Journal of Automata, Languages and Combinatorics **24** (2019) 2–4, 343 – 365
© Institut für Informatik · Justus-Liebig-Universität Giessen

# THE ČERNÝ CONJECTURE HOLDS WITH HIGH PROBABILITY

Cyril Nicaud

*Université Paris-Est, LIGM (UMR 8049), CNRS, ENPC, ESIEE Paris, UPEM,*
*5 bd Descartes, 77454 Marne-la-Vallée, France*
Cyril.Nicaud@u-pem.fr

ABSTRACT

An automaton is synchronizing when there is a word that brings every state into one and the same state. Such a word is called a synchronizing word, and Černý conjectured in 1964 that if a $n$-state deterministic automaton is synchronizing, then it has a synchronizing word of length at most $(n-1)^2$. The best bound known so far is cubic in $n$ and was obtained by Szykuła in 2017.

In this article, we study the synchronization properties of random deterministic automata, for the uniform distribution. Berlinkov recently proved that they are synchronizing with high probability. Our contribution is to study the typical length of the smallest synchronizing word, when such a word exists: we establish that with high probability, such an automaton with $n$ states admits a synchronizing word of length $\mathcal{O}(n \log^3 n)$. As a byproduct, we get that for most automata, the Černý conjecture holds.

*Keywords:* random automata, synchronization, discrete probabilities

## 1. Introduction

For a given automaton, a *synchronizing word* (or a *reset word*) is a word that brings that automaton into one and the same state, regardless of the starting position. This notion, first formalized by Černý in the sixties, arises naturally in automata theory and its extensions, and plays an important role in several application areas, most of them related to the idea of being able to reset a device from every unknown state (see [30] for some examples). Beside applications, one of the reasons synchronizing automata are still intensively studied in theoretical computer science is the following question asked by Černý [9] back in 1964: "*Does every synchronizing n-state automaton admit a synchronizing word of length at most* $(n-1)^2$*?*" The upper bound of $(n-1)^2$, as shown by Černý by providing a matching family of automata, is best possible. This question, now known as *the Černý conjecture*, is one of the most famous conjectures in automata theory. Though established for important subclasses of automata, the Černý conjecture remains open in the general case. The best known bound is $\left(\frac{7}{48} + \frac{2\cdot 15\,625}{1\,597\,536}\right) n^3 + o(n^3)$ which is due to Shitov [27] who improved the bound of $\frac{114}{685}n^3 + \mathcal{O}(n^2)$ by Szykuła [29] which was the first improvement in decades over the bound of $\frac{1}{6}(n^3 - n)$ established in the early eighties by Pin and Frankl [26, 14]. Observe that there still is a significant gap between the quadratic bound conjectured by Černý and the cubic one obtained by Szykuła. We refer the interested reader to Volkov's article [30] for a more detailed account on the Černý conjecture.

The study of random deterministic automata originates in the pioneer works of Grusho [16] and Korshunov [21], who studied the typical size of the accessible part and the asymptotic number of accessible automata, respectively. Since then, a lot of results were obtained on the structure of large random deterministic automata, such as [8, 2, 6], and on the average case analysis of algorithms dealing with automata, such as [1, 10, 11]. The reader is referred to the survey [23] for more information on this topic.

In this article, we consider the Černý conjecture from a probabilistic point of view and look at the synchronization properties of random deterministic automata, for the uniform distribution. The question is quite natural, and was proposed, for instance, by Cameron [7]. Also, many experiments on the Černý conjecture were conducted while attempting to solve it, and a significant amount of experimental evidences have been collected. They suggest that most automata are synchronized by a short reset word, of length sublinear in the number of states. Note that though it is computationally easy to check whether an automaton is synchronizing, finding the shortest reset word is hard [25] (for instance, deciding whether the shortest reset word as length $\ell$ is **DP**-complete, where **DP** is the closure of **NP** $\cup$ **coNP** for finite intersections). Approximating the result is also difficult: Gawrychowski and Straszak [15] proved that for every positive $\varepsilon$, it is **NP**-hard to approximate the length of the shortest reset word within a factor of $n^{1-\varepsilon}$. The best experimental results we are aware of were obtained by Kisielewicz, Kowalski, and Szykuła [19]. Their experiments seem to indicate that the expected length of the reset word grows in $\Theta(\sqrt{n})$.

Berlinkov recently made a breakthrough [3] in this area by proving that the probability that a random automaton is not synchronizing is $\mathcal{O}(n^{-\frac{1}{2}|A|})$, for an alphabet $A$ with at least two letters. That is, random automata are synchronizing with high probability.[1] The techniques used in his proof allow to estimate precisely the probability of not being synchronizing (his result is tight for 2-letter alphabets), but do not provide information on the length of the reset word.

Before the work presented in this article, only partial results were obtained concerning the typical length of the shortest reset word for uniform random deterministic automata: Skvortsov and Zaks [28] proved that the Černý conjecture holds with high probability for large alphabets whose cardinality grows with the number of states, at the rate $n^\beta$ for some $\beta > \frac{1}{2}$. They also proved that the probability of having a short reset word is non-negligible, but not tending to 1, for alphabets with at least four letters [31].

In this paper, we prove that when the automaton is chosen uniformly at random among deterministic and complete $n$-state automata on an alphabet with at least two

[1] *with high probability* means "with probability that tends to 1 as $n$ goes to infinity".

letters, the Černý conjecture holds with high probability. More precisely, we show that with high probability, a random $n$-state automaton admits a synchronizing word of length $\mathcal{O}(n \log^3 n)$. Even if the Černý conjecture is settled in the positive, this result remains interesting, as it yields that most automata admit a synchronizing word of length almost linear (up to some logarithmic factors).

Our proof also gives another way to show that automata are synchronizing with high probability, based on a method that completely differs from Berlinkov's work [3]. He used recent results on synchronization, as well as some advanced properties of random mappings. In our proof, we directly build words that iteratively shrink the set of states, using only basic discrete probabilities and variations on the probabilistic pigeonhole principle (also known as the Birthday Paradox). The proof proposed by Berlinkov is arguably more complicated, but also more precise, since it gives a sharp estimation of the probability of not being synchronizing.[2] Also note that our main result is used by Berlinkov and Szykuła [5] to prove that the probability that the conjecture does not hold for a random synchronizing binary automaton is exponentially small in its number of states.

This article is the long version of the extended abstract [24] presented at the conference RANDOM in 2016, which contained none of the proofs and where the discussions were limited due to the lack of space.

## 2. Definitions and Notations

For any integer $n \geq 1$, let $[n] = \{1, \ldots, n\}$ be the set of integers between 1 and $n$. The cardinality of a finite set $E$ is denoted by $|E|$.

### 2.1. Probabilities

Let $(E, s)$ be a pair where $E$ is a set and $s$ is a *size function* from $E$ to $\mathbb{Z}_{\geq 0}$. The pair $(E, s)$ is a combinatorial set[3] when for every integer $n \geq 0$, the set $E_n$ of size-$n$ elements of $E$ is finite. To simplify the definitions, we also assume that $E_n \neq \emptyset$ for every $n \geq 1$, which will always be the case in the following. Let $(\mathbb{P}_n)_{n \geq 1}$ be a sequence of total functions such that for each $n \geq 1$, $\mathbb{P}_n$ is a probability on $E_n$. We say that a property $P$ holds *with high probability* for $(\mathbb{P}_n)_{n \geq 1}$ when $\mathbb{P}_n[P \text{ holds}] \to 1$ as $n \to \infty$.

We will often consider the *uniform distribution* on $E$, which is the sequence $(\mathbb{P}_n)_{n \geq 1}$ defined by $\mathbb{P}_n[\{e\}] = \frac{1}{|E_n|}$ for any $e$ in $E_n$: A sentence like "property $P$ holds with high probability for the uniform distribution on $E$" therefore means that the probability that $P$ holds tends to 1 as $n$ tends to infinity, when for each $n$ we consider the uniform distribution on $E_n$. The reader is referred to [13] for more information on combinatorial probabilistic models.

[2] Knowing the probability of not being synchronizing is important in many situations, especially for the average case analysis of algorithms, as illustrated in the conclusions of [3]. Berlinkov also replies precisely to a question asked by Cameron [7].

[3] The size is often clear in the context (number of nodes in a tree, ...) and can be omitted.

### *2.2. Mappings, Random Mappings and Random p-Mappings*

A *mapping* on a set $E$ is a total function from $E$ to $E$. When $E$ is finite, a mapping $f$ on $E$ can be seen as a directed graph with an edge $i \to j$ whenever $f(i) = j$. An example of such a graph is depicted in Figure 1 page 346.

Let $f$ be a mapping on $E$. The element $x \in E$ is a *cyclic point*[4] of $f$ when there exists an integer $i > 0$ such that $f^i(x) = x$. In the sequel, $E$ will often be the set of states of an automaton, and we will therefore use the term “state” instead of “point”.

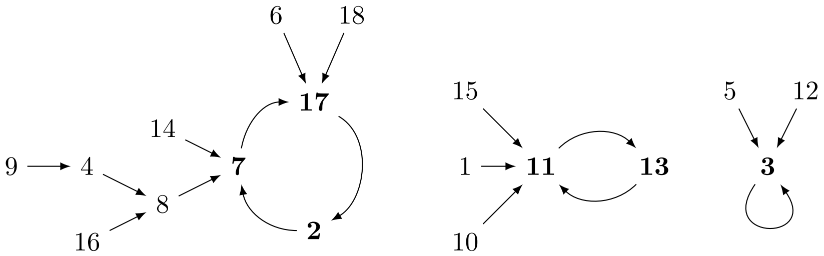


Figure 1: A mapping for $n = 18$. The cyclic points are indicated in bold.

If $f$ is a mapping on $E$ and $x \in E$, the *height* of $x$ is the smallest $i \geq 0$ such that $f^i(x)$ is a cyclic point. The height of a cyclic point is therefore 0. The *height* of a mapping on $E$ is the maximal height of an element of $E$. The mapping depicted in Figure 1 has height 3, and its maximal height is reached by the state 9.

A *random mapping* of size $n \geq 1$ is a mapping on $[n]$ taken with the uniform distribution amongst the $n^n$ possibilities. Random mappings have been intensively studied in the litterature, see for instance the book of Kolčin [20] or the analytic approach developed by Flajolet and Odlyzko in [12].

If $p$ is a probability mass function on $[n]$, a *random p-mapping* is the distribution on the mappings on $[n]$ such that the probability of a mapping $f$ is $\prod_{i\in[n]} p(f(i))$: the image of each $i \in [n]$ is chosen independently following the probability $p$.

**Example 1.** Assume that $n = 3$ and that $p$ is the probability on $\{1, 2, 3\}$ defined by

$$p(1) = \frac{1}{2}, \quad p(2) = \frac{1}{3}, \quad \text{and} \quad p(3) = \frac{1}{6},$$

then a random $p$-mapping has probability

$$\frac{1}{3} \times \frac{1}{6} \times \frac{1}{3} = \frac{1}{54}$$

to be the mapping $1 \mapsto 2$, $2 \mapsto 3$ and $3 \mapsto 2$, and probability

$$\frac{1}{2} \times \frac{1}{3} \times \frac{1}{6} = \frac{1}{36}$$

to be the identity.

[4] We will also say that $x$ is an $f$*-cyclic point* when the mapping under consideration is not clear in the context.

A result stated as “a random $p$-mapping satisfies property $P$ with high probability” means that for *any* sequence $(p_n)_{n\geq 1}$, where $p_n$ is a probability on $[n]$, the probability that a $p_n$-random mapping on $[n]$ satisfies $P$ tends to 1 as $n$ tends to infinity. It is therefore a very strong result that does not depend on the choice of $(p_n)_{n\geq 1}$.

### *2.3. Automata and Synchronization*

Let $A$ be a finite alphabet, a *deterministic automaton* on $A$ is a pair $(Q, \delta)$, where $Q$ is a finite set of *states* and $\delta$ is the *transition function*, a (possibly partial) function from $Q \times A$ to $Q$. If $p, q \in Q$ and $a \in A$ are such that $\delta(p, a) = q$, then $(p, a, q)$ is the *transition* from $p$ to $q$ labelled by $a$, and is denoted by $p \xrightarrow{a} q$. It is the *$a$-transition* outgoing from $p$.

Note that in this article, we are not interested in initial and final states since they do not change anything regarding synchronization. We will also focus on deterministic automata only, and therefore, throughout the article, we will simply call “automaton” a deterministic automaton with no initial and final states.

An automaton $\mathcal{A} = (Q, \delta)$ on $A$ is classically seen as a $A$-labelled directed graph, whose set of vertices is $Q$ and whose edges are the transitions of $\mathcal{A}$.

An automaton is *complete* when its transition function is a total function and *incomplete* otherwise. The transition function is extended inductively to $Q \times A^*$ by setting $\delta(p, \varepsilon) = p$ for every $p \in Q$ and, for every $u \in A^*$, $\delta(p, ua) = \delta(\delta(p, u), a)$ when everything is defined, and undefined otherwise. If $u \in A^*$, we denote by $\delta_u$ the (possibly partial) function from $Q$ to $Q$ defined by $\delta_u(p) = \delta(p, u)$, for all $p \in Q$.

If $\mathcal{A} = (Q, \delta)$ is an automaton on $A$, an *extension* of $\mathcal{A}$ is an automaton $\mathcal{B} = (Q, \lambda)$ on $A$ such that for all $p \in Q$ and for all $a \in A$, if $\delta(p, a)$ is defined then $\lambda(p, a) = \delta(p, a)$. The automaton $\mathcal{B}$ is therefore obtained from $\mathcal{A}$ by adding some missing transitions. We denote by $\mathbf{Ext}(\mathcal{A})$ the set of all the extensions of an automaton $\mathcal{A}$. If $\mathcal{H}$ is a set of automata, we denote by $\mathbf{Ext}(\mathcal{H})$ the union of all the $\mathbf{Ext}(\mathcal{A})$ for $\mathcal{A} \in \mathcal{H}$.

Let $\mathcal{A}$ be an automaton on the alphabet $A$. Two states $p$ and $q$ of $\mathcal{A}$ are *synchronized* by the word $w \in A^*$ when both $\delta_w(p)$ and $\delta_w(q)$ are defined and equal.

A *synchronizing word*, or *reset word*, for an automaton $\mathcal{A} = (Q, \delta)$ is a word $w \in A^*$ such that $\delta_w$ is a constant map: there exists a state $r \in Q$ such that for every $p$ in $Q$, $\delta_w(p) = r$. An automaton that admits a synchronizing word is said to be *synchronizing*.

### *2.4. Random Automata*

In the sequel, the set of states of an $n$-state automaton will always be $[n]$. With this condition, there are exactly $n^{|A|n}$ complete automata with $n$ states on $|A|$. Therefore, for the uniform distribution, each size-$n$ complete automaton has probability $n^{-|A|n}$.

Though we will not need it directly in the sequel, it is convenient to have an idea of the typical shape of a random deterministic automaton, which is provided by many results of the literature [16, 6, 8, 2]. With high probability, such an automaton has a huge terminal strongly connected component $\mathcal{C}$ of size around $\nu n$, for some known constant $\nu > \frac{1}{2}$ that only depends on the size of the alphabet. States that are not in $\mathcal{C}$

can reach it using a very short path, and there are only a few number of cycles that does not belong to $\mathcal{C}$. As a consequence, starting from any state one can reach $\approx \nu n$ states of the automaton (this is the property used for random sampling in [8]).

Moreover, Bassino, David and Sportiello [2] proved that random *accessible* deterministic automata are minimal with high probability for alphabets of size at least three, and with probability tending to $\gamma$, for some positive $\gamma$, for two-letter alphabets. This implies that, when looking at the described languages, these distribution is not degenerated and provide a way to study random languages for the uniform distribution related to the state complexity.

See the survey [23] for an account on the typical properties of uniform random deterministic automata.

Observe that one can also see the uniform distribution on complete automata with $n$ states as drawing uniformly at random and independently in $[n]$ the image of each $\delta(p, a)$, for all $p \in [n]$ and for all $a \in A$. These alternative way to look at random automata will widely be used in the sequel, especially in the following way: Let $\mathcal{A}$ be a fixed incomplete automaton with $n$ states. The uniform distribution on complete automata of $\mathbf{Ext}(\mathcal{A})$ is obtained by choosing uniformly at random and independently in $[n]$ the ending state of the transitions that are undefined in $\mathcal{A}$.

## 3. Preliminary Classical Results

In this section, we recall some classical results that will be useful in sequel. Though elementary, these results are the main ingredients of this article.

We start with the following classical property of synchronizing automata: an automaton is synchronizing if and only if every pair of states can be synchronized.

**Lemma 2.** *Let $\mathcal{A}$ be an $n$-state automaton and $\ell$ be a non-negative integer. If for every pair of states $(p, q)$ in $\mathcal{A}$ there exists a word $u$ of length at most $\ell$ such that $\delta_u(p) = \delta_u(q)$, then $\mathcal{A}$ admits a synchronizing word of length at most $\ell(n-1)$.*

*Proof.* Assume by induction that we successfully synchronized $i \geq 2$ pairwise distinct states $q_1, \ldots, q_i$ using a word $u$ of length smaller than or equal to $\ell(i-1)$: for all $j, k \in \{1, \ldots, i\}$, $\delta_u(q_j) = \delta_u(q_k)$. Let $q_{i+1}$ be a state distinct from $q_1, \ldots, q_i$ and let $v$ be a word of length at most $\ell$ that synchronizes $\delta_u(q_1)$ and $\delta_u(q_{i+1})$. Then the word $uv$ synchronizes $q_1, \ldots, q_{i+1}$ and has length at most $\ell i$. □

Our next lemma is a bit technical, but it will be used several times in the following, in particular to generalize some results on random mappings to random $p$-mappings.

**Lemma 3.** *Let $n$ and $\ell$ be two positive integers such that $\ell \leq n$. Let $(E, \leq)$ be a totally ordered finite set of cardinality $n$. Let $f$ be a mapping from $E$ to $\mathbb{R}_{\geq 0}$, and denote by $s$ the sum of the images of the elements of $E$ by $f$: $s = \sum_{x \in E} f(x)$. The following result holds:*

$$\sum_{x_1 < x_2 < \cdots < x_\ell} f(x_1) f(x_2) \cdots f(x_\ell) \leq \binom{n}{\ell} \left(\frac{s}{n}\right)^\ell,$$

*where the sum ranges over all increasing $\ell$-tuples of elements of $E$. The sum on the left is therefore maximal when $f(x) = \frac{s}{n}$, for every $x \in E$.*

*Proof.* Let $\nu(f)$ denote the number of elements $x \in E$ such that $f(x)$ is different from $\frac{s}{n}$:

$$\nu(f) = \left|\left\{ x \in E \mid f(x) \neq \frac{s}{n} \right\}\right|.$$

We prove by induction on the value of $\nu$ that every mapping from $E$ to $\mathbb{R}_{\geq 0}$ whose images sum to $s$ satisfies the inequality stated in the lemma.

If $\nu(f) = 0$, then we have $\sum_{x_1<\cdots<x_\ell} f(x_1)\cdots f(x_\ell) = \binom{n}{\ell}\left(\frac{s}{n}\right)^\ell$ since there are $\binom{n}{\ell}$ increasing sequences $x_1 < \cdots < x_\ell$.

Otherwise, $\nu(f) \neq 0$ and we build another map $g$, starting from $f$, such that $g$ also sums to $s$, with $\nu(g) < \nu(f)$ and having the following property:

$$\sum_{x_1<\cdots<x_\ell} f(x_1)\cdots f(x_\ell) \leq \sum_{x_1<\cdots<x_\ell} g(x_1)\cdots g(x_\ell). \tag{1}$$

This is done as follows. Let $y \in E$ be an element such that $|f(y) - \frac{s}{n}|$ is minimal amongst the $y$'s such that $f(y) \neq \frac{s}{n}$. We assume that $f(y) - \frac{s}{n} > 0$ (the proof is similar if $f(y) - \frac{s}{n} < 0$). Since

$$f(y) > \frac{s}{n} \quad \text{and} \quad \sum_{x\in E} f(x) = s,$$

there exists an element $z \neq y$ such that $f(z) < \frac{s}{n}$. Consider the new map $g$ obtained from $f$ by changing the value at $y$ and $z$ the following way:

$$\begin{aligned} &g(x) = f(x) \quad \text{if } x \neq y \text{ and } x \neq z,\\ &g(y) = \frac{s}{n},\\ &g(z) = f(z) + f(y) - \frac{s}{n}. \end{aligned}$$

One can directly verify that $g$ is always non-negative and sums to $s$. Moreover, by construction, we have $\nu(g) < \nu(f)$. We claim that Equation (1) holds. To prove this inequality, we distinguish three cases for the $\ell$-tuples:

- If $(x_1, \ldots, x_\ell)$ is an increasing $\ell$-tuple that does not contain $y$ nor $z$, then we have $g(x_1)\cdots g(x_\ell) = f(x_1)\cdots f(x_\ell)$.
- We sum the contributions of tuples containing exactly one element of $\{y, z\}$: if $\{x_1, \ldots, x_{\ell-1}\}$ are $\ell - 1$ elements of $[n] \setminus \{y, z\}$, the definition of $g$ yields that

  $$\begin{aligned} g(x_1)\cdots g(x_{\ell-1})\, g(y) &+ g(x_1)\ldots g(x_{\ell-1})\, g(z)\\ &= f(x_1)\cdots f(x_{\ell-1})\, f(y) + f(x_1)\cdots f(x_{\ell-1})\, f(z). \end{aligned}$$

  Hence, the contributions of such tuples globally do not change the value of the sum when switching from $f$ to $g$.

- If both $y$ and $z$ are in the tuple, then

$$f(x_1)\cdots f(x_\ell) = f(y)f(z)\prod_{\substack{x_i\neq y\\ x_i\neq z}} f(x_i),$$

$$g(x_1)\cdots g(x_\ell) = g(y)g(z)\prod_{\substack{x_i\neq y\\ x_i\neq z}} g(x_i) = g(y)g(z)\prod_{\substack{x_i\neq y\\ x_i\neq z}} f(x_i).$$

  Let $\alpha$ and $\beta$ be the two positive real numbers defined by $\alpha = f(y) - \frac{s}{n}$ and $\beta = \frac{s}{n} - f(z)$. We have

$$g(z)g(y) = \frac{s}{n}\left(f(z) + f(y) - \frac{s}{n}\right) = \frac{s}{n}\left(\frac{s}{n} + \alpha - \beta\right) = \frac{s^2}{n^2} + \frac{s(\alpha-\beta)}{n},$$

  whereas

$$f(y)\,f(z) = \left(\frac{s}{n} + \alpha\right)\left(\frac{s}{n} - \beta\right) = \frac{s^2}{n^2} + \frac{s(\alpha-\beta)}{n} - \alpha\beta,$$

  therefore $f(y)\,f(z) \leq g(y)\,g(z)$ and $f(x_1)\cdots f(x_\ell) \leq g(x_1)\cdots g(x_\ell)$ for such a tuple.

This proves Equation (1) and concludes the proof by induction on the value of $\nu$. □

Random mappings and random $p$-mappings have been studied intensively in the literature [17, 12, 20], using probabilistic techniques or methods from analytic combinatorics. In this section, we only recall basic properties of the typical number of cyclic points and of the typical height of a random $p$-mapping. This can be achieved using variations on the probabilistic pigeonhole principle only (also called the Birthday Paradox); more advanced techniques can be used to obtain more precise statements,[5] but we will not need such advanced properties. Such results are folklore, but our exact statement given in Lemma 4 below is chosen to fit our needs in the sequel, and we provide an elementary proof of it for self completeness (and because it is difficult to find this exact statement in the literature). The lemma is proved in two steps. It is first established for uniform random mappings then extended to general $p$-random mappings, using Lemma 3.

**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 $\mathcal{O}(\frac{1}{n})$.*

*Proof.* We start with the number of cyclic points in the uniform case. For any integer $\ell$ such that $1 \leq \ell \leq n$, the probability that there is a cyclic part of size $\ell$ in a uniform random mapping is at most

$$P(n,\ell) = \binom{n}{\ell}\ell!\; n^{-\ell}\,:$$

[5] For instance, limit distributions of some parameters [13] or even a notion of continuous limit for random mappings.

There are

$$\binom{n}{\ell}\ell!$$

different ways to choose the $\ell$ elements that form the cyclic part and the permutation that is the restriction of the mapping to its cyclic part. Since it exactly determines the images of $\ell$ elements, having this cyclic part happens with probability $\frac{1}{n^\ell}$. This is an upper bound, as we do not prevent the formation of other cycles in our counting. Moreover, by standard computations,

$$P(n,\ell) = \left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{\ell-1}{n}\right) \le \exp\left(-\frac{\ell(\ell-1)}{2n}\right).$$

Observe also that the product form above prove that $P(n,\ell)$ is increasing in $\ell$. Hence, the probability that the cyclic part has at least $2\sqrt{n\log n}$ cyclic points is at most

$$\sum_{\ell=\lceil 2\sqrt{n\log n}\,\rceil}^{n} P(n,\ell) \le n\cdot P(n,\lceil 2\sqrt{n\log n}\rceil) = \mathcal{O}\left(\frac{1}{n}\right). \tag{2}$$

We now consider the height, still in the uniform case. Consider an element $i \in [n]$. For any integer $\ell$ such that $1 \le \ell < n$, the probability that a uniform random mapping $f$ on $[n]$ is such that $f(i)$, $f^2(i) = f(f(i))$, …, $f^\ell(i)$ are all distinct is classically

$$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{\ell-1}{n}\right) = P(n,\ell).$$

Therefore, we can reuse the previous computations. If $f$ has height greater than or equal to $\ell$, then there exists a $i$ with at least $\ell$ distinct iterates. Hence, summing the contribution of all $i \in [n]$ with the union bound, we get that the probability that $f$ has height greater than $\lceil 2\sqrt{n\log n}\rceil$ is at most $nP(n,\lceil 2\sqrt{n\log n}\rceil)$. Thus, by Equation (2), it is also $\mathcal{O}(\frac{1}{n})$.

This concludes the proof for the uniform case. We now generalize the statement to random $p$-mappings. For the number of cyclic points, we start as for the uniform case. The only difference is that if the points involved in the cyclic part of length $\ell$ are $x_1, x_2, \ldots, x_\ell$, then the probability of having a given permutation of those points is not $\ell!\,n^{-\ell}$ anymore, it is

$$P_n(x_1,\ldots,x_\ell) = \ell!\; p(x_1)p(x_2)\cdots p(x_\ell).$$

If we sum this quantity for all possible $\ell$-subsets of $[n]$, we obtain the upper bound

$$P_n(\ell) = \ell! \sum_{1\le x_1<x_2<\cdots<x_\ell\le n} p(x_1)p(x_2)\cdots p(x_\ell).$$

At this point, we can apply Lemma 3 with $f = p$, $E = [n]$ and $s = 1$ to obtain an upper bound for $P_n(\ell)$ that does not depend on the probability $p$:

$$P_n(\ell) \le \ell!\binom{n}{\ell}n^{-\ell}.$$

This is the same bound as for the uniform case, yielding the same result.

It remains to study the height of random $p$-mappings. Let $x$ be some element of $[n]$. Let $(x_1, \dots, x_\ell)$ be a $\ell$-tuple of distinct elements in $[n] \setminus \{x\}$. The probability that a map $f$ is such that $x_i = f^i(x)$, for all $1 \leq i \leq \ell$, is exactly $p(x_1)p(x_2) \cdots p(x_\ell)$. Hence, the probability that $x$ has $\ell$ distinct iterates that are different from $x$ when applying $f$ is $p(x_1)p(x_2) \cdots p(x_\ell)$ where $(x_1, \dots, x_\ell)$ ranges over all $\ell$-tuples of pairwise distinct elements of $[n] \setminus \{x\}$. We obtain an upper bound by allowing one of the $x_i$'s to be equal to $x$, which simplifies the writing. This bound is

$$\ell! \sum_{1 \leq x_1 < x_2 < \cdots < x_\ell \leq n} p(x_1)p(x_2) \cdots p(x_\ell),$$

since there are $\ell!$ ways to permute the $x_i$'s. This is exactly $P_n(\ell)$ obtained for the number of cyclic points, yielding the same result and concluding the proof. □

## 4. Main Result

The main result of this article is the following theorem.

**Theorem 5.** *Let $A$ be an alphabet with at least two letters. For the uniform distribution, an $n$-state deterministic and complete automaton on $A$ admits a synchronizing word of length $\mathcal{O}(n \log^3 n)$ with high probability. More precisely, the probability that no such word exists is $\mathcal{O}(n^{-\frac{1}{8}} \log^4 n)$.*

The statement does not hold for alphabets with only one letter, since there are cycles of length greater than 1 in a random mapping with high probability [12]: two distinct states in such a cycle cannot be synchronized.

As a consequence of Theorem 5, a random deterministic and complete automaton is synchronizing with high probability; our proof therefore constitutes an alternative proof of [3] for that property. Our statement is weaker for just synchronization, since Berlinkov also obtained the upper bound $\mathcal{O}(n^{-\frac{1}{2}|A|})$ for the error term (the number of automata that are not synchronizing), which is tight for two-letter alphabets. On the other hand, it is arguably more elementary as we mostly rely on Lemma 4 and some basic discrete probabilities; in any case, beside providing information on the typical length of the shortest reset word, we hope that our proof sheds a new light on the reasons why automata are often synchronizing.

If we consider the uniform distribution on synchronizing automata, we directly obtain from Theorem 5 that there exists a small synchronizing word with high probability, yielding the following corollary.

**Corollary 6.** *For the uniform distribution on synchronizing deterministic and complete automata on an alphabet with at least two letters, the Černý conjecture holds with high probability.*

We prove Theorem 5 in two main steps, which are informally as follows:

(i) We first construct a word $w_n \in \{a, b\}^*$ such that the image of $\delta_{w_n}$ for a random $n$-state automaton has size at most $n^{1/8} \log^{7/8} n$ with high probability. This is done by building a set $\mathcal{G}_n$ of incomplete automata that have this property, and by showing that a random $n$-state automaton extends an element of $\mathcal{G}_n$ with high probability. Roughly speaking, $\mathcal{G}_n$ and $w_n$ are built by three consecutive applications of Lemma 4, starting with incomplete automata with only $a$-transitions, which we then augment by $b$-transitions in two rounds.

(ii) It remains to synchronize those $n^{1/8} \log^{7/8} n$ states. This is done by showing that for a random automaton that extends an element of $\mathcal{G}_n$, with high probability any two of those states can be synchronized by a word of the form $b^i w_n$, with $i \leq n^{1/4}$. Lemma 2 is then used to combine these words, and also $w_n$, into a synchronizing word for the automaton.

The remainder of this section is devoted to a more detailed proof of Theorem 5. For the presentation, we will follow an idea used by Karp in his article on random direct graphs [18]: we start from an automaton with no transition, then add new random transitions during at each step of the construction, progressively improving the synchronization. This is the classical "Principle of Deferred Decisions" of the field of randomized algorithms [22, p. 69].

Since it is clearly sufficient to establish the result for a two-letter alphabet, we consider that $A = \{a, b\}$ from now on, except for the informal discussion at the beginning of Section 4.3.

### *4.1. Generating the a-Transitions*

The first step consists in generating all the $a$-transitions. This forms a mapping for $\delta_a$ that follows the uniformly distribution on size-$n$ mappings. We can therefore apply Lemma 4, and obtain that words of the form $a^i$ can already be used to reduce significantly the number of states to be synchronized.

Let $\alpha_n = \lfloor 2\sqrt{n \log n} \rfloor$ and let $\mathcal{E}_n$ denote the set of incomplete automata $\mathcal{A}$ with $n$ states such that:

(i) The defined transitions of $\mathcal{A}$ are exactly its $a$-transitions.

(ii) The action $\delta_a$ of $a$ has at most $\alpha_n$ cyclic states.

(iii) The height of $\delta_a$ is at most $\alpha_n$.

**Example 7.** Let $\mathcal{A}$ be an automaton with 18 states, which has only $a$-transitions and such that $\delta_a$ is the mapping of Figure 1 (Page 346). Its set of $\delta_a$-cyclic states $\mathbf{Cyc_a}(\mathcal{A})$ is $\{\mathbf{2}, \mathbf{3}, \mathbf{7}, \mathbf{11}, \mathbf{13}, \mathbf{17}\}$. Since $\alpha_{18} = 14$, the word $u_{18} = a^{14}$ is used to start the synchronization:

$$\{6, 7, 9, 18\} \xrightarrow{u_{18}} \mathbf{2}; \qquad \{3, 5, 12\} \xrightarrow{u_{18}} \mathbf{3}; \qquad \{4, 16, 17\} \xrightarrow{u_{18}} \mathbf{7};$$
$$\{11\} \xrightarrow{u_{18}} \mathbf{11}; \qquad \{1, 10, 13, 15\} \xrightarrow{u_{18}} \mathbf{13}; \quad \{2, 8, 14\} \xrightarrow{u_{18}} \mathbf{17}.$$

As there are $6 \leq \alpha_{18}$ cyclic states and since this mapping's height is $3 \leq \alpha_{18}$, the automaton $\mathcal{A}$ is an element of $\mathcal{E}_{18}$.

As the action of the letter $a$ in a uniform random complete automaton is exactly a uniform random mapping, the following result is a direct consequence of Lemma 4.

**Lemma 8.** *A random complete automaton with $n$ states extends an element of $\mathcal{E}_n$ with high probability. More precisely, the probability that such an automaton does not extend an element of $\mathcal{E}_n$ is $\mathcal{O}(\frac{1}{n})$.*

For any automaton $\mathcal{A}$ whose $a$-transitions are all defined, let $\mathbf{Cyc_a}(\mathcal{A})$ denote its set of $\delta_a$-cyclic states. They also are the $\delta_a$-cyclic states of any automaton that extends $\mathcal{A}$.

Let $u_n = a^{\alpha_n}$. By Lemma 8, we can already start the synchronization using $u_n$, as the image of the set of states $[n]$ by $\delta_{u_n}$ is included in $\mathbf{Cyc_a}(\mathcal{A})$, which is much smaller than $n$ with high probability: if we find a word $v$ that synchronizes $\mathbf{Cyc_a}(\mathcal{A})$, then $u_n v$ is a synchronizing word for $\mathcal{A}$. In the sequel, we therefore work on synchronizing the elements of $\mathbf{Cyc_a}(\mathcal{A})$.

### *4.2. Adding a First Round of Random b-Transitions*

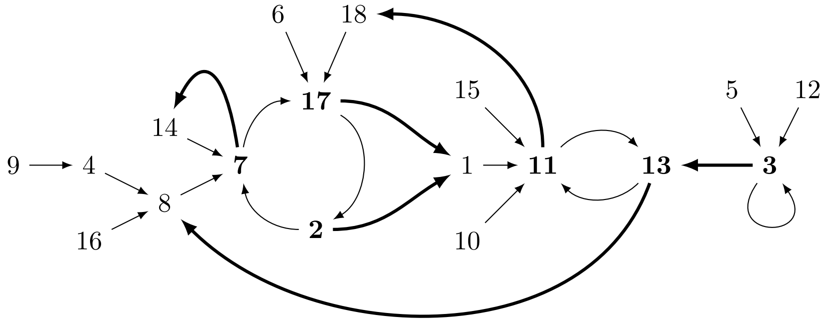
Let $\mathcal{A}$ be a fixed element of $\mathcal{E}_n$. We are now working on $\mathbf{Ext}(\mathcal{A})$ and we consider the process of adding a random $b$-transition starting from every state of $\mathbf{Cyc_a}(\mathcal{A})$.

Let $\mathcal{B} \in \mathbf{Ext}(\mathcal{A})$ be an automaton obtained this way and let $f_{\mathcal{B}}$ denote the restriction of $\delta_{bu_n}$ to $\mathbf{Cyc_a}(\mathcal{A})$. It is a total map, since all the needed $b$-transitions are defined. Moreover, the image of $f_{\mathcal{B}}$ is included in $\mathbf{Cyc_a}(\mathcal{A})$, as

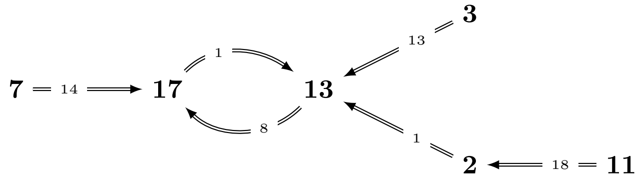
$$f_{\mathcal{B}}(x) = \delta_{bu_n}(x) = \delta_{u_n}(\delta_b(x)),$$

for every $x \in \mathbf{Cyc_a}(\mathcal{A})$. Hence, $f_{\mathcal{B}}$ is a total map from $\mathbf{Cyc_a}(\mathcal{A})$ to itself.

**Example 9.** This is the automaton of Example 7, where the $b$-transitions originating from the elements of $\mathbf{Cyc_a}(\mathcal{A})$ have been added (in bold):



The map $f_{\mathcal{B}}$, which is the restriction of $\delta_{bu_n}$ to $\mathbf{Cyc_a}(\mathcal{A})$, is depicted below. An edge $\mathbf{p} = x \Longrightarrow \mathbf{q}$ means that $\delta_b(p) = x$ and $\delta_{u_n}(x) = q$, so that $f_{\mathcal{B}}(p) = q$:



From a probabilistic point of view, if we fix $\mathcal{A}$ and build $\mathcal{B}$ by adding uniformly at random and independently the $b$-transitions that start from the states of $\mathbf{Cyc_a}(\mathcal{A})$, the induced distribution for the mapping $f_{\mathcal{B}}$ is usually not the uniform distribution on the mappings of $\mathbf{Cyc_a}(\mathcal{A})$. More precisely, for any $q \in \mathbf{Cyc_a}(\mathcal{A})$ the probability that the image by $f_{\mathcal{B}}$ of an element of $\mathbf{Cyc_a}(\mathcal{A})$ is $q$ is proportional to the number of preimages of $q$ by $\delta_{u_n}$. It is exactly $\frac{1}{n}|\delta_{u_n}^{-1}(\{q\})|$, the probability that a random state is mapped to $q$ when reading $u_n$. For any word $\omega \in A^*$, let $\mathbb{P}_{\mathcal{A},\omega}$ be the function from $[n]$ to $[0,1]$ defined by

$$\mathbb{P}_{\mathcal{A},\omega}(q) = \frac{|\delta_\omega^{-1}(\{q\})|}{n}, \text{ for all } q \in [n]. \tag{3}$$

From the observations above, we get that once $\mathcal{A}$ is fixed, $f_{\mathcal{B}}$ is a random $p$-mapping, where the distribution on $\mathbf{Cyc_a}(\mathcal{A})$ is given by the restriction of $\mathbb{P}_{\mathcal{A},u_n}$ to $\mathbf{Cyc_a}(\mathcal{A})$ ($\mathbb{P}_{\mathcal{A},u_n}$ only charges $\mathbf{Cyc_a}(\mathcal{A})$ since $\mathcal{A} \in \mathcal{E}_n$).

Let $\beta_n = \lfloor 3\, n^{1/4} \log^{3/4} n \rfloor$. Applying Lemma 4 to $f_{\mathcal{B}}$ yields the following result.

**Lemma 10.** *Let $\mathcal{A}$ be a fixed automaton of $\mathcal{E}_n$. Consider the random process of building $\mathcal{B}$ by adding a $b$-transition to every element of $\mathbf{Cyc_a}(\mathcal{A})$, choosing the target uniformly and independently in $[n]$. For $n$ sufficiently large, the probability that $f_{\mathcal{B}}$ has more than $\beta_n$ cyclic states or that it has height greater than $\beta_n$ is smaller than $\frac{M}{n^{1/4}}$, for some positive constant $M$ that does not depends on $\mathcal{A}$.*

*Proof.* Let $c$ denote the number of $\delta_a$-cyclic states in $\mathcal{A}$. Recall that $f_{\mathcal{B}}$ is the map from $\mathbf{Cyc_a}(\mathcal{A})$ to itself defined by $f_{\mathcal{B}}(x) = \delta_{bu_n}(x)$, for every $x \in \mathbf{Cyc_a}(\mathcal{A})$. First observe that if $c \leq \beta_n$, then there is nothing to prove as $\mathbf{Cyc_a}(\mathcal{A})$ already has at most $\beta_n$ states. The probability under consideration is therefore 0 in this case. In the case $c > \beta_n$, we can apply Lemma 4 when $n$ is sufficiently large, since $f_{\mathcal{B}}$ is a $p$-random mapping on a set with $c$ elements. Hence, the probability that there are more than $2\sqrt{c \log c}$ cyclic points or that the height is greater than $2\sqrt{c \log c}$ is at most $\frac{M}{c}$, for some positive constant $M$. Moreover, observe that since $\mathcal{A} \in \mathcal{E}_n$, we have, for $n$ sufficiently large,

$$2\sqrt{c \log c} \leq 2\sqrt{\alpha_n \log \alpha_n} = 2\, n^{1/4} \log^{3/4} n \,\big(1 + o(1)\big) \leq \beta_n.$$

Since $c > \beta_n \geq n^{\frac{1}{4}}$, this yields the announced upper bound of $Mn^{-\frac{1}{4}}$. □

For any automaton $\mathcal{B}$ whose $a$-transitions are all defined and whose $b$-transitions starting from an element of $\mathbf{Cyc_a}(\mathcal{B})$ are also all defined, let $\mathbf{Cyc_f}(\mathcal{B})$ denote the set of $f_{\mathcal{B}}$-cyclic states of $\mathcal{B}$.

Let $v_n = u_n(bu_n)^{\beta_n}$. At this point, the number of states to be synchronized has been reduced to less than $\beta_n$ with high probability, since the image of $\delta_{v_n}$ is usually included in $\mathbf{Cyc_f}(\mathcal{B})$. It has been achieved by generating all the $a$-transitions, but using only the $b$-transitions that start from the $\delta_a$-cyclic states: there still remain at least $n - \alpha_n$ undefined $b$-transitions that can be used to continue the synchronization. Nonetheless, before going on, we first refine the construction of $\mathcal{B}$ introduced in this section by forbidding some cases, for technical reasons explained in the next section.

### *4.3. Forbidding Correlated Shapes*

The number of states to be synchronized has been reduced to no more than $\beta_n$ states with high probability, but this quantity is still too large. For the technique used as the last step of the proof (see the informal presentation at the beginning of Section 4), we need to shrink this set once more. Should the alphabet contain one more letter $c$, we could use the same kind of construction as in Section 4.2, and be left with at most, roughly, $n^{1/8}$ states to synchronize. This is because $c$-transitions can be generated independently of what has been done during the previous steps. This quantity, $n^{1/8}$, is sufficiently small for our last step of the proof to work, but we do not have this third letter $c$ at hand.

Some care is required to adapt this idea for a two-letter alphabet. We aim at using the word $bb$ instead of the letter $c$ in the informal description above. Let $\mathcal{B}$ be an incomplete automaton that extends $\mathcal{A} \in \mathcal{E}_n$ and whose defined transitions are all the $a$-transitions and also the $b$-transitions that start from the $\delta_a$-cyclic states. We are interested in building an automaton $\mathcal{C}$ from $\mathcal{B}$, by adding some new random $b$-transitions, in a way such that $\delta_{bbv_n}$ is totally defined on $\mathbf{Cyc_f}(\mathcal{B})$. It means that for every $q \in \mathbf{Cyc_f}(\mathcal{B})$, the state $\delta_b(q)$ must have an outgoing $b$-transition in $\mathcal{C}$. For such an extension $\mathcal{C}$ of $\mathcal{B}$, let $g_{\mathcal{C}}$ denote the restriction of $\delta_{bbv_n}$ to $\mathbf{Cyc_f}(\mathcal{B})$.

The main point here is that for a fixed $\mathcal{B}$, we want $g_{\mathcal{C}}$ to be defined as a random $p$-mapping, so that we can use Lemma 4 once more. There are, *a priori*, two kind of issues that can prevent this from happening:

(i) When there exists a state $q \in \mathbf{Cyc_f}(\mathcal{B})$ such that the $b$-transition starting from $\delta_b(q)$ is already defined in $\mathcal{B}$, that is, when $\delta_b(q) \in \mathbf{Cyc_a}(\mathcal{B})$.

(ii) When two distinct states $q$ and $q'$ in $\mathbf{Cyc_f}(\mathcal{B})$ are such that $\delta_b(q) = \delta_b(q')$.

Fortunately, the second case cannot occur: if $\delta_b(q) = \delta_b(q')$ then $f_{\mathcal{B}}(q) = f_{\mathcal{B}}(q')$, which is not possible for two distinct $f_{\mathcal{B}}$-cyclic states.

The first case can occur, and then the image of $\delta_b(q)$ by $b$ is already defined in $\mathcal{B}$ and therefore $g_{\mathcal{C}}$ does not follow a $p$-distribution when we build $\mathcal{C}$ by generating the missing transitions uniformly at random.[6]

[6] Except in the very degenerate case where the restriction of $\delta_{bb}$ to $\mathbf{Cyc_f}(\mathcal{B})$ is already a totally defined and constant map in $\mathcal{B}$.

Conversely, if for every $q \in \mathbf{Cyc_f}(\mathcal{B})$, $\delta_b(q) \notin \mathbf{Cyc_a}(\mathcal{B})$, then it is easy to verify that $g_{\mathcal{C}}$ is a random $p$-mapping: the image of $q \in \mathbf{Cyc_f}(\mathcal{B})$ by $g_{\mathcal{C}}$ is a given $x$ when $\delta_{bbv_n}(q) = x$, which is equivalent to $\delta_b(\delta_b(q)) \in \delta_{v_n}^{-1}(\{x\})$. Since $\delta_b(\delta_b(q))$ is chosen uniformly at random in $[n]$, it happens with probability $\mathbb{P}_{\mathcal{B},v_n}(x)$, using the notation of Equation (3).

We therefore forbid the bad cases and define the set $\mathcal{F}_n$ of incomplete automata $\mathcal{B}$ with $n$ states such that (we add the last condition to what was done in the previous section):

(i) $\mathcal{B}$ extends an element of $\mathcal{E}_n$.

(ii) The defined transitions of $\mathcal{B}$ are all the $a$-transitions and the $b$-transitions starting from the states of $\mathbf{Cyc_a}(\mathcal{B})$.

(iii) The map $f_{\mathcal{B}}$ has height at most $\beta_n$ and has at most $\beta_n$ cyclic states.

(iv) For every $q \in \mathbf{Cyc_f}(\mathcal{B})$, $\delta_b(q) \notin \mathbf{Cyc_a}(\mathcal{B})$.

**Example 11.** The automaton of Example 9 is in $\mathcal{F}_n$. For the fourth condition, observe that the $f_{\mathcal{B}}$-cyclic states are **13** and **17**. Their images by $\delta_b$, which are 8 and 1 respectively, are not in $\mathbf{Cyc_a}(\mathcal{B})$. The fact that $\delta_b(\mathbf{3})$ is in $\mathbf{Cyc_a}(\mathcal{B})$ is not a problem here, since **3** is not an $f_{\mathcal{B}}$-cyclic state.

If we forget the last condition in the definition of $\mathcal{F}_n$, the other requirements hold with high probability for every fixed $\mathcal{A} \in \mathcal{E}_n$, as a consequence of Lemma 10. Lemma 12 below states that after our additional restriction, the set we obtain is still sufficiently large.

**Lemma 12.** *With high probability a random complete automaton with $n$ states extends an element of $\mathcal{F}_n$. More precisely, the probability that it does not extend an element of $\mathcal{F}_n$ is at most $n^{-1/4}\log^2 n$, for $n$ sufficiently large.*

*Proof.* Fix $\mathcal{A} \in \mathcal{E}_n$, and consider the extensions $\mathcal{B}$ of $\mathcal{A}$ obtained by adding $b$-transitions to the $\delta_a$-cyclic states. A state $x$ of $\mathbf{Cyc_f}(\mathcal{B})$ is a *bad state* when there exists $y \in \mathbf{Cyc_f}(\mathcal{B})$ and $z \in \mathbf{Cyc_a}(\mathcal{A})$ such that

$$y \xrightarrow{b} z \quad \text{and} \quad z \xrightarrow{u_n} x.$$

In such a case, $y$ is the cyclic predecessor of $x$ for the mapping $f_{\mathcal{B}}$ and it does not satisfy the last condition of $\mathcal{F}_n$'s definition. Clearly, if $\mathcal{B}$ is not in $\mathcal{F}_n$ then either Condition 3 is not satisfied or there is at least one bad state in $\mathcal{B}$.

For a given $x \in \mathbf{Cyc_a}(\mathcal{A})$ and $\ell \in \{0, \dots, n-1\}$, let us bound from above the probability that $x$ is a bad state and in a $f_{\mathcal{B}}$-cycle of length $\ell + 1$ when adding the $b$-transitions. In such a case, there must exist $\ell$ distinct states $x_1, \dots, x_\ell$ of $\mathbf{Cyc_a}(\mathcal{A})$, all distinct from $x$, such that

$$x \xrightarrow{f_{\mathcal{B}}} x_1, x_1 \xrightarrow{f_{\mathcal{B}}} x_2, \dots, x_\ell \xrightarrow{f_{\mathcal{B}}} x,$$

and the image of $x_\ell$ by $b$ must be in $\mathbf{Cyc_a}(\mathcal{A})$. Hence, $\delta_b(x_\ell)$ must belong to $\mathbf{Cyc_a}(\mathcal{A}) \cap \delta_{u_n}^{-1}(\{x\})$. Consequently, the probability that such a cycle exists when we randomly add the $b$-transitions is

$$\mathbb{P}_{\mathcal{A},u_n}(x_1)\mathbb{P}_{\mathcal{A},u_n}(x_2)\cdots\mathbb{P}_{\mathcal{A},u_n}(x_\ell)\cdot\frac{|\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})|}{n}.$$

We sum this quantity for every possible tuple $(x_1,\dots,x_\ell)$ of distinct elements of $E_x=[n]\setminus\{x\}$. Since there are $\ell!$ ways to order each $\{x_1,\dots,x_\ell\}$, we get

$$\ell!\sum_{\substack{x_1<\cdots<x_\ell\\ x_i\in E_x}}\mathbb{P}_{\mathcal{A},u_n}(x_1)\mathbb{P}_{\mathcal{A},u_n}(x_2)\cdots\mathbb{P}_{\mathcal{A},u_n}(x_\ell)\cdot\frac{|\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})|}{n}$$
$$\leq\frac{|\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})|}{n}\ell!\binom{n-1}{\ell}\left(\frac{1-\mathbb{P}_{\mathcal{A},u_n}(x)}{n-1}\right)^{\ell}.$$

The upper bound is obtained by applying Lemma 3 with $f=\mathbb{P}_{\mathcal{A},u_n}$, $E=E_x$, and $s=1-\mathbb{P}_{\mathcal{A},u_n}(x)$. As $\ell!\binom{n-1}{\ell}\leq(n-1)^\ell$, the probability that a given $x$ is a bad state in a $f_{\mathcal{B}}$-cycle of length $\ell+1$ is at most $\frac{1}{n}|\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})|$.

We now use the union bound and sum the contribution of all $x\in\mathbf{Cyc_a}(\mathcal{A})$. Since the $\delta_{u_n}^{-1}(\{x\})$ are pairwise disjoint, then

$$\sum_{x\in\mathbf{Cyc_a}(\mathcal{A})}|\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})|=\left|\bigcup_{x\in\mathbf{Cyc_a}(\mathcal{A})}\mathbf{Cyc_a}(\mathcal{A})\cap\delta_{u_n}^{-1}(\{x\})\right|\leq|\mathbf{Cyc_a}(\mathcal{A})|.$$

Hence, the probability that there is a bad state in a cycle of length $\ell+1$ is at most $\frac{1}{n}|\mathbf{Cyc_a}(\mathcal{A})|$. As $\mathcal{A}\in\mathcal{E}_n$, this probability is at most $\frac{\alpha_n}{n}$.

By Lemma 10, the probability that Condition 3 of the definition of $\mathcal{F}_n$ is not satisfied is smaller than $\frac{M}{n^{1/4}}$, for some positive constant $M$ and for $n$ sufficiently large. Hence, for every fixed $\mathcal{A}\in\mathcal{E}_n$, the probability that there is a bad state or that Condition 3 does not hold is at most, for $n$ sufficiently large,

$$\underbrace{\sum_{\ell=0}^{\beta_n-1}\frac{\alpha_n}{n}}_{\substack{\text{bad state}\\ \text{for }\ell<\beta_n}}+\underbrace{\frac{M}{n^{1/4}}}_{\substack{\text{Condition 3}\\ \text{does not hold}}}=\frac{\alpha_n\beta_n}{n}+\frac{M}{n^{1/4}}\leq\frac{\log^2 n}{n^{1/4}}.$$

Note that we do not need to consider the cases where $\ell\geq\beta_n$ in the first sum, since they do not satisfy Condition 3 and are therefore counted in the second summand.

We therefore obtained a uniform upper bound for every $\mathcal{A}\in\mathcal{E}_n$. Since a complete automaton can extend at most one element of $\mathcal{E}_n$, the law of total probabilities applies: the probability that a complete automaton with $n$ states that extends an element of $\mathcal{E}_n$ does not satisfy Condition 3 or Condition 4 is at most $n^{-1/4}\log^2 n$, for $n$ sufficiently large. This concludes the proof since the probability of not being in $\mathcal{E}_n$ is $\mathcal{O}(\frac{1}{n})$. □

### *4.4. Adding More Random b-Transitions*

Starting from an element of $\mathcal{B} \in \mathcal{F}_n$, we can now use the idea explained at the beginning of Section 4.3, and add the random $b$-transitions that are needed for $\delta_{bb}$ to be totally defined on $\mathbf{Cyc_f}(\mathcal{B})$. For such an extension $\mathcal{C}$ of $\mathcal{B}$, recall that the mapping $g_\mathcal{C}$ is the restriction of $\delta_{bbv_n}$ to $\mathbf{Cyc_f}(\mathcal{B})$. Let $\mathbf{Cyc_g}(\mathcal{C})$ denote the set of $g_\mathcal{C}$-cyclic states in $\mathcal{C}$. Thanks to the last condition of the definition of $\mathcal{F}_n$, we need to randomly choose the $b$-transitions starting from the images by $\delta_b$ of $\mathbf{Cyc_f}(\mathcal{B})$, which are all distinct since two distinct states of $\mathbf{Cyc_f}(\mathcal{B})$ cannot have the same image by $\delta_b$.

Let $\gamma_n = \lfloor 2\,n^{1/8} \log^{7/8} n \rfloor$ and let $X_\mathcal{B}$ denote the set of images of $\mathbf{Cyc_f}(\mathcal{B})$ by $\delta_b$, i. e., $X_\mathcal{B} = \{\, \delta_b(x) \mid x \in \mathbf{Cyc_f}(\mathcal{B}) \,\}$. We define the set $\mathcal{G}_n$ of incomplete automata $\mathcal{C}$ with $n$ states that satisfy the following conditions:

(I) $\mathcal{C}$ extends an automaton $\mathcal{B}$ of $\mathcal{F}_n$.

(II) The only $b$-transitions of $\mathcal{C}$ are those starting from $\mathbf{Cyc_a}(\mathcal{B})$ and from $X_\mathcal{B}$.

(III) The map $g_\mathcal{C}$ has no more than $\gamma_n$ cyclic states and has height at most $\gamma_n$.

(IV) For every $q \in \mathbf{Cyc_g}(\mathcal{C})$, the $b$-transition of $\delta_{bb}(q)$ is undefined.

The last condition in the definition of $\mathcal{G}_n$ is useful for the same kind of reasons than the last condition of $\mathcal{F}_n$ is. It ensures some independency for the final step of the synchronization, which is presented in Section 4.5.

**Lemma 13.** *With high probability, a random complete automaton with n states extends an element of $\mathcal{G}_n$. More precisely, the probability it does not extends an element of $\mathcal{G}_n$ is $\mathcal{O}(\frac{1}{\gamma_n})$.*

*Proof.* We proceed as for Lemma 10 to establish that Condition 3 holds with high probability. Let $\mathcal{B}$ be an element of $\mathcal{F}_n$. When we add random $b$-transitions to the elements of $X_\mathcal{B}$, we obtain an automaton $\mathcal{C}$ whose map $g_\mathcal{C}$ is a random $p$-mapping of $\mathbf{Cyc_f}(\mathcal{B})$. Indeed, for any $x, y \in \mathbf{Cyc_f}(\mathcal{B})$, $g_\mathcal{C}(x) = y$ if and only if $\delta_b(\delta_b(x)) \in \delta_{v_n}^{-1}(\{y\})$, which happens with probability exactly $\frac{1}{n}|\delta_{v_n}^{-1}(\{y\})|$. Let $c$ be the number of elements of $\mathbf{Cyc_f}(\mathcal{B})$. If $c \le \gamma_n$, then Condition 3 holds trivially. Otherwise, by Lemma 4, the probability that $g_\mathcal{C}$ has height greater then $2\sqrt{c \log c}$ or that it has more than $2\sqrt{c \log c}$ cyclic points is at most $\frac{M}{c}$ for some positive constant $M$. Moreover, since $\mathcal{B} \in \mathcal{F}_n$, we know that $c \le \beta_n$. Therefore, for $n$ sufficiently large we have

$$2\sqrt{c \log c} \le 2\sqrt{\beta_n \log \beta_n} = \frac{\sqrt{3}}{2} n^{1/8} \log^{7/8} n \,\big(1 + o(1)\big) \le \gamma_n .$$

As for $c > \gamma_n$ we have $\frac{M}{c} \le \frac{M}{\gamma_n}$, we obtain that $\mathcal{C}$ does not satisfy Condition 3 with probability at most $\frac{M}{\gamma_n}$.

We now handle Condition 4: we prove that with high probability, for every $q \in \mathbf{Cyc_f}(\mathcal{B})$, the $b$-transition of $\delta_{bb}(q)$ is undefined. Once $\mathcal{C}$ is built by adding the $b$-transitions, the defined $b$-transitions start from $\mathbf{Cyc_a}(\mathcal{B})$ or from $X_\mathcal{B}$. Since $\mathcal{B} \in \mathcal{F}_n$, the cardinality of $\mathbf{Cyc_a}(\mathcal{B})$ and $X_\mathcal{B}$ are at most $\alpha_n$ and $\beta_n$, respectively. To build $\mathcal{C}$, we iteratively add a new random outgoing $b$-transitions for each element of $X_\mathcal{B}$; when we add the $i$-th such transition, the probability it ends in a state that has a defined outgoing $b$-transition is therefore at most $\frac{1}{n}(\alpha_n + \beta_n + i - 1)$, which is smaller than $p_n = \frac{3\alpha_n}{n}$ for $n$ sufficiently large, as $i \leq |X_{\mathcal{B}}| \leq \beta_n \leq \alpha_n$. Hence, the probability that Condition 4 holds is at least $(1-p_n)^{|X_{\mathcal{B}}|}$, and for $n$ sufficiently large, we have

$$(1-p_n)^{|X_{\mathcal{B}}|} \geq \left(1 - \frac{3\alpha_n}{n}\right)^{\beta_n} = 1 - \frac{18 \log^{5/4} n}{n^{1/4}} + \mathcal{O}\left(\frac{1}{n^{1/4}}\right) \geq 1 - \frac{\log^2 n}{n^{1/4}}.$$

This conclude the proof, since we get a uniform bound of $\frac{\log^2 n}{n^{1/4}} + \frac{M}{\gamma_n}$ for any base automaton $\mathcal{B} \in \mathcal{F}_n$, and since the probability of not being in $\mathcal{F}_n$ is $\mathcal{O}(n^{-1/4} \log^2 n)$. □

Let $w_n = v_n(bbv_n)^{\gamma_n}$. Lemma 13 ensures that for a random complete automaton $\mathcal{A}$, the image of $\delta_{w_n}$ is usually included in $\mathbf{Cyc_g}(\mathcal{A})$, which has size at most $\gamma_n$. This concludes the first part of the synchronization: with high probability, the word $w_n$ maps the set of states of $\mathcal{A}$ to the much smaller set of states $\mathbf{Cyc_g}(\mathcal{A})$.

### *4.5. Synchronizing the Remaining Cyclic States*

Let $\lambda_n = \lfloor n^{1/4} \rfloor$ and let $\mathcal{C}$ be a fixed automaton of $\mathcal{G}_n$. Starting from $\mathcal{C} \in \mathcal{G}_n$, we now prove that the elements of $\mathbf{Cyc_g}(\mathcal{C})$ can be synchronized with high probability when randomly setting the $b$-transitions that are still undefined. We follow the idea given at the beginning of Section 4 and first prove that with high enough probability, two states of $\mathbf{Cyc_g}(\mathcal{C})$ can be synchronized by a word of the form $b^j w_n$, for some integer $j \geq 0$.

**Lemma 14.** *Let $\mathcal{C} \in \mathcal{G}_n$ and let $q$ and $r$ be two distinct states of $\mathbf{Cyc_g}(\mathcal{C})$. If we add all the missing $b$-transitions to $\mathcal{C}$ by drawing them uniformly at random and independently, then the probability that for all $j \in \{0, \ldots, \lambda_n\}$ we have $\delta_{b^j \cdot w_n}(q) \neq \delta_{b^j \cdot w_n}(r)$ is at most $n^{-3/8} \log^2 n$, for $n$ sufficiently large.*

*Proof.* We say that two states $x$ and $y$ are *$b$-synchronizable* if there exists an integer $j \in \{0, \ldots, \lambda_n\}$ such that $\delta_{b^j \cdot w_n}(x) = \delta_{b^j \cdot w_n}(y)$. In the sequel, we give an upper bound for the probability that $q$ and $r$ are not $b$-synchronizable.

By definition of $\mathcal{G}_n$, the states $q_2 = \delta_{bb}(q)$ and $r_2 = \delta_{bb}(r)$ have no outgoing $b$-transitions in $\mathcal{C}$. If $q_2 = r_2$, then $q$ and $r$ are $b$-synchronizable and we are done. For the remainer of the proof, we therefore assume that $q_2 \neq r_2$. Let us consider the sequence of pairs of states $(q_i, r_i)$ generated iteratively using the following random process, starting with $i = 3$:

(i) Generate $(q_i, r_i)$ uniformly at random in $[n] \times [n]$, and set $\delta_b(q_{i-1}) = q_i$ and $\delta_b(r_{i-1}) = r_i$ in the automaton.

(ii) If $\delta_{w_n}(q_i) = \delta_{w_n}(r_i)$ then stop the process and return a `success` ($q$ and $r$ are $b$-synchronizable).

(iii) Otherwise, if either $q_i$ or $r_i$ already have an outgoing $b$-transition, then stop the process and return a `failure`.

(IV) In other cases, iterate the process for the next value of $i$ by going back to step 1, until $i = \lambda_n$. When $i = \lambda_n$, the process halts and return a `failure`.

Hence, we iteratively and in parallel generate a sequence of missing $b$-transitions, starting from $q_2$ and $r_2$. If the process returns a `success`, then clearly the states are $b$-synchronizable. Thus the probability of returning a `failure` is an upper bound for the probability that they are not $b$-synchronizable.

Given that the process did not halt after building up to $(p_{i-1}, q_{i-1})$ for $3 \leq i < \lambda_n$, the probability that it halts at the next step and returns a `success` is the probability that two randomly chosen elements of $[n]$ have the same image by $\delta_{w_n}$ is exactly

$$s := \sum_{x \in \mathbf{Cyc_g}(\mathcal{C})} \mathbb{P}_{\mathcal{C},w_n}(x)^2. \tag{4}$$

In particular, it does not depend on $i$, it is the same at each step.

Let $Y_{\mathcal{C}}$ denote the set of states of $\mathcal{C}$ that have a defined $b$-transition. Since $\mathcal{C} \in \mathcal{G}_n$, the $b$-transitions of $\mathcal{C}$ start from the elements of $\mathbf{Cyc_a}(\mathcal{C})$ and from their images by $b$. Hence, $|Y_{\mathcal{C}}| \leq 2\alpha_n$. Therefore, given that the process did not halt after building up to $(q_{i-1}, r_{i-1})$ for $3 \leq i < \lambda_n$, the probability $f_i$ that it halts at the next step and returns a `failure` satisfies

$$f_i \leq 1 - \left(1 - \frac{|Y_{\mathcal{C}}| + 2(i-3)}{n}\right)^2.$$

Indeed, it is not a `failure` when both $q_i$ and $r_i$ are not in $Y_{\mathcal{C}}$ and are not one of the $2(i-3)$ states that received a $b$-transition during the previous iterations of the process. This is an upper bound, since some of theses cases yield a `success` (the case (II)). As $\lambda_n = o(\alpha_n)$, for $n$ sufficiently large we have

$$\begin{aligned} f_i &\leq 1 - \left(1 - \frac{|Y_{\mathcal{C}}| + 2(i-3)}{n}\right)^2 = 2\,\frac{|Y_{\mathcal{C}}| + 2(i-3)}{n} - \frac{(|Y_{\mathcal{C}}| + 2(i-3))^2}{n^2} \\ &\leq 2\frac{|Y_{\mathcal{C}}| + 2i}{n} \leq 2\frac{|Y_{\mathcal{C}}| + 2\lambda_n}{n} \leq \frac{5\,\alpha_n}{n}. \end{aligned}$$

Observe that this upper bound does not depend on $i$. For $j \in \{2, \ldots, \lambda_n - 1\}$, the probability that the process did not halt at a step $\leq j$ is, for $n$ sufficiently large,

$$\mathbb{P}(\text{did not halt at a step } \leq j) = \prod_{i=3}^{j} \bigl(1 - (s + f_i)\bigr) \geq \left(1 - s - \frac{5\alpha_n}{n}\right)^{j-2}.$$

The probability that the process halts with a `success` at a given step $i \in \{3, \ldots, \lambda_n\}$ is the probability that it did not halt before multiplied by $s$, the probability that two random elements of $[n]$ have the same image by $w_n$. Thus, the following inequality holds:

$$\mathbb{P}(\text{halts at step } i \text{ with a } \texttt{success}) \geq \left(1 - s - \frac{5\alpha_n}{n}\right)^{i-3} s.$$

Hence, the probability that the process halts with a success satisfies

$$\begin{aligned}\mathbb{P}(\texttt{success}) &= \sum_{i=3}^{\lambda_n} \mathbb{P}(\text{halts at step } i \text{ with a } \texttt{success})\\ &\geq s \sum_{j=0}^{\lambda_n - 3} \left(1 - s - \frac{5\alpha_n}{n}\right)^j = \frac{s}{s + \frac{5\alpha_n}{n}} \left(1 - \left(1 - s - \frac{5\alpha_n}{n}\right)^{\lambda_n - 2}\right)\end{aligned}$$

By Cauchy-Schwarz inequality applied to Equation (4), we have $s \geq \frac{1}{|\mathbf{Cyc_g}(\mathcal{C})|} \geq \frac{1}{\gamma_n}$. Hence, as $\frac{1}{1+x} \geq 1 - x$, for $n$ sufficiently large, we have

$$\frac{s}{s + \frac{5\alpha_n}{n}} = \frac{1}{1 + \frac{5\alpha_n}{ns}} \geq 1 - \frac{5\alpha_n}{ns} \geq 1 - \frac{5\alpha_n \gamma_n}{n} \geq 1 - \frac{\log^2 n}{2n^{3/8}}.$$

And also, for $n$ sufficiently large we have

$$\begin{aligned}\left(1 - s - \frac{5\alpha_n}{n}\right)^{\lambda_n - 2} &\leq \left(1 - \frac{1}{\gamma_n}\right)^{\lambda_n - 2} = \exp\left((\lambda_n - 2)\log\left(1 - \gamma_n^{-1}\right)\right)\\ &\leq \exp\left(-(\lambda_n - 2)\gamma_n^{-1}\right) \leq \exp\left(-n^{1/9}\right)\end{aligned}$$

Therefore, for $n$ sufficiently large,

$$\mathbb{P}(\texttt{failure}) = 1 - \mathbb{P}(\texttt{success}) \leq \frac{\log^2 n}{2n^{3/8}} + \mathcal{O}\left(\exp\left(-n^{1/9}\right)\right) \leq \frac{\log^2 n}{n^{3/8}}.$$

This concludes the proof. □

To conclude the proof of Theorem 5, we use the union bound: for any automaton $\mathcal{A}$ that extends an element of $\mathcal{G}_n$, which happens with high probability, there are less than $\gamma_n^2$ pairs of states in $\mathbf{Cyc_g}(\mathcal{A})$; the probability that one of these pairs $(q, r)$ cannot be synchronized using a word of the form $b^j \cdot w_n$ is therefore at most $\gamma_n^2 \cdot n^{-3/8} \log^2 n$, which is $\mathcal{O}(n^{-\frac{1}{8}} \log^4 n)$.

To obtain the length of the synchronizing word, we apply Lemma 2 to the elements of $\mathbf{Cyc_g}(\mathcal{A})$: with high probability there are at most $\gamma_n$ such states, which can be pairwise synchronized using words of the form $b^j w_n$, of length at most $|w_n| + \lambda_n$. Hence, the set $\mathbf{Cyc_g}(\mathcal{A})$ can be synchronized using a word $z$ of length at most $(\gamma_n - 1)(|w_n| + \lambda_n)$, which is $\mathcal{O}(n \log^3 n)$ as $|w_n|$ is $\mathcal{O}(n^{7/8} \log^{17/8} n)$. This concludes the proof, as $w_n z$ is synchronizing and has length in $\mathcal{O}(n \log^3 n)$.

## 5. Conclusion

In this article, we proved that most complete automata are synchronizing and admit a synchronizing word of length $\mathcal{O}(n \log^3 n)$, for the uniform distribution on deterministic and complete automata on an alphabet with at least two letters.

Our proof can be turned into an heuristic that try to find a short synchronizing word, which succeeds with high probability for uniform random automata: $\delta_{w_n}$

and $\mathbf{Cyc_g}(\mathcal{A})$ can be computed by just verifying some conditions on the height and cycle length of three mappings; once it is done, checking whether the property of Lemma 14 holds for every pair of elements of the image of $\delta_{w_n}$ can be achieved in sublinear expected time, as it is very small with high probability. Experiments seem to indicate that this algorithm behaves better in practice than its theoretical analysis: it looks like an important proportion of automata that fail to fulfill every step of our construction are still detected as synchronizing by the combination of computing $\delta_{w_n}$ and synchronizing the states of its image with the $b^j$'s.

A natural continuation of this work is to prove that with high probability automata are synchronized by words that are way shorter than $n \log^3 n$. Experiments have been done in [19], and seem to indicate that the expected length of the smallest synchronizing word is often sublinear, probably in $\Theta(\sqrt{n})$. But one can see in our proof that we obtained the synchronization in a very specific way: we have a fixed word $w_n$ and synchronize pairwise the elements of $\delta(Q, w_n)$ using words of the form $b^i w_n$ only. There are probably plenty of other ways to synchronize random automata with high probability, possibly leading to shorter reset words. It still might be quite difficult to match the bounds predicted in [19].

Since our construction relies on the fact that a typical random mapping has a small number of cyclic points, one can wonder if random automata with a large number of cyclic states, for every letter, are still synchronizing with high probability. Together with Berlinkov, we recently obtained a result in that direction [4]: most almost-group automata are synchronizing, where in an almost-group automata every letter acts as a permutation, except one of them which permutes only $n-1$ states. These automata are very different from uniform random automata, but they are still synchronizing with high probability.

## Acknowledgements

The author would like to thank Marie-Pierre Béal and Dominique Perrin for their interest in this work since the very beginning, and Mikhail Berlinkov for our fruitful discussions on this topic.

## References

[1] F. Bassino, J. David, C. Nicaud, Average case analysis of Moore's state minimization algorithm. *Algorithmica* **63** (2012) 1–2, 509–531.

[2] F. Bassino, J. David, A. Sportiello, Asymptotic enumeration of minimal automata. In: C. Dürr, T. Wilke (eds.), *29th International Symposium on Theoretical Aspects of Computer Science, STACS 2012, February 29th – March 3rd, 2012, Paris, France*. LIPIcs 14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2012, 88–99.

[3] M. V. Berlinkov, On the probability of being synchronizable. In: S. Govindarajan, A. Maheshwari (eds.), *Algorithms and Discrete Applied Mathematics – Second International Conference, CALDAM 2016, Thiruvananthapuram, India, February 18 – 20, 2016, Proceedings*. LNCS 9602, Springer, 2016, 73–84.

[4] M. V. Berlinkov, C. Nicaud, Synchronizing random almost-group automata. In: C. Câmpeanu (ed.), *Implementation and Application of Automata – 23rd International Conference, CIAA 2018, Charlottetown, PE, Canada, July 30 – August 2, 2018, Proceedings*. LNCS 10977, Springer, 2018, 84–96.

[5] M. V. Berlinkov, M. Szykuła, Algebraic synchronization criterion and computing reset words. *Information Sciences* **369** (2016), 718–730.

[6] X. S. Cai, L. Devroye, The graph structure of a deterministic automaton chosen at random. *Random Structures and Algorithms* **51** (2017) 3, 428–458.

[7] P. J. Cameron, Dixon's theorem and random synchronization. *Discrete Mathematics* **313** (2013) 11, 1233–1236.

[8] A. Carayol, C. Nicaud, Distribution of the number of accessible states in a random deterministic automaton. In: C. Dürr, T. Wilke (eds.), *29th International Symposium on Theoretical Aspects of Computer Science, STACS 2012, February 29th – March 3rd, 2012, Paris, France*. LIPIcs 14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2012, 194–205.

[9] J. Černý, Poznámka k homogénnym eksperimentom s konečnými automatmi. *Matematicko-fyzikalny Časopis Slovenskej Akadémie Vied* **14** (1964) 3, 208–216. (Translation: A note on homogeneous experiments with finite automata. *Journal of Automata, Languages and Combinatorics* **24** (2019) 2–4, 123–132).

[10] J. David, Average complexity of Moore's and Hopcroft's algorithms. *Theoretical Computer Science* **417** (2012), 50–65.

[11] S. de Felice, C. Nicaud, Average case analysis of Brzozowski's algorithm. *International Journal of Foundations of Computer Science* **27** (2016) 2, 109–126.

[12] P. Flajolet, A. M. Odlyzko, Random mapping statistics. In: J. Quisquater, J. Vandewalle (eds.), *Advances in Cryptology – EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10 – 13, 1989, Proceedings*. LNCS 434, Springer, 1990, 329–354.

[13] P. Flajolet, R. Sedgewick, *Analytic Combinatorics*. Cambridge University Press, 2009.

[14] P. Frankl, An extremal problem for two families of sets. *European Journal of Combinatorics* **3** (1982), 125–127.

[15] P. Gawrychowski, D. Straszak, Strong inapproximability of the shortest reset word. In: G. F. Italiano, G. Pighizzini, D. Sannella (eds.), *Mathematical Foundations of Computer Science 2015 – 40th International Symposium, MFCS 2015, Milan, Italy, August 24 – 28, 2015, Proceedings, Part I*. LNCS 9234, Springer, 2015, 243–255.

[16] A. A. Grusho, О предельных распределениях некоторых характеристик случайных автоматных графов. *Математические заметки* **14** (1973) 1, 133–141. (Translation: Limit distributions of certain characteristics of random automaton graphs. *Mathematical notes of the Academy of Sciences of the USSR* **14** (1973) 1, 633–637).

[17] B. Harris, Probability distributions related to random mappings. *The Annals of Mathematical Statistics* **31** (1960) 4, 1045–1062.

[18] R. M. Karp, The transitive closure of a random digraph. *Random Structures and Algorithms* **1** (1990) 1, 73–94.

[19] A. Kisielewicz, J. Kowalski, M. Szykuła, A fast algorithm finding the shortest reset words. In: D.-Z. Du, G. Zhang (eds.), *Computing and Combinatorics, 19th International Conference, COCOON 2013, Hangzhou, China, June 21 – 23, 2013, Proceedings*. LNCS 7936, Springer, 2013, 182–196.

[20] V. F. Kolchin, Случайные отображения. Наука, Москва, 1984. (Translation: *Random Mappings*. Translations series in Mathematics and Engineering, Springer, 1986).

[21] A. D. Korshunov, О перечислении конечных автоматов (Translation: On the enumeration of finite automata). Проблемы Кибернетики **34** (1978), 5–82.

[22] R. Motwani, P. Raghavan, *Randomized algorithms*. Cambridge university press, 1995.

[23] C. Nicaud, Random deterministic automata. In: E. Csuhaj-Varjú, M. Dietzfelbinger, Z. Ésik (eds.), *Mathematical Foundations of Computer Science 2014 – 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25 – 29, 2014. Proceedings, Part I*. LNCS 8634, Springer, 2014, 5–23.

[24] C. Nicaud, Fast synchronization of random automata. In: K. Jansen, C. Mathieu, J. D. P. Rolim, C. Umans (eds.), *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2016, September 7 – 9, 2016, Paris, France*. LIPIcs 60, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2016, 43:1–43:12.

[25] J. Olschewski, M. Ummels, The complexity of finding reset words in finite automata. In: P. Hliněný, A. Kučera (eds.), *Mathematical Foundations of Computer Science 2010 – 35th International Symposium, MFCS 2010, Brno, Czech Republic, August 23 – 27, 2010, Proceedings*. LNCS 6281, Springer, 2010, 568–579.

[26] J.-E. Pin, On two combinatorial problems arising from automata theory. *Annals of Discrete Mathematics* **17** (1983), 535–548.

[27] Y. Shitov, An improvement to a recent upper bound for synchronizing words of finite automata. *Journal of Automata, Languages and Combinatorics* **24** (2019) 2–4, 367–373.

[28] E. S. Skvortsov, Y. Zaks, Synchronizing random automata. *Discrete Mathematics & Theoretical Computer Science* **12** (2010) 4, 95–108.

[29] M. Szykuła, Improving the upper bound on the length of the shortest reset word. In: R. Niedermeier, B. Vallée (eds.), *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France*. LIPIcs 96, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018, 56:1–56:13.

[30] M. V. Volkov, Synchronizing automata and the Černý conjecture. In: C. Martín-Vide, F. Otto, H. Fernau (eds.), *Language and Automata Theory and Applications, Second International Conference, LATA 2008, Tarragona, Spain, March 13 – 19, 2008. Revised Papers*. LNCS 5196, Springer, 2008, 11–27.

[31] Y. I. Zaks, E. S. Skvortsov, Синхронизируемые случайные автоматы над 4-буквенным алфавитом. *Комбинаторика и теория графов, IV.* Записки научных семинаров ПОМИ **402**, 2012, ПОМИ, СПб., 83–90. (Translation: Synchronizing random automata on a 4-letter alphabet. *Journal of Mathematical Sciences* **192** (2013), 303–306).

(Received: October 31, 2018; revised: February 4, 2019)