An Extremal Series of Eulerian Synchronizing Automata

Marek Szykuła[1(✉)] and Vojtěch Vorel[2(✉)]

[1] Institute of Computer Science, University of Wrocław,
Joliot-Curie 15, Wrocław, Poland
`msz@cs.uni.wroc.pl`
[2] Faculty of Mathematics and Physics, Charles University,
Malostranské nám. 25, Prague, Czech Republic
`vorel@ktiml.mff.cuni.cz`

Abstract. We present an infinite series of n-state Eulerian automata whose reset words have length at least $(n^2 - 3)/2$. This improves the current lower bound on the length of shortest reset words in Eulerian automata. We conjecture that $(n^2 - 3)/2$ also forms an upper bound for this class and we experimentally verify it for small automata by an exhaustive computation.

Keywords: Eulerian automaton · Reset threshold · Reset word · Synchronizing automaton

1 Introduction

A complete deterministic finite automaton is *synchronizing* if there exists a word whose action maps all states to a single one. Such words are called *reset words*. Synchronizing automata find applications in various fields such as robotics, coding theory, bioinformatics, and model-based testing. Besides of these, synchronizing automata are of great theoretical interest, mainly because of the famous Černý conjecture [9], which is one of the most long-standing open problems in automata theory. The conjecture states that each synchronizing n-state automaton has a reset word of length at most $(n-1)^2$. The best known general upper bound on this length is $\frac{1}{6}n^3 - \frac{1}{6}n - 1$ for each $n \geq 4$ [21]. Surveys on the field can be found in [16,26].

Major research directions in this field include proving the Černý conjecture for special classes of automata or showing specific upper bounds for them. For example, the Černý conjecture has been positively solved for the classes of monotonic automata [11], circular automata [10], Eulerian automata [15], aperiodic automata [25], one-cluster automata with a prime-length cycle [24],

automata respecting intervals of a directed graph [12] (under an inductive assumption), and automata with a letter of rank at most $\sqrt[3]{6n-6}$ [6]. Moreover, there are many improvements of upper bounds for important special classes, for example, generalized and weakly monotonic automata [2,27], one-cluster automata [4], quasi-Eulerian and quasi-one-cluster automata [5], and decoders of finite prefix codes [2,6,7]. On the other hand, several lower bounds have been established by showing extremal series of automata for particular classes [2,7,9,13]. Still, for many classes the best known upper bound does not match the lower bound.

In this paper we deal with the class of Eulerian automata, which is one of the most remarkable classes due to its properties with regard to synchronization. In particular, the lengths of shortest words extending subsets are at most $n-1$ for each n-state Eulerian automaton [15], whereas they can be quadratic in general [19]. An upper bound $(n-1)(n-2)+1$ on the length of the shortest reset words for Eulerian automata was obtained by Kari [15]. Several generalizations of Eulerian automata were proposed: the class of pseudo-Eulerian automata [23], for which the same bound $(n-1)(n-2)+1$ was obtained, unambiguous Eulerian automata [8] for which the Černý bound $(n-1)^2$ was obtained, and quasi-Eulerian automata [5], for which a quadratic upper bound was obtained. The best lower bound so far was $\frac{1}{2}n^2 - \frac{3}{2}n + 2$, found by Gusev [13]. A series whose shortest reset words seem to have length $\frac{1}{2}n^2 - \frac{5}{2}$ was found by Martyugin (unpublished), but no proof has been established. Further discussion on the bounds for Eulerian automata can be found in the survey [16].

Here we improve the lower bound by introducing an extremal series of Eulerian automata over a quaternary alphabet with the shortest reset words of length $\frac{1}{2}n^2 - \frac{3}{2}$. To prove that, we use a technique of *backward tracing*, which turns out to be very useful in analysis of extremal series of automata in general. We conjecture that the new lower bound is tight for the class of Eulerian automata. Our exhaustive search over small automata did not find any counterexample.

The new series exhibits the extremal property that some of its subsets require extending words of length exactly $n-1$. This matches the upper bound, which was used in [15] to obtain the best known upper bound $(n-1)(n-2)+1$ on the length of shortest reset words. Thus, possible improvements of the upper bound require a more subtle method.

2   Preliminaries

A *deterministic finite automaton* (*DFA*) is a triple $\mathcal{A} = (Q, \Sigma, \delta)$, where Q is a finite non-empty set of *states*, Σ is a finite non-empty *alphabet*, and $\delta \colon Q \times \Sigma \mapsto Q$ is a complete *transition function*. We extend δ to $Q \times \Sigma^*$ and $2^Q \times \Sigma^*$ as usual. When $\mathcal{A}$ is fixed, we write shortly $q \cdot w$ and $S \cdot w$ for $\delta(q, w)$ and $\delta(S, w)$ respectively. The *preimage* of $S \subset Q$ by $w \in \Sigma^*$ is defined as

$$\delta^{-1}(S, w) = \{q \in Q \mid q \cdot w \in S\},$$

which is also denoted by $S \cdot w^{-1}$. If $S = \{q\}$ is a singleton, we write $q \cdot w^{-1}$.

A word $w \in \Sigma^*$ is a *reset word* if $|Q \cdot w| = 1$. Note that in this case $Q \cdot w = \{q_0\}$ and $\{q_0\} \cdot w^{-1} = Q$ for some $q_0 \in Q$. A DFA is called *synchronizing* if it admits a reset word. The *reset threshold* of a synchronizing DFA $\mathcal{A}$ is the length of the shortest reset words and is denoted by $\mathrm{rt}(\mathcal{A})$.

A word w *extends* a subset $S \subset Q$ if $|S \cdot w^{-1}| > |S|$. In this case we say that S is *w-extensible*.

A DFA $\mathcal{A}$ is *Eulerian* if the underlying digraph of $\mathcal{A}$ is strongly connected and the in-degree equals the out-degree for each vertex of the underlying digraph. Equivalently, at every vertex there must be exactly $|\Sigma|$ incoming edges.

We say that a word $w \in \Sigma^*$ is:

- *permutational* if $Q \cdot w = Q$,
- *involutory* if $q \cdot w^2 = q$ for each $q \in Q$,
- *unitary* if $p \cdot w \neq p$ holds for exactly one $p \in Q$.

Note that each involutory word is permutational. Also, w is unitary if and only if its action maps exactly one state to another one and fixes all the other states. For $p, r \in Q$, we write $w = (p \to r)$ if the action of $w \in \Sigma^*$ is defined as $p \cdot w = r$ and $q \cdot w = q$ for each $q \in Q \setminus \{p\}$.

The reversal of a word w is denoted by w^{R}.

Lemma 1. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a DFA. Let $w \in \Sigma^*$ contain only involutory letters. Then $S \cdot w^{-1} = S \cdot w^{\mathrm{R}}$ for each $S \subseteq Q$.*

Proof. If $|w| = 0$, the claim is trivial. Inductively, let $w = xv$ for $x \in \Sigma$. We have $S \cdot (xv)^{-1} = (S \cdot v^{-1}) \cdot x^{-1} = (S \cdot v^{\mathrm{R}}) \cdot x^{-1}$ by the inductive assumption, which is equal to $(S \cdot v^{\mathrm{R}}) \cdot x^{-1} \cdot x^2 = (S \cdot v^{\mathrm{R}}) \cdot x$ since x is involutory.   □

3   Backward Tracing

There exist several methods of proving reset thresholds of particular series of automata. Here we discuss one of them as a general approach, which we call *backward tracing*.

Definition 2. *Let $\mathcal{A}$ be a synchronizing DFA and let u be a reset word for $\mathcal{A}$ with $Q \cdot u = \{q_0\}$. We say that u is* straight *if*

$$q_0 \cdot (u_{\mathbf{m}} u_{\mathbf{s}})^{-1} \nsubseteq q_0 \cdot (u_{\mathbf{s}})^{-1}$$

for each $u_{\mathbf{p}}, u_{\mathbf{m}}, u_{\mathbf{s}} \in \Sigma^*$ with $u_{\mathbf{p}} u_{\mathbf{m}} u_{\mathbf{s}} = u$.

The following is a simple observation (cf. [17, Theorem 1]):

Proposition 3. *In a synchronizing DFA each shortest reset word is straight.*

The observation above leads to a method of proving reset thresholds of particular DFA series by analyzing subsets that are preimages of a singleton under the action of suffixes of length $i = 1, 2, \ldots, \mathrm{rt}(\mathcal{A})$ of straight reset words. This works well if the number of such subsets is small in every step, i.e., for each i. Note that in general it can grow exponentially.

Interestingly, all known series of most extremal automata, such as the Černý automata having reset threshold $(n-1)^2$ [9], the twelve known *slowly synchronizing series* having only slightly smaller reset thresholds [1,3,19], and DFAs with cycles of two different lengths [14], have the property that the number of possible subsets in each step is bounded by a constant. We call such series *backward tractable*. It is worth mentioning that for such automata we can compute shortest reset words in polynomial time [17].

In this paper, we apply this method to a new series of Eulerian automata, which is backward tractable as well, and whose construction is different from the other known extremal series; in particular, the letters act in many short cycles instead of few large ones.

The new DFAs use only permutational and unitary letters. This property (which also implies an upper bound $2(n-1)^2$ on the reset threshold [22]) allows us to strengthen the restriction on suffixes to be considered within the backward tracing:

Definition 4. *With respect to a fixed DFA $\mathcal{A}$, a reset word $u \in \Sigma^*$ with $Q \cdot u = \{q_0\}$ is* greedy, *if for each suffix v of u it holds that: if some $x \in \Sigma$ extends $q_0 \cdot v^{-1}$, then yv is a suffix of u for some $y \in \Sigma$ that extends $q_0 \cdot v^{-1}$.*

Lemma 5. *If a synchronizing DFA $\mathcal{A}$ has only permutational and unitary letters, then there exists a shortest reset word that is greedy.*

Proof. Let $\Sigma = \Sigma_{\mathrm{p}} \cup \Sigma_{\mathrm{u}}$, where Σ_{p} contains permutational letters and Σ_{u} contains unitary letters.

Suppose for a contradiction that there is no shortest reset word that is greedy. Let u be a shortest reset word of $\mathcal{A}$ with the property that its shortest suffix v violating the greediness is the longest possible. In other words, the shortest suffix yv of u, $y \in \Sigma$, such that some $x \in \Sigma$ extends $q_0 \cdot v^{-1}$ but y doesn't, is the longest possible.

For each suffix zt of u with $z = (p \rightarrow q) \in \Sigma_{\mathrm{u}}$, the set $S = q_0 \cdot t^{-1}$ is necessarily z-extensible. Indeed, if $q \in S$ and $p \notin S$, then S is clearly z-extensible. If $q \notin S$ or $p \in S$, then $S \cdot z^{-1} \subseteq S$, which contradicts Proposition 3. Since the inverse actions of the letters from Σ_{p} preserve sizes of subsets, it follows that u contains exactly $|Q| - 1$ occurrences of unitary letters.

Write $u = v'v$ and let $u' = v'xv$. Observe that u' is also a reset word for $\mathcal{A}$: $q_0 \cdot (xv)^{-1}$ is a (possibly proper) superset of $q_0 \cdot v^{-1}$; hence, we still have $q_0 \cdot (v'xv)^{-1} = Q$. Since u' contains $|Q|$ occurrences of letters from Σ_{u}, and letters from Σ_{p} do not decrease the size of a subset, at least one occurrence of $y \in \Sigma_{\mathrm{u}}$ is not applied to an y-extensible subset. Moreover, this occurrence lies within v', because v is the shortest suffix violating the greediness. Let v'' be the word obtained by removing that occurrence of y. We have $u'' = v''xv$, $|u''| = |u|$,

and the shortest suffix violating the greediness is longer than v. This yields a contradiction with the choice of u.   □

4   The Extremal Series of Eulerian Automata

Fix an arbitrary $m \geq 1$. Let $N = 4m + 1$ and $\mathcal{A}_m = \langle Q, \Sigma, \delta \rangle$, where $Q = \{0, 1, \ldots, N-1\}$, $\Sigma = \{\alpha, \beta, \omega_0, \omega_1\}$. The action of α and β is defined by

$$q \cdot \alpha = (-q - 1) \bmod N,$$
$$q \cdot \beta = (-q + 1) \bmod N,$$

for $q \in Q$, while the action of ω_0, ω_1 is defined by

$$\omega_0 = (1 \rightarrow 0),$$
$$\omega_1 = (0 \rightarrow 1).$$

The automaton $\mathcal{A}_m$ is illustrated in Fig. 1. We are going to prove that

$$\mathrm{rt}(\mathcal{A}_m) = \frac{N^2 - 3}{2}.$$

Throughout the proof we use usual operations and inequalities on integers. Each use of modular arithmetic is described explicitly using the binary operator "mod".
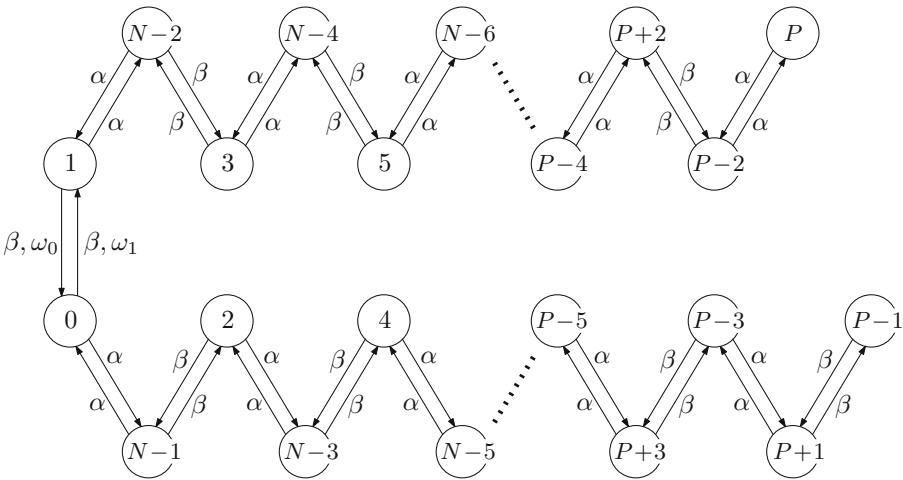

Fig. 1. The DFA $\mathcal{A}_m$, loops are omitted, $P = \frac{N+1}{2}$

We use backward tracing to show that there is a unique optimal way to extend a singleton to Q. Note that ω_0 and ω_1 are unitary, while α and β are

involutory. The following notation will be very useful in the analysis of reset words for $\mathcal{A}_m$:

For $j = 0, \ldots, N$ we set:

$$Q_j = \{q \mid 0 \leq q \leq j - 1\}, \qquad R_j = Q_j \cdot \beta,$$
$$Q_j^\diamond = Q_j \setminus \{0\} = \{q \mid 1 \leq q \leq j\}, \quad R_j^\diamond = R_j \setminus \{1\} = Q_j^\diamond \cdot \beta.$$

4.1 Construction of a Reset Word

For an odd $i \geq 1$, we define

$$t_i = \alpha \left(\beta\alpha\right)^{\frac{i-1}{2}}.$$

Note that:

1. $|t_i| = i$,
2. t_i is a palindrome (i.e., $t_i = t_i^{\mathrm{R}}$).

By Lemma 1, $S \cdot t_i = S \cdot t_i^{\mathrm{R}} = S \cdot t_i^{-1}$ for each $S \subseteq Q$, and we will often interchange t_i^{-1} with t_i. It follows that $qt_i^2 = qt_it_i^{-1} = q$ for every $q \in Q$ and t_i is involutory.

Lemma 6. *Let $q \in Q$. It holds that:*

1. $q \cdot (\beta\alpha)^h = (q - 2h) \bmod N$ *for each $h \geq 0$,*
2. $q \cdot t_i = (-q - i) \bmod N$ *for each $i \geq 1$.*

Proof. The first claim follows trivially from the case of $h = 1$. In this case we have $(q \cdot \beta) \cdot \alpha = (-(-q+1) - 1) \bmod N = (q - 2) \bmod N$. For the second claim we observe $k \cdot t_i = (k \cdot \alpha) \cdot (\beta\alpha)^{\frac{i-1}{2}}$, which equals $(-q - 1 - (i - 1)) \bmod N = (-q - i) \bmod N$. □

Lemma 7. *Let $2 \leq j \leq N - 2$. It holds that:*

1. $Q_j \cdot t_{N-j} = Q_{j+1}^\diamond$ *if j is even,*
2. $R_j \cdot t_{j-2} = R_{j+1}^\diamond$ *if j is odd,*
3. $Q_{j+1} \cdot t_{N-j} = Q_{j+1}$ *if j is even,*
4. $R_{j+1} \cdot t_{j-2} = R_{j+1}$ *if j is odd.*

Proof. For (1) and (2) we use Lemma 6(2) with $i = N - j$ and $i = j - 2$ respectively and then substitute $d = j - q$:

$$Q_j \cdot t_{N-j} = \{j - q \mid q \in Q_j\} = \{d \mid 1 \leq d \leq j\} = Q_{j+1}^\diamond,$$
$$R_j \cdot t_{j-2} = \{q \cdot \beta t_{j-2} \mid q \in Q_j\} = \{(-(-q+1) - (j-2)) \bmod N \mid q \in Q_j\}$$
$$= \{(q - j + 1) \bmod N \mid q \in Q_j\} = \{(-d + 1) \bmod N \mid 1 \leq d \leq j\}$$
$$= \{d \cdot \beta \mid 1 \leq d \leq j\} = R_{j+1}^\diamond.$$

For (3) and (4) we use (1) and (2) respectively and the fact that t_{N-j} and t_{j-2} are involutory. We have:

$$Q_{j+1} \cdot t_{N-j} = Q_{j+1}^\diamond \cdot t_{N-j} \cup \{0 \cdot t_{N-j}\} = Q_j \cup \{j\} = Q_{j+1},$$
$$R_{j+1} \cdot t_{j-2} = R_{j+1}^\diamond \cdot t_{j-2} \cup \{1 \cdot t_{j-2}\} = R_j \cup \{N - j + 1\}$$
$$= R_j \cup \{j \cdot \beta\} = R_{j+1}. \qquad □$$

Let

$$w = v_{N-1}\beta v_{N-2}\beta v_{N-3} \ldots \beta v_3 \beta v_2,$$

where

$$v_j = \begin{cases} \omega_1 t_{N-j} & \text{if } j \text{ is even,} \\ \omega_0 t_{j-2} & \text{if } j \text{ is odd.} \end{cases}$$

In Lemma 10 below, we show that w extends Q_2 to Q_N according to the following scheme:

$$Q_2 \overset{v_2^{-1}}{\mapsto} Q_3 \overset{\beta^{-1}}{\mapsto} R_3 \overset{v_3^{-1}}{\mapsto} R_4 \overset{\beta^{-1}}{\mapsto} Q_4 \overset{v_4^{-1}}{\mapsto} Q_5 \overset{\beta^{-1}}{\mapsto} R_5 \overset{v_5^{-1}}{\mapsto} R_6 \overset{\beta^{-1}}{\mapsto} Q_6 \mapsto \cdots$$

$$\cdots \mapsto Q_{N-3} \overset{v_{N-3}^{-1}}{\mapsto} Q_{N-2} \overset{\beta^{-1}}{\mapsto} R_{N-2} \overset{v_{N-2}^{-1}}{\mapsto} R_{N-1} \overset{\beta^{-1}}{\mapsto} Q_{N-1} \overset{v_{N-1}^{-1}}{\mapsto} Q_N,$$

and thus the word $w\omega_0$ is a reset word for $\mathcal{A}_m$.

Remark 8. The word w ends with α. The other occurrences of α in w are directly followed by β.

Remark 9. A set $S \subseteq Q$ is:

- ω_0-extensible if and only if $S \cap \{0,1\} = \{0\}$,
- ω_1-extensible if and only if $S \cap \{0,1\} = \{1\}$.

We say that a set $S \subseteq Q$ is ω-*extensible* if it is ω_0-extensible or ω_1-extensible.

Lemma 10. *Let $2 \leq j \leq N-1$. It holds that:*

1. $Q_2 \cdot (v_j \beta v_{j-1} \ldots \beta v_2)^{-1} = Q_{j+1}$ *if j is even,*
2. $Q_2 \cdot (v_j \beta v_{j-1} \ldots \beta v_2)^{-1} = R_{j+1}$ *if j is odd,*
3. $w\omega_0$ *is a reset word of $\mathcal{A}_m$.*

Proof. We prove the first two claims by induction. For $j = 2$, using Lemma 7(1) we have:

$$Q_2 \cdot v_2^{-1} = (Q_2 \cdot t_{N-2}^{-1}) \cdot \omega_1^{-1} = Q_3^\diamond \cdot \omega_1^{-1} = Q_3.$$

Next, take $j \geq 2$ and suppose that both the claims hold for $j-1$. We use the induction hypothesis and, depending on the parity of j, Lemma 7(1) or Lemma 7(2) respectively. For an even j we have:

$$Q_2 \cdot (v_j \beta v_{j-1} \ldots \beta v_2)^{-1} = R_j \cdot (v_j \beta)^{-1} = Q_j \cdot v_j^{-1} = Q_j \cdot (\omega_1 t_{N-j})^{-1}$$
$$= Q_{j+1}^\diamond \cdot \omega_1^{-1} = Q_{j+1},$$

and for an odd j we have:

$$Q_2 \cdot (v_j \beta v_{j-1} \ldots \beta v_2)^{-1} = Q_j \cdot (v_j \beta)^{-1} = R_j \cdot v_j^{-1} = R_j \cdot (\omega_0 t_{j-2})^{-1}$$
$$= R_{j+1}^\diamond \cdot \omega_0^{-1} = R_{j+1}.$$

The Claim (3) follows from $Q_1 \cdot (w\omega_0)^{-1} = Q_2 \cdot w^{-1} = Q_N$, according to the first claim with $j = N-1$. $\qquad\square$

It remains to calculate the length of w.

Lemma 11. *The length of w is $\frac{N^2-5}{2}$.*

Proof. The sum of $|v_i|$ with even i is

$$\sum_{i=1}^{\frac{N-1}{2}} (1+N-2i) = \frac{(N-1)(1+N)}{2} - \frac{(N-1)(1+N)}{4} = \frac{1}{4}\left(N^2-1\right),$$

and the sum of $|v_i|$ with odd i is

$$\sum_{i=1}^{\frac{N-3}{2}} 2i = \frac{(N-3)(N-1)}{4} = \frac{1}{4}\left(N^2-4N+3\right).$$

Together with the $N-3$ occurrences of β, we have $|w| = \frac{N^2-5}{2}$.   □

Thus, we have that $w\omega_0$ is a reset word for $\mathcal{A}_m$ with length $|w\omega_0| = \frac{N^2-3}{2}$.

4.2 Lower Bound on the Reset Threshold

Finally, let us show that no reset word for $\mathcal{A}_k$ is shorter than $w\omega_0$.

Lemma 12. *If $v \in \Sigma^*$ is greedy and straight reset word with $Q \cdot v = \{q_0\}$, then v does not contain $\omega_0\beta$ nor $\omega_1\beta$ as a factor.*

Proof. Suppose for a contradiction that $v = u''x\beta u'$ for $x \in \{\omega_0,\omega_1\}$. Since v is greedy, $\{q_0\} \cdot (u')^{-1}$ is not ω-extensible, so it contains both 0 and 1 or neither of them. Since β switches these states, $\{q_0\} \cdot (\beta u')^{-1}$ has the same property. Then $\{q_0\} \cdot (\beta u')^{-1} = \{q_0\} \cdot (x\beta u')^{-1}$ and so v is not straight.   □

Lemma 13. *Let $2 \leq j \leq N-1$. It holds that:*

1. *$\{0,1\} \cap (Q_j \cdot t_h) = \emptyset$ for $1 \leq h < N-j$ if j is even,*
2. *$\{0,1\} \subseteq (R_j \cdot t_h)$ for $1 \leq h < j-2$ if j is odd.*

Proof. As t_h is involutory, it is enough to show for $q \in \{0,1\}$ that $q \cdot t_h \notin Q_j$ or $q \cdot t_h \in R_j$ respectively.

As for (1), by Lemma 6(2) we have $q \cdot t_h = N-q-h > j-1$, thus $q \cdot t_h \notin Q_j$. As for (2), denoting $q' = q \cdot t_h$, we have $q' = N-q-h$. Then $q' \cdot \beta = (q+h+1) \bmod N$, and since $q \leq 1$ and $h < j-2$, we get $q' \cdot \beta < j$, which implies $q' \cdot \beta \in Q_j$ and $q' \in R_j$.

Lemma 14. *For each suffix xu of w with $x \in \{\omega_0,\omega_1\}$ and $u \in \Sigma^*$ it holds that x extends $Q_2 \cdot u^{-1}$.*

Proof. For every suffix $\omega_1 u$ we have $Q_2 \cdot u^{-1}\omega_1^{-1} = Q_{j+1}^\diamond \cdot \omega_1^{-1} = Q_{j+1}$ for some even j, and for every suffix $\omega_0 u$ we have $Q_2 \cdot u^{-1}\omega_0^{-1} = R_{j+1}^\diamond \cdot \omega_0^{-1} = R_{j+1}$ for some odd j.   □

Lemma 15. *The word $w\omega_0$ is greedy.*

Proof. Let u be the shortest suffix of $w\omega_0$ that violates the greediness, i.e., suppose that $Q_1 \cdot u^{-1}$ is z-extensible for $z \in \{\omega_0, \omega_1\}$, but zu is not a suffix of $w\omega_0$. This simplification works because $Q_1 \cdot u^{-1}$ cannot be both ω_0-extensible and ω_1-extensible. Fix $x \in \Sigma$ such that xu is a suffix of w. Let $u = yu_{\mathbf{s}}$ with $y \in \Sigma$.

If $y \in \{\omega_0, \omega_1\}$ then $Q_1 \cdot (yu_{\mathbf{s}})^{-1}$ is not ω-extensible. If $x \in \{\omega_0, \omega_1\}$, then $Q_1 \cdot (yu_{\mathbf{s}})^{-1}$ is x-extensible due to Lemma 14. Thus, necessarily $x, y \in \{\alpha, \beta\}$.

Assume $y = \beta$. If $Q_1 \cdot (yu_{\mathbf{s}})^{-1}$ is ω-extensible, then $Q_1 \cdot (u_{\mathbf{s}})^{-1}$ is ω-extensible as well due to $0 \cdot \beta = 1$ and $1 \cdot \beta = 0$, implying that $u_{\mathbf{s}}$ is a shorter suffix violating the greediness.

Assume $y = \alpha$. Because w does not contain the factor $\alpha\alpha$, it follows that $x = \beta$. According to (Sect. 4.1), i.e., the definition of w, and the fact that $v_{N-1} = \alpha$, the factor $xy = \beta\alpha$ occurs only within the factors $v_2 \ldots, v_{N-2}$. Thus,

$$yu_{\mathbf{s}} = \alpha \left(\beta\alpha\right)^i \beta \left(v_{j-1}\beta v_{j-2} \ldots \beta v_3 \beta v_2\right) \omega_0,$$

where $\alpha \left(\beta\alpha\right)^i$ is a suffix of v_j. We apply Lemma 10:

1. If j is odd, we get $Q_2 \cdot (v_{j-1}\beta v_{j-2} \ldots \beta v_2)^{-1} = Q_j$, while $v_j = \omega_0 t_{j-2}$ and $i \leq \frac{j-3}{2}$. Then

   $$Q_1 \cdot (yu_{\mathbf{s}})^{-1} = Q_j \cdot \left(\alpha \left(\beta\alpha\right)^i \beta\right)^{-1} = Q_j \cdot (t_h\beta)^{-1} = R_j \cdot t_h^{-1} = R_j \cdot t_h,$$

   where $h = 2i + 1$. We see that $1 \leq h \leq j - 2$. If $h = j - 2$, then $\omega_0 t_h = v_j$, so $x = \omega_0$. Otherwise we apply Lemma 13(2) to get $\{0, 1\} \subseteq R_j \cdot t_h$, which contradicts that $Q_1 \cdot (yu_{\mathbf{s}})^{-1}$ is ω-extensible.
2. If j is even, we get $Q_2 \cdot (v_{j-1}\beta v_{j-2} \ldots \beta v_2)^{-1} = R_j$, while $v_j = \omega_1 t_{N-j}$ and $i \leq \frac{N-j-1}{2}$. Then

   $$Q_1 \cdot (yu_{\mathbf{s}})^{-1} = R_j \cdot \left(\alpha \left(\beta\alpha\right)^i \beta\right)^{-1} = R_j \cdot (t_h\beta)^{-1} = Q_j \cdot t_h,$$

   where $h = 2i + 1$. We see that $1 \leq h \leq N - j$. If $h = N - j$, then $\omega_1 t_h = v_j$, so $x = \omega_1$. Otherwise we apply Lemma 13(1) to get $\{0, 1\} \cap Q_j \cdot t_h = \emptyset$, which contradicts that $Q_1 \cdot (yu_{\mathbf{s}})^{-1}$ is ω-extensible. □

Lemma 16. *There exists a shortest reset word for $\mathcal{A}_m$ that ends with ω_0 and is greedy.*

Proof. Lemma 5 gives a shortest reset word that is greedy. Clearly, a shortest reset word ends with a non-permutational letter, i.e., ω_0 or ω_1. In the latter case, replacing the ending ω_1 with ω_0 yields a reset word of the same length and preserves greediness. □

Theorem 17. *The word $w\omega_0$ is a shortest reset word for $\mathcal{A}_m$.*

Proof. Using Lemma 5, let $w'\omega_0$ be a greedy shortest reset word of $\mathcal{A}_m$. If $w' = w$, we are done, so let $w' \neq w$ and let $w_{\mathbf{s}}$ be the longest common suffix of w' and w.

If $w_{\mathbf{s}} = w'$, then w' is a proper suffix of w and so it contains at most $N - 3$ letters from $\{\omega_0, \omega_1\}$, which contradicts that $w_{\mathbf{s}}\omega_0$ is a reset word. So we can write $w = w_{\mathbf{p}}xw_{\mathbf{s}}$ and $w' = w'_{\mathbf{p}}x'w_{\mathbf{s}}$, where $x, x' \in \Sigma$ and $x' \neq x$. We will show that each of the following cases according to x and x' leads to a contradiction:

1. Suppose that $x \in \{\omega_0, \omega_1\}$. Then Lemma 14 implies that $Q_2 \cdot w_{\mathbf{s}}$ is x-extensible, which contradicts $x' \neq x$ and the greediness of $w'\omega_0$.
2. Suppose that $x' \in \{\omega_0, \omega_1\}$. According to Proposition 3, $w'\omega_0$ is straight, which implies that $Q_2 \cdot w_{\mathbf{s}}$ is x'-extensible, which contradicts $x' \neq x$ and Lemma 15, i.e., the greediness of $w\omega_0$.
3. Suppose that $x = \alpha$ and $x' = \beta$. According to Remark 8, $w_{\mathbf{s}} = \epsilon$ or $w_{\mathbf{s}}$ starts with β. The case of $w_{\mathbf{s}} = \epsilon$ contradicts the straightness of $w'\omega_0$ because each $x' \in \Sigma \setminus \{\alpha\}$ satisfies $Q_2 \cdot (x')^{-1} = Q_2$. The other case implies $\beta\beta$ occurring in w' and thus also contradicts the straightness of $w'\omega_0$.
4. Suppose that $x = \beta$ and $x' = \alpha$. Then $w_{\mathbf{s}} \neq \epsilon$. If $w_{\mathbf{s}}$ starts with α or β, then either w' or w contains the factor $\alpha\alpha$ or $\beta\beta$, which contradicts the straightness of $w'\omega_0$ or the definition of w. Hence, $w_{\mathbf{s}}$ starts with ω_0 or ω_1. Since this starts a factor v_j for some $j \geq 2$, we can write

$$w_{\mathbf{s}} = v_j\beta v_{j-1} \ldots \beta v_3\beta v_2.$$

We consider the following two subcases:

(a) Suppose that $w_{\mathbf{s}}$ starts with ω_1. Note that $j \geq 2$ is even and $Q_2 \cdot w_{\mathbf{s}}^{-1} = Q_{j+1}$ by Lemma 10. Let $w_{\mathbf{m}}$ be the longest common suffix of $w'_{\mathbf{p}}x' = w'_{\mathbf{p}}\alpha$ and t_{N-j}. Clearly, $|w_{\mathbf{m}}| \geq 1$. If $w_{\mathbf{m}} = t_{N-j}$, then from Lemma 7(3) we have $Q_{j+1} \cdot t_{N-j} = Q_{j+1}$, which contradicts the straightness of $w'\omega_0$. If $w_{\mathbf{m}} = w'_{\mathbf{p}}x'$, then w' starts with α or β, which contradicts that $w'\omega_0$ is a shortest reset word. It follows that we can write $w' = w'_{\mathbf{pp}}y'w_{\mathbf{m}}w_{\mathbf{s}}$ for $y' \in \Sigma$. Moreover, as w' does not contain the factors $\alpha\alpha$ and $\beta\beta$, we have $y' \neq \alpha$ and $y' \neq \beta$, so $y' \in \{\omega_0, \omega_1\}$. Due to Lemma 12, $w_{\mathbf{m}}$ cannot start with β, and from the construction of t_{N-j} we have $w_{\mathbf{m}} = t_h$ for $h \leq N - j - 2$. It holds that $Q_{j+1} \cdot w_{\mathbf{m}}^{-1} = Q_{j+1} \cdot t_h = Q_j \cdot t_h \cup \{j \cdot t_h\}$. Lemma 13(1) provides that $\{0, 1\} \cap Q_j \cdot t_h = \emptyset$. Also, $j \cdot t_h = N - j - h \geq 2$. Together, $Q_{j+1} \cdot w_{\mathbf{m}}^{-1} \cap \{0, 1\} = \emptyset$, and thus this set is not ω-extensible, which contradicts $y' \in \{\omega_0, \omega_1\}$ and the straightness of $w'\omega_0$.

(b) Suppose that $w_{\mathbf{s}}$ starts with ω_0. Note that $j \geq 3$ is odd and $Q_2 \cdot w_{\mathbf{s}}^{-1} = R_{j+1}$ by Lemma 10. Let $w_{\mathbf{m}}$ be the longest common suffix of $w'_{\mathbf{p}}x' = w'_{\mathbf{p}}\alpha$ and t_{j-2}. Clearly, $|w_{\mathbf{m}}| \geq 1$. If $w_{\mathbf{m}} = t_{j-2}$, then from Lemma 7(4) we have $R_{j+1} \cdot t_{j-2} = R_{j+1}$, which contradicts the straightness of $w'\omega_0$. If $w_{\mathbf{m}} = w'_{\mathbf{p}}x'$, then w' starts with α or β, which contradicts that $w'\omega_0$ is a shortest reset word. It follows that we can write $w' = w'_{\mathbf{pp}}y'w_{\mathbf{m}}w_{\mathbf{s}}$ for $y' \in \Sigma$. Moreover, as w' does not contain the factors $\alpha\alpha$ and $\beta\beta$, we have $y' \neq \alpha$ and $y' \neq \beta$, so $y' \in \{\omega_0, \omega_1\}$. Due to Lemma 12, $w_{\mathbf{m}}$ cannot start with β, and from construction of t_{j-2} we have $w_{\mathbf{m}} = t_h$ for $h \leq j - 4$.

We have $R_{j+1} \cdot w_{\mathbf{m}}^{-1} = R_{j+1} \cdot t_h \supseteq R_j \cdot t_h$. Lemma 13(2) gives $\{0,1\} \subseteq R_j \cdot t_h$. Thus, $\{0,1\} \subseteq R_{j+1} \cdot w_{\mathbf{m}}^{-1}$, and thus this set is not ω-extensible, which contradicts $y' \in \{\omega_0, \omega_1\}$ and the straightness of $w'\omega_0$.   □

Theorem 17 implies that $\mathrm{rt}(\mathcal{A}_m) = |w\omega_0| = \frac{N^2-3}{2}$.

4.3   Extending Words

The general upper bound $(n-2)(n-1)+1$ for reset thresholds of synchronizing Eulerian DFAs comes from the fact that any proper and non-empty subset of Q is extended by a word of length at most $n-1$ [15], while in the general case the minimum length of extending words can be quadratic (this was shown recently – see [19]). In view of this, our series shows that this bound is tight for infinitely many n, and so the upper bound for reset thresholds for this class cannot be improved only by reducing this particular bound. The following remark follows from the analysis in the proof of Theorem 17:

Remark 18. The shortest extending word of $\{0,1\}$ in $\mathcal{A}_m$ is $v_2 = \omega_1\alpha(\beta\alpha)^{(N-3)/2}$ of length $N-1$.

5   Experiments

Using the algorithm from [18,20], we have performed an exhaustive search over small synchronizing Eulerian DFAs. We verified the bound $(n^2-3)/2$ for the case of binary DFAs with $n \leq 11$ states, automata with four letters and $n \leq 7$ states, DFAs with eight letters and $n \leq 5$ states, and all DFAs with $n \leq 4$ states.

For $n \in \{3, 4, 5, 7\}$ the bound $(n^2-3)/2$ is reachable. For $n = 7$, up to isomorphism, we identified 2 ternary examples and 12 quaternary examples which also meet the bound. It seems that our series $\mathcal{A}_m$ is not unique meeting the bound, as some of the quaternary examples could be generalizable to series with the same reset thresholds. Also, for the binary case we found that for $n \in \{5, 7, 8, 9, 11\}$ the bound $(n^2-5)/2$ is met uniquely by DFAs from the Martyugin's series, but it is not reachable for $n \in \{6, 10\}$.

Conjecture 19. For $n \geq 3$, $(n^2-3)/2$ is an upper bound for the reset threshold of an n-state Eulerian synchronizing automaton. If $|\Sigma| = 2$, then the bound can be improved to $(n^2-5)/2$.

References

1. Ananichev, D., Gusev, V., Volkov, M.: Slowly synchronizing automata and digraphs. In: Hliněný, P., Kučera, A. (eds.) MFCS 2010. LNCS, vol. 6281, pp. 55–65. Springer, Heidelberg (2010)
2. Ananichev, D.S., Volkov, M.V.: Synchronizing generalized monotonic automata. Theor. Comput. Sci. **330**(1), 3–13 (2005)

3. Ananichev, D.S., Volkov, M.V., Gusev, V.V.: Primitive digraphs with large exponents and slowly synchronizing automata. J. Math. Sci. **192**(3), 263–278 (2013)
4. Béal, M.P., Berlinkov, M.V., Perrin, D.: A quadratic upper bound on the size of a synchronizing word in one-cluster automata. Int. J. Found. Comput. Sci. **22**(2), 277–288 (2011)
5. Berlinkov, M.V.: Synchronizing quasi-Eulerian and quasi-one-cluster Automata. Int. J. Found. Comput. Sci. **24**(6), 729–745 (2013)
6. Berlinkov, M., Szykuła, M.: Algebraic synchronization criterion and computing reset words. In: Italiano, G.F., Pighizzini, G., Sannella, D.T. (eds.) MFCS 2015. LNCS, vol. 9234, pp. 103–115. Springer, Heidelberg (2015)
7. Biskup, M.T., Plandowski, W.: Shortest synchronizing strings for Huffman codes. Theor. Comput. Sci. **410**(38–40), 3925–3941 (2009)
8. Carpi, A., D'Alessandro, F.: Strongly transitive automata and the Černý conjecture. Acta Informatica **46**(8), 591–607 (2009)
9. Černý, J.: Poznámka k homogénnym experimentom s konečnými automatmi. Matematicko-fyzikálny Časopis Slovenskej Akadémie Vied **14**(3), 208–216 (1964)
10. Dubuc, L.: Sur les automates circulaires et la conjecture de Černý. Informatique Théorique et Appl. **32**, 21–34 (1998)
11. Eppstein, D.: Reset sequences for monotonic automata. SIAM J. Comput. **19**, 500–510 (1990)
12. Grech, M., Kisielewicz, A.: The Černý conjecture for automata respecting intervals of a directed graph. Discr. Math. Theor. Comput. Sci. **15**(3), 61–72 (2013)
13. Gusev, V.: Lower bounds for the length of reset words in Eulerian automata. Int. J. Found. Comput. Sci. **24**(2), 251–262 (2013)
14. Gusev, V.V., Pribavkina, E.V.: Reset thresholds of automata with two cycle lengths. In: Holzer, M., Kutrib, M. (eds.) CIAA 2014. LNCS, vol. 8587, pp. 200–210. Springer, Heidelberg (2014)
15. Kari, J.: Synchronizing finite automata on Eulerian digraphs. Theor. Comput. Sci. **295**(1–3), 223–232 (2003)
16. Kari, J., Volkov, M.V.: Černý's conjecture and the road coloring problem. In: Handbook of Automata, European Science Foundation (2013)
17. Kisielewicz, A., Kowalski, J., Szykuła, M.: Computing the shortest reset words of synchronizing automata. J. Combin. Optim. **29**(1), 88–124 (2015)
18. Kisielewicz, A., Szykuła, M.: Generating small automata and the Černý conjecture. In: Konstantinidis, S. (ed.) CIAA 2013. LNCS, vol. 7982, pp. 340–348. Springer, Heidelberg (2013)
19. Kisielewicz, A., Szykuła, M.: Synchronizing automata with extremal properties. In: Italiano, G.F., Pighizzini, G., Sannella, D.T. (eds.) MFCS 2015. LNCS, vol. 9234, pp. 331–343. Springer, Heidelberg (2015)
20. Kisielewicz, A., Kowalski, J., Szykula, M.: Experiments with synchronizing automata. In: Han, Y.-S., Salomaa, K. (eds.) CIAA 2016. LNCS, vol. 9705, pp. 176–188. Springer, Heidelberg (2016). doi:10.1007/978-3-319-40946-7_15
21. Pin, J.E.: On two combinatorial problems arising from automata theory. In: Proceedings of the International Colloquium on Graph Theory and Combinatorics. North-Holland Mathematics Studies, vol. 75, pp. 535–548 (1983)
22. Rystsov, I.K.: Estimation of the length of reset words for automata with simple idempotents. Cybern. Syst. Anal. **36**(3), 339–344 (2000)
23. Steinberg, B.: The averaging trick and the Černý conjecture. Int. J. Found. Comput. Sci. **22**(7), 1697–1706 (2011)
24. Steinberg, B.: The Černý conjecture for one-cluster automata with prime length cycle. Theor. Comput. Sci. **412**(39), 5487–5491 (2011)

25. Trahtman, A.N.: The Černý conjecture for aperiodic automata. Discr. Math. Theor. Comput. Sci. **9**(2), 3–10 (2007)
26. 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)
27. Volkov, M.V.: Synchronizing automata preserving a chain of partial orders. Theor. Comput. Sci. **410**(37), 3513–3519 (2009)