



Fast synchronization of inhomogenous random automata

Balázs Gerencsér^{a,b,1}, Zsombor Várkonyi^{b,*,2}

^a Alfred Renyi Institute of Mathematics, Reáltanoda utca 13-15, 1053, Budapest, Hungary

^b Institute of Mathematics, Eotvos Lorand University, Pazmany Peter setany 1/C, 1117, Budapest, Hungary

ARTICLE INFO

Article history:

Received 16 February 2023

Received in revised form 2 October 2023

Accepted 30 November 2023

Available online 5 December 2023

Keywords:

Random deterministic automata

Fast synchronization

Transitivity

ABSTRACT

We examine the reset threshold of randomly generated deterministic automata. We present a simple proof that an automaton with a random mapping and two random permutation letters has a reset threshold of $\mathcal{O}(\sqrt{n \log^3 n})$ with high probability, assuming only certain partial independence of the letters. Our observation is motivated by Nicaud (2019) providing a near-linear bound in the case of two random mapping letters, among multiple other results. The upper bound for the latter case has been recently improved by the breakthrough work of Chapuy and Perarnau (2023) to $\mathcal{O}(\sqrt{n \log n})$.

© 2023 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The synchronization of automata has been intensively studied in the literature since the sixties. Recently, a related area has been spotlighted, namely synchronizing random automata, viewing automata theory in a probabilistic way.

For a complete finite automaton, a word is called a *synchronizing word* if it maps to a state independent of the initial state. The *reset threshold* of an automaton with a synchronizing word is the length of its shortest synchronizing word. In 1964, Černý conjectured [3] that if an n -state automaton can be synchronized, then its reset threshold is at most $(n - 1)^2$. This is an open question ever since, however some partial results were proven over the years. In particular, this is a strict bound, meaning that for all $n \in \mathbb{N}$ there is an n -state automaton with reset threshold exactly $(n - 1)^2$. The best known upper bound was attained by Shitov [12] which improved the previous upper bound of Szykula [14]. Both of these results provide a bound of $\Theta(n^3)$ and only differ by the leading coefficient. The first cubic upper bound with leading coefficient in this regime near $1/6$ was reached by Pin and Frankl [11],[6].

A strongly related area of study is the investigation of randomly generated deterministic automata, in which the aim is to prove statements that hold with high probability for a certain class of automata. Most of these works concern automata with independent letters.

On the analytical side, Nicaud [10] showed that an automaton with at least two random mapping letters in its alphabet has reset threshold of $\mathcal{O}(n \log^3 n)$ with high probability. Nicaud and Berlinkov [1] also investigated almost-group random automata, which are automata on n states with $k - 1$ random permutation letters and one letter which is a permutation on $n - 1$ states. They proved that assuming being strongly connected, almost-group automata are synchronizing with high

* Corresponding author.

E-mail addresses: gerencser.balazs@renyi.hu (B. Gerencsér), zsvarkonyi@student.elte.hu (Z. Várkonyi).

¹ He was supported by NRDI (National Research, Development and Innovation Office) grant KKP 137490 and the János Bolyai Research Scholarship BO/00166/20 of the Hungarian Academy of Sciences.

² He was supported by the ÚNKP-21-6-ELTE-1153 New National Excellence Program of the Ministry for Innovation and Technology from the source of the NRDI Fund.

probability, i.e. failing to synchronize with probability $\frac{2^{k-1}-1}{n^{2(k-1)}}(1+o(1))$. Recent related results include the paper of Catalano and Jungers [2] in which the positivity of exponents of quasi-permutation matrices is examined and the breakthrough article of Chapuy and Perarnau [4] in which the long sought after $\mathcal{O}(\sqrt{n} \log n)$ upper bound is proved for random automata with two random mappings. Another interesting result stating that an automaton with two random mappings has a reset word of $\mathcal{O}(\varepsilon^{-1} \sqrt{n \log n})$ with probability $1 - \varepsilon$ for any $\varepsilon > 0$ was recently proved by Martinsson [9]. In terms of lower bounds, so far $\Omega(n^{1/3})$ is known, as spelled out in [4].

From a numerical perspective, Skvortsov and Tipikin performed an experimental study [13] and conjectured that the expected value of the reset threshold of an n -state finite automaton is sublinear, more precisely $\mathcal{O}(n^{0.55})$. Kisielewicz et al. examined [8] a large number of random automata up to at most 300 states and conjectured that the expected reset threshold of a random automaton with two random mappings is $\mathcal{O}(\sqrt{n})$. These results indicate that the upper bounds of [4], [9] are expected to be tight (up to logarithmic factors).

In this paper, we are going to examine a class of letter-inhomogenous random automata with some dependence structure allowed, and prove that for an n -state automaton of this class, its reset threshold is $\mathcal{O}(\sqrt{n \log^3 n})$ with high probability. This result remains interesting on its own even in view of a possible worst-case quadratic bound of the Černý conjecture as the target high probability bound is substantially lower.

2. Definitions and notations

A deterministic finite automaton is denoted by $\mathcal{A} = (Q, \Sigma, \delta)$ where the set of states is Q , the set of letters is Σ and the transition function of letters over the states is $\delta : Q \times \Sigma \rightarrow Q$. A word is a finite series of not necessarily distinct letters, formally words are the elements of Σ^k for arbitrary $k \in \mathbb{N}$. The transition function δ extends to words in a natural way. Automaton \mathcal{A} is called *synchronizing* if a word u exists such that the action of word u leaves the automaton in a state independent of the initial state, that is $\exists T_0 \in Q, \forall T \in Q : T_0 = \delta(T, u)$. A word u with this property is called a *synchronizing word*. A series of events $(A_n)_{n \in \mathbb{N}}$ is said to hold *with high probability* if $P(A_n) \rightarrow 1$ as n tends to infinity.

A randomly generated deterministic automaton can be built up by random letters of different nature. Let us present the different types of random letters we will be using.

Definition 1. Let us define *random mapping*, *random p-mapping* and *random permutation* as possible letters of a finite automaton. Let $Q = \{1, 2, \dots, n\}$.

- $f : Q \rightarrow Q$ is called a *random mapping* if $f(i)$ is chosen uniformly randomly from Q , independently for all $i = 1, 2, \dots, n$.
- Given a probability mass function p on Q , $g : Q \rightarrow Q$ is a *random p-mapping* if $g(i)$ is chosen from Q according to the probability p independently for all $i = 1, 2, \dots, n$.
- $h : Q \rightarrow Q$ is a *random permutation* if it is chosen uniformly randomly from the permutation group S_n .

Note that an automaton with random mapping, random p-mapping or random permutation letters still has deterministic actions for every realisation of the letters.

Considering the structure of random letters, we introduce the following concepts. For a random mapping f a state T is a *cyclic point* if $f^i(T) = T$ for some $i > 0$. The *height* of a state T is the smallest $i \geq 0$ such that $f^i(T)$ is a cyclic point. The height of f is maximal height among all states.

3. Tools

Before presenting our main result, let us cite two important lemmas which will be useful for us. The first one is about random mappings from Nicaud [10]:

Lemma 2 ([10], Lemma 4). *The probability that a random p-mapping of size n has more than $2\sqrt{n \log n}$ cyclic points or that it has height greater than $2\sqrt{n \log n}$ is $\mathcal{O}(\frac{1}{n})$.*

As a consequence, by repeating the same random p-mapping letter several times, the number of possible states can be significantly decreased with high probability. In [10] this lemma was used to prove that a random automaton with at least two random mapping letters in its alphabet has a reset threshold at most $\mathcal{O}(n \log^3 n)$ with high probability.

In their paper [7], Friedman and his coauthors proved a general statement about the transitivity properties of random permutations. Their result is the following:

Lemma 3 ([7], Theorems 2.2., 3.3.). *For every r and $d \geq 2$ there is a C such that for uniformly random choices of d permutations $\pi_1, \pi_2, \dots, \pi_d$ of S_n , the following holds with high probability: for any two r -tuples of distinct elements in $\{1, \dots, n\}$, there is a product of at most $C \log n$ of the given permutations which maps the first r -tuple to the second.*

4. Main result

Theorem 4. Let \mathcal{A} be a randomly generated deterministic complete automaton with $|Q| = n$ and $\Sigma = \{a, b, c\}$. Let a be a random mapping, b and c be random permutations such that b and c are independent. The reset threshold of \mathcal{A} is $\mathcal{O}(\sqrt{n \log^3 n})$ with high probability.

Remark 5. Let us highlight the most important differences between the model we investigate and the usual model of independent uniform random mappings. The independence of the two random permutations guarantees that our automaton is strongly connected with high probability [7], moreover generates S_n or A_n with high probability [5], neither of which holds for an automaton with three random mappings. The idea of using permutations is motivated by the work of Nicaud and Berlinkov [1].

Proof. Concerning Lemma 3, let us fix $d = r = 2$, with the resulting constant being C . Let R_n denote the event that both the conclusions of Lemma 2 and Lemma 3 hold true for our automaton. Since both conclusions hold with high probability, it follows that R_n holds with high probability as well. For simplicity, let us use the notation $H(n) = 2\sqrt{n \log n}$.

First we apply $a^{H(n)}$ to the entire set Q . By Lemma 2, after applying $a^{H(n)}$, the maximal number of possible states is $H(n)$ on R_n , from which we proceed as follows. Thanks to a contracting the original set of possible states, we may choose two states (P_1 and P_2) that are being merged by a . Formally, $\exists P_1, P_2 \in Q : \delta(P_1, a) = \delta(P_2, a)$.

We repeat the following procedure until the automaton is synchronized:

- We search for two different possible states of the automaton. If there is only one, then the automaton is synchronized and we are done. Let these two different states be named T_1, T_2 .
- Now we will map (T_1, T_2) pair to (P_1, P_2) pair. By Lemma 3 on R_n , we can do this step in $C \log n$ transitions.
- Now apply letter a and this reduces the number of possible states by at least one, since P_1 and P_2 are merged by a .

We have to repeat this process at most $H(n) - 1$ times as there were at most $H(n)$ possible states on R_n after applying $a^{H(n)}$. The upper bound for the number of letters needed is: $H(n) + (H(n) - 1)(C \log n + 1) \sim CH(n) \log n = \mathcal{O}(\sqrt{n \log^3 n})$. Here we calculated the length of the word using the idea of Lemma 2 in [10], namely that pairwise synchronization is sufficient for the entire automaton to be synchronized.

Note that the subset $\delta(Q, a^{H(n)})$ and the functions (b, c) might not be independent, but we only use the consequences of the lemmas via assuming R_n , no further structure is exploited. As this event holds with high probability, this confirms the claim. \square

CRedit authorship contribution statement

Balázs Gerencsér: Conceptualization, Formal analysis, Methodology, Writing – original draft, Writing – review & editing.
Zsombor Várkonyi: Conceptualization, Formal analysis, Methodology, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

We are grateful for the reviewers of our manuscript for their insightful comments and remarks.

References

- [1] Mikhail V. Berlinkov, Cyril Nicaud, Synchronizing almost-group automata, *Int. J. Found. Comput. Sci.* 31 (08) (2020) 1091–1112.
- [2] Costanza Catalano, Raphaël M. Jungers, On randomized generation of slowly synchronizing automata, in: *43rd International Symposium on Mathematical Foundations of Computer Science*, 2018.
- [3] Ján Černý, Poznámka k homogénnym experimentom s konečnými automatmi, *Mat.-Fyz. Čas.* 14 (3) (1964) 208–216.
- [4] Guillaume Chapuy, Guillem Perarnau, Short synchronizing words for random automata, in: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, SIAM, 2023, pp. 581–604.
- [5] John D. Dixon, The probability of generating the symmetric group, *Math. Z.* 110 (1969) 199–205.
- [6] P. Frankl, An extremal problem for two families of sets, *Eur. J. Comb.* 3 (2) (1982) 125–127.

- [7] Joel Friedman, Antoine Joux, Yuval Roichman, Jacques Stern, Jean-Pierre Tillich, The action of a few permutations on r -tuples is quickly transitive, *Random Struct. Algorithms* 12 (4) (1998) 335–350.
- [8] Andrzej Kisielewicz, Jakub Kowalski, Marek Szykuła, A fast algorithm finding the shortest reset words, in: *International Computing and Combinatorics Conference*, Springer, 2013, pp. 182–196.
- [9] Anders Martinsson, Synchronizing random automata through repeated inputs, arXiv preprint, arXiv:2306.09040, 2023.
- [10] Cyril Nicaud, The Černý conjecture holds with high probability, *J. Autom. Lang. Comb.* 24 (2–4) (2019) 343–365.
- [11] Jean-Eric Pin, On two combinatorial problems arising from automata theory, in: *North-Holland Mathematics Studies*, vol. 75, Elsevier, 1983, pp. 535–548.
- [12] Yaroslav Shitov, An improvement to a recent upper bound for synchronizing words of finite automata, *J. Autom. Lang. Comb.* 24 (2–4) (2019) 367–373.
- [13] Evgeny Skvortsov, Evgeny Tipikin, Experimental study of the shortest reset word of random automata, in: *International Conference on Implementation and Application of Automata*, Springer, 2011, pp. 290–298.
- [14] Marek Szykuła, Improving the upper bound on the length of the shortest reset words, in: *35th Symposium on Theoretical Aspects of Computer Science*, 2018.