated by $\mathscr{A}^*$, then $\mathcal{H}$ is also a left (right) ideal of $\mathcal{R}$. Moreover, it is nilpotent: if $H^m = 0$, then it is straightforward to check that also $\mathcal{H}^m = 0$. Thus, $\mathcal{H} \subseteq \mathrm{Rad}(\mathcal{R})$ and so in particular we have $H \subseteq \mathcal{H} \cap \mathscr{A}^* \subseteq \mathrm{Rad}(\mathcal{R}) \cap \mathscr{A}^* = \mathrm{Rad}(\mathscr{A}^*)$. If $\varphi : \Sigma^*/\mathcal{S} \to \mathscr{A}^*$ is the representation map, then it is routine to check that $\mathrm{Rad}(\mathscr{A})/\mathcal{S} = \varphi^{-1}(\mathrm{Rad}(\mathscr{A}^*))$ is also the largest nilpotent left (right) ideal of $\Sigma^*/\mathcal{S}$. □

From this proposition it is evident that if one is able to find a radical word u, then a synchronizing word may be obtained by considering a suitable power of u. Therefore, for $u \in \mathrm{Rad}(\mathscr{A})$ it is important defining the index $\mathrm{Depth}(u)$ as the smallest positive integer $n \geq 1$ such that $u^n \in \mathcal{S}$. We may extend this parameter to the whole automaton by putting $\mathrm{Depth}(\mathscr{A}) = \min\{m : \mathrm{Rad}(\mathscr{A})^m = \mathcal{S}\}$. Note that $\mathrm{Depth}(u) \leq \mathrm{Depth}(\mathscr{A})$. Moreover, the search for bounds for such quantities may lead to bounds for short synchronizing words. In this way we may split the task of finding bounds for the shortest synchronizing words into the problem of bounding the shortest radical word u and to bound one of the quantities $\mathrm{Depth}(\mathscr{A})$, $\mathrm{Depth}(u)$. Note that $\mathrm{Depth}(\mathscr{A}) = 1$ iff $\mathscr{A}$ is semisimple. The following general bound of these quantities holds.

Lemma 3. *For any $u \in \mathrm{Rad}(\mathscr{A})$, $u^{n-1} \in \mathcal{S}$. In particular we have:*

$$\mathrm{Depth}(u) \leq \mathrm{Depth}(\mathscr{A}) \leq n-1$$

Proof. Consider the automaton $\mathscr{A}_u = \langle Q, \{u\}, \delta\rangle$ obtained from $\mathscr{A}$ by restricting the action on the single element $\{u\}$. Since u^m is a reset word for some m, then $\mathscr{A}_u$ is a synchronizing automaton with a sink state $s \in Q$ and no cycles, except the loops at the sink state. Hence, there is an integer $\ell \leq n-1$ such that $q \cdot u^\ell = s$ for all $q \in Q$, i.e., $u^{n-1} \in \mathcal{S}$. □

We now frame the combinatorial class of simple synchronizing automata into the class of semisimple synchronizing automata. Given an automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, we recall that an equivalence relation σ on the set of states Q is an (automaton) *congruence* if $x\sigma y$ implies $(x \cdot u)\sigma(y \cdot u)$ for any $u \in \Sigma^*$. Note that the *quotient automaton* $\mathscr{A}/\sigma = \langle Q/\sigma, \Sigma, \delta'\rangle$ with $\delta'([q]_\sigma, a) = [\delta(q,a)]_\sigma$, $q \in Q, a \in \Sigma$, is a well defined DFA. Furthermore, it is straightforward to check that if $\mathscr{A}$ is synchronizing, then $\mathscr{A}/\sigma$ is also synchronizing. We denote the lattice of congruences of $\mathscr{A}$ by $\mathrm{Cong}(\mathscr{A})$ with maximum given by the universal relation $\nabla_{\mathscr{A}}$ and minimum the identity relation $\Delta_{\mathscr{A}}$. For a given equivalence relation σ we denote by $\mathrm{Cong}_\sigma(\mathscr{A})$ the sub-lattice of the congruences of $\mathscr{A}$ contained in σ. We have the following lemma.

Lemma 4. *Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a synchronizing automaton which is not semisimple. Let $h \in \mathrm{Rad}(\mathscr{A}) \setminus \mathcal{S}$ and let $\mathrm{Ker}(h)$ be the kernel of the transformation induced by the word h. It follows that*

$$\mathrm{Cong}_{\mathrm{Ker}(h)}(\mathscr{A}) \neq \{\Delta_{\mathscr{A}}\}$$

Proof. We have to show that $\mathrm{Cong}_{\mathrm{Ker}(h)}(\mathscr{A})$ is non-trivial. Since $h \in \mathrm{Rad}(\mathscr{A}) \setminus \mathcal{S}$, by Proposition 2 there is a minimum integer $m > 1$ such that:

$$\underbrace{h\Sigma^* h\Sigma^* h \ldots \Sigma^* h}_{m-\text{times}} = 0 \text{ in } \Sigma^*/\mathcal{S} \tag{1}$$

By the minimality of m there are words $u_1, \ldots u_{m-2} \in \Sigma^*$ such that

$$hu_1 hu_2 \ldots u_{m-2} h$$

is not synchronizing. Then, there are two different states $q_1, q_2 \in Q$ such that

$$\overline{q}_1 = q_1 \cdot (hu_1 hu_2 \ldots u_{m-2}h) \neq q_2 \cdot (hu_1 hu_2 \ldots u_{m-2}h) = \overline{q}_2$$

Define the relation σ by putting $x\sigma y$ if there is a $u \in \Sigma^*$ such that $\{\overline{q}_1, \overline{q}_2\} \cdot u = \{x, y\}$. It is evident that σ is symmetric. Let σ^t be the reflexive and transitive closure of σ. This is an equivalence relation which is also a congruence, in fact it is the smallest congruence that identifies $\overline{q}_1$ with $\overline{q}_2$. We claim that $\sigma^t \subseteq \mathrm{Ker}(h)$ or equivalently $|[q]_{\sigma^t} \cdot h| = 1$ for any $q \in Q$, where $[q]_{\sigma^t}$ is the equivalence class of σ^t containing q. Indeed, assume, contrary to our claim, that there is some non-trivial class $[q]_{\sigma^t}$ such that $|[q]_{\sigma^t} \cdot g| > 1$. Thus, there are two distinct states $p, p' \in [q]_{\sigma^t} \cdot h$ and a sequence $x_1, \ldots, x_n$ of states of $[q]_{\sigma^t}$ such that $x_i \sigma x_{i+1}$ for $i = 1, \ldots, n-1$ and $x_1 \cdot h = p$, $x_n \cdot h = p'$. This implies the existence of an index $i \in \{1, \ldots, n-1\}$

such that $x_i \cdot h \neq x_{i+1} \cdot h$. Hence, there is some word $u \in \Sigma^*$ such that $\{\overline{q}_1, \overline{q}_2\} \cdot u = \{x_i, x_{i+1}\}$ which implies

$$q_1 \cdot (hu_1hu_2 \dots u_{m-2}huh) \neq q_2 \cdot (hu_1hu_2 \dots u_{m-2}huh)$$

which contradicts (1). Hence, $|[q]_{\sigma^t} \cdot h| = 1$ for every $q \in Q$, and $\sigma^t \subseteq \mathrm{Ker}(h)$. □

We recall that an automaton $\mathscr{A}$ is called *simple* whenever $\mathrm{Cong}(\mathscr{A}) = \{\nabla_{\mathscr{A}}, \Delta_{\mathscr{A}}\}$ (see [6, 20]). Therefore, by the previous lemma we have the following immediate theorem:

Theorem 5. *A synchronizing simple automaton is also semisimple.*

Proof. Since $\mathscr{A}$ is not semisimple, we may take any $g \in \mathrm{Rad}(\mathscr{A}) \setminus \mathcal{S}$. Then, by Lemma 4 there is a congruence $\sigma \in \mathrm{Cong}_{\mathrm{Ker}(g)}(\mathscr{A})$ with $\sigma \neq \Delta_{\mathscr{A}}$. Moreover, since g is not synchronizing $\mathrm{Ker}(g) \neq \nabla_{\mathscr{A}}$, whence $\sigma \neq \nabla_{\mathscr{A}}$ as well. □

A kind of converse of the previous result has been obtained by Rystov in Theorem 4 of [17]. There it is proved that an irreducible automaton, i.e. an automaton whose whose basic linear representation $\varphi : \Sigma^*/\mathcal{S} \to \mathbb{M}_{n-1}(\mathbb{Q})$ is irreducible, is necessarily simple (in [17] called primitive). Using Theorem 5 we may find another class of semisimple automata as the following proposition shows.

Proposition 6. *Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a synchronizing automaton with $|Q|$ prime and having a subset $P \subseteq \Sigma$ such that P^* acts as a transitive permutation group on Q. Then, the automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is semisimple.*

Proof. If $\mathscr{A}$ is not semisimple, then by Theorem 5 there is a congruence $\sigma \in \mathrm{Cong}(\mathscr{A})$ with $\sigma \neq \Delta_{\mathscr{A}}, \nabla_{\mathscr{A}}$. Thus, there is a class $[q]_\sigma$ of Q/σ with $1 < |[q]_\sigma| < |Q|$. Since σ is a congruence and P^* acts as a transitive permutation group transitively on Q, then $|[q']_\sigma \cdot u| = |[q']_\sigma|$ for all $q' \in Q$ and $u \in P^*$. Thus, by transitivity we may factorize $|Q| = |Q/\sigma|\,|[q]_\sigma|$ with $1 < |[q]_\sigma| < |Q|$, a contradiction. Hence, $\mathscr{A}$ is semisimple. □

The previous proposition holds in the more general context of groups acting on a set that are primitive. We recall that a group G acting on a set Q is called *primitive* whenever there are no non-trivial equivalence relations on Q preserved by G. Thus, any automaton having a subset $P \subseteq \Sigma$ acting primitively on Q is simple and so semisimple. Another example of simple, and therefore semisimple, automaton is given by the well known series of Černý. We recall that this series is formed by the automata (see Fig. 1) $\mathscr{C}_n = \langle \{1, \dots, n\}, \{a, b\}, \delta\rangle$ where $\delta(i, a) = i + 1 \mod n$, $\delta(i, b) = i$ for all $1 \leq i \leq n - 1$ and $\delta(n, b) = 1$. We have the following proposition.

Proposition 7. *For all $n \geq 1$ the automata $\mathscr{C}_n$ are simple.*

Proof. In case $n \leq 2$, the automaton is clearly simple. Thus, suppose $n \geq 3$, and assume, contrary to our claim, that $\mathrm{Cong}(\mathscr{A})$ contains a non-trivial congruence ρ. The relative distance between i, j is given by

$$d(i, j) = \min\{k : i \cdot a^k = j \vee j \cdot a^k = i\}$$

It is sufficient to prove that for any pair (i, j) with $i\rho j$ and $i \neq j$, there is a word $u \in \{a, b\}^*$ such that $d(i \cdot u, j \cdot u) = 1$. Indeed, in this case we

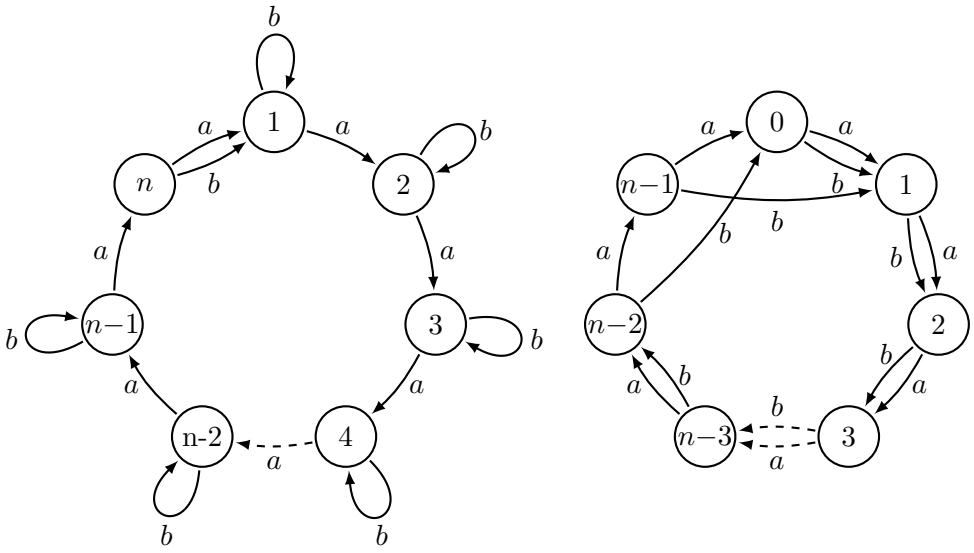

FIGURE 1. Černý's series $\mathscr{C}_n$ on the left, and the automaton $\mathcal{D}'_n$ on the right.

may assume without loss of generality that there are two states s, t with $s\rho t$ and $s = i \cdot u = (j \cdot u) + 1 = t + 1$. Hence, since ρ is congruence we get $(s \cdot a^k)\rho(t \cdot a^k)$ for all $k \geq 1$, and so by the transitivity of ρ we get $1\rho 2\rho \dots \rho n$, i.e. $\rho = \nabla_{\mathscr{A}}$, a contradiction. If $d(i, j) = 1$ then we are done. Otherwise assume without loss of generality that $j = i \cdot a^{d(i,j)}$. Let us apply a suitable power of a to have $i \cdot a^k = n$. It is clear that this action does not change the relative distance between the two states, i.e. $d(i, j) = d(i \cdot a^k, j \cdot a^k)$. Since b leaves all the states unchanged but n, if we apply the letter b then it is straightforward to check that $d(i \cdot a^k b, j \cdot a^k b) = d(i \cdot a^k, j \cdot a^k) - 1$. Continuing in this way, applying powers of a interjected with one application of b, we eventually obtain the desired states $s = i \cdot u$, $t = j \cdot u$ with $d(s, t) = 1$. □

The previous strategy may be applied to all circular automata, i.e. automata with a letter acting like a circular permutation. Indeed, for such automata we have the notion of relative distance $d(q, p)$ given as in the proof of the previous lemma. Therefore, by a similar argument, if the automaton has the contracting property

$$\forall q, p \in Q : d(q, p) > 1 \text{ there is a } u \in \Sigma^* \text{ such that } d(q \cdot u, p \cdot u) < d(q, p),$$

then the corresponding automaton is simple. This observation may be immediately applied to prove the simplicity of other slowly synchronizing automata, like the Wielandt automaton $\mathcal{W}_n$, and the automaton $\mathcal{D}'_n$ described in [4] (see Fig. 1). These automata have shortest reset words whose length is close to the quadratic bound $(n-1)^2$ in Černý's conjecture. Hence, it appears that there is a connection between "slowly synchronizing" automata and the property of being simple (semisimple), and this is probably not a coincidence, and, in general, synchronizing automata which are "difficult" to synchronize may be simple or semisimple. In particular, is it always the

case that a circular synchronizing automaton on n states with letters having rank at least $n-1$ is simple (semisimple)? What about when one-cluster automata are considered? Some interesting cases in which one may prove (or disprove) simplicity (semisimplicity) could be the series of slowly synchronizing automata found in [4]. Note that the previous slowly synchronizing automata $\mathscr{C}_n, \mathscr{W}_n, \mathscr{D}'_n$ share the common property of having letters whose rank is at least $n-1$. In [17] these automata are called *weakly defective*. Since in Theorem 5 of [17] it is shown that every weakly defective simple automaton is irreducible, we may conclude, that all the automata $\mathscr{C}_n, \mathscr{W}_n, \mathscr{D}'_n$ give rise to a linear representation $\varphi : \Sigma^*/\mathcal{S} \to \mathbb{M}_{n-1}(\mathbb{Q})$ which is irreducible. While for the semisimple case looking for radical "short" words is the same as looking for "short" reset words, in the general case to build a reset word from a radical word, it is enough to consider a suitable power (at most $n-1$ by Lemma 3). However, we now show another way to build synchronizing words from radical words that is more efficient than just simple exponentiation. Moreover, the Černý series in conjunction with Proposition 7 and Theorem 5 show that $(n-1)^2$ is a lower bound for the shortest radical word. This motivates the following Radical Conjecture, whose solution could be a major breakthrough toward a full solution of Černý's conjecture.

Conjecture 1 (Weak Černý's conjecture/Radical Conjecture)**.** *Every synchronizing automaton with n states has a radical word of length at most $(n-1)^2$.*

Note that the solution of this conjecture would solve Černý's conjecture for the class of semisimple automata. Furthermore, we now prove that this conjecture would imply a quadratic upper bound $2(n-1)^2$ for strongly connected synchronizing automata. We first give the following crucial definition. Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a strongly connected synchronizing automaton, i.e., a synchronizing automaton such that for any $q, q' \in Q$ there is a word $u \in \Sigma^*$ such that $\delta(q, u) = q'$. The automaton $\mathscr{A}$ is called 1-*class reducible* if there is a congruence $\rho \in \mathrm{Cong}(\mathscr{A}) \setminus \{\Delta_{\mathscr{A}}\}$ and $q \in Q$ such that $|[q]_\rho| = 1$. We have the following theorem.

Theorem 8. *Assume Conjecture 1 holds. Then, for any strongly connected synchronizing automata $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with $n = |Q|$ states, there is a synchronizing word u with $|u| \leq 2(n-1)^2$.*

Proof. We prove the statement by induction on $|Q|$. The base of induction $|Q| = 1$ clearly holds, whence we may assume $|Q| > 1$. We consider two mutually exclusive cases.

- Suppose $\mathscr{A}$ is 1-class reducible. Thus, let $\rho \in \mathrm{Cong}(\mathscr{A}) \setminus \{\Delta_{\mathscr{A}}\}$ such that there is a $q \in Q$ with $|[q]_\rho| = 1$. The automaton $\mathscr{A}/\rho = \langle Q/\rho, \Sigma, \delta' \rangle$ is synchronizing and strongly connected. Since $m = |Q/\rho| < |Q| = n$ by the induction hypothesis there is a synchronizing word u of $\mathscr{A}/\rho$ with $|u| \leq 2(m-1)^2$. Furthermore, since $\mathscr{A}/\rho$ is strongly connected, there is a word u' with $|u'| \leq m-1$ such that $\delta'(Q/\rho, uu') = [q]_\rho$. Since $|[q]_q| = 1$, we deduce that uu' is also a reset word for $\mathscr{A}$. Moreover, since $m \leq n-1$ we get:

$$|uu'| \leq 2(m-1)^2 + (m-1) \leq 2(n-2)^2 + (n-2) \leq 2(n-1)^2$$

- Suppose that $\mathscr{A}$ is not 1-class reducible. Since Conjecture 1 holds, there is a radical word $u \in \mathrm{Rad}(\mathscr{A})$ with $|u| \leq (n-1)^2$. If $\mathscr{A}$ is semisimple, then u is a reset word, and we are done. Otherwise, by Lemma 4 there is a non-trivial congruence $\sigma \in \mathrm{Cong}_{\mathrm{Ker}(u)}(\mathscr{A}) \setminus \{\Delta_{\mathscr{A}}\}$. Consider the quotient automaton $\mathscr{A}/\sigma = \langle Q/\sigma, \Sigma, \delta' \rangle$. Since $\mathscr{A}$ is not 1-class reducible, $|[p]_\sigma|$ must be at least 2 for every $p \in Q$. It follows that $m = |Q/\sigma| \leq n/2$. Thus, by the induction hypothesis there is a reset word u' of $\mathscr{A}/\sigma$ with

$$|u'| \leq 2(m-1)^2 \leq 2(\frac{n}{2}-1)^2 \leq (n-1)^2$$

since $n > 1$. Furthermore, since $\sigma \subseteq \mathrm{Ker}(u)$, we deduce that $u'u$ is a reset word for $\mathscr{A}$ with $|u'u| \leq 2(n-1)^2$ and this concludes the proof of the theorem.

□

By Proposition 2.1 of [22] we immediately obtain the following corollary.

Corollary 9. *If Conjecture 1 holds, then for any synchronizing automata with n states there is a synchronizing word u with $|u| \leq 2(n-1)^2$.*

Note that no quadratic bound for the length of shortest reset words in synchronizing automata have yet been established.

It is possible to refine the bound $2(n-1)^2$ in Theorem 8 and therefore in the previous corollary. For instance, if we assume $n \geq 2$, then using the same argument one can prove that the bound $2(n-1)^2$ may be substituted by $c(n-1)^2$ with $c = \frac{4}{3}$. However, it does not seem that with the same techniques it is possible to get $c = 1$. This leaves open the following conjecture/open-problem.

Conjecture 2. *The Radical Conjecture implies Černý's conjecture.*

4. Factoring the problem via the Wedderburn-Artin theorem

Since $\overline{\mathcal{R}} = \mathcal{R}/\mathrm{Rad}(\mathcal{R})$ is left artinian and $\mathrm{Rad}(\overline{\mathcal{R}}) = \{0\}$, by Theorem 4.14 of [11] $\overline{\mathcal{R}}$ is semisimple. Therefore, the Wedderburn-Artin Theorem (see Theorem 3.5 of [11]) applies to have the following decomposition:

$$\overline{\mathcal{R}} \simeq \mathbb{M}_{n_1}(D_1) \times \ldots \times \mathbb{M}_{n_k}(D_k)$$

for some (uniquely determined) positive integers $n_1, \ldots, n_k$, and $D_1, \ldots, D_k$ (finite dimensional) $\mathbb{C}$-division algebras. Since $\mathbb{C}$ is an algebraically closed field, we must have

$$D_1 = \cdots = D_k = \mathbb{C}.$$

Indeed, if $d \in D_i$, then $\mathbb{C}[d]$ is a finite field extension of $\mathbb{C}$, whence $d \in \mathbb{C}$. For the Černý series $\mathscr{C}_n$, by direct calculation in case $n = 4$, it is not difficult to see that for the associated synchronized $\mathbb{C}$-algebra $\overline{\mathcal{R}} \simeq \mathcal{R}_n = \mathbb{M}_{n-1}(\mathbb{C})$. This may be true in general, but we did not establish such a result.

Let $\varphi_i : \overline{\mathcal{R}} \to \mathbb{M}_{n_i}(\mathbb{C})$ for $i = 1, \ldots, k$ be the projection map onto the i-th simple component. We recall that $\psi : \mathcal{R} \to \overline{\mathcal{R}}$ is the canonical epimorphism,

and ρ is composition of the Rees morphism $\theta : \Sigma^* \to \Sigma^*/\mathcal{S}$ with the representation φ. Henceforth, we consider the morphism $\overline{\varphi}_i : \Sigma^* \to \mathbb{M}_{n_i}(\mathbb{C})$ for $i = 1, \ldots, k$ defined by:

$$\overline{\varphi}_i = \varphi_i \circ \psi \circ \rho$$

and let $\mathcal{M}_i = \overline{\varphi}_i(\Sigma^*)$ be the subsemigroup of $\mathbb{M}_{n_i}(\mathbb{C})$ generated by Σ^*, for $i = 1, \ldots, k$. We call $\mathcal{M}_i$ the i-th factor monoid. Thus, we factorize the problem of finding a radical word into the problems of finding words u_i, $i = 1, \ldots, k$ with $\overline{\varphi_i}(u_i) = 0$. Indeed, a radical word may be obtained by the concatenation of these words u_i, $i = 1, \ldots, k$. We have the following lemma.

Lemma 10. *The i-th factor monoid $\mathcal{M}_i$ has a unique 0-minimal ideal $\mathcal{I}_i$ which is a 0-simple semigroup. Furthermore, $\mathcal{M}_i$ acts faithfully on both left and right of $\mathcal{I}_i$.*

Proof. Note that $\mathcal{M}_i$ being the image of a finite semigroup is a finite semigroup with 0. Therefore, there is a 0-minimal ideal $\mathcal{I}_i$. By Proposition 3.1.3 of [9] either $\mathcal{I}_i^2 = 0$ or $\mathcal{I}_i$ is a 0-simple semigroup. Since $\mathbb{M}_{n_i}(\mathbb{C})$ is a simple ring, for any $r \in \mathcal{I}_i \setminus \{0\}$ we have:

$$\mathbb{M}_{n_i}(\mathbb{C}) r \mathbb{M}_{n_i}(\mathbb{C}) = \mathbb{M}_{n_i}(\mathbb{C})$$

Therefore, if 1_i denotes the unit of $\mathbb{M}_{n_i}(\mathbb{C})$ and since $\mathcal{I}_i$ is an ideal, it follows that $\sum_j \lambda_j r_j = 1_i$ for some $r_j \in \mathcal{I}_i$, $\lambda_i \in \mathbb{C}$; this decomposition of the identity also shows the faithfulness of the action of $\mathcal{M}_i$ on both the right and left of $\mathcal{I}_i$. Suppose that $\mathcal{I}_i^2 = 0$ and take any non-zero element $s \in \mathcal{I}_i$. Hence, $\sum_j \lambda_j r_j s = s$ and since $r_j s \in \mathcal{I}_i^2 = 0$, we have $s = 0$, a contradiction. Therefore, $\mathcal{I}_i$ is a 0-simple semigroup.

The proof of the uniqueness follows the same argument. Indeed, assume, contrary to our statement, that $\mathcal{I}_i'$ is another 0-minimal ideal, then for all $b \in \mathcal{I}_i'$ we have $\sum_j \lambda_j r_j b = b$. Since $r_j b \in \mathcal{I}_i' \cap \mathcal{I}_i = \{0\}$, then $b = 0$ for all $b \in \mathcal{I}_i'$, a contradiction.

□

We recall that given $u \in \Sigma^*$, the *rank* of u is the cardinality of the rank of the function associated to u, equivalently $\mathrm{rk}(u) = |Q \cdot u|$. By the usual laws of composition of functions, the following holds:

$$\mathrm{rk}(uv) \leq \min\{\mathrm{rk}(u), \mathrm{rk}(v)\}, \quad \forall u, v \in \Sigma^* \tag{2}$$

The following definition extends this parameter to elements of $\mathcal{I}_i \setminus \{0\}$.

Definition 11. For any $g \in \mathcal{I}_i \setminus \{0\}$ the i-th rank of g is given by:

$$\mathrm{Rk}_i(g) = \min\{\mathrm{rk}(u) : \overline{\varphi}_i(u) = g\}$$

The rank of $\mathcal{I}_i$ is defined as:

$$\mathrm{Rk}_i(\mathcal{I}_i) = \min\{\mathrm{Rk}_i(g) : g \in \mathcal{I}_i \setminus \{0\}\}$$

Note that for a non-zero element g, we have $\mathrm{Rk}_i(g) > 1$. Indeed if for some $u \in \Sigma^*$ with $\overline{\varphi}_i(u) = g$, we have $\delta(Q, u) = 1$, then $u \in \mathcal{S}$, whence $\overline{\varphi}_i(u) = 0$. Consequently we have $\mathrm{Rk}_i(\mathcal{I}_i) > 1$. The following lemma shows that the rank is the same for all elements of $\mathcal{I}_i \setminus \{0\}$.

Lemma 12. *For any $g \in \mathcal{I}_i \setminus \{0\}$ we have $\mathrm{Rk}_i(g) = \mathrm{Rk}_i(\mathcal{I}_i)$.*

Proof. Let $g \in \mathcal{I}_i \setminus \{0\}$. By definition we have $\mathrm{Rk}_i(g) \geq \mathrm{Rk}_i(\mathcal{I}_i)$. On the other hand, let $s \in \mathcal{I}_i \setminus \{0\}$ with $\mathrm{Rk}_i(s) = \mathrm{Rk}_i(\mathcal{I}_i)$, and let $u \in \Sigma^*$ such that $\overline{\varphi}_i(u) = s$, $\mathrm{Rk}_i(s) = \mathrm{rk}(u)$. Since, by Lemma 10, the ideal $\mathcal{I}_i$ is 0-simple, $\mathcal{I}_i \setminus \{0\}$ is a $\mathcal{J}$-class. Thus, there are $x, y \in \Sigma^*$ such that $g = \overline{\varphi}_i(xuy)$. Hence, by (2) we get

$$\mathrm{Rk}_i(g) \leq \mathrm{rk}(xuy) \leq \mathrm{rk}(u) = \mathrm{Rk}_i(s) = \mathrm{Rk}_i(\mathcal{I}_i)$$

from which it follows the statement $\mathrm{Rk}_i(g) = \mathrm{Rk}_i(\mathcal{I}_i)$. □

We recall that *the deficiency* of a word $w \in \Sigma^*$ with respect to $\mathscr{A}$ is the (positive) integer $\mathrm{df}(w) = |Q| - |Q \cdot w|$. We make use of the following result which is a consequence of Corollary 3.4 of [12].

Proposition 13. *Given a synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ and the words $v', v \in \Sigma^+$ such that $\mathrm{df}(v') = \mathrm{df}(v) = k > 1$, there exists a word $u \in \Sigma^*$, with $|u| \leq k + 1$, such that $\mathrm{df}(v'uv) > k$.*

This proposition lead to the following interesting lemma which will be useful later.

Lemma 14. *With the above notation, for every $g, h \in \mathcal{I}_i \setminus \{0\}$ there is a word $u \in \Sigma^*$ with $|u| \leq n - \mathrm{Rk}_i(\mathcal{I}_i) + 1$ such that $g\overline{\varphi}_i(u)h = 0$.*

Proof. By Lemma 12 we have $\mathrm{Rk}_i(g) = \mathrm{Rk}_i(\mathcal{I}_i)$. Let $v, z \in \Sigma^*$ be words such that $\overline{\varphi}_i(v) = g$ and $\overline{\varphi}_i(z) = h$, so that $\mathrm{rk}(v) = \mathrm{rk}(z) = \mathrm{Rk}_i(\mathcal{I}_i)$ and $\mathrm{df}(v) = \mathrm{df}(z) = n - \mathrm{Rk}_i(\mathcal{I}_i)$. By Proposition 13, there is $u \in \Sigma^*$ with $|u| \leq n - \mathrm{Rk}_i(\mathcal{I}_i) + 1$ such that $\mathrm{df}(vuz) > n - \mathrm{Rk}_i(\mathcal{I}_i)$ or, equivalently, $\mathrm{rk}(vuz) < \mathrm{Rk}_i(\mathcal{I}_i)$. We claim that $\overline{\varphi}_i(vuz) = 0$. Write $gth = \overline{\varphi}_i(vuz)$ with $\overline{\varphi}_i(u) = t$, and assume, contrary to our claim, that $gth \neq 0$. Since $g \in \mathcal{I}_i$ and this is an ideal, we have $gth \in \mathcal{I}_i \setminus \{0\}$. Therefore, by Lemma 12 we have $\mathrm{Rk}_i(gth) = \mathrm{Rk}_i(\mathcal{I}_i)$. However this implies:

$$\mathrm{Rk}_i(\mathcal{I}_i) = \mathrm{Rk}_i(gth) \leq \mathrm{rk}(vuz) < \mathrm{Rk}_i(\mathcal{I}_i)$$

which is a contradiction, whence $g\overline{\varphi}_i(u)h = 0$. □

An interesting situation occurs when $\mathcal{I}_i \setminus \{0\}$ is a semigroup. In this case a better bound may be obtained using the faithfulness of the action of $\mathcal{M}_i$ on $\mathcal{I}_i$.

Lemma 15. *If $\mathcal{I}_i \setminus \{0\}$ is a semigroup, then there is $a \in \Sigma$ such that $\overline{\varphi}_i(a) = 0$.*

Proof. Let $x, y \in \mathcal{M}_i \setminus \{0\}$. By Lemma 10 $\mathcal{M}_i$ acts faithfully on both left and right of $\mathcal{I}_i$. Hence, there are $x', y' \in \mathcal{I}_i \setminus \{0\}$ such that $x'x \in \mathcal{I}_i \setminus \{0\}$ and $yy' \in \mathcal{I}_i \setminus \{0\}$. Hence, since $\mathcal{I}_i \setminus \{0\}$ is a semigroup we get $x'xyy' \in \mathcal{I}_i \setminus \{0\}$, and so $xy \neq 0$. Thus, since $\overline{\varphi}_i(u) = 0$ holds for every $u \in \mathcal{S}$, there is a letter $a \in \Sigma$ such that $\overline{\varphi}_i(a) = 0$. □

We have the following lemma.

Lemma 16. *Consider an ideal I of $\overline{\mathcal{R}}$ of the form*

$$I = \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \cdots \times \mathbb{M}_{n_{i_m}}(\mathbb{C})$$

for some choices $i_1, \ldots, i_m$ of $\{1, \ldots, k\}$. Assume that there is an integer $\ell \geq 1$ and words $u_j \in \Sigma^*$ with $|u_j| \leq n_{i_j}\ell$ such that $\overline{\varphi}_{n_{i_j}}(u_j) = 0$, $j =$

$1, \ldots, m$. *Let* $J = \psi^{-1}(I)$, *then there is a word* $u \in \Sigma^*$ *with* $|u| \leq \ell(n-1)$ *such that*

$$\rho(u)J = 0.$$

Proof. Since $\mathcal{R}$ is a subalgebra of $\mathbb{M}_{n-1}(\mathbb{C})$, the vector space $V = \mathbb{C}^{n-1}$ is a J-module. By Proposition 4.8 of [11] J and $J/\operatorname{Rad}(J)$ have the same simple left modules. By Exercise 4.7 of [11] we have $\operatorname{Rad}(J) = J \cap \operatorname{Rad}(\mathcal{R})$, hence $J/\operatorname{Rad}(J) = I$. Let

$$V = V_1 \supset V_2 \supset \ldots \supset V_i \supset \ldots \supset V_k = 0$$

be a Jordan-Hölder series. Each module V_{i-1}/V_i for $i = 2, \ldots, k$ is a simple J-module and so, by the above argument, also an I-module. In particular, we have $uv = \psi(u)v$ for all $u \in J$, $v \in V_{i-1}/V_i$. We claim that either $mv = 0$ for all $m \in J$, $v \in V_{i-1}/V_i$ or there is a $v \in V_{i-1}/V_i$ such that

$$V_{i-1}/V_i = \mathbb{M}_{n_{i_j}}(\mathbb{C})v \tag{3}$$

for some $i_j \in \{i_1, \ldots, i_m\}$ and $n_{i_j} = \dim_{\mathbb{C}}(V_{i-1}/V_i)$, where $\dim_{\mathbb{C}}(V_{i-1}/V_i)$ is the dimension of the $\mathbb{C}$-vector space V_{i-1}/V_i. Indeed, the first condition occurs only if for every $v \in V_{i-1}/V_i$, $mv = 0$ for all $m \in \mathbb{M}_{n_{i_j}}(\mathbb{C})$ with $i_j \in \{i_1, \ldots, i_m\}$. Otherwise we may assume that $mv \neq 0$, for some $v \in V_{i-1}/V_i$ and $m \in \mathbb{M}_{n_{i_j}}(\mathbb{C})$ for some $i_j \in \{i_1, \ldots, i_m\}$. Thus, $\mathbb{M}_{n_{i_j}}(\mathbb{C})v$ is a left I-submodule of V_{i-1}/V_i which is non-trivial, whence $V_{i-1}/V_i = \mathbb{M}_{n_{i_j}}(\mathbb{C})v$. Therefore, V_{i-1}/V_i is a simple $\mathbb{M}_{n_{i_j}}(\mathbb{C})$-module and by Theorem 3.3 of [11] $n_{i_j} = \dim_{\mathbb{C}}(V_{i-1}/V_i)$. Let us fix a letter $a \in \Sigma$. For each $i = 2, \ldots, k$ in the Jordan-Hölder series $V_1 \supset V_2 \supset \ldots \supset V_i \supset \ldots \supset V_k = 0$ we have that either $\rho(w_i)JV_{i-1}/V_i = 0$ for $w_i = a$ or (3) holds. Thus, by the hypothesis of the statement there is a word w_i with $|w_i| \leq \dim_{\mathbb{C}}(V_{i-1}/V_i)\ell$ such that

$$\rho(w_i)JV_{i-1}/V_i = \psi(\rho(w_i))\mathbb{M}_{n_{i_j}}(\mathbb{C})v = \overline{\varphi}_{n_{i_j}}(w_i)\mathbb{M}_{n_{i_j}}(\mathbb{C})v = 0$$

Therefore, taking the word $u = w_k \ldots w_2$ one deduces that $\rho(u)JV = 0$, i.e. $\rho(u)J = 0$. Moreover, since $\sum_{i=2}^{k} \dim_{\mathbb{C}}(V_{i-1}/V_i) \leq \dim_{\mathbb{C}}(V) = n-1$, we get the bound of the statement:

$$|u| = \sum_{i=2}^{k} |w_i| \leq \ell \sum_{i=2}^{k} \dim_{\mathbb{C}}(V_{i-1}/V_i) \leq \ell(n-1)$$

□

In case all the 0-minimal ideals are semigroups with 0 adjoined, the Radical Conjecture holds.

Theorem 17. *With the above notation, if* $\mathcal{I}_i \setminus \{0\}$, *for* $i = 1, \ldots k$, *are semigroups, there is a word* $w \in \operatorname{Rad}(\mathscr{A})$ *with* $|w| \leq n-1$.

Proof. Combining Lemma 15 with Lemma 16 we conclude that there is a word $w \in \operatorname{Rad}(\mathscr{A})$ with $|w| \leq n-1$. □

Corollary 18. *With the above notation, if* $\mathcal{I}_i \setminus \{0\}$, *for* $i = 1, \ldots k$, *are semigroups, then there is a reset word of length* $2(n-1)$.

Proof. It follows from the same strategy of the proof of Theorem 8 by using the fact that there is a radical word of length $n-1$ stated in Theorem 17. □

Note that if the transition monoid $M(\mathscr{A})$ belongs to the variety **DS**, then $\mathcal{I}_i \setminus \{0\}$, for $i = 1, \dots k$, are semigroups, whence this last theorem implies Theorem 7.3 of [1], but it does not yield the linear bound $(n-1)$ provided in Theorem 2.6 of [3]. Furthermore, we do not know if Corollary 18 is more general, since it is not known whether the fact that $\mathcal{I}_i \setminus \{0\}$, for $i = 1, \dots k$, are semigroups implies the membership of $M(\mathscr{A})$ to **DS**.

5. Černý's conjecture for strongly semisimple synchronizing automata

In this section we prove that Černý's conjecture holds for a particular class of semisimple synchronizing automata. From Section 3 and Proposition 2, a particular case where $\mathrm{Rad}(\mathscr{A}) = \mathcal{S}$ is when the following closure property holds: the roots of the words in $\mathcal{S}$ are still elements of $\mathcal{S}$. This condition may be expressed using the *root operator* on a regular language. For any regular language L on an alphabet Σ, this operator is defined by:

$$\mathrm{root}(L) = \{u \in \Sigma^* : \exists m \geq 1 \text{ such that } u^m \in L\}$$

This is an operator that returns a regular language (see for instance [10, 18]). Henceforth, we call an *ideal language* any regular language $I \subseteq \Sigma^*$ which is also a two-sided ideal of Σ^*. We say that a synchronizing automaton $\mathscr{A}$ with the ideal language of the reset words $\mathcal{S}$ is *strongly semisimple* if $\mathrm{root}(\mathcal{S}) = \mathcal{S}$. The approach of studying Černý's conjecture from the language theoretic point of view of the ideal language of the synchronizing words is relatively recent and may be drawn back to [13]. In general, given an ideal language I it is easy to see that the minimal DFA recognizing I is actually a synchronizing automaton whose language of reset words is exactly I. However, this automaton has a sink state, and Černý's conjecture has been verified for such automata [16]. On the other hand, it is well known that if Černý's conjecture is solved for the class of strongly connected synchronizing automaton, then this conjecture holds in general. Thus, the approach of studying synchronizing automata via their languages of synchronizing words is supported by the following result presented in a first version in [14] and then improved in [15] which we partially report here in the following theorem.

Theorem 19. *Let I be an ideal language on a non-unary alphabet, then there is a strongly connected synchronizing automaton having I as the set of synchronizing words.*

We now characterize the ideal languages I satisfying $\mathrm{root}(I) = I$ but first we need some definitions. We recall that for a regular language $L \subseteq \Sigma^*$, the language $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$ is also regular. Given two words $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x that is also a suffix of y, we define the *concatenation with overlap* as $y \circ x = y'vx'$. An ideal language $I \subseteq \Sigma^*$ is called a *cyclic ideal language* whenever $\mathrm{root}(I) = I$. We have the following characterization.

Proposition 20. *Given an ideal language I, the following are equivalent.*

(i) $\sqrt{I} \subseteq I$;
(ii) *for any $u \in I$ and any factorization $u = xy$, for some $x, y \in \Sigma^*$, then $y \circ x \in I$;*

(iii) $\mathrm{root}(I) = I$;
(iv) $I = \eta^{-1}(0)$ *where* $\eta : \Sigma^* \to S$ *is a morphism onto a finite monoid with* 0 *satisfying the condition* $x^2 = 0 \Rightarrow x = 0$.

Proof. $(i) \Rightarrow (ii)$. Assume $\sqrt{I} \subseteq I$ and let $u \in I$ with $u = xy$. Suppose that $x = vx'$ and $y = y'v$ for some $v \in \Sigma^*$ which is the maximal prefix of x which is also a suffix of y. Let $h = y \circ x = y'vx'$. Since I is an ideal we have $h^2 = y'vx'y'vx' = y'ux' \in I$. Hence, since $\sqrt{I} \subseteq I$, we deduce $h \in I$.

$(ii) \Rightarrow (iii)$. Assume I is closed under concatenation with overlap. Since $I \subseteq \mathrm{root}(I)$, we have to prove the other inclusion. Let $u \in \mathrm{root}(I)$ and let $n > 1$ be the integer such that $u^n \in I$. Since $u^n = uu^{n-1}$ and I is closed by concatenation with overlap, then we have $u^{n-1} = u^{n-1} \circ u \in I$. Thus, using induction we get $u \in I$.

$(iii) \Rightarrow (iv)$. Since I is regular there is a morphism $\chi : \Sigma^* \to T$, for some finite monoid with $I = \chi^{-1}(\chi(I))$. Since $J = \chi(I)$ is a two-sided ideal of T, we may consider the Rees quotient semigroup $S = T/J$. Thus, the morphism $\eta : \Sigma^* \to S$, which is the composition of χ with the Rees morphism $T \to T/J$, satisfies $\eta^{-1}(0) = I$. Furthermore, if $x^2 = 0$ in T/J, then $x^2 \in J$ in T. Hence, if $u \in \Sigma^*$ such that $\chi(u) = x$, then $u \in \mathrm{root}(I) = I$, and so $\chi(u) \in J$, i.e. $x = 0$ in T/J.

$(iv) \Rightarrow (i)$. If $u^2 \in I$, then $\eta(u)^2 = 0$, whence $\eta(u) = 0$, i.e. $u \in I$.

□

This proposition also justifies the name cyclic since these are ideal languages that are also cyclic languages in the sense of [7]. Indeed, the first condition of the definition of cyclic language, namely $u \in I$ if and only if $u^n \in I$, is satisfied since I is an ideal and $\mathrm{root}(I) = I$. We claim that the second condition, which states that $uv \in I$ if and only if $vu \in I$, is also satisfied. To prove the claim, assume that $uv \in I$. Since I is an ideal, then $uvu \in I$. Hence, by Proposition 20, we also have $(vu) \circ u \in I$, i.e. $vu \in I$.

By Proposition 2 and the definition it is clear that a strongly semisimple synchronizing automaton is semisimple. We have the following main theorem.

Theorem 21. *A strongly semisimple synchronizing automaton* $\mathscr{A}$ *with* n *states has a reset word of length* $(n-1)$. *In particular, it satisfies Černý's conjecture.*

Proof. Keeping the notation of Section 4, let $\mathcal{M}_i$ for $i = 1, \ldots, k$ be the factor monoids. We say that $T \subseteq \{1, \ldots, k\}$ is a *core* whenever the condition $\overline{\varphi}_i(u) = 0$ for all $i \in T$ implies $\overline{\varphi}_i(u) = 0$ for all $i \in \{1, \ldots, k\}$. Let $C \subseteq \{1, \ldots, k\}$ be a minimal core with respect to inclusion and let

$$I = \prod_{j \in C} \mathbb{M}_{n_j}(\mathbb{C})$$

be the corresponding ideal in $\overline{\mathcal{R}}$. For a fixed $j \in C$, we claim that the associated 0-minimal ideal $\mathcal{I}_{n_j} \setminus \{0\}$ is a semigroup. Since C is a minimal core, there is a word $w \in \Sigma^*$ such that $\overline{\varphi}_j(w) \neq 0$ and $\overline{\varphi}_r(w) = 0$ for all $r \in C \setminus \{j\}$. We claim that there is an element $t \in \mathcal{I}_{n_j} \setminus \{0\}$ such that $t\overline{\varphi}_j(w) \neq 0$. Indeed, assume contrary to our claim, that $t\overline{\varphi}_j(w) = 0$ for all $t \in \mathcal{I}_{n_j} \setminus \{0\}$. In the proof of Lemma 10 we show that $\mathcal{I}_{n_j} \setminus \{0\}$ generates the

identity 1_j of the ring $\mathbb{M}_{n_j}(\mathbb{C})$, i.e. $\sum_m \lambda_m r_m = 1_j$ for some $r_m \in \mathcal{I}_{n_j} \setminus \{0\}$, $\lambda_m \in \mathbb{C}$. Thus, $1_j\overline{\varphi}_j(w) = 0$ which implies $\overline{\varphi}_j(w) = 0$, a contradiction. Thus, there is $v \in \Sigma^*$ such that $\overline{\varphi}_j(v) = t$, and so

$$\overline{\varphi}_j(vw) = t\overline{\varphi}_j(w) \neq 0. \tag{4}$$

We have two possibilities: either $\overline{\varphi}_j(vwvw) = 0$ or $\overline{\varphi}_j(vwvw) \neq 0$. In the former case $vwvw \in \mathcal{S}$ because $\mathscr{A}$ is semisimple. Since $\mathscr{A}$ is also strongly semisimple we get $vw \in \mathrm{root}(\mathcal{S}) = \mathcal{S}$, which implies $\overline{\varphi}_j(vw) = 0$. However, this contradicts (4). Hence, we must have $\overline{\varphi}_j(vwvw) \neq 0$ which implies by Lemma 3.2.7 of [9] that $\overline{\varphi}_j(vw)$ belong to some $\mathcal{H}$-class containing an idempotent e. In particular, since $\mathcal{M}_j$ is finite, we may assume $\overline{\varphi}_j((vw)^m) = e$ for some integer $m \geq 0$. Assume, contrary to our claim, that $\mathcal{I}_{n_j} \setminus \{0\}$ is not a semigroup. Hence, by Lemma 3.2.7 of [9], there is a zero $\mathcal{H}$-class H of $\mathcal{I}_{n_j} \setminus \{0\}$. Let $h \in H$. Suppose that $h \in R_e$ and let $s \in \Sigma^*$ such that $\overline{\varphi}_j(s) = h$. Consider the word $(vw)^m s$. Since e is a left identity for h, we have $\overline{\varphi}_j((vw)^m s) = h \neq 0$. However, $\overline{\varphi}_j(((vw)^m s)^2) = h^2 = 0$, which with $\overline{\varphi}_r(w) = 0$ for all $r \in C \setminus \{j\}$, implies $(vw)^m s \in \mathrm{root}(\mathcal{S}) = \mathcal{S}$, and so $h = 0$, a contradiction. On the other hand, we may assume that $R_e \cap L_h$ is an $\mathcal{H}$-class containing an idempotent g (otherwise the zero $\mathcal{H}$-class $H = R_e \cap L_h$ could have been chosen instead). Let $u \in \Sigma^*$ such that $\overline{\varphi}_j(u) = g$. Using the fact that e is a left identity for g and g is a right identity for h we get $\overline{\varphi}_j(s(vw)^m u) = h \neq 0$. However, $\overline{\varphi}_j((s(vw)^m u)^2) = h^2 = 0$ which implies $s(vw)^m u \in \mathrm{root}(\mathcal{S}) = \mathcal{S}$, and so $h = 0$, a contradiction. Therefore, $\mathcal{I}_{n_j} \setminus \{0\}$ is a semigroup. Applying Lemma 16 to I we deduce that there is a word u with $|u| \leq (n-1)$ such that $\overline{\varphi}_i(u) = 0$ for all $i \in C$. Hence, since C is a core, $\overline{\varphi}_i(u) = 0$ for all $i = 1, \ldots k$, i.e. $u \in \mathrm{Rad}(\mathscr{A}) = \mathcal{S}$ since $\mathscr{A}$ is semisimple. □

6. The Radical Conjecture in some cases

In this section we analyze two further cases in which the Radical Conjecture (Conjecture 1) holds. We start considering the situation where $\mathrm{Rad}(\mathscr{A})$ is a cyclic ideal. We use the same notation as in Section 4 where $\overline{\mathcal{R}} \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$. For an element $u \in \Sigma^*$, we denote by $\mathrm{Supp}(u)$ the maximal subset A of $\{1, \ldots, k\}$ such that for any $i \in A$, $\overline{\varphi}_i(u) \neq 0$. For a word $u \in \Sigma^*$, consider the poset $S(u) = \{\mathrm{Supp}(v) : v \in \Sigma^* u \Sigma^*\}$, ordered by inclusion. A minimal element in $S(u)$, for some $u \in \Sigma^*$, is called *a minimal section*. By the minimality we have the following immediate lemma.

Lemma 22. *Let A be a minimal section of $S(u)$ with $u \in \Sigma^*$. Let $v \in \Sigma^*$ be a word such that $\mathrm{Supp}(v) = A$. Then, for every $w \in \Sigma^* v \Sigma^*$, $\overline{\varphi}_i(w) = 0$ holds for some $i \in A$ if and only if $\overline{\varphi}_j(w) = 0$ holds for all $j \in \{1, \ldots, k\}$.*

We have the following theorem.

Theorem 23. *If $\mathrm{Rad}(\mathscr{A})$ is a cyclic ideal, then Conjecture 1 is valid.*

Proof. Similarly to the proof of Theorem 21, consider a minimal core $C \subseteq \{1, \ldots, k\}$ and let

$$I = \prod_{j \in C} \mathbb{M}_{n_j}(\mathbb{C})$$

be the corresponding ideal in $\overline{\mathcal{R}}$. Since the union of the minimal sections contained in C is a core, by minimality of C, it follows that there is a covering $\{s_1, \ldots, s_\ell\}$ of C formed by minimal sections. Let u_i, $i = 1, \ldots, \ell$, be the corresponding words such that $s_i = \mathrm{Supp}(u_i)$. If we prove that there are words v_i with

$$|v_i| \leq \min\{n_j : j \in s_i\}(n-1)$$

such that $\overline{\varphi}_r(v_i) = 0$ for all $r \in s_i$, then the statement of the theorem follows from Lemma 16 applied to the ideal I. We devote the rest of the proof to show this last claim. Let $j \in s_i$ such that $n_j = \min\{n_k : k \in s_i\}$, and write $R = \mathbb{M}_{n_j}(\mathbb{C})$. By Lemma 10 since $\mathcal{M}_j$ acts faithfully on the right of $\mathcal{I}_j$, and $\overline{\varphi}_j(u_i) \neq 0$, there is a word $\overline{u}_i \in \Sigma^* u_i \Sigma^*$ such that $\overline{\varphi}_j(\overline{u}_i) \in \mathcal{I}_j \setminus \{0\}$. Hence, since R is simple, there are words $h_1, \ldots, h_m \in \Sigma^* u_i \Sigma^*$ such that

$$R\overline{\varphi}_j(h_1) + \cdots + R\overline{\varphi}_j(h_m) = R$$

Since R is the direct sum of n_i left ideals, by the Jordan-Hölder Theorem we may assume $m \leq n_j$. Since $\mathrm{Rk}_i(\mathcal{I}_j) > 1$, by Lemma 14, for every $g \in \mathcal{I}_j \setminus \{0\}$ there is a word w with $|w| \leq n-1$ such that $g\overline{\varphi}_j(w)g = 0$. Applying this last fact to $\overline{\varphi}_j(h_1)$ then there is a word w_1 with $|w_1| \leq n-1$ such that $\left(\overline{\varphi}_j(h_1 w_1)\right)^2 = 0$. Since $h_1 w_1 \in \Sigma^* u_i \Sigma^*$, by Lemma 22 we get $\overline{\varphi}_r\left((h_1 w_1)^2\right) = 0$ for all $r \in \{1, \ldots, k\}$, i.e., $(h_1 w_1)^2 \in \mathrm{Rad}(\mathscr{A})$. Hence, by the closure property of $\mathrm{Rad}(\mathscr{A})$ we get $(h_1 w_1) \in \mathrm{Rad}(\mathscr{A})$, or equivalently, $\overline{\varphi}_j(h_1 w_1) = 0$. Hence, multiplying $h_1, \ldots, h_m$ on the right by $\overline{\varphi}_j(w_1)$ we get $h_2\overline{\varphi}_j(w_1), \ldots, h_m\overline{\varphi}_j(w_1) \in \mathcal{I}_i$. Now, applying the same argument at most $m \leq n_j$ times, we may find words $w_1, \ldots, w_t \in \Sigma^*$ with $t \leq m \leq n_j$ and $|w_i| \leq n-1$, $i = 1, \ldots, t$ such that $h_i\overline{\varphi}_j(w_1 \ldots w_t) = 0$ for all $i = 1, \ldots, m$. Thus, if we put $v_i = w_1 \ldots w_t$ we have $R\overline{\varphi}_j(v_i) = 0$, i.e. $\overline{\varphi}_j(v_i) = 0$ with $|v_i| \leq t(n-1) \leq n_i(n-1) \leq \min\{n_j : j \in s_i\}(n-1)$. □

We now consider another situation of an automaton $\mathscr{A}$ for which the associated set $E(\mathcal{I}_i)$ of idempotents of the ideal $\mathcal{I}_i$ forms a semilattice for each $i = 1, \ldots, k$. We first need the following proposition.

Proposition 24. *With the notation of Section 4, if $E(\mathcal{I}_i)$ is a semilattice, then there is a word $u \in \Sigma^*$ with $|u| \leq n_i(n_i+1)/2$ such that $\overline{\varphi}_i(u) = 0$.*

Proof. Since $\mathcal{I}_i$ is a completely 0-simple semigroup, we have that the $\mathcal{D}$-class $\mathcal{I}_i \setminus \{0\}$ is regular. Therefore, each $\mathcal{L}$-class L_j for $j = 1, \ldots, p$ has at least an idempotent e_j (see Proposition 2.3.2 of [9]). By the Rees Theorem (see Theorem 3.2.3 of [9]) every idempotent of $\mathcal{I}_i$ is primitive. Since $E(\mathcal{I}_i)$ is a semilattice, for all $j, s \in \{1, \ldots, p\}$, the product $e_j e_s$ is an idempotent with $e_j e_s \leq e_j, e_s$, hence, since $e_j e_s$ is primitive we get $e_j e_s = 0$. Write $R = \mathbb{M}_{n_i}(\mathbb{C})$ and consider the R-submodule of R:

$$H = Re_1 \oplus \ldots \oplus Re_p \tag{5}$$

We claim that $H = R$ and $p \leq n_i$. If $x \in \mathcal{I}_i \setminus \{0\}$, then there is e_j for some $j \in \{1, \ldots, p\}$ such that $x \mathcal{L} e_j$. Thus, $x = y e_j$ for some $y \in \mathcal{I}_i$ and so $x \in H$. Hence, we have proved $\mathcal{I}_i \subseteq H$. Using the same argument of Lemma 10, we deduce that the unit of R is a $\mathbb{C}$-linear combination of elements of $\mathcal{I}_i$, and so $R \subseteq H$ from which it follows that $R = H$. By Theorem 3.3 of [11] R is the direct sum of n_i simple left submodules. Hence, by the Jordan-Hölder

Theorem we obtain the last claim $p \leq n_i$. We now show that there is a word u satisfying the statement of the proposition. For $x \in \mathcal{M}_i$, we denote by $L(x)$ the $\mathcal{L}$-class containing x. Consider the DFA $\mathcal{D}_i = \langle Q_i, \Sigma, \delta_i \rangle$ whose set of states Q_i consists of all the $\mathcal{L}$-classes $L_1, \ldots, L_p$ of $\mathcal{I}_i$ plus a sink state 0 and δ_i is defined on the non-sink states by

$$\delta_i(L_j, a) = \begin{cases} L(x\overline{\varphi}_i(a)) & \text{for some } x \in L_j, \\ 0 & \text{if } x\overline{\varphi}_i(a) = 0. \end{cases}$$

Note that δ_i is well defined since $x\mathcal{L}y$ implies $x\overline{\varphi}_i(a)\mathcal{L}y\overline{\varphi}_i(a)$ and $\mathcal{I}_i$ is an ideal. Moreover, $\mathcal{D}_i$ is synchronizing since $\mathcal{R}$ is synchronizing. Indeed, there is a word $w \in \Sigma^*$ such that $\rho(w) = 0$, hence $x\overline{\varphi}_i(w) = 0$ for any $x \in \mathcal{I}_i$. Hence, $\mathcal{D}_i$ is a synchronizing DFA with $p \leq n_i$ states with a zero. Therefore, by Theorem 6.1 of [16] there is a word $u \in \Sigma^*$ with $|u| \leq n_i(n_i+1)/2$ with $\delta_i(q, u) = 0$ for all $q \in Q_i$. This is equivalent to saying that $x\overline{\varphi}_i(u) = 0$ for all $x \in \mathcal{I}_i$. In particular, $e_j\overline{\varphi}_i(u) = 0$ for all $j = 1, \ldots, p$. Hence, by (5) and $H = R$, we get $\overline{\varphi}_i(u) = 0$. □

From the previous proposition we obtain the following result.

Theorem 25. *With the notation of Section 4, if $E(\mathcal{I}_i)$ is a semilattice for each $i = 1, \ldots, k$, then Conjecture 1 holds.*

Proof. By Proposition 24 for each $i = 1, \ldots, k$ there is a word u_i such that $\overline{\varphi}_i(u_i) = 0$ and $|u_i| \leq n_i(n_i+1)/2$. Thus, the word $u = u_1 \ldots u_k$ satisfies $u \in \mathrm{Rad}(\mathscr{A})$. Using the equality (2) of Proposition 7.2 of [11] and the fact that $\mathbb{C}$ is an algebraically closed field we get:

$$\dim_{\mathbb{C}}(\mathcal{R}) = \dim_{\mathbb{C}}(\mathrm{Rad}(\mathcal{R})) + \sum_{i=1}^{k} n_i^2$$

Hence, since $\dim_{\mathbb{C}}(\mathcal{R}) \leq (n-1)^2$, and $n_i(n_i+1)/2 \leq n_i^2$ $(n_i \geq 1)$ we obtain:

$$|u| \leq \sum_{i=1}^{k} n_i^2 \leq (n-1)^2 - \dim_{\mathbb{C}}(\mathrm{Rad}(\mathcal{R})) \tag{6}$$

which concludes the proof. □

Note that Theorem 25 may be applied to the case where the transition monoid $E(M(\mathscr{A}))$ is a semilattice. In this case the stronger result for the variety **EDS** stated in Theorem 4.2 of [3] holds. However, we do not know whether the condition that $E(\mathcal{I}_i)$ is a semilattice for each $i = 1, \ldots, k$ implies that $E(M(\mathscr{A}))$ is also a semilattice.

Acknowledgements

This work has been partially supported by the European Regional Development Fund through the program COMPETE and by the Portuguese Government through the FCT – Fundação para a Ciência e a Tecnologia under the project PEst-C/MAT/UI0144/2013. The second author also acknowledges the support of the FCT project SFRH/BPD/65428/2009.
The authors thank the anonymous referees of the preliminary version of this paper published in the proceedings of DLT 2015 [2] for the precious suggestions and comments provided.

References

[1] J. Almeida, S. Margolis, B. Steinberg, M. Volkov, *Representation theory of finite semigroups, semigroup radicals and formal language theory*, Trans. Amer. Math. Soc., 361(3) (2009), pp. 1429-1461.

[2] J. Almeida, E. Rodaro, *Semisimple Synchronizing Automata and the Wedderburn-Artin Theory*, In: DLT 2015, Vol 8633 of Lect. Notes Comput. Sci. Springer Berlin Heidelberg, (2015), pp. 49-60.

[3] J. Almeida, B. Steinberg, *Matrix Mortality and the Černý-Pin Conjecture*, In: DLT 2009, Vol 5583 of Lect. Notes Comput. Sci. Springer Berlin Heidelberg, (2009), pp. 67-80.

[4] D. S. Ananichev, M. V. Volkov, and V. V. Gusev, *Primitive digraphs with large exponents and slowly synchronizing automata*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 402, no. Kombinatorika i Teoriya Grafov. IV, (2012), pp. 9-39

[5] F. Arnold, B. Steinberg, *Synchronizing groups and automata*. Theor. Comput. Sci., 359(1-3), (2006), pp. 101-110.

[6] I. Babcsányi, *Automata with Finite Congruence Lattices*, Acta Cybernet., Vol. 18, issue 1 (2007), pp. 155-165.

[7] M.-P. Béal, O. Carton, C. Reutenauer, *Cyclic languages and Strongly cyclic languages*, In: STACS 96, Vol. 1046 of Lect. Notes Comput. Sci. Springer Berlin Heidelberg, (1996), pp. 49-59.

[8] J. Černý, *Poznámka k homogénnym eksperimentom s konečnými automatami [in Slovak]*, Mat.-Fyz. Čas. Slovensk. Akad. Vied., 14 (1964), pp. 208-216.

[9] J. M. Howie, *Fundamentals of Semigroup Theory*, Clarendon Press, Oxford (1995).

[10] B. Krawetz, *Monoids and the State Complexity of the Operation root(L)*, Master's thesis, University of Waterloo (2003).

[11] T.Y. Lam, *A first course in noncommutative rings*, Springer.

[12] S. Margolis, J.-E. Pin, M. Volkov, *Words guaranteeing minimum image*, Int. J. Found. Comput. Sci. 15 (2004) pp. 259-276.

[13] E. Pribavkina, E. Rodaro, *Synchronizing automata with finitely many minimal synchronizing words*, Inform. and Comput., 209(3) (2011) pp. 568-579.

[14] R. Reis, E. Rodaro, *Regular Ideal Languages and Synchronizing Automata*, In: Karhumäki, J., Lepistö, A., Zamboni, L. (Eds.), Combinatorics on Words. Vol. 8079 of Lect. Notes Comput. Sci. Springer Berlin Heidelberg, (2013) pp. 205-216.

[15] R. Reis, E. Rodaro, *Ideal Regular Languages and Strongly Connected Synchronizing Automata*, preprint (2014).

[16] I.K. Rystsov, *Reset words for commutative and solvable automata*, Theor. Comp. Sci. 172, Issues 1-2, 10 (1997), pp. 273-279.

[17] I.K. Rystsov, *Primitive and Irreducible Automata*, Cybern. Syst. Anal. 51(4) (2015) pp. 506-513.

[18] J. Shallit, *A Second Course in Formal Languages and Automata Theory*, Cambridge University Press.

[19] B. Steinberg, *The Černý conjecture for one-cluster automata with prime length cycle*, Theor. Comp. Sci. 412, Issue 39, 9 (2011), pp. 5487-5491.

[20] G. Thierrin, *Simple automata*, Kybernetika, Vol. 6, No. 5 (1970), pp. 343-350.

[21] M. V. Volkov, *Synchronizing automata and the Černý conjecture*, In: LATA 2008, Vol 5196 of Lect. Notes Comput. Sci. Springer Berlin Heidelberg, (2008), pp. 11-27.

[22] M. V. Volkov, *Synchronizing automata preserving a chain of partial orders*, Theor. Comp. Sci. 410, (2009), pp. 3513-3519.

Centro de Matemática, Faculdade de Ciências, Universidade do Porto, 4169-007 Porto, Portugal, Rua do Campo Alegre, 687, Porto, 4169-007, Portugal

E-mail address: jalmeida@fc.up.pt

E-mail address: emanuele.rodaro@fc.up.pt