Words of Minimum Rank in Deterministic Finite Automata

Jarkko Kari[1⋆], Andrew Ryzhikov[2], and Anton Varonka[3]

[1] University of Turku, Turku, Finland
[2] LIGM, Université Paris-Est, Marne-la-Vallée, France
[3] Belarusian State University, Minsk, Belarus

Abstract. The rank of a word in a deterministic finite automaton is the size of the image of the whole state set under the mapping defined by this word. We study the length of shortest words of minimum rank in several classes of complete deterministic finite automata, namely, strongly connected and Eulerian automata. A conjecture bounding this length is known as the Rank Conjecture, a generalization of the well known Černý Conjecture. We prove upper bounds on the length of shortest words of minimum rank in automata from the mentioned classes, and provide several families of automata with long words of minimum rank. Some results in this direction are also obtained for automata with rank equal to period (the greatest common divisor of lengths of all cycles) and for circular automata.

Keywords: Minimum rank word · Synchronizing automaton · Eulerian automaton.

1 Introduction

A *complete deterministic finite automaton* (which we simply call an *automaton* in this paper) is a triple $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$, where Q is a finite non-empty set of *states*, Σ is a finite non-empty *alphabet*, and $\delta : Q \times \Sigma \to Q$ is a complete *transition function*. We extend δ to $Q \times \Sigma^*$ and $2^Q \times \Sigma^*$ in the usual way: $\delta(q, w) = \delta(\delta(q, v), a)$ if $w = va$ for some word $v \in \Sigma^*$ and $a \in \Sigma$, and $\delta(S, w) = \{\delta(q, w) \mid q \in S\}$ for $S \subseteq Q$. We call the automaton *binary* or *ternary* if $|\Sigma| = 2$ or $|\Sigma| = 3$, respectively.

An automaton $\mathcal{A}$ is called *synchronizing* if there is a word w that resets it, that is, brings it to a particular state no matter at which state the word has been applied: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. Any such word w is said to be a *synchronizing word* (or a *reset word*) for the automaton while the minimum length of a synchronizing word for $\mathcal{A}$ is called the *reset threshold* of $\mathcal{A}$ and is denoted $\mathrm{rt}(\mathcal{A})$.

A natural question arises: *how large can the reset threshold of n-state synchronizing automaton be?* In 1964 Černý [9] constructed an n-state synchronizing

⋆ Research supported by the Academy of Finland grant 296018

automaton $\mathcal{C}_n$ with two letters which reset threshold is $(n-1)^2$ for all $n > 1$. The state set of $\mathcal{C}_n$ is $Q = \{1, 2, \ldots, n\}$ and the letters a and b act on it as follows:

$$\delta(i,a) = \begin{cases} i, & \text{if } i > 1 \\ 2, & \text{if } i = 1; \end{cases} \quad \delta(i,b) = \begin{cases} i+1, & \text{if } i < n \\ 1, & \text{if } i = n. \end{cases}$$

We refer to automata of this series as *the Černý automata*.

Some time later (e.g. [8]) it was conjectured that every synchronizing automaton with n states can be reset by a word of length $(n-1)^2$. This is known as *the Černý Conjecture* which remains open more than 50 years later (for a survey on this topic see [20]).

Given an automaton $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$, the *rank* of a word $w \in \Sigma^*$ with respect to $\mathcal{A}$ is the number of states active after applying it, that is, the number $|\delta(Q, w)|$. When the automaton is clear from the context, we just call it the rank of w. The *rank* of an automaton is the minimum rank among all words with respect to the automaton. A *synchronizing* word (automaton) is thus a word (automaton) of rank 1. We call the length of a shortest word of minimum rank of an automaton $\mathcal{A}$ the *minimum rank threshold* of $\mathcal{A}$. We denote it $\mathrm{mrt}(\mathcal{A})$.

Pin [17] proposed the following generalization of the Černý Conjecture: for every n-state automaton having a word of rank at most r, there exists such a word of length at most $(n-r)^2$. A cubic upper bound is proved for this conjecture [16]. However, Kari [14] found a counterexample to the conjectured $(n-r)^2$ bound for $r = 2$, which is a binary automaton $\mathcal{K}$ with $n = 6$ states. As a consequence, a modification of this generalized conjecture was proposed by Pribavkina restricting it to r being the rank of the considered automaton ($\mathcal{K}$ is synchronizing but the Pin's bound is exceeded for a word of rank 2). This restricted case has not been disproved yet, and is sometimes referred to as the Rank Conjecture (or the Černý-Pin Conjecture in [1]). The case $r = 1$ is the Černý Conjecture.

It was pointed out in [2] that one of the reasons why the Černý Conjecture is so hard to tackle is the lack of examples of slowly synchronizing automata. The same is true concerning the Rank Conjecture. Pin [18] provided the following example. The automaton with two letters consists of r connected components, one of which is the Černý automaton $\mathcal{C}_{n-r+1}$ and $r-1$ others are isolated states with loops labeled with both letters. The automaton thus constructed has n states, rank r and its minimum rank threshold is precisely $(n-r)^2$. However, this automaton is not strongly connected (an automaton is called *strongly connected* if any state can be mapped to any other state by some word), so this case in some sense reduces to the rank 1 case. No series of strongly connected automata with $\mathrm{mrt}(\mathcal{A})$ close to the $(n-r)^2$ bound were introduced so far.

In this paper, we propose a number of techniques to construct strongly connected automata of rank r with large minimum rank thresholds. The families of automata we obtain do not reach the conjectured bound $(n-r)^2$, but the minimum rank threshold is typically of the order $\frac{(n-r)^2}{r}$, or within a constant multiple of this. We provide families of automata having additional properties

such as being Eulerian or circular, or having rank equal to the period (see Section 2 for definitions of these concepts). We also consider upper bounds: we prove the Rank Conjecture for Eulerian automata, and obtain an upper bound on the minimum rank threshold of circular automata.

The paper is organized as follows. In Section 2 we provide the main definitions and preliminary results. In Section 3 we provide constructions for turning a binary synchronizing automaton into a higher rank ternary (Section 3.1) or binary (Section 3.2) automaton having its minimum rank threshold close to the reset threshold of the original automaton. Applying these constructions on known series of synchronizing automata yield new series of automata of higher ranks $r > 1$. In Section 3.3 we show how upper bounds on the reset threshold can be turned into upper bounds on the minimum rank thresholds on automata with period equal to rank. In Section 4 we prove the Rank Conjecture for automata based on Eulerian digraphs, along with exhibiting lower bounds on minimum rank thresholds. In Section 4.2 we present a way to transform known bounds from Eulerian automata to circular automata. In particular, quadratic upper bounds on minimum rank thresholds for circular automata (including the reset threshold) are proved. In Section 4.3 we contribute to the Road Coloring Problem, presenting a nearly-linear algorithm of finding a coloring of minimum rank for an Eulerian digraph.

2 Main definitions and preliminary results

All our digraphs are multigraphs and they are allowed to have loops. The *underlying digraph* $D(\mathcal{A})$ of an automaton $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ has vertex set Q, and for any $q, p \in Q$, there are as many edges from q to p as there are letters $a \in \Sigma$ such that $\delta(q, a) = p$. An automaton $\mathcal{A}$ is called a *coloring* of its multigraph $D(\mathcal{A})$. The underlying digraph of every automaton has the same outdegree at all its vertices. From now on, we consider only digraphs with this property.

A digraph D is called *strongly connected* if for every pair (v, v') of vertices there exists a directed path from v to v'. An automaton is *strongly connected* if its underlying digraph is strongly connected.

The *period* of a digraph D is the greatest common divisor of the lengths of its cycles, and the period of an automaton is defined as the period of its underlying digraph. Let us remark explicitly that digraphs with period $p > 1$ do not have synchronizing colorings. The following lemma is essential to understand the period of a digraph.

Lemma 1 ([5], p.29). *Let D be a digraph with period p. Then the set V of vertices of D can be partitioned into p nonempty sets $V_1, V_2, \ldots, V_p$ where each edge of D goes from a vertex from V_i and enters some vertex in V_{i+1} for some i (the indices are taken modulo p).*

We will call this partition a *p-partition* of a digraph or of its coloring.

Much of the literature on synchronizing automata concentrates on the primitive case. A digraph is called *primitive* if it is strongly connected and the period

is $p = 1$. In this paper we are interested in automata with underlying digraphs which are strongly connected but not primitive.

A digraph is *Eulerian* if for each vertex the outdegree is equal to the indegree. The automaton is *Eulerian* if it is strongly connected and its underlying digraph is Eulerian. Equivalently, at every state there must be exactly $|\Sigma|$ incoming transitions, where Σ is the alphabet of the automaton. An automaton is *circular* if there is a letter which acts on its set of states as a cyclic permutation.

3 Strongly connected automata

3.1 A lower bound for ternary automata

We start with a construction yielding a series of strongly connected ternary automata. We transform a synchronizing binary automaton $\mathcal{A}$ into a ternary automaton $\mathcal{A}'$ of a given rank $r > 1$ such that $\mathrm{mrt}(\mathcal{A}')$ is related to $\mathrm{rt}(\mathcal{A})$.

We start with a synchronizing binary automaton $\mathcal{A} = \langle Q, \{a, b\}, \delta\rangle$ with t states $q_1, \ldots, q_t$. We define a ternary automaton $\mathcal{A}' = \langle Q', \{a, b, c\}, \delta'\rangle$ of rank r with the size $n = r \cdot t$ state set $Q' = \bigcup_{i=0}^{r-1} Q_i$ where each Q_i contains t states $q_{i,1}, \ldots, q_{i,t}$. The action of the transition function δ' on the set Q_0 repeats the action of δ on set Q for the letters a, b: for $x = a$ and $x = b$ we have $\delta'(q_{0,j}, x) = q_{0,k}$ if and only if $\delta(q_j, x) = q_k$. On the other sets $Q_1, \ldots, Q_{r-1}$ the transitions by the letters a, b are self-loops: we set $\delta'(q_{i,k}, x) = q_{i,k}$ for $x = a$ and $x = b$, for all $i \neq 0$ and all k. Finally, the letter c shifts states of Q_i to the next set Q_{i+1}: we define $\delta'(q_{i,k}, c) = q_{i+1,k}$ where $i + 1$ is counted modulo r, that is, elements of Q_{r-1} are shifted to the set Q_0. Note that the construction preserves the property of the automaton to be strongly connected or Eulerian.

Since $\mathcal{A}$ is synchronizing, we certainly obtain an automaton of rank r as the result of this construction. No two states from different sets Q_i, Q_j with $i \neq j$ can be merged for the obvious reason. Each of them though can be mapped using the letter c to Q_0 which, in turn, can be mapped to a single state.

If w is a shortest reset word for $\mathcal{A}$, a trivial way to compose a word of rank r for $\mathcal{A}'$ is as follows. We use w to merge the states of Q_0 to one particular state, then use the letter c to shift the set at play and continue until every set Q_i is merged into one state. The resulting word $w' = wcw \ldots cw$ thus has length $\mathrm{rt}(\mathcal{A}) \cdot r + r - 1$. Moreover, w' is the shortest word of rank r. Indeed, since all the transitions in the sets $Q_1, Q_2, \ldots, Q_{r-1}$ are self-loops for a, b, the only place where merging of states takes place is inside Q_0. While states of some Q_i are treated there, the states of all $Q_j, j \neq i$, remain invariant. Obviously, c has to be applied at least $r - 1$ times. Hence, by the pigeonhole principle, the existence of a shorter word of minimum rank would imply that an automaton induced by the action of $\{a, b\}$ on Q_0 can be synchronized faster than in $\mathrm{rt}(\mathcal{A})$ steps.

If we apply the construction to the Černý automaton $\mathcal{C}_{\frac{n}{r}}$, we get the following.

Proposition 1. *For every n and every $r > 1$ such that r divides n, there exists a ternary strongly connected automaton with n states and rank r such that the length of its shortest word of minimum rank is $\frac{(n-r)^2}{r} + r - 1$.*

It is natural to ask for a lower bound on the minimum rank threshold for binary automata. There are some techniques known to decrease the alphabet size of an automaton while not changing the length of a shortest synchronizing word significantly. By carefully applying the construction encoding letters in states [4, 21] one can get a lower bound of $\frac{n^2}{3r} - \frac{7}{3}n + 5r$ for the binary case. Another technique decreasing alphabet size, namely by encoding binary representation of letters in states [4, Lemma 3], does not yield any better bounds. Below we present some different ideas providing stronger lower bounds on $\mathrm{mrt}(\mathcal{A})$ in the class of binary strongly connected automata.

3.2 Lower bounds for binary automata

In the ternary construction above we may represent the actions of words ac and bc by two new letters, and afterwards remove the original letters a, b, c. This yields a binary automaton of rank r. More generally, we can do this on the analogous construction from an automaton with alphabet size k to size $k+1$, obtaining again an automaton with alphabet size k and having rank r.

The detailed construction goes as follows. Given a strongly connected synchronizing automaton $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ over any alphabet Σ and with state set $Q = \{q_1, \ldots, q_t\}$, we define the automaton $\mathcal{A}' = \langle Q', \Sigma, \delta' \rangle$ over the same alphabet as follows. As in the ternary construction, the state set is $Q' = \bigcup_{i=0}^{r-1} Q_i$ where each Q_i contains t states $q_{i,1}, \ldots, q_{i,t}$. The transitions from Q_0 to Q_1 imitate the transitions of $\mathcal{A}$: for every letter $a \in \Sigma$ we set $\delta'(q_{0,j}, a) = q_{1,k}$ if and only if $\delta(q_j, a) = q_k$. For the states in Q_i with $i \neq 0$ we define the transitions by just shifting a state to the state with the same index in the next set: for every $a \in \Sigma$ we set $\delta'(q_{i,j}, a) = q_{i+1,j}$, with the index $i+1$ taken modulo p.

Observe that the action of the set of words Σ^r on the set Q_i in $\mathcal{A}'$ induces the automaton $\mathcal{A}$ (up to duplicating its letters). Moreover, the words of length $r-1$ only shift the states of the set Q_1 to Q_0. Thus, any word synchronizing Q_1 is of length at least $\mathrm{rt}(\mathcal{A}) \cdot r$ over the initial alphabet. Clearly, this automaton has rank r, and its period is also r because $\mathcal{A}$ is synchronizing and thus primitive. We obtain the following result.

Proposition 2. *For every t-state strongly connected synchronizing automaton $\mathcal{A}$ and for every r there exists a tr-state strongly connected automaton $\mathcal{A}'$ over the same alphabet, with period and rank equal to r, such that* $\mathrm{mrt}(\mathcal{A}') = \mathrm{rt}(\mathcal{A}) \cdot r$.

Observe that the construction described preserves the property of the automaton to be strongly connected, circular or Eulerian. Applied to the Černý automaton this construction yields the following result.

Corollary 1. *For every n and every r such that r divides n, there exists an n-state circular binary automaton of period and rank r with minimum rank threshold $\frac{(n-r)^2}{r}$.*

The *Wielandt digraph* W_n has $n > 1$ vertices $0, \ldots, n-1$. From each vertex $i > 0$ there are two edges to the next vertex $i+1$ modulo n, and from vertex 0

there are single edges to vertices 1 and 2. Introduced in [22], and studied in connection to synchronizing automata in [2], these digraphs have the interesting property that they admit only one coloring, when automata obtained by renaming letters are considered identical. The reset threshold of this n-state Wielandt automaton was proved in [2] to be $n^2 - 3n + 3$.

The Hybrid Černý-Road Coloring problem (see [2], [7]) asks for the shortest length of a synchronizing word among all colorings of a fixed primitive digraph with n vertices. Since W_n has only one coloring, it provides the lower bound $n^2 - 3n + 3$ on this quantity. We can apply the binary construction of this section on the Wielandt automaton. The resulting automaton of rank r also admits only one coloring. Hence we get the following result in the spirit of the Hybrid Černý-Road Coloring problem, generalizing it to cases $r > 1$.

Corollary 2. *For every $n > 1$ and every r such that r divides n, there exists an n-vertex strongly connected digraph D of constant outdegree 2 such that all colorings of D are circular, have the same period and rank r, and for every coloring the length of a word of minimum rank is $\frac{(n-r)^2}{r} - n + 2r$.*

It is interesting to note that the digraphs D in Corollary 2 are the digraphs with the largest possible index, described in Theorem 4.3 of [13], after duplicating some edges to make all outdegrees equal to 2. Recall that the *index* of a strongly connected digraph with period r is the smallest k such that any pair of vertices are connected by a directed path of length k if and only if they are connected by a path of length $k + r$. In fact, one can easily show the following relationship (proof omitted), which also appears in [12] for the primitive case $r = 1$.

Proposition 3. *For a strongly connected n-state automaton $\mathcal{A}$ of rank r and period r the following holds:*

$$\mathrm{mrt}(\mathcal{A}) \geq k(\mathcal{A}) - n + r,$$

where $k(\mathcal{A})$ is the index of the underlying digraph of $\mathcal{A}$.

Since the index of D in Corollary 2 was proved in [13] to be $\frac{(n-r)^2}{r} + r$, we get from Proposition 3 the same lower bound as in Corollary 2.

We finish this section with a family of strongly connected binary automata that reach the same minimum rank threshold as the ternary automata in Proposition 1. Recall the n-state Černý automaton from Section 1. Let r be a number that divides n. Change in the Černý automaton the transition from state 1 by letter a to go into state $r + 1$ instead of state 2. After this change, for any states i and j such that $i \equiv j$ modulo r, also $\delta(i, x) \equiv \delta(j, x)$ modulo r holds for both $x = a$ and $x = b$. This means that states in different residue classes modulo r cannot be merged, so that the rank of this automaton is at least r. Using the trick from [2], we introduce a new input letter c that acts as the word ab does. Now letters c and b define exactly the modified Wielandt automaton leading to Corollary 2 above, so there is a word of rank r with letters c and b. Hence our automaton has rank r as well.

Since the action of word aa is the same as the action of a, a shortest minimum rank word w cannot contain factor aa. The word wb has also minimum rank, and it can be factored into ab's and b's. Viewing this as a word over letters c and b, we see that the number of c's and b's must be at least the minimum rank threshold $\frac{(n-r)^2}{r} - n + 2r$ from Corollary 2. Since b is a permutation and since c merges at most one pair of states, there must be at least $n - r$ letters c used. Each c counts as two letters over the alphabet $\{a, b\}$, so the length of word wb is at least

$$\frac{(n-r)^2}{r} - n + 2r + (n-r) = \frac{(n-r)^2}{r} + r.$$

Removing the last b from wb we obtain the following lower bound. Observe that the bound is exactly the same as in the ternary case in Proposition 1.

Proposition 4. *For every n and every $r > 1$ such that r divides n, there exists a binary n-state circular automaton $\mathcal{A}$ of rank r having* $\mathrm{mrt}(\mathcal{A}) = \frac{(n-r)^2}{r} + r - 1$.

3.3 Upper bound in the case when the rank equals the period

Obviously, the period of an automaton is a lower bound on its rank. It is interesting to consider the special case of automata where these two values are equal. For lower bounds, observe that the rank r automata reported in Corollaries 1 and 2 have the same period as the rank. In this section we obtain upper bounds on the minimum rank threshold from any known upper bounds on the reset threshold, in the case that the rank equals the period.

For every n, let $f(n)$ denote the maximum of reset thresholds of n-state synchronizing automata.

Theorem 1. *Let $\mathcal{A}$ be an automaton of rank r and period r. Then* $\mathrm{mrt}(\mathcal{A}) \leq r^2 \cdot f(\frac{n}{r}) + (r-1)$.

Proof. Let $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$. By Lemma 1 there exists a partition of the set Q into the sets $Q_0, \ldots, Q_{r-1}$ such that every transition maps a state in Q_i to a state in Q_{i+1} (with the index $i+1$ taken modulo r). Since the rank of $\mathcal{A}$ equals its period, each of the sets $Q_0, \ldots, Q_{r-1}$ is synchronizable (a set is called *synchronizable* if there is a word mapping this set to a single state). Assume without loss of generality that Q_0 is the smallest set in the partition. Consider then the automaton $\mathcal{A}^r = \langle Q_0, \Sigma^r, \delta' \rangle$ induced by the actions of all the words of length r on Q_0. This automaton is synchronizing, and by our assumption there is a word synchronizing it of length at most $f(|Q_0|) \leq f(\frac{n}{r})$ over the alphabet Σ^r. Over the alphabet Σ this word has length at most $r \cdot f(\frac{n}{r})$. Then to find a word of minimum rank it is enough to subsequently map each set $Q_1, \ldots, Q_{r-1}$ to Q_0 and apply the described word. In total we get a word of minimum rank of length at most $r^2 \cdot f(\frac{n}{r}) + (r-1)$. □

For example, using the unconditional upper bound $f(n) \leq \frac{n^3-n}{6}$ on the reset threshold [17] we get that for every n-state automaton of rank r and period r

we have $\mathrm{mrt}(\mathcal{A}) \leq \frac{n(n^2-r^2)}{6r} + (r-1)$, which is roughly r times stronger than the best known upper bound for the general case [16]. The Černý Conjecture implies the upper bound of $(n-r)^2 + (r-1)$. Thus, in the case of automata with rank equal to period the Rank Conjecture is implied by the Černý Conjecture up to an additive factor of $(r-1)$. However we conjecture that in this case the upper bound can be improved to $\frac{(n-r)^2}{r} + O(n)$.

4 Eulerian automata

4.1 The Rank Conjecture

We continue our discussion on the Rank Conjecture proving it for a particular class of automata, namely the Eulerian automata. Eulerian automata have been widely studied, in particular, Kari [15] showed that $\mathrm{rt}(\mathcal{A}) \leq (n-1)(n-2) + 1$ for any synchronizing Eulerian n-state automaton, thus proving the Černý Conjecture for this class of automata. We extend the mentioned result to the case of arbitrary minimum rank.

Theorem 2. *Let $\mathcal{A}$ be an n-state Eulerian automaton of rank r. Then $\mathcal{A}$ has a word of rank r of length at most $(n-r-1)(n-r)+1$.*

Proof. Let $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$. Following [15], we consider the set Q, $|Q| = n$, of states as an orthonormal basis of $\mathbb{R}^n$ with subsets of states corresponding to the sums of the basis vectors. Thus, a set $S \subseteq Q$ is viewed as a vector $\sum_{q \in S} q$.

Every word $w \in \Sigma^*$ defines a state transition function $f_w : Q \to Q$ on the set of states, with $f_w(q) = \delta(q, w)$. Furthermore, $f_w^{-1}(q) = \{v \mid f_w(v) = q\}$. Since we know the values of f_w^{-1} on all the basis vectors, there is a unique way to extend it to a linear mapping $f_w^{-1} : \mathbb{R}^n \to \mathbb{R}^n$. Clearly, for a set $S \subseteq Q$ we have $f_w^{-1}(S) = \sum_{q \in S} f_w^{-1}(q)$. Moreover, for a vector $x = (x_1, \ldots, x_n)$ we define a linear *weight* function $|x|$ such that $|(x_1, \ldots, x_n)| = x_1 + \ldots + x_n$. The weight of a set $S \subseteq Q$ is just its cardinality.

Let $Z_1 \subseteq \mathbb{R}^n$ be the set of all *non-extendable* vectors, i.e. such vectors x that there exists no word w with $|f_w^{-1}(x)| \neq |x|$ (all the remaining vectors we call *extendable*). Observe that $\sum_{w \in \Sigma^k} |f_w^{-1}(S)| = |\Sigma|^k \cdot |S|$. Thus, if there exists a word w of length k such that $|f_w^{-1}(S)| \neq |S|$ then there is a word of the same length extending S (a word v is said to *extend* S if $|f_v^{-1}(S)| > |S|$). We will refer to that as the *averaging argument*.

Note that Z_1 is a linear subspace of $\mathbb{R}^n$ of dimension at least r. First we prove that it is a linear subspace. Indeed, consider a linear combination $\lambda_1 v_1 + \ldots + \lambda_k v_k$ of vectors from Z_1. Since the weight function is linear, any image of this combination under f_w^{-1} has the same weight, and thus the combination belongs to Z_1. To bound the dimension of Z_1 from below, consider a word w of minimum rank such that there exists a partition of Q into sets $S_1, \ldots, S_r$, such that each S_i is a maximal synchronizable set. Such a word exists by Proposition 1 of [15]. The vectors corresponding to $S_1, \ldots, S_r$ are then non-extendable,and linearly independent since they have disjoint non-zero coefficients in the standard basis decomposition. We apply some linear algebra to obtain the following lemma.

Lemma 2. *For every extendable vector x there exists a word w of length at most $n-r$ such that $|f_w^{-1}(x)| \neq |x|$.*

Proof. Suppose the contrary: let x be extendable such that that shortest word w such that $|f_w^{-1}(x)| \neq |x|$ has length $m > n-r$. Note that for any words u, v we have $f_{uv}^{-1}(x) = f_u^{-1}(f_v^{-1}(x))$. Take Z_0 to be the orthogonal complement of Z_1. Since the dimension of Z_1 is at least r, the dimension of Z_0 is at most $n-r$. For every $i \leq m$ we denote $x_i = f_{w_i}^{-1}(x)$ where w_i is the suffix of w of length i, and we write $x_i = x_i^{(0)} + x_i^{(1)}$ for $x_i^{(0)} \in Z_0$ and $x_i^{(1)} \in Z_1$. Since m is greater than the dimension of Z_0, vectors $x_0^{(0)}, x_1^{(0)}, \ldots, x_{m-1}^{(0)}$ are linearly dependent. This means that for some $k < m$ the vector $x_k^{(0)}$ is a linear combination $\lambda_0 x_0^{(0)} + \cdots + \lambda_{k-1} x_{k-1}^{(0)}$ of vectors before it, with coefficients $\lambda_i \in \mathbb{R}$. The corresponding linear combination of vectors x_i is $\lambda_0 x_0 + \cdots + \lambda_{k-1} x_{k-1} = x_k + x'$ for some $x' \in Z_1$. Let $w = uv$ where v is the suffix of w of length k. Then, $f_u^{-1}(x_k) = f_u^{-1}(f_v^{-1}(x)) = f_w^{-1}(x)$. Moreover, for every $i < k$ we have $|f_u^{-1}(x_i)| = |x_i|$. Indeed, $f_u^{-1}(x_i) = f_u^{-1}(f_{w_i}^{-1}(x)) = f_{uw_i}^{-1}(x)$ has the same weight as x because uw_i is shorter than w, and of course $|x_i| = |x|$. Also, because x' is non-extendable, we have $|f_u^{-1}(x')| = |x'|$. Putting all together, using linearity of f_u^{-1} and the weight function, we obtain $|f_w^{-1}(x)| = |x|$, a contradiction. □

By the averaging argument we obtain from Lemma 2 that for any extendable set S of states there is a word w of length at most $n-r$ such that $|f_w^{-1}(S)| \geq |S| + 1$. Now we apply this extension procedure as follows. Start with a one-state set. Extend it step by step to a maximal synchronizable set (having size $\frac{n}{r}$). Then add another state to this maximal synchronizable set and extend this new set to a union of two disjoint maximal synchronizable sets. Repeat this procedure of adding a new state and extending the set to a union of several maximal synchronizable sets until the whole set of states of the automaton is reached. The extension is possible, since at every step the set S that we have to extend is a disjoint union of several maximal synchronizable subsets and a non-maximal synchronizable subset S'. Any word extending S' extends S, since f_w^{-1} preserves the weights of all the maximal synchronizable subsets for any word w (since otherwise by the averaging argument such sets are extendable).

For each step of this algorithm, we have a word of length at most $n-r$ to extend a set by one element. Each maximal synchronizable set has size $\frac{n}{r}$, and we have to reach r such sets, so the total length of the word is at most $(n-r)(\frac{n}{r}-1)r = (n-r)^2$. We can initially choose a one-state set extendable by a word of length 1, which improves the bound to $(n-r)(n-r-1)+1$. □

To obtain a lower bound on the minimum rank threshold of Eulerian automata, recall the construction used to prove the bound of Proposition 1. It was mentioned previously that applying it to an Eulerian automaton yields another Eulerian automaton. Thus, we repeat the same reasoning starting with a synchronizing n-state Eulerian automaton over alphabet of size 4 having reset threshold $\frac{n^2-3}{2}$, for any $n > 1$ such that $n \equiv 1 \pmod 4$, see [19].

Proposition 5. *For every n and every $r < n$ such that $n = (4p+1)r$, there exists an n-state Eulerian automaton $\mathcal{A}$ of rank r with* $\mathrm{mrt}(\mathcal{A}) = \frac{n^2-r^2}{2r} - 1$.

The standard binarization methods cannot be applied to provide the lower bounds for binary Eulerian automata. However, we can apply the argument of Proposition 2 to the n-state binary Eulerian automaton whose reset threshold is at least $\frac{n^2-3n+4}{2}$ for odd $n \geq 3$ [12]. (This was proved for all odd $n \geq 5$ in [12] but the same construction also covers the case $n = 3$.) The automaton we obtain is also Eulerian.

Proposition 6. *For every n and every r such that r divides n and $n/r \geq 3$ is odd, there exists an n-state binary Eulerian automaton $\mathcal{A}$ of rank r having* $\mathrm{mrt}(\mathcal{A}) \geq \frac{(n-2r)^2+nr}{2r}$.

The multiplicative gap between the lower and the upper bounds consists intuitively of two parts. The factor of two comes from the gap between the known bounds on the reset threshold of Eulerian automata, while the factor r comes from the gap on the minimum rank threshold in general strongly connected automata that we see in the results in Section 3.

4.2 A corollary for circular automata

In this section we provide a simple trick, similar to the idea of [6], which allows to transfer the results on Eulerian automata to the class of circular automata. Recall that an automaton is called circular if there is a letter which acts on its set of states as a cyclic permutation. The Černý Conjecture for this automata class was proved by Dubuc [11]. Note that the Černý automata are circular and possess the largest known reset thresholds.

Let us consider an n-state circular automaton $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ such that some letter $b \in \Sigma$ acts as a cyclic permutation on Q. Let us replace each $a \in \Sigma$ by n letters $a_0, \ldots, a_{n-1}$, where a_i acts on Q the same way as the word ab^i does in the original automaton. Let Σ' be the obtained new alphabet of size $n \cdot |\Sigma|$. It is not hard to prove that the obtained automaton is Eulerian (we omit the proof because of the space constraints).

Observe that this transformation preserves the synchronization properties of the initial automaton in the following sense. A word of rank r over Σ is clearly a word of rank r over Σ' because $\Sigma \subset \Sigma'$. The opposite holds as well since every word over Σ' can be rewritten as a word over Σ. It follows that the rank of the resulting automaton is equal to the rank of the initial one.

Theorem 3. *Every n-state circular automaton of rank $r < n$ has a minimum rank word of length at most* $(2n - r - 1)(n - r - 1) + 1$.

Proof. Let $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ be an n-state circular automaton with a cyclic permutation letter b. An Eulerian automaton $\mathcal{A}' = \langle Q, \Sigma', \delta' \rangle$ with n states is constructed as above. Now we show how to use the procedure described in Theorem 2 to get the upper bound.

According to the proof of Theorem 2, for every $s \in \mathbb{R}^n$ there exists a unique representation $s = s_0 + s_1$ where $s_0 \in Z_0$ and $s_1 \in Z_1$. Furthermore, $|f_w^{-1}(s)| \neq |s|$ is equivalent to $|f_w^{-1}(s_0)| \neq |s_0|$.

Observe that any word in Σ' can be written as a concatenation of words over Σ. Thus we can apply Lemma 3 of [15] on the linear transformations f_a^{-1}, for $a \in \Sigma$, in the automaton $\mathcal{A}'$, and get that the shortest word $w \in \Sigma^*$ such that $|f_w^{-1}(s_0)| \neq |s_0|$ has length at most $n - r$. Consequently, w is the shortest word over Σ such that $|f_w^{-1}(s)| \neq |s|$.

Let $w = cv$ where $c \in \Sigma$ and $v \in \Sigma^*$. Now consider all the words of the form σv with $\sigma \in \Sigma'$. Clearly, w is one of them. Because $\mathcal{A}'$ is Eulerian, we have

$$\sum_{\sigma \in \Sigma'} |f_{\sigma v}^{-1}(x)| = \sum_{\sigma \in \Sigma'} |f_\sigma^{-1}(f_v^{-1}(x))| = |\Sigma'| \cdot |f_v^{-1}(x)| = |\Sigma'| \cdot |x|.$$

Since there exists a word $w = cv$ such that $|f_w^{-1}(x)| \neq |x|$, the above equality implies that there is $u = \sigma v$ such that $|f_u^{-1}(x)| > |x|$. Notice that v is a word of length at most $n-r-1$ over Σ, and hence u is of length $|\sigma|+|v| \leq n+(n-r-1) = 2n - r - 1$ over Σ.

Thus we showed that every extendable set of states in $\mathcal{A}'$ can be extended by a word of length at most $2n - r - 1$ (over the alphabet Σ). We can now use the extension procedure described in Theorem 2 (starting from a one-state set extendable by a word of length 1) and get the upper bound of $(2n - r - 1)(n - r - 1) + 1$ on the length of a shortest word of minimum rank in $\mathcal{A}$. □

4.3 A road coloring algorithm

As proved by Kari [15], every primitive strongly connected Eulerian digraph such that all its vertices have equal outdegrees has a synchronizing coloring. If the primitiveness condition is omitted, the period of a digraph is the lower bound on the rank of any coloring. A coloring of rank equal to period always exists and can be found in quadratic time [3]. We show that for Eulerian digraphs it can be found in almost linear time. We use the approach described in Section 3 of [15] and show how to generalize it and turn into an algorithm.

First observe that a permutation coloring (a coloring of rank n) of an Eulerian digraph with n vertices and constant outdegree k corresponds to a partition of a regular bipartite graph with n vertices and kn edges into k perfect matchings (Lemma 1 of [15]), and thus can be computed in $O(kn \log k)$ time [10].

The construction of a permutation coloring is used as a subroutine in order to construct a coloring with a stable pair of states. A pair of states p, q of an automaton is called *stable* if application of any word to this pair results in a synchronizable pair. For a permutation coloring $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ of a digraph take a state $x \in Q$ such that $y = \delta(x, a) \neq \delta(x, b) = z$ for some letters $a, b \in \Sigma$. Note that in a strongly connected digraph such state always exists, otherwise the digraph consists of one cycle and we have nothing to prove. We swap the letters coloring the edges $x \to y$ and $x \to z$. As proved in Theorem 1 of [15], the pair y, z is then stable in the resulting automaton $\mathcal{A}'$ and thus defines a congruence

relation (that is, an equivalence relation invariant under application of any word) $\equiv$ on its state set. The quotient automaton $\mathcal{A}'/\equiv$ is then obtained by merging all the states of each congruence class. If $\mathcal{A}'$ is Eulerian, so is $\mathcal{A}'/\equiv$ [15].

Lemma 3. *Let $\mathcal{A}'$ be the Eulerian automaton, and y, z be the stable pair with corresponding congruence relation $\equiv$ obtained as described above. Then the quotient automaton $\mathcal{A}'/\equiv$ has at most half as many states as $\mathcal{A}'$.*

Proof. We compute $\mathcal{A}'/\equiv$ following the Merge procedure described in [3]. We start by merging the congruent pair y, z and then propagate this equivalence to the images of y, z under all the letters in Σ until we get a deterministic automaton. Observe that since we start with a permutation coloring, each state that has not yet been merged with some other state has all incoming edges of different colors. Thus, if there is such a state in the pair to be merged, the second state in this pair is different from it, and thus further calls of merging their successor will be performed. Moreover, assume that some state is not merged with any state during this procedure. Then there is such a state p having a transition going to it from some already merged state q, otherwise the digraph is not strongly connected. This means that during the first merging for q, merging for p has to be called, which is a contradiction. Hence, each state is in a congruence class of cardinality at least 2, and after taking the quotient, the number of states of $\mathcal{A}'/\equiv$ is at most half of the number of states $\mathcal{A}'$. □

Theorem 4. *Given a strongly connected Eulerian digraph of period r with n vertices and outdegree k, a coloring of rank r of this digraph can be found in $O((k \log k + \alpha(n)) \cdot n)$ time, where $\alpha(\cdot)$ is the inverse Ackermann function.*

Proof. The algorithm is recursive. At each iteration we start by finding a coloring with a stable pair as described above. Then we proceed by computing the quotient automaton as in Lemma 3. The automaton we obtain is Eulerian [15], moreover, it has the same period since no pair of states from different sets in a p-partition can be stable (since no such pair can be synchronized). If the automaton has rank r, we stop, otherwise we call the same algorithm for coloring it and then recover the final coloring by taking for every vertex the same permutation of the colors of outgoing edges as used for the equivalence class of this vertex (see Theorem 1 of [15]).

To analyze the time complexity, we estimate the complexity of one recursion step. Let ℓ be the size of the automaton at some iteration. As it was mentioned before, it takes $O(k\ell \log k)$ time to find a permutation coloring. The Merge procedure requires $O(k\ell)$ time for traversing and $O(\ell\alpha(\ell))$ time for merging the sets. Moreover, recovering the coloring from the smaller automaton can be done in $O(k\ell)$ time by storing the quotient automaton (together with the correspondence between the states and their equivalence classes) at each iteration. Hence, the time complexity of one iteration is $O(\ell(k \log k + \alpha(\ell)))$.

Now we can sum up the time complexity of all recursion steps. Lemma 3 implies that the number of states of each next automaton in the recursion call is decreased at least twice. Thus, the total time complexity is $O(n(k \log k + \alpha(n)))$, where n is the number of vertices of the initial digraph. □

References

1. Almeida, J., Steinberg, B.: Matrix mortality and the Černý-Pin conjecture. In: Diekert, V., Nowotka, D. (eds.) DLT 2009. LNCS, vol. 5583, pp. 67–80. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
2. Ananichev, D., Gusev, V., Volkov, M.: Slowly synchronizing automata and digraphs. In: Hliněný, P., Kučera, A. (eds.) Mathematical Foundations of Computer Science 2010, pp. 55–65. Springer Berlin Heidelberg (2010)
3. Béal, M., Perrin, D.: A quadratic algorithm for road coloring. Discrete Applied Mathematics 169, 15–29 (2014), https://doi.org/10.1016/j.dam.2013.12.002
4. Berlinkov, M.V.: On two algorithmic problems about synchronizing automata. In: Shur, A.M., Volkov, M.V. (eds.) DLT 2014. LNCS, vol. 8633, pp. 61–67. Springer, Cham (2014)
5. Berman, A., Plemmons, R.: Nonnegative Matrices in the Mathematical Sciences. Classics in Applied Mathematics, Society for Industrial and Applied Mathematics (1994)
6. Carpi, A., D'Alessandro, F.: Strongly transitive automata and the černý conjecture. Acta Informatica 46(8), 591–607 (2009)
7. Carpi, A., D'Alessandro, F.: On the Hybrid Černý-Road Coloring Problem and Hamiltonian paths. In: Gao, Y., Lu, H., Seki, S., Yu, S. (eds.) DLT 2010. LNCS, vol. 6224, pp. 124–135. Springer Berlin Heidelberg (2010)
8. Černý, J., Pirická, A., Rosenauerova, B.: On directable automata. Kybernetika 7(4), 289–298 (1971)
9. Černý, J.: Pozńamka k homoǵennym eksperimentom s konečńymi automatami. Matematicko-fyzikalny Casopis Slovensk. Akad. Vied 14(3) (1964)
10. Cole, R., Ost, K., Schirra, S.: Edge-coloring bipartite multigraphs in $O(E \log D)$ time. Combinatorica 21(1), 5–12 (2001)
11. Dubuc, L.: Sur les automates circulaires et la conjecture de černý. RAIRO – Theoretical Informatics and Applications 32(1-3), 21–34 (1998)
12. Gusev, V.V.: Lower bounds for the length of reset words in eulerian automata. International Journal of Foundations of Computer Science 24(2), 251–262 (2013), https://doi.org/10.1142/S0129054113400108
13. Heap, B.R., Lynn, M.S.: The structure of powers of nonnegative matrices: I. the index of convergence. SIAM Journal on Applied Mathematics 14(3), 610–639 (1966)
14. Kari, J.: A counter example to a conjecture concerning synchronizing words in finite automata. Bulletin of the EATCS 73, 146 (2001)
15. Kari, J.: Synchronizing finite automata on Eulerian digraphs. Theoretical Computer Science 295(1), 223–232 (2003)
16. Klyachko, A.A., Rystsov, I.K., Spivak, M.A.: In extremal combinatorial problem associated with the bound on the length of a synchronizing word in an automaton. Cybernetics 23(2), 165–171 (1987)
17. Pin, J.: On two combinatorial problems arising from automata theory. In: Berge, C., Bresson, D., Camion, P., Maurras, J., Sterboul, F. (eds.) Combinatorial Mathematics, North-Holland Mathematics Studies, vol. 75, pp. 535–548. North-Holland (1983)
18. Pin, J.E.: Le problème de la synchronisation et la conjecture de Cerný. In: Luca, A.D. (ed.) Non-commutative structures in algebra and geometric combinatorics vol. 109, pp. 37–48. Quaderni de la Ricerca Scientifica, CNR (Consiglio nazionale delle ricerche, Italy) (1981)

19. Szykuła, M., Vorel, V.: An extremal series of Eulerian synchronizing automata. In: Brlek, S., Reutenauer, C. (eds.) DLT 2016. LNCS, vol. 9840. pp. 380–392. Springer Berlin Heidelberg (2016)
20. Volkov, M.V.: Synchronizing automata and the Černý conjecture. In: Martín-Vide, C., Otto, F., Fernau, H. (eds.) LATA 2008. LNCS, vol. 5196, pp. 11–27. Springer, Heidelberg (2008)
21. Vorel, V.: Subset synchronization and careful synchronization of binary finite automata. International Journal of Foundations of Computer Science 27(5), 557–577 (2016), https://doi.org/10.1142/S0129054116500167
22. Wielandt, H.: Unzerlegbare, nicht negative matrizen. Mathematische Zeitschrift 52(1), 642–648 (1950)