On the Interplay Between Babai and Černý's Conjectures

François Gonze[1], Vladimir V. Gusev[1,2], Balázs Gerencsér[3], Raphaël M. Jungers[1], and Mikhail V. Volkov[2⋆]

[1] ICTEAM Institute, Université Catholique de Louvain, Louvain-la-Neuve, Belgium
{francois.gonze,vladimir.gusev,raphael.jungers}@uclouvain.be
[2] Ural Federal University, Ekaterinburg, Russia
mikhail.volkov@usu.ru
[3] Alfréd Rényi Institute of Mathematics, Budapest, Hungary
gerencser.balazs@renyi.mta.hu

Abstract. Motivated by the Babai conjecture and the Černý conjecture, we study the reset thresholds of automata with the transition monoid equal to the full monoid of transformations of the state set. For automata with n states in this class, we prove that the reset thresholds are upper-bounded by $2n^2 - 6n + 5$ and can attain the value $\frac{n(n-1)}{2}$. In addition, we study diameters of the pair digraphs of permutation automata and construct n-state permutation automata with diameter $\frac{n^2}{4} + o(n^2)$.

1 Background and Overview

Completely reachable automata, i.e., deterministic finite automata in which every non-empty subset of the state set occurs as the image of the whole state set under the action of a suitable input word, appeared in the study of descriptional complexity of formal languages [26] and in relation to the Černý conjecture [13]. In [6] an emphasis has been made on automata in this class with minimal transition monoid size. In the present paper we focus on automata being in a sense the extreme opposites of those studied in [6], namely, on automata of maximal transition monoid size. In other words, we consider automata *with full transition monoid*, i.e., transition monoid equal to the full monoid of transformations of the state set; clearly, automata with this property are completely reachable. There are several reasons justifying special attention to automata with full transition monoid. First, as observed in [6], the membership problem for this class of automata is decidable in polynomial time (of the size of the input automaton) while

⋆ Vladimir Gusev and Mikhail V. Volkov were supported by RFBR grant no. 16-01-00795, Russian Ministry of Education and Science project no. 1.3253.2017, and the Competitiveness Enhancement Program of Ural Federal University. Balázs Gerencsér was supported by PD grant no. 121107, National Research, Development and Innovation Office of Hungary. This work was supported by the French Community of Belgium and by the IAP network DYSCO. Raphaël Jungers is a Fulbright Fellow and a FNRS Research Associate.
A short version of this work has been presented at the conference DLT 2017.

the complexity of membership in the class of all completely reachable automata still remains unknown. Second, this class contains automata that correspond to Brzozowski's most complex regular languages [7] and to other regular languages that play a distinguished role in descriptive complexity analysis. Finally, and most importantly from our viewpoint, automata with full transition monoid are synchronizing and their synchronization issues constitute a sort of meeting point for two famous open problems—the *Babai conjecture* and the *Černý conjecture*. Next, we recall these conjectures and outline the contribution of the present paper in view of these problems.

1.1. The Babai Conjecture. Let A be a set of generators of a finite group G. The *Cayley graph* $\Gamma(G, A)$ consists of G as the set of vertices and the edges $\{g, ga\}$ for all $g \in G$, $a \in A$. The *diameter* of $\Gamma(G, A)$ is the maximum among the lengths of shortest paths between any two vertices. In group theory terms, the diameter of $\Gamma(G, A)$ is the smallest ℓ such that every $g \in G$ can be represented as $g = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_\ell^{\varepsilon_\ell}$, where $\varepsilon_i \in \{1, -1\}$ and $a_i \in A$ for all $i = 1, \ldots, \ell$. The *diameter* $\mathrm{diam}(G)$ of G is the maximal diameter of $\Gamma(G, A)$ among all generating sets A of G. The notion of group diameter is related to the growth rate in groups, expander graphs, random walks on groups and their mixing times, see, e.g., [23, 33]. Recently, the following conjecture received significant attention:

Conjecture 1 (Babai [4]) *The diameter of each non-abelian finite simple group G does not exceed $(\log |G|)^{O(1)}$, where the implied constant is absolute.*

Note that for the case of the symmetric group S_n, this conjecture readily implies $\mathrm{diam}(S_n) \leq n^{O(1)}$. (The group S_n is not simple but for $n \geq 5$ it contains a non-abelian simple subgroup of index 2.)

The Babai conjecture was proved for various classes of groups, but despite intensive research effort it remains open, see [22] for an overview. In the case of S_n, a recent breakthrough gives only a quasipolynomial upper bound, namely, $\exp(O((\log n)^4 \log \log n)$, and it relies on the Classification of Finite Simple Groups [22]. It is even more astonishing if we compare it to the best known lower bound in this case: for the classical set of generators consisting of the transposition $(1, 2)$ and the full cycle $(1, 2, \ldots, n)$, every permutation in S_n can be expressed as a product of at most $\sim \frac{3n^2}{4}$ (asymptotically) generators [40].

1.2. The Černý Conjecture. Recall that a deterministic finite state automaton (DFA) is a triple[1] $\langle Q, \Sigma, \delta \rangle$, where Q is a finite set of states, Σ is a finite set of input symbols called the *alphabet*, and δ is a function $\delta\colon Q \times \Sigma \to Q$ called the *transition function*. A *word* is a sequence of letters from the alphabet. The *length* of a word is the number of its letters. We can look at $\delta(q, a)$ as the result of the *action* of the letter $a \in \Sigma$ at the state $q \in Q$. We extend this action to the action of words over Σ on Q denoting, for any word w and any state $q \in Q$, the state resulting in successive applications of the letters of w from left to right by $q{\cdot}w$. For a subset $P \subseteq Q$, we write $P{\cdot}w$ for the set $\{p{\cdot}w \mid p \in P\}$.

[1] As initial and final states play no role in our considerations, we omit them.

A DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is called *synchronizing* if there exist a word w and a state f such that $Q \cdot w = \{f\}$. Any such word is called a *synchronizing* or *reset* word. The minimum length of reset words for $\mathscr{A}$ is called the *reset threshold* of $\mathscr{A}$ and is denoted by $\mathrm{rt}(\mathscr{A})$. Synchronizing automata appear in various branches of mathematics and are related to synchronizing codes [5], part orienting problems [27, 28], substitution systems [16], primitive sets of matrices [19], synchronizing groups [3], convex optimization [20], and consensus theory [11].

Conjecture 2 (Černý [9, 10]) *The reset threshold of an n-state synchronizing automaton is at most $(n-1)^2$.*

If the conjecture holds true, then the value $(n-1)^2$ is optimal, since for every n there exists an n-state automaton $\mathscr{C}_n$ with the reset threshold equal to $(n-1)^2$ [9].

The Černý conjecture has gained a lot of attention in automata theory. It has been shown to hold true in various special classes [14,21,24,31,35,36], but in the general case, it remains open for already half a century. For more than 30 years, the best upper bound was $\frac{n^3-n}{6}$, obtained in [15, 30] and independently in [25]. Recently, a small improvement on this bound has been reported in [37]: the new bound is still cubic in n but improves the coefficient $\frac{1}{6}$ at n^3 by $\frac{4}{46875}$. A survey on synchronizing automata and the Černý conjecture can be found in [38].

In order to make the relationship between the Černý and the Babai conjectures more visible, we borrow from [2] the idea of restating the former in terms similar to those used in the formulation of the latter. Let T_n be the full transformation monoid of an n-element set Q. A transformation $t \in T_n$ is a *constant* if there exists $f \in Q$ such that for all $q \in Q$ we have $t(q) = f$. We can state the Černý conjecture as follows: for every set of transformations $A \subseteq T_n$, if the submonoid generated by A contains a constant, then there exists a constant g such that $g = a_1 a_2 \cdots a_\ell$, where $\ell \leq (n-1)^2$ and $a_i \in A$ for all $i = 1, \ldots, \ell$. It is easy to see that this formulation is equivalent to the original one by treating the letters of an automaton as the transformations of its state set since reset words precisely correspond to constant transformations.

1.3. Our Contributions. The first part of our paper is devoted to the following *hybrid Babai–Černý problem*[2]: given a set of generators A of the full transformation monoid T_n, what is the length $\ell(A)$ of the shortest product $a_1 a_2 \cdots a_\ell$ with $a_i \in A$ which is equal to a constant? Namely, we are interested in the bounds on $\ell(A)$ that depend only on n. The hybrid Babai–Černý problem is a special case of the Černý problem. Indeed, it is a restriction to the class of DFAs with the *transition monoid*, i.e., the transformation monoid generated by the actions of letters, equal to T_n. Of course, the general cubic upper bound is valid, but not the lower bound, since the Černý automata $\mathscr{C}_n$ do not belong to this class (even though they are completely reachable, see [6]). In Section 2 we establish that the growth rate of $\ell(n)$ is $\Theta(n^2)$, more precisely, we show that

[2] During the preparation of this paper we discovered that the same question was also posed in [34, Conjecture 3], though its connection with Babai's problem was not registered there.

$\frac{n(n-1)}{2} \leq \ell(n) \leq 2n^2 - 6n + 5$. We also present the exact values of $\ell(n)$ for small values of n resulting from our computational experiments. Our contribution can be also seen as a progress towards resolution of Conjecture 3 from [34].

The second part of our paper is devoted to a "local" version of the Babai problem where we restrict our attention to the action on the set of (unordered) pairs. Let A be a set of permutations from S_n. The *pair digraph* $P(A)$ consists of pairs $\{i, j\}$ as the set of vertices and the edges $(\{i, j\}, \{ia, ja\})$ for all i, j and $a \in A$. The *diameter* of $P(A)$, denoted $\operatorname{diam} P(A)$, is the maximum among the lengths of shortest (directed) paths between any two vertices. We study the behavior of $\operatorname{diam} P(A)$ in terms of n. The problem comes from analysis of certain aspects of Markov chains and group theory [17], but our interest in it is mainly motivated by its importance for the theory of synchronizing automata. Indeed, every synchronizing automaton $\mathscr{A}$ must have a letter a, say, whose action merges a pair of states. Thus, one can construct a reset word for $\mathscr{A}$ by successively moving pairs of states to a pair merged by a. If $\mathscr{A}$ possesses sufficiently many letters acting as permutations (as automata with the full transition monoid do), one can move pairs by these permutations, and hence, upper bounds on the diameter of the corresponding pair digraph induce upper bounds on $\operatorname{rt}(\mathscr{A})$.

Clearly, $\operatorname{diam} P(A) \leq \frac{n(n-1)}{2}$ for all $A \subseteq S_n$. In Section 3 we establish the lower bound $\frac{n^2}{4} + o(n^2)$ on $\operatorname{diam} P(A)$ by presenting a series of examples with only two generators for every odd n.

1.4. Related Work. The diameters of groups and semigroups constitute a relatively well studied topic. A general discussion on diameters and growth rates of groups can be found in [23]. Various results about the diameter of T_n and its submonoids are described in [29,34]. The length of the shortest representation of a constant (including the case of partially defined transformations) is typically studied in the framework of synchronizing automata, see [1, 38, 39].

2 Automata with Full Transition Monoid

2.1. Naïve Construction. Recall that, on the one hand, the Černý automata $\mathscr{C}_n$ from [9] have two letters of which one acts as a cyclic permutation and the other fixes all states, except one, which is mapped to the next element in the cyclic order defined by the cyclic permutation. On the other hand, the extremal case of the Babai conjecture for S_n is composed of a cyclic permutation and the transformation which fixes all elements except two, which are neighbors in the cyclic order defined by the cyclic permutation. Therefore, one could wonder if a combination of these transformations could result in a DFA with both large reset threshold and full transition monoid.

The construction is defined as follows. There are n states $q_1, \ldots, q_n$ and three letters a, b, and c. The letter a acts as a cyclic permutation on the states, following their indices. The letter b fixes all states, except q_1, which is mapped to q_2 by b. The letter c fixes all states, except q_k and q_{k+1}, for some k, which are swapped by c. The resulting automaton $\mathscr{CB}_{n,k}$ is shown in Fig. 1. We notice that

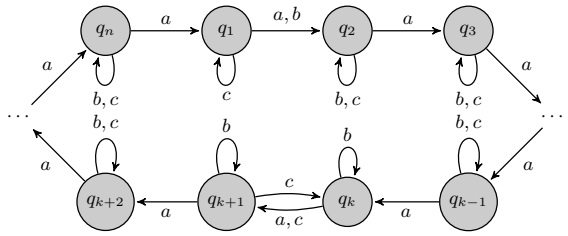

Fig. 1: The automaton $\mathscr{CB}_{n,k}$

if we remove the letter c, we obtain the automaton $\mathscr{C}_n$ from the Černý family providing the largest currently existing lower bound in the Černý problem, and if we remove the letter b, we obtain a generating set of the group S_n providing the largest currently existing lower bound in the Babai problem for S_n. Also observe that in the case where $k = 2$, our automaton is nothing but Brzozowski's "Universal Witness" [7] recognizing the most complex regular language, i.e., the language witnessing at once practically all tight lower bounds found for the state complexity of various operations with regular languages, see [7, Theorem 6]. The next result shows that, however, the reset threshold of the automaton $\mathscr{CB}_{n,k}$ is upper-bounded by $O(n \log n)$, while, as we show later, among automata with full transition monoid there exist ones whose reset threshold is a quadratic function of their state number.

Theorem 1. *The automaton $\mathscr{CB}_{n,k}$ has a reset word of length at most $4n\lceil \log_2 n \rceil$.*

Proof. Recall that we aim to show that, for each k, the automaton $\mathscr{CB}_{n,k}$ has a reset word of length at most $4n\lceil \log_2 n \rceil$. It is easy to see that the word $b(cab)^{n-2}$ of length $3n - 5 < 4n\lceil \log_2 n \rceil$ resets the automaton $\mathscr{CB}_{n,1}$, so that we assume that $k > 1$ in the rest of the proof.

We construct a word w letter-by-letter in several rounds, starting with the empty word. The main parameter in our construction is the current image of the state set of $\mathscr{CB}_{n,k}$ under the action of the word constructed so far; let S stand for this image. (Thus, we have $S = \{q_1, \ldots, q_n\}$ at the beginning, and S becomes a singleton at the end of the process.) It is quite helpful to visualize S as the set whose states bear certain tokens. If one colors states covered by tokens light-gray, then Fig. 1 represents the initial position while Fig. 2 shows some intermediate situation. When a letter $x \in \{a, b, c\}$ is applied to S, the token that covers q_i, say, moves to the state $q_i \cdot x$; in more visual terms, the token "slides" along the arrow representing the transition $q_i \to q_i \cdot x$. If two tokens arrive at the same state, which happens whenever both q_1 and q_2 bear tokens and the letter b is applied, we remove one of the tokens.

In the course of our construction, rounds of two sorts alternate: *merging*, in which only a's and b's are applied to S, and *pairing*, in which only a's and c's are applied. We call a state from S *isolated* if both its neighbor states (with respect

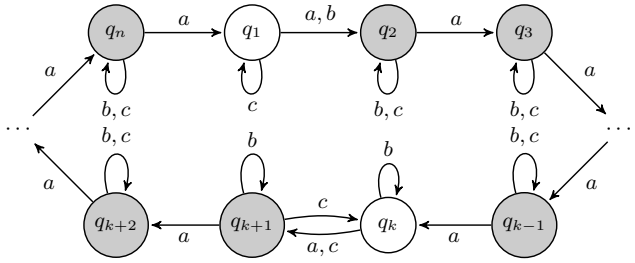

Fig. 2: Tokens mark a subset in $\mathscr{CB}_{n,k}$

to the cyclic order defined by a) are not in S. A merging round starts whenever $|S| > 1$ and S has at most one isolated state, and it lasts while S contains non-isolated states; a pairing round starts whenever $|S| > 1$ and all states in S are isolated, and it lasts while S contains more than one isolated state. Every round consists of a number of steps, in each of which we choose a letter, append the chosen letter to the word w and update the set S by applying the letter to it. The choice is done according to one of the two following rules (M) and (P) used during merging and pairing rounds, respectively:

(M) b is chosen whenever $q_1, q_2 \in S$; otherwise a is chosen;
(P) c is chosen whenever $q_{k+1} \in S$, but $q_k, q_{k+2} \notin S$ (so that q_{k+1} is isolated); otherwise a is chosen.

Clearly, at the beginning no state is isolated, and hence, the first round of our construction must be merging. It amounts to an immediate calculation to see that by the end of the first round, we have $w = b(a^2b)^{\lfloor \frac{n-1}{2} \rfloor}$ and $S = \{q_2, q_4, \dots q_{2\lfloor \frac{n}{2} \rfloor}\}$.

Now we are going to verify two claims.

Claim 1. If $|S| = m$ before any of the next merging rounds, then $|S| = \lceil \frac{m}{2} \rceil$ at the end of the round.

We say that two neighbor states $q_\ell, q_\ell{\cdot}a \in S$ form an *isolated couple* if each of these states has exactly one neighbor in S.

Claim 2. If $|S| = m$ before a pairing round, then at the end of the round S is partitioned in either $\frac{m}{2}$ isolated couples (if m is even) or $\frac{m-1}{2}$ isolated couples and one isolated state (if m is odd).

First we prove Claim 2. The *distance from q_i to q_j* is $\min\{d \in \mathbb{N} \mid q_i{\cdot}a^d = q_j\}$. We order tokens that cover the states in S according to the distance from their states to the state q_{k+1}: the i-th token is the one that covers the state with the distance d_i to q_{k+1}, where $0 \le d_1 < d_2 < \cdots < d_m < n$. Now consider the evolution of the set S under the choice of letters according to the rule (P). Clearly, the first d_1 choices are all a's. After that the first token reaches q_{k+1}. Since the action of a translates the set S, without affecting distances between its states, all states in S remain isolated at this point. In particular, q_{k+1} is isolated, and hence, (P) forces the letter c to be applied. This moves the first token "backwards" to the state q_k while all other tokens keep their positions.

The next letter to be applied is a, and its application moves all tokens one step "forwards" so that the token from q_k returns to q_{k+1}. Clearly, the distance from the state that holds the second token to q_{k+1} becomes d_2-d_1-1 after these two moves. If the state q_{k+1} remains isolated, another application of c is invoked, followed by another application of a, and this results in a further decrement of the distance from the state that holds the second token to q_{k+1}. Eventually, after the suffix $a^{d_1}(ca)^{d_2-d_1}$ is appended to w, the second token reaches the state q_k. At this moment, the third token (if it exists) covers a state with distance $d_3-d_2>1$ to q_k whence q_{k+1},q_k form an isolated couple in S. The two tokens covering these states will then remain adjacent till the end of the round.

If $m=2$ or $m=3$, we are done. If $m>3$, we proceed in the same way. Namely, the next d_3-d_2 choices are all a's. After that the third token reaches q_{k+1}. Except the first two, all other tokens remain isolated. Now (P) forces c and a to be alternatively chosen d_4-d_3 times each. This makes the third token shuffle between q_{k+1} and q_k, while the fourth and the next tokens move d_4-d_3 steps "forwards". After that q_{k+1},q_k form yet another isolated couple in S, etc.

We have shown that at the end of the round, the set S indeed consists of either $\frac{m}{2}$ isolated couples (if m is even) or $\frac{m-1}{2}$ isolated couples and one isolated state (if m is odd). Moreover, the suffix appended to w during the round is of the form

$$a^{d_1}(ca)^{d_2-d_1}a^{d_3-d_2}(ca)^{d_4-d_3}a^{d_5-d_4}(ca)^{d_6-d_5}\cdots. \tag{1}$$

The letter a occurs in this suffix d_m times if m is even and d_{m-1} times if m is odd, and the number of occurrences of c is less than that of a. Since $d_{m-1}<d_m<n$, we conclude that the length of the suffix (1) is less than $2n$.

Now it is easy to prove Claim 1. In view of Claim 2, at the beginning of the round, the set S consists of either $\frac{m}{2}$ isolated couples (if m is even) or $\frac{m-1}{2}$ isolated couples and one isolated state (if m is odd). If $\{q_\ell, q_\ell\cdot a\}$ is an isolated couple, we say that q_ℓ is its *left state*. Now we order isolated couples in S according to the distance from their left states to the state q_1: the i-th couple is the one with the distance d_i from its left state to q_1, where $0\le d_1<d_2<\cdots<d_{\lceil\frac{m}{2}\rceil}<n$. Consider the evolution of the set S under the choice of letters according to the rule (M). The first d_1 choices are all a's. After that the tokens that initially covered the states of the first isolated couple arrive at the states q_1 and q_2, and hence, (M) forces the letter b to be applied. This application removes the token from q_1 and does not change anything else. The state q_2 then becomes isolated. The next d_2-d_1 choices are again all a's, and the successive applications of these a's bring tokens that initially covered the states of the second isolated couple to the states q_1 and q_2. Then, again, b is chosen, removing the token from q_1 and creating yet another isolated state in S, etc. At the end of the round, exactly one token from each isolated couple is removed and all remaining states are isolated. The number of these states is $\frac{m}{2}$ if m is even or $\frac{m+1}{2}$ if m is odd; in short, $\lceil\frac{m}{2}\rceil$, as claimed.

Moreover, the suffix appended to w during the round is of the form

$$a^{d_1}ba^{d_2-d_1}b\cdots a^{d_{\lceil\frac{m}{2}\rceil}-d_{\lceil\frac{m}{2}\rceil-1}}b. \tag{2}$$

The letter a occurs in this suffix $d_{\lceil \frac{m}{2} \rceil} < n$ times and the letter b occurs $\lceil \frac{m}{2} \rceil < n$ times, whence the length of the suffix (2) is less than $2n$.

Claim 1, together with the observation we made about the first merging round, readily implies that the number of merging rounds is at most $\lceil \log_2 n \rceil$. Since merging and pairing rounds alternate, the total number of rounds is upper-bounded by $2\lceil \log_2 n \rceil$. As observed after the proofs of Claims 1 and 2, a suffix of length less than $2n$ is appended to the current word w during each round. Clearly, at the end of the process, w becomes a reset word for $\mathscr{CB}_{n,k}$, and by the construction the length of w is less than $2n \cdot 2\lceil \log_2 n \rceil = 4n\lceil \log_2 n \rceil$. □

2.2. Random Sampling and Exhaustive Search. Every DFA with the transition monoid T_n necessarily has permutation letters that generate the whole symmetric group S_n and a letter of rank $n-1$ (i.e., a letter whose image has $n-1$ elements). It is a well known fact that the converse is also true, i.e., the transition monoid of any automaton with permutation letters generating S_n and a letter of rank $n-1$ is equal to T_n, see, e.g., [18, Theorem 3.1.3].

Relying on a group-theoretic result by Dixon [12], Cameron [8] observed that an automaton formed by two permutation letters taken uniformly at random and an arbitrary non-permutation letter is synchronizing with high probability. We give an extension by using another non-trivial group-theoretical result, namely, the following theorem by Friedman *et al.* [17]:

Theorem 2. *For every r and $d \geq 2$ there is a constant C such that for d permutations $\pi_1, \pi_2, \ldots, \pi_d$ of S_n taken uniformly at random, the following property F_r holds with probability tending to 1 as $n \to \infty$: for any two r-tuples of distinct elements in $\{1, 2, \ldots, n\}$, there is a product of less than $C \log n$ of the π_i's which maps the first r-tuple to the second.*

Corollary 3. *There is a constant C such that the reset threshold of an n-state automaton with two random permutation letters and an arbitrary non-permutation letter does not exceed $Cn \log n$ with probability that tends to 1 as $n \to \infty$.*

Proof. Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ stand for the automaton in the formulation of the corollary. We let $a \in \Sigma$ be the non-permutation letter and assume that the two permutation letters in Σ have the property F_2 of Theorem 2 for $r = 2$ with some constant C. By Theorem 2 this assumption holds true with probability that tends to 1 as $n \to \infty$.

There exists two different states $q_1, q_2 \in Q$ such that $q_1 \cdot a = q_2 \cdot a$. The set $Q \cdot a$ contains less than n elements. If $|Q \cdot a| = 1$, then a is a reset word for $\mathscr{A}$. If $|Q \cdot a| > 1$, take two different states $p_1, p_2 \in Q \cdot a$. By F_2, there is a product w of less than $C \log n$ of the permutation letters such that $p_i \cdot w = q_i$ for $i = 1, 2$. Now $|Q \cdot awa| < |Q \cdot a|$. If $|Q \cdot awa| = 1$, awa is a reset word for $\mathscr{A}$. If $|Q \cdot awa| > 1$, we apply the same argument to a pair of different states in $Q \cdot awa$. Clearly, the process results in a reset word in at most $n-1$ steps while the suffix appended at each step is of length at most $C \log n + 1$. Hence the length of the reset word constructed this way is at most $(C+1)n \log n$. □

Corollary 3 indicates that one can hardly discover an n-state automaton with the transition monoid equal to T_n and sufficiently large reset threshold by a random sampling. Therefore, we performed an exhaustive search among all automata with two permutation letters generating S_n and one letter of rank $n-1$. Our computational results are summarized in Table 1.

Number of states	2	3	4	5	6	7
Reset threshold	1	4	8	14	19	27

Table 1: The largest reset thresholds of n-state automata two permutation letters generating S_n and one letter of rank $n-1$

As n grows, the reset thresholds of the obtained examples become much smaller than $(n-1)^2$. We were unable to derive a series of n-state three-letter automata with the transition monoid T_n and quadratically growing reset thresholds. We suspect that the reset threshold of automata in this class is $o(n^2)$.

In the case of unbounded alphabet, for every n, we present an n-state automaton $\mathscr{V}_n$ with the transition monoid T_n such that $\mathrm{rt}(\mathscr{V}_n) = \frac{n(n-1)}{2}$. The state set of $\mathscr{V}_n$ is $Q_n = \{q_0, \ldots, q_{n-1}\}$ and the input alphabet consists of n letters $a_1, \ldots, a_n$. The transition function is defined as follows:

$$\begin{cases} q_i{\cdot}a_j = q_i & \text{for } 0 \le i < n,\ 1 \le j < n,\ i \ne j,\ i \ne j+1,\ j \ne n, \\ q_i{\cdot}a_i = q_{i-1} & \text{for } 0 < i \le n-1, \\ q_i{\cdot}a_{i+1} = q_{i+1} & \text{for } 0 \le i < n-1, \\ q_0{\cdot}a_n = q_1{\cdot}a_n = q_0, & \\ q_i{\cdot}a_n = q_i & \text{for } 2 \le i \le n-1. \end{cases}$$

Simply speaking, every letter a_i for $i \le n-1$ swaps the states q_i and q_{i-1} and fixes the other states. The letter a_n brings both q_0 and q_1 to q_0 and fixes the other states. The automaton $\mathscr{V}_5$ is depicted in Fig. 3.

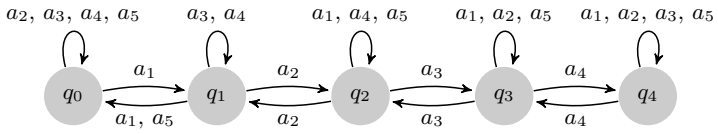

Fig. 3: The automaton $\mathscr{V}_5$

Recall that a state z of an DFA is said to be a *sink state* (or *zero*) if $z{\cdot}a = z$ for every input letter a. It is known that every n-state synchronizing automaton with zero can be reset by a word of length $\frac{n(n-1)}{2}$, cf. [31]. To show that this upper bound is tight for each n, Rystsov [31] constructed an n-state and $(n-1)$-letter synchronizing automaton $\mathscr{R}_n$ with zero which cannot be reset by any word of length less than $\frac{n(n-1)}{2}$. In fact, our automaton $\mathscr{V}_n$ is a slight modification of $\mathscr{R}_n$ as the latter automaton is nothing but $\mathscr{V}_n$ without the letter a_1.

Theorem 4. *For every n, the automaton $\mathscr{V}_n$ has T_n as its transition monoid and* $\mathrm{rt}(\mathscr{V}_n) = \frac{n(n-1)}{2}$.

Proof. The letters $a_1, \ldots, a_{n-1}$ generate S_n because the product $a_1 \cdots a_{n-1}$ is a full cycle and any full cycle together with any transposition generates S_n. Since the letter a_n has rank $n-1$, it together with $a_1, \ldots, a_{n-1}$ generates T_n.

The automaton $\mathscr{V}_n$ is synchronizing because so is the restricted automaton $\mathscr{R}_n$, and $\mathrm{rt}(\mathscr{V}_n) \leq \frac{n(n-1)}{2}$ because every reset word for $\mathscr{R}_n$ resets $\mathscr{V}_n$ as well. It remains to verify that the length of any reset word for $\mathscr{V}_n$ must be at least $\frac{n(n-1)}{2}$. Let w be a reset word of minimum length for $\mathscr{V}_n$. Since a_n is the only non-permutation letter, we must have $w = w'a_n$ for some w' such that $|Q_n{\cdot}w'| > 1$. This is only possible when $Q_n{\cdot}w' = \{q_0, q_1\}$ whence $Q_n{\cdot}w = \{q_0\}$. Consider the function f from the set of all non-empty subsets of Q_n into the set of non-negative integers defined as follows: if $S = \{q_{s_1}, \ldots, q_{s_t}\}$, then $f(S) = \sum_{i=1}^{t} s_i$. Clearly, $f(\{q_0\}) = 0$ and $f(Q_n) = \frac{n(n-1)}{2}$. For any set S and any letter a_j, we have $f(S{\cdot}a_j) \geq f(S) - 1$ since each letter only exchanges two adjacent states or maps q_1 and q_0 to q_0. Thus, when we apply the word w letter-by-letter, the value of f after the application of the prefix of w of length i cannot be less than $\frac{n(n-1)}{2} - i$. Hence, to reach the value 0, we need at least $\frac{n(n-1)}{2}$ letters. □

2.3. Upper Bound on the Reset Threshold. We now provide a quadratic upper bound on the reset words of automata with the transition monoid equal to T_n. Our proof is inspired by the method of Rystsov [32] adapted to our case.

Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a DFA. Given a proper non-empty subset $R \subset Q$ and a word w over Σ, we say that R *can be extended by* w if the cardinality of the set $Rw^{-1} = \{q \in Q \mid q{\cdot}w \in R\}$ is greater than $|R|$. Now assume that $|Q| = n$ and the transition monoid of $\mathscr{A}$ coincides with the full transformation monoid T_n. Then there is a letter x of rank $n-1$. The set $Q \setminus Q{\cdot}x$ consists of a unique state, which is called the *excluded state* for x and is denoted by $\mathrm{excl}(x)$. Furthermore, the set $Q{\cdot}x$ contains a unique state p such that $p = q_1{\cdot}x = q_2{\cdot}x$ for some $q_1 \neq q_2$; this state p is called the *duplicate state* for x and is denoted by $\mathrm{dupl}(x)$. We notice that a non-empty subset $R \subset Q$ can be extended by x if and only if $\mathrm{dupl}(x) \in R$ and $\mathrm{excl}(x) \notin R$. Moreover, if a word w is a product of permutation letters, R can be extended by the word wx if and only if $\mathrm{dupl}(x) \in Rw^{-1}$ and $\mathrm{excl}(x) \notin Rw^{-1}$. To better understand which extensions are possible, we construct a series of directed graphs (digraphs) Γ_i, $i = 0, 1, \ldots$, with the set Q as the vertex set.

The digraph Γ_0 has the set $E_0 = \{(\mathrm{excl}(x), \mathrm{dupl}(x))\}$ as its edge set. Let Π be the set of permutation letters of $\mathscr{A}$. Notice that Π generates the symmetric group S_n. By Π^i we denote the set of words of length at most i over the letters in Π. The digraph Γ_i for $i > 0$ has the edge set $E_i = \{(\mathrm{excl}(x){\cdot}w, \mathrm{dupl}(x){\cdot}w) \mid w \in \Pi^i\}$. The digraphs Γ_i, $i = 0, 1, \ldots$, form a sort of stratification for the graph Γ_∞ with the edge set $E_\infty = \cup_{i=0}^{\infty} E_i$; the latter digraph has been studied in [32] and [6] (in the context of arbitrary completely reachable automata). Observe that none of the digraphs Γ_i, $i = 0, 1, \ldots$, have loops.

Recall that a digraph is said to be *strongly connected* if for every pair of its vertices, there exists a directed path from the first vertex to the second. We need the two following lemmas.

Lemma 5. *If the digraph Γ_k is strongly connected, then every proper non-empty subset in Q can be extended by a word of length at most $k+1$.*

Proof. let R be a proper non-empty subset in Q. If Γ_k is strongly connected, there exists an edge $(q,p) \in E_k$ that connects $Q \setminus R$ and R in the sense that $q \in Q \setminus R$ while $p \in R$. As $(q,p) \in E_k$, there exists a word $w \in \Pi^k$ such that $(q,p) = (\mathrm{excl}(x)\cdot w, \mathrm{dupl}(x)\cdot w)$. Then $\mathrm{dupl}(x) \in Rw^{-1}$ and $\mathrm{excl}(x) \notin Rw^{-1}$, whence the word xw extends R and has length at most $k+1$. □

Lemma 6. *The digraph Γ_{2n-3} is strongly connected.*

Proof. We start with showing that the digraph Γ_{n-1} contains an oriented cycle.

Consider the underlying digraph Δ of the automaton $\langle Q, \Pi, \delta|_{Q\times\Pi}\rangle$, i.e., the digraph with the vertex set Q and the edge set $\{(q, q\cdot a) \mid q \in Q,\, a \in \Pi\}$. This digraph is strongly connected since Π generates the whole symmetric group S_n. Therefore, for every $q \in Q\cdot x$, there exists a directed path in Δ from $\mathrm{excl}(x)$ to q. If one takes such a path $\mathrm{excl}(x) \xrightarrow{a_1} \cdots \xrightarrow{a_\ell} q$ of minimum length, it does not traverse any vertex in Q more than once, whence the length ℓ of the path is at most $n-1$. Thus, the word $u = a_1 \cdots a_\ell$ belongs to Π^{n-1} and the pair $(\mathrm{excl}(x)\cdot u, \mathrm{dupl}(x)\cdot u)$ is an outgoing edge of the vertex $q = \mathrm{excl}(x)\cdot u$ in the digraph Γ_{n-1}. We see that every state in $Q\cdot x$ has an outgoing edge in Γ_{n-1}. Now, we can walk along the edges of Γ_{n-1}, starting at $\mathrm{excl}(x)$, which has the outgoing edge $(\mathrm{excl}(x), \mathrm{dupl}(x))$, until we reach an already visited state, thus getting an oriented cycle in the graph.

If $\Gamma = (V, E)$ is a digraph, we say that a vertex $v' \in V$ is *reachable* from a vertex $v \in V$ if either $v' = v$ or there is a directed path from v to v'. The mutual reachability relation is an equivalence on the set V, and the digraphs induced on the classes of the mutual reachability relation are either strongly connected or singletons (i.e., digraphs with 1 vertex and no edge). Slightly abusing terminology, we call these induced digraphs (including singletons) the *strongly connected components* of the digraph Γ.

Consider the strongly connected components of the digraph Γ_{n-1} and let $C_1, \ldots, C_m$ denote their vertex sets. Without any loss we may assume that $|C_1| \geq |C_2| \geq \cdots \geq |C_m|$. Observe that $m < n$ since Γ_{n-1} contains an oriented cycle which is not a loop whence at least one strongly connected component is non-singleton. (Recall that digraphs of the form Γ_i are loopless.) If $m = 1$, then already the digraph Γ_{n-1} is strongly connected, and we are done. Otherwise we analyze the evolution of the partition of Γ_k with $k \geq n-1$ into strongly connected components under the action of the letters in Π. Since Π generates the symmetric group S_n, it cannot preserve any non-trivial partition of Q. Thus, there is a non-singleton component C among $C_1, \ldots, C_m$ and a letter a in Π

whose action sends two elements of C to different components, i.e. $C{\cdot}a \cap C_i \neq \varnothing$ and $C{\cdot}a \cap C_j \neq \varnothing$ for some $C_i \neq C_j$.

By the definition of the sets E_k, if $(p, q) \in E_{n-1}$, then $(p{\cdot}a, q{\cdot}a) \in E_n$. Therefore each edge from E_{n-1} that connects some vertices in C_s, $s = 1, \ldots, m$, translates into an edge from E_n that connects the images of these vertices in $C_s{\cdot}a$. Therefore, the digraphs of Γ_n induced on the sets $C_1{\cdot}a, \ldots, C_m{\cdot}a$ are either strongly connected or singletons. In particular, the digraph of Γ_n induced on $C{\cdot}a$ is strongly connected. Since $C{\cdot}a \cap C_i \neq \varnothing$ and $C{\cdot}a \cap C_j \neq \varnothing$, the digraph of Γ_n induced on the set $C{\cdot}a \cup C_i \cup C_j$ also is strongly connected. This implies that the number m' of strongly connected components in Γ_n is less than m. If Γ_n is not yet strongly connected, the same reasoning applied to its strongly connected components, shows that the number of strongly connected components in Γ_{n+1} is less than m', etc.

Since at each step the number of strongly connected components is reduced at least by 1, we conclude that we reach a strongly connected digraph in at most $n-2$ steps. Therefore, Γ_{2n-3} is strongly connected. □

Theorem 7. *Let $\mathscr{A}$ be an n-state automaton with the transition monoid equal to T_n. The reset threshold of $\mathscr{A}$ is at most $2n^2 - 6n + 5$.*

Proof. Let x be a letter of rank $n-1$ and $h = \mathrm{dupl}(x)$. We extend the set $\{h\}$ by x, getting a subset R_2 with $|R_2| \geq 2$. Lemmas 5 and 6 imply that proper non-empty subsets in Q can be extended by words of length at most $2n-2$. Starting with R_2, we extend subsets until we reach the full state set. Let u_i be the word of length at most $2n-2$ used for the i-th of these extensions and let m be the number of the extensions. Observe that $m \leq n-2$. Clearly, the word $u_m \cdots u_1 x$ resets $\mathscr{A}$ and has the length at most $1 + (n-2)(2n-2) = 2n^2 - 6n + 5$. □

Remark 8. Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be an n-state DFA that has a letter of rank $n-1$, and let P be the subgroup of the symmetric group S_n generated by the permutation letters from Σ. Our proof of Theorem 7 actually works in the case if P is a *2-transitive* group, that is, P acts transitively on the set of ordered pairs of Q.

3 Bounds on the Diameter of the Pair Digraph

In this section we present a lower bound on the largest diameter of the pair digraph $P(A)$ for $A \subseteq S_n$. We proceed by presenting subsets $A \subseteq S_n$ for every odd n whose diameter is $\frac{n^2}{4} + o(n^2)$. In order to simplify the presentation, we mostly use automata terminology and describe the corresponding examples as a family of automata $\mathscr{F}_n = \langle Q_n, A, \delta \rangle$ (the input letters of $\mathscr{F}_n$ form the subset A). We let $Q_n = \{q_1, \ldots, q_n\}$ and denote pairs of states such as $\{q_i, q_j\}$ simply by $q_i q_j$.

The automaton $\mathscr{F}_7$ shown in Fig. 4 is the first of the family $\mathscr{F}_n$. The digraph of pairs of its states is shown in Fig. 5. One can verify that the shortest word mapping q_2q_4 to q_4q_7 has length 15.

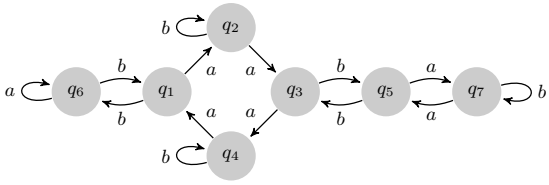

Fig. 4: The automaton $\mathscr{F}_7$

The automata of the family are obtained recursively, starting with $\mathscr{F}_7$. From $\mathscr{F}_n$, we construct $\mathscr{F}_{n+2}$. The effect of the letters is the same for the states $q_1, \ldots, q_{n-2}$ in $\mathscr{F}_n$ and $\mathscr{F}_{n+2}$. The effect of the letters a and b at the states q_{n-1}, q_n, q_{n+1} and q_{n+2} is defined as follows: the letters mapping q_{n-1} and q_n to themselves in $\mathscr{F}_n$ exchange q_{n-1} with q_{n+1} and q_n with q_{n+2} respectively in $\mathscr{F}_{n+2}$. The other letter maps q_{n+1} and q_{n+2} to themselves and q_{n-1}, q_n to q_{n-3} and respectively q_{n-2}. The result is shown in Fig. 6 (for $n \equiv 3 \pmod 4$), in which k stands for $\frac{n-5}{2}$.

Theorem 9. *For odd $n \geq 7$, the diameter of the pair digraph of the automaton $\mathscr{F}_n$ is at least $\frac{n^2}{4} + o(n^2)$.*

Proof sketch. For the automaton $\mathscr{F}_n$ ($n > 7$, $n \equiv 3 \pmod 4$), we claim that any word mapping q_2q_4 to $q_{k+2}q_{k+4}$ with $k = \frac{n-5}{2}$ has length at least $\frac{n^2}{4} + \frac{5n}{4} - 7$. For this, we define a function N which associates a non-negative integer $N(q_iq_j)$ to each pair q_iq_j, $i < j$. This function is such that if a pair q_iq_j is mapped by a or b to a pair $q_{i'}q_{j'}$, then $N(q_{i'}q_{j'}) \geq N(q_iq_j) - 1$. This implies that if $(q_iq_j)\cdot w = q_sq_t$ for some word w, then the length of w is at least $N(q_iq_j) - N(q_sq_t)$. The number assigned to $q_{k+2}q_{k+4}$ is 0, while the number given to q_2q_4 is equal to $\frac{n^2}{4} + \frac{5n}{4} - 7$, thus, the claim holds.

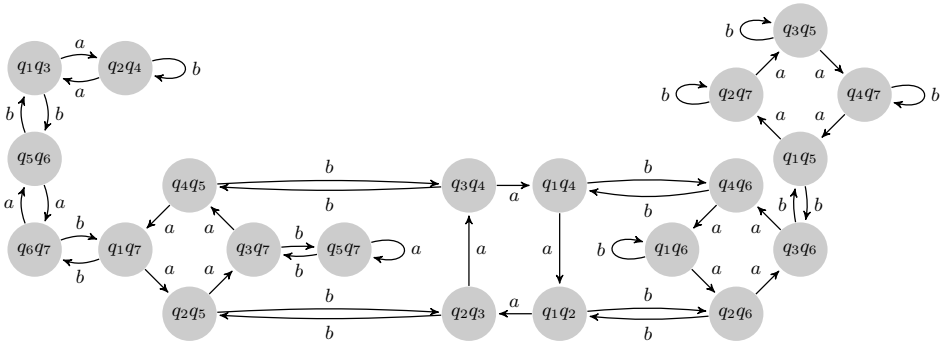

Fig. 5: The pair digraph of $\mathscr{F}_7$

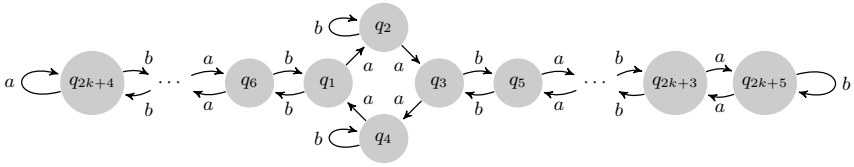

Fig. 6: The automaton $\mathscr{F}_{2k+5}$, with k odd

In addition, we describe a word of length $\frac{n^2}{4} + \frac{5n}{4} - 7$ that maps q_2q_4 to $q_{k+2}q_{k+4}$. Therefore $\frac{n^2}{4} + \frac{5n}{4} - 7$ is the exact value of the "distance" between these two particular pairs.

A similar argument holds for $n \equiv 1 \pmod 4$, with the distance between two particular pairs of states being at least $\frac{n^2}{4} + \frac{5n}{4} - 7.5$. □

Proof. Recall that we aim to define a function N which associates an integer $N(q_iq_j) \geq 0$ to each pair q_iq_j, $i < j$, and has the following property:

$$\text{if } q_iq_j \text{ is mapped by } a \text{ or } b \text{ to a pair } q_{i'}q_{j'}, \text{ then } N(q_{i'}q_{j'}) \geq N(q_iq_j) - 1. \quad (3)$$

For an illustration, see Fig. 7 which presents the pair digraph of the automaton $\mathscr{F}_7$ with the values of the corresponding function N shown at each vertex.

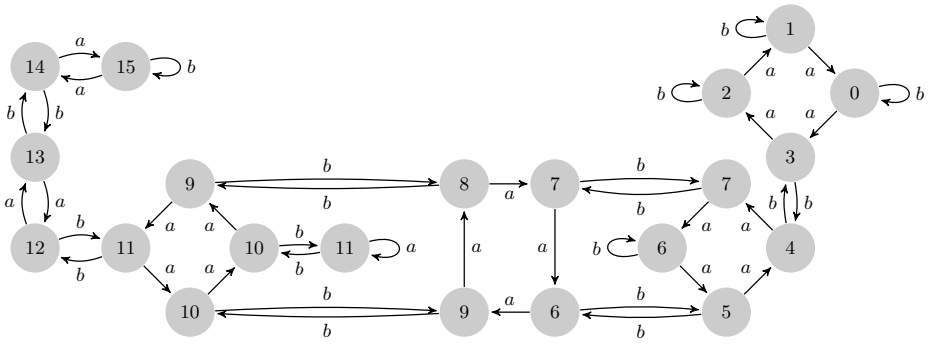

Fig. 7: The pair digraph of $\mathscr{F}_7$, with function values

For $n > 7$, $n \equiv 3 \pmod 4$, the values of the function N are provided in the two lists below. Some of the formulas in the lists involve one or two positive integer parameters denoted by m and m'. We always use m' for the index of the first state of a pair and m for the index of the second state; we do not specify the ranges of these parameters as they should be clear from the context. We use the following conventions: $k = \frac{n-5}{2}$, $N_1 = \frac{k+3}{2}$, $N_2 = (k+4)(k-1)$.

Our first list contains the values of N for the pairs that involve one or two of the "central" states q_1, q_2, q_3, q_4 of the automaton $\mathscr{F}_n$ or one or two of its "extreme" states q_{2k+4} and q_{2k+5}. (Our terminology follows the pictorial presentation of $\mathscr{F}_n$ in Fig. 6.)

- $N(q_1q_2) = N_1 + N_2 + 2k + 1$;
- $N(q_1q_3) = N_1 + N_2 + 4k + 7$;
- $N(q_1q_4) = N_1 + N_2 + 2k + 2$;
- $N(q_1q_{4m+1}) = \begin{cases} \frac{k+3}{2} & \text{if } m = N_1 - 1, \\ N_1 + (k+4)(k-2m-1) + 2k + 3 & \text{otherwise;} \end{cases}$
- $N(q_1q_{4m+2}) = N_1 + (k+4)(k-2m-1) + 2k - 2m + 2$;
- $N(q_1q_{4m+3}) = \begin{cases} N_1 + N_2 + 2k + 6 & \text{if } m = 1, \\ N_1 + (k+4)(k-2m+1) + 2k + 8 & \text{otherwise;} \end{cases}$
- $N(q_1q_{4m+4}) = N_1 + (k+4)(k-2m+1) + 2k - 2m + 3$;
- $N(q_1q_{2k+4}) = N_1 + k + 2$;
- $N(q_1q_{2k+5}) = N_1 + 2k + 8$;

- $N(q_2q_3) = N_1 + N_2 + 2k + 4$;
- $N(q_2q_4) = N_1 + N_2 + 4k + 8$;
- $N(q_2q_{4m+1}) = \begin{cases} N_1 + N_2 + 2k + 5 & \text{if } m = 1, \\ N_1 + (k+4)(k-2m+1) + 2k + 7 & \text{otherwise;} \end{cases}$
- $N(q_2q_{4m+2}) = N_1 + (k+4)(k-2m+1) + 2k - 2m + 2$;
- $N(q_2q_{4m+3}) = N_1 + (k+4)(k-2m-1) + 2k + 6$;
- $N(q_2q_{4m+4}) = N_1 + (k+4)(k-2m-1) + 2k - 2m + 1$;
- $N(q_2q_{2k+4}) = N_1 + k + 1$;
- $N(q_2q_{2k+5}) = N_1 - 1$;

- $N(q_3q_4) = N_1 + N_2 + 2k + 3$
- $N(q_3q_{4m+1}) = \begin{cases} \frac{k-1}{2} & \text{if } m = N_1 - 1, \\ N_1 + (k+4)(k-2m-1) + 2k + 5 & \text{otherwise;} \end{cases}$
- $N(q_3q_{4m+2}) = N_1 + (k+4)(k-2m-1) + 2k - 2m + 4$;
- $N(q_3q_{4m+3}) = \begin{cases} N_1 + N_2 + 2k + 5 & \text{if } m = 1, \\ N_1 + (k+4)(k-2m+1) + 2k + 6 & \text{otherwise;} \end{cases}$
- $N(q_3q_{4m+4}) = N_1 + (k+4)(k-2m+1) + 2k - 2m + 1$;
- $N(q_3q_{2k+4}) = N_1 + k$;
- $N(q_3q_{2k+5}) = N_1 + 2k + 6$;

- $N(q_4q_{4m+1}) = \begin{cases} N_1 + N_2 + 2k + 4 & \text{if } m = 1, \\ N_1 + (k+4)(k-2m+1) + 2k + 5 & \text{otherwise;} \end{cases}$
- $N(q_4q_{4m+2}) = N_1 + (k+4)(k-2m+1) + 2k - 2m + 4$;
- $N(q_4q_{4m+3}) = N_1 + (k+4)(k-2m-1) + 2k + 4$;
- $N(q_4q_{4m+4}) = N_1 + (k+4)(k-2m-1) + 2k - 2m + 3$;
- $N(q_4q_{2k+4}) = N_1 + k + 3$;

- $N(q_4 q_{2k+5}) = N_1 + 1$;
- $N(q_{4m'+1} q_{2k+4}) = \begin{cases} N_1 + N_2 + 3k + 7 & \text{if } 2m' = k+1, \\ N_1 + (k+4)(2m') + k + 1 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+1} q_{2k+5}) = \begin{cases} N_1 + (k+4)(2m'-2) + 2k + 4 + 2m' & \text{if } m' = N_1 - 1; \\ N_1 + (k+4)(2m'-2) + 2k + 5 + 2m' & \text{otherwise;} \end{cases}$
- $N(q_{4m'+2} q_{2k+4}) = N_1 + (k+4)2m' + k + 1 + 4m'$;
- $N(q_{4m'+2} q_{2k+5}) = \begin{cases} N_1 + 2k + 9 & \text{if } m' = 1, \\ N_1 + N_2 + 2k + m' + 8 & \text{if } 2m' = k+1, \\ N_1 + (k+4)(2m'-2) + 2k + 2m' + 7 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+3}, q_{2k+4}) = N_1 + (k+4)(2m') + k$;
- $N(q_{4m'+3} q_{2k+5}) = \begin{cases} N_1 + (k+4)(2m') + 2k + 2m' + 5 & \text{if } 2m' = k-1, \\ N_1 + (k+4)(2m') + 2k + 2m' + 6 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+4} q_{2k+4}) = N_1 + (k+4)2m' + k + 2 + 4m'$;
- $N(q_{4m'+4}, q_{2k+5}) = \begin{cases} N_1 + N_2 + 3k + 5 & \text{if } 2m' = k-1, \\ N_1 + (k+4)(2m') + 2k + 2m' + 8 & \text{otherwise;} \end{cases}$
- $N(q_{2k+4} q_{2k+5}) = N_1 + N_2 + 3k + 6$.

Our second list contains the values of N for the remaining pairs. In addition to our earlier conventions, we also use $M = m + m'$ and $M' = m - m'$ here.

- $N(q_{4m'+1} q_{4m+1}) = N_1 + (k+4)(k - 2M' + 1) + 2k + 2m' + 5$;
- $N(q_{4m'+1} q_{4m+2}) = \begin{cases} N_1 + N_2 + 4k + 8 - 2m & \text{if } m' = m, \\ N_1 + (k+4)(k - 2M' + 1) + 2k - 2m + 2 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+1} q_{4m+3}) = \begin{cases} N_1 + (k+4)(k - 2M - 1)) + 2k + 2m' + 4 & \text{if } 2M < k+1; \\ \frac{4m-k-1}{2} & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M - k - 3) + 2k + 2m' + 5 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+1} q_{4m+4}) = \begin{cases} N_1 + (k+4)(k - 2M - 1) + 2k - 2m + 3 & \text{if } 2M < k+1; \\ N_1 + 2m & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M - k - 3) + 2k + 2m + 8 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+2} q_{4m+1}) = \begin{cases} N_1 + N_2 + 2k + 2m' + 5 & \text{if } m' = m - 1, \\ N_1 + (k+4)(k - 2M' + 1) + 2k + 2m' + 7 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+2} q_{4m+2}) = N_1 + (k+4)(k - 2M' + 1) + 2k - 2m + 4m' + 2$;
- $N(q_{4m'+2} q_{4m+3}) = \begin{cases} N_1 + (k+4)(k - 2M - 1) + 2k - 2m + 4 & \text{if } 2M < k+1; \\ N_1 + 2m' - 1 & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M - k - 3) + 2k + 2m' + 7 & \text{otherwise;} \end{cases}$
- $N(q_{4m'+2} q_{4m+4}) = \begin{cases} N_1 + (k+4)(k - 2M - 1) + 2k - 2m' + 1 & \text{if } 2M < k+1; \\ N_1 + k + 2m' + 1 & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M - k - 1) + 4m' + 2m & \text{otherwise;} \end{cases}$

– $N(q_{4m'+3}q_{4m+1}) = \begin{cases} N_1 + (k+4)(k-2M-1)) + 2k + 2m' + 5 & \text{if } 2M < k+1; \\ \frac{4m-k-3}{2} & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M-k-3) + 2k + 2m' + 6 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+3}q_{4m+2}) = \begin{cases} N_1 + (k+4)(k-2M+1) + 2k - 2m + 4 & \text{if } 2M < k+1; \\ N_1 + 2m - 1 & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M-k-3) + 2k + 2m + 7 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+3}q_{4m+3}) = \begin{cases} N_1 + (k+4)(k-2M'+1) + 2k + 2m + 3 & \text{if } m = m'+1, \\ N_1 + (k+4)(k-2M'+1) + 2k + 2m' + 6 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+3}q_{4m+4}) = \begin{cases} N_1 + N_2 + 4k + 7 - 2m & \text{if } m' = m, \\ N_1 + (k+4)(k-2M'+1) + 2k - 2m + 1 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+4}q_{4m+1}) = \begin{cases} N_1 + (k+4)(k-2M-1) + 2k - 2m' + 3 & \text{if } 2M < k+1; \\ N_1 + 2m' & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M-k-3) + 2k + 2m' + 8 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+4}, q_{4m+2}) = \begin{cases} N_1 + (k+4)(k-2M-1) + 2k - 2m' + 1 & \text{if } 2M < k+1; \\ N_1 + k + 2m' + 2 & \text{if } 2M = k+1; \\ N_1 + (k+4)(2M-k-1) + 4m + 2m' - 1 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+4}q_{4m+3}) = \begin{cases} N_1 + N_2 + 2k + 2m' + 6 & \text{if } m = m'+1, \\ N_1 + (k+4)(k-2M'+1) + 2k + 2m' + 8 & \text{otherwise;} \end{cases}$

– $N(q_{4m'+4}q_{4m+4}) = N_1 + (k+4)(k-2M'+1) + 2k - 2m + 4m' + 3.$

It can be routinely verified that the function N defined this way satisfies (3). Therefore the shortest word mapping q_2q_4 to $q_{k+2}q_{k+4}$ is at least $N(q_2q_4) - N(q_{k+2}q_{k+4})$ letters long. Unfolding the definition, we obtain $N(q_{k+2}q_{k+4}) = 0$ and

$$N(q_2q_4) = N_1 + N_2 + 4k + 8 = \frac{k+3}{2} + (k+4)(k-1) + 4k + 8 \\ = k^2 + \frac{15k}{2} + \frac{11}{2} = \frac{n^2}{4} + \frac{5n}{4} - 7.$$

In addition, Table 2 provides the construction for a word of length $\frac{n^2}{4} + \frac{5n}{4} - 7$ which maps q_2q_4 to $q_{k+2}q_{k+4}$. The word is composed of several factors being labels of a certain segments of the directed path from q_2q_4 to $q_{k+2}q_{k+4}$ in the pair digraph of the automaton $\mathscr{F}_n$. For each segment we give its start and end pairs as well as its label and length. There are 4 "starting" factors of total length $4k + 8$, followed by $2(k-1)$ "inner" factors, forming $\frac{k-1}{2}$ words of total length $2k+8$ each, and 2 "finishing" factors of total length $\frac{k+3}{2}$. Altogether they indeed form a word of length

$$4k + 8 + k^2 + 3k - 4 + \frac{k+3}{2} = k^2 + \frac{15k}{2} + \frac{11}{2} = \frac{n^2}{4} + \frac{5n}{4} - 7.$$

Start pair	End pair	Factor	Length of the factor	Sum of lengths of factors within the group
q_2q_4	q_1q_3	a	1	
q_1q_3	q_1q_7	$(ba)^kb$	$2k+1$	
q_1q_7	q_3q_8	aba^3ba	7	
q_3q_8	q_1q_{11}	$(ba)^{k-1}b$	$2k-1$	
				$4k+8$
q_1q_{11}	q_1q_5	a^3ba	5	
q_1q_5	q_3q_6	b	1	
q_3q_6	q_3q_{12}	a^3ba	5	
q_3q_{12}	q_1q_{15}	$(ba)^{k-2}b$	$2k-3$	
q_1q_{15}	q_1q_9	a^3ba	5	
q_1q_9	q_3q_{10}	bab	3	
q_3q_{10}	q_3q_{16}	a^3ba	5	
q_3q_{16}	q_1q_{19}	$(ba)^{k-3}b$	$2k-5$	
$\dots$	$\dots$	$\dots$	$\dots$	
q_1q_{2k+1}	q_1q_{2k-5}	a^3ba	5	
q_1q_{2k-5}	q_3q_{2k-4}	$(ba)^{\frac{k-5}{2}}b$	$k-4$	
q_3q_{2k-4}	q_3q_{2k+2}	a^3ba	5	
q_3q_{2k+2}	q_1q_{2k+5}	$(ba)^{\frac{k+1}{2}}b$	$k+2$	
q_1q_{2k+5}	q_1q_{2k-1}	a^3ba	5	
q_1q_{2k-1}	q_3q_{2k}	$(ba)^{\frac{k-3}{2}}b$	$k-2$	
q_3q_{2k}	q_3q_{2k+4}	a^3ba	5	
q_3q_{2k+4}	q_1q_{2k+3}	$(ba)^{\frac{k-1}{2}}b$	k	
				$(2k+8)\frac{k-1}{2}$ $= k^2+3k-4$
q_1q_{2k+3}	q_3q_{2k+3}	a^2	2	
q_3q_{2k+3}	$q_{k+2}q_{k+4}$	$(ba)^{\frac{k-3}{4}}b$	$\frac{k-1}{2}$	
				$\frac{k+3}{2}$

Table 2: Construction of a word bringing q_2q_4 to $q_{k+2}q_{k+4}$

Our numerical experiments confirm that $\frac{n^2}{4}+\frac{5n}{4}-7$ is indeed the diameter of the pair graph of the automaton $\mathscr{F}_n$ for $n \equiv 3 \pmod 4$ from $n=11$ to $n=31$ while $\frac{n^2}{4}+\frac{5n}{4}-7.5$ is the exact value of the diameter for $n \equiv 1 \pmod 4$ from $n=13$ to $n=29$.

We have also computed the largest diameter of the pair digraph $P(A)$ for all $A \subseteq S_n$ with $|A| = 2$ and $n = 5, 7, 9$ and performed a number of random sampling experiments with two permutations for larger values of n. The experimental results suggest that the pair digraph of the automaton $\mathscr{F}_n$ has the largest diameter among all possible pair digraphs. Thus, we formulate the following:

Conjecture 3 *The diameter of the pair digraph for a subset of S_n is bounded above by $\frac{n^2}{4} + o(n^2)$.*

Conclusion

We studied the hybrid Babai–Černý problem, where the question is to find tight bounds on the reset threshold for automata with the full transition monoid. We presented a series of n-state automata $\mathscr{V}_n$ in this class with the reset threshold equal to $\frac{n(n-1)}{2}$, thus establishing a lower bound for the problem, and found an upper bound with the same growth rate, namely, $2n^2+o(n^2)$. We also described a series of n-state automata with diameter of the pair digraph equal to $\frac{n^2}{4} + o(n^2)$.

For follow-up work, one direction is to refine the bounds with respect to the constants that do not match yet. Also, a lower bound for the hybrid problem using only three letters (generators) is of interest, since the number of letters of the presented family $\mathscr{V}_n$ is equal to the number of states.

References

1. Ananichev, D.S., Gusev, V.V., Volkov, M.V.: Primitive digraphs with large exponents and slowly synchronizing automata. J. Math. Sci. 192(3), 2635–278 (2013)
2. Ananichev, D.S., Volkov, M.V.: Some results on Černy type problems for transformation semigroups. In: Araújo, I.M., Branco, M.J.J., Fernandes, V.H., Gomes, G.M.S. (eds.) Semigroups and Languages. pp. 23–42. World Scientific (2004)
3. Araújo, J., Cameron, P.J., Steinberg, B.: Between primitive and 2-transitive: Synchronization and its friends. CoRR abs/1511.03184 (2015)
4. Babai, L., Seress, A.: On the diameter of permutation groups. European J. Combinatorics 13(4), 231–243 (1992)
5. Berstel, J., Perrin, D., Reutenauer, C.: Codes and Automata. CUP (2009)
6. Bondar, E.A., Volkov, M.V.: Completely reachable automata. In: Câmpeanu, C., Manea, F., Shallit, J. (eds.) DCFS 2016. LNCS, vol. 9777, pp. 1–17. Springer (2016)
7. Brzozowski, J.A.: In search of most complex regular languages. Int. J. Found. Comput. Sci. 24(6), 691–708 (2013)
8. Cameron, P.J.: Dixon's theorem and random synchronization. Discrete Math. 313(11), 1233–1236 (2013)
9. Černý, J.: Poznámka k homogénnym experimentom s konečnými automatami. Mat.-fyz. Časopis Slovenskej Akadémie Vied 14(3), 208–216 (1964), in Slovak
10. Černý, J., Pirická, A., Rosenauerová, B.: On directable automata. Kybernetica 7, 289–298 (1971)
11. Chevalier, P.Y., Hendrickx, J.M., Jungers, R.M.: Reachability of consensus and synchronizing automata. In: 54th IEEE Conf. on Decision and Control (CDC). pp. 4139–4144. IEEE (2015)

12. Dixon, J.D.: The probability of generating the symmetric group. Math. Z. 110, 199–205 (1969)
13. Don, H.: The Černý conjecture and 1-contracting automata. Electr. J. Comb. 23(3), P3.12 (2016)
14. Dubuc, L.: Sur les automates circulaires et la conjecture de Černý. RAIRO Informatique Théorique et Applications 32, 21–34 (1998), in French
15. Frankl, P.: An extremal problem for two families of sets. European J. Combinatorics 3, 125–127 (1982)
16. Frettlöh, D., Sing, B.: Computing modular coincidences for substitution tilings and point sets. Discrete Comput. Geom. 37, 381–407 (2007)
17. Friedman, J., Joux, A., Roichman, Y., Stern, J., Tillich, J.P.: The action of a few permutations on r-tuples is quickly transitive. Random Structures & Algorithms 12(4), 335–350 (1998)
18. Ganyushkin, O., Mazorchuk, V.: Classical Finite Transformation Semigroups: An Introduction. Springer (2009)
19. Gerencsér, B., Gusev, V.V., Jungers, R.M.: Primitive sets of nonnegative matrices and synchronizing automata. CoRR abs/1602.07556 (2016)
20. Gonze, F., Jungers, R.M.: On the synchronizing probability function and the triple rendezvous time for synchronizing automata. SIAM J. Discrete Math. 30(2), 995–1014 (2016)
21. Grech, M., Kisielewicz, A.: The Černý conjecture for automata respecting intervals of a directed graph. Discrete Math. & Theoret. Comput. Sci. 15(3), 61–72 (2013)
22. Helfgott, H.A., Seress, A.: On the diameter of permutation groups. Ann. Math. (2) 179(2), 611–658 (2014)
23. Helfgott, H.A.: Growth in groups: ideas and perspectives. Bull. Amer. Math. Soc. (N.S.) 52(3), 357–413 (2015)
24. Kari, J.: Synchronizing finite automata on Eulerian digraphs. Theoret. Comput. Sci. 295, 223–232 (2003)
25. Klyachko, A.A., Rystsov, I.K., Spivak, M.A.: An extremal combinatorial problem associated with the bound on the length of a synchronizing word in an automaton. Cybernetics and System Analysis 23(2), 165–171 (1987)
26. Maslennikova, M.: Reset complexity of ideal languages. In: Bieliková, M. (ed.) SOFSEM 2012. Proc. Institute of Computer Science Academy of Sciences of the Czech Republic. vol. II, pp. 33–44 (2012)
27. Natarajan, B.K.: An algorithmic approach to the automated design of parts orienters. In: 27th FOCS. pp. 132–142. IEEE (1986)
28. Natarajan, B.K.: Some paradigms for the automated design of parts feeders. Int. J. Robotics Research 8(6), 89–109 (1989)
29. Panteleev, P.: Preset distinguishing sequences and diameter of transformation semigroups. In: Dediu, A.H., Formenti, E., Martín-Vide, C., Truthe, B. (eds.) LATA 2015. LNCS, vol. 8977, pp. 353–364. Springer (2015)
30. Pin, J.E.: On two combinatorial problems arising from automata theory. Ann. Discrete Math. 17, 535–548 (1983)
31. Rystsov, I.K.: Reset words for commutative and solvable automata. Theoret. Comput. Sci. 172(1), 273–279 (1997)
32. Rystsov, I.K.: Estimation of the length of reset words for automata with simple idempotents. Cybernetics and Systems Analysis 36(3), 339–344 (2000)
33. Saloff-Coste, L.: Random walks on finite groups. In: Kesten, H. (ed.) Probability on Discrete Structures. pp. 263–346. Springer (2004)
34. Salomaa, A.: Composition sequences for functions over a finite domain. Theoret. Comput. Sci. 292(1), 263–281 (2003)

35. Steinberg, B.: The averaging trick and the Černý conjecture. Int. J. Found. Comput. Sci. 22(7), 1697–1706 (2011)
36. Steinberg, B.: The Černý conjecture for one-cluster automata with prime length cycle. Theoret. Comput. Sci. 412(39), 5487–5491 (2011)
37. Szykuła, M.: Improving the upper bound the length of the shortest reset words. CoRR abs/1702.05455 (2017)
38. 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 (2008)
39. Vorel, V.: Subset synchronization of transitive automata. In: Ésik, Z., Fülöp, Z. (eds.) AFL 2014. EPTCS, vol. 151, pp. 370–381 (2014)
40. Zubov, A.Y.: On the diameter of the group S_N with respect to a system of generators consisting of a complete cycle and a transposition. Tr. Diskretn. Mat. 2, 112–150 (1998), in Russian