Discrete Mathematics and Theoretical Computer Science DMTCS vol. **12:4**, 2010, 95–108

Synchronizing random automata

Evgeny Skvortsov[1†] and Yulia Zaks[2‡]

[1] *School of Computing Science, Simon Fraser University, Burnaby, BC, CANADA*
[2] *Department of Mathematics and Mechanics, Ural State University, Yekaterinburg, RUSSIA*

received 31st October 2009, revised 27th August 2010, accepted 5th October 2010.

Conjecture that any synchronizing automaton with n states has a reset word of length $(n-1)^2$ was made by Černý in 1964. Notwithstanding the numerous attempts made by various researchers this conjecture hasn't been definitively proven yet. In this paper we study a random automaton that is sampled uniformly at random from the set of all automata with n states and $m(n)$ letters. We show that for $m(n) > 18 \ln n$ any random automaton is synchronizing with high probability. For $m(n) > n^{\beta}$, $\beta > 1/2$ we also show that any random automaton with high probability satisfies the Černý conjecture.

Keywords: Synchronizing DFA; Random DFA; Wormald's Theorem; Černý problem

Introduction

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a *deterministic finite automaton* (DFA), where Q denotes a state set, Σ stands for an input alphabet, and $\delta : Q \times \Sigma \to Q$ is a transition function defining an action of the letters in Σ on Q. A word w is said to be a *reset word* for DFA $\mathcal{A}$ if its action leaves $\mathcal{A}$ in one particular state no matter what state it starts at: $\delta(q_1, w) = \delta(q_2, w)$ for all $q_1, q_2 \in Q$. A DFA $\mathcal{A}$ is called *synchronizing* if it possesses a reset word.

It is not too difficult to see that if an automaton with n states is synchronizing then there exists a reset word of length n^3 or shorter. It is not that easy, however, to see whether or not this bound is tight. In 1964 Černý formulated a conjecture concerning an upper bound of the length of the shortest reset word of a synchronizing DFA [4]: the length cannot be larger than $(n-1)^2$. By now the Černý conjecture is arguably the most long standing open problem in the combinatorial theory of finite automata. The best upper bound has been obtained so far is $(n^3 - n)/6$; it was proved by Pin [10] in 1983.

In fact, *slowly synchronizing automata*, i.e. automata with the shortest reset word of length $\Theta(n^2)$ are known to be exceptional. For a long time the only infinite series of such automata was the original one proposed by Černý [4]. The other substantially different ones [2] have only recently been constructed.

On the other hand, Higgins has shown that a composition of $2n$ random mappings of a set of size n into itself *with high probability* (whp) is a mapping with an image of size 1. (By "high probability" we mean

† Email: `skvortsoves@googlemail.com`. Current affiliation Google Inc.

‡ Email: `yuzaks@gmail.com`. The second author acknowledges support from the Federal Education Agency of Russia, grant 2.1.1/3537, and from the Russian Foundation for Basic Research, grants 09-01-12142 and 10-01-00793.

that the probability tends to 1 with n going to infinity.) In terms of automata, Higgins's result means that a random automaton with an alphabet of size larger than $2n$ whp has a reset word of length $2n$. Indeed, if we pick an automaton uniformly at random among all automata with n states and $2n$ letters then the action of a word composed of all the letters is identical to a mapping composed of $2n$ random mappings.

The problem of finding the shortest reset word for a given automaton is both NP-hard [5] and co-NP-hard [12], which dramatically limits a size of automata feasible for numerical experiments. A limited simulation that we conducted supposedly shows that a random automaton on 2-letter alphabet whp has a reset word of a length sublinear with respect to the number of states.

The numerical experiment output combined with Higgins's result offers a new field of research: study of the shortest reset word of random automata, or the *most probable* length of the shortest reset word, as opposed to the classical problem of the upper bound; and allows to put forward a hypothesis that the most probable length should be much smaller than the upper bound.

Starting this new line of research we address the following questions.

- What size of an alphabet implies that almost all automata with the alphabet of this size are synchronizing and what is the length of the shortest reset word in this case?

- What size of an alphabet implies that almost all automata with the alphabet of this size are synchronizing and comply with the Černý conjecture?

In this paper we show that $2n$ upper bound can be improved with regards to both of these questions. We show that if an alphabet size is greater than $18 \ln n$ then an automaton whp is synchronizing and if an alphabet consists of more than $n^{1/2+\epsilon}$ letters for some positive ϵ then it whp satisfies the Černý conjecture.

To get the latter bound we apply the Wormald's theorem [13]. The theorem allows one to reduce the analysis of a stochastic process to a system of differential equations. This method was originally developed for the analysis of algorithms on random graphs [13] and was later used to proof the efficiency of algorithms for the random Satisfiability problem [1].

Also as a byproduct of the latter bound we address the problem of an epidemia spreading invertedly to the edges of a directed graph corresponding to two mappings. The problem of the epidemia spread along a digraph of one random mapping was formulated and initially studied by B. Gertbakh [6], and further explored by J. Jaworski [8]. We show that in a digraph with edges corresponding to two random mappings if one individual is infected, then the whole population will be with constant probability infected, too.

The paper is organized as follows. The results of the work are stated and discussed in Section 1. The proofs of the two main theorems are stated in Section 1 and presented in Sections 2 and 3. The Wormald's theorem and the other results used in the work are formulated in Appendix.

1 Main result

Consider a set of states Q and an alphabet Σ. Let us pick uniformly at random a transition function δ from the set $\{\delta : Q \times \Sigma \to Q\}$. A resulting triple (Q, Σ, δ) defines a *random deterministic finite automaton*. It is important to note that a random automaton can be constructed as follows: for each $q \in Q$ and for each $a \in \Sigma$ we choose $q' = \delta(q, a)$ uniformly at random from Q.

The following theorem states the lower bound of the alphabet size that whp guarantees synchronizability of the random automaton.

Theorem 1 *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a random automaton such that $|Q| = n$, $|\Sigma| > 18 \ln n$. Then A is synchronizing whp. Moreover, the length of the shortest reset word of $\mathcal{A}$ is whp less than $3n^2 \ln n$.*

The theorem proof is presented in Section 2.

The natural question is whether the bound stated in Theorem 1 is tight. From our point of view it is not and we conjecture that even a 2-letter alphabet is sufficient for synchronizability of a random automaton. At the moment, however, this question remains open.

The length of the shortest reset word $3n^2 \ln n$ is smaller than the one obtained by Pin, but is still larger than Černý's. To comply with the Černý Conjecture we should enlarge our alphabet. Here we state the following theorem.

Theorem 2 *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a random automaton such that $|Q| = n$, $|\Sigma| > n^{1/2+\epsilon}$ for some $\epsilon > 0$. Then $\mathcal{A}$ is whp synchronizing. Moreover, the length of the shortest reset word of $\mathcal{A}$ is whp at most $(n-1)^2$ letters.*

The theorem proof is presented in Section 3.

We believe that the bound stated by the Černý Conjecture is far from being tight for random automata and according to numerical experiments the tight one should be a sublinear one, as well.

2 The proof of Theorem 1

Let $\mathbf{u}, \mathbf{v}$ be a pair of states of a random automaton $\mathcal{A} = (Q, \Sigma, \delta)$. Consider the process called VACUUM procedure. The aim of the process is to find a word $w = a_1 \ldots a_k$ such that $\mathbf{u}w = \mathbf{v}w$.

At the first step of the process we randomly choose a letter $a_1 \in \Sigma$ and move from $\mathbf{u} = \mathbf{u}_0$ to $\mathbf{u}_1 = \mathbf{u}_0 a_1$ and from $\mathbf{v} = \mathbf{v}_0$ to $\mathbf{v}_1 = \mathbf{v}_0 a_1$. If $\mathbf{u}_1 = \mathbf{v}_1$ then the process successfully finishes with $w = a_1$, else it continues.

At the m-th step we have two states $\mathbf{u}_{m-1}$ and $\mathbf{v}_{m-1}$. Let us choose a letter a_m that has not been applied yet to any of the states $\mathbf{u}_{m-1}$ and $\mathbf{v}_{m-1}$. If we cannot choose such a letter, the process fails. If we can choose a_m, we make a move from $\mathbf{u}_{m-1}, \mathbf{v}_{m-1}$ to $\mathbf{u}_m, \mathbf{v}_m$ similar to the first one. If $\mathbf{u}_m = \mathbf{v}_m$ the process finishes with $w = a_1 a_2 \ldots a_m$, else it continues. Obviously, at any step there are three possible outcomes for the process: it can fail, it can successfully finish and it can continue. So if it does not fail then at some step k it finishes with $w = a_1 \ldots a_k$ such that $\mathbf{u}w = \mathbf{v}w$.

A formal description of the procedure is presented at Fig. 1

Now let us pass over to the behavior of the VACUUM procedure.

Lemma 1 *If the* VACUUM *procedure is applied to a random automaton $\mathcal{A} = (Q, \Sigma, \delta)$ and performs at least t steps then each of the paths $\{\mathbf{u}_0, \ldots, \mathbf{u}_t\}$ and $\{\mathbf{v}_0, \ldots, \mathbf{v}_t\}$ is indistinguishable from a random walk path on a complete directed graph.*

Proof: In other words, we should prove, that any $\mathbf{u}_i$ is selected uniformly at random. Indeed, if we choose a letter a_i at any step t we will get $\mathbf{u}_i = \mathbf{u}_{i-1} a_i$ for a letter a_i that has never been used at the state $\mathbf{u}_{i-1}$. Random selection of a new letter for the transition from the state in a random automaton is equal to uniformly-at-random selection of the transition result $\mathbf{u}_t$. Thus, $\mathbf{u}_i$ (similarly $\mathbf{v}_i$) is selected uniformly at random from Q and is history-independent.

The same proposition can be proved constructively. Let $B = (Q, E)$ be a complete directed graph; $\{\mathbf{u}_0, \ldots, \mathbf{u}_t\}$ and $\{\mathbf{v}_0, \ldots, \mathbf{v}_t\}$ - random walk paths in B of the length t. We construct from B a random

INPUT: A random automaton $\mathcal{A} = (Q, \Sigma, \delta)$ and a pair of states $\mathbf{u} \in Q, \mathbf{v} \in Q$
OUTPUT: **failure** or a word $w = a_1 \dots a_k$ such that $\mathbf{u}w = \mathbf{v}w$
METHOD:
  let $\Delta_q \subseteq \Sigma$, $w \in \Sigma^*$
  initialize $\Delta_q = \varnothing$ for all $\mathbf{q} \in Q$, $w = \varepsilon$
  while $\mathbf{u}w \neq \mathbf{v}w$
    if $\Delta_{\mathbf{u}w} \cup \Delta_{\mathbf{v}w} \neq \Sigma$ **then**
      choose $a \in \Sigma \setminus (\Delta_{\mathbf{u}w} \cup \Delta_{\mathbf{v}w})$
    else
      return failure
    let $\Delta_{\mathbf{u}w} = \Delta_{\mathbf{u}w} \cup \{a\}$, $\Delta_{\mathbf{v}w} = \Delta_{\mathbf{v}w} \cup \{a\}$
    let $w = wa$
  return w

Fig. 1: VACUUM procedure

automaton A with 2 paths performing first t steps of the VACUUM procedure. We label all edges in E with letters from Σ using the following algorithm: moving along the random paths we label the edge from $\mathbf{u}_i$ (then similarly $\mathbf{v}_i$) with an arbitrary letter never used in this vertex before, then we label other edges uniformly at random such that every vertex has $|\Sigma|$ outgoing edges labelled with different letters. After labelling we remove all unlabelled edges. The result is by defintion a random automaton and our paths are precisely the first t steps of VACUUM (while labelling the edges we were using the same logic). The construction of B from A consists in adding edges and erasing labels from the existing ones. Explanation of the fact that $\{\mathbf{u}_0, \dots, \mathbf{u}_t\}$ and $\{\mathbf{v}_0, \dots, \mathbf{v}_t\}$ are the random walk paths in B is completely equivalent to one performed in the first proof of the lemma. □

Next we are bounding the probability of long executions of the VACUUM procedure.

Lemma 2 *If the* VACUUM *procedure is applied to a pair* $\mathbf{u}, \mathbf{v}$ *of states of a random automaton* $\mathcal{A} = (Q, \Sigma, \delta)$ *such that* $|Q| = n$ *then for an arbitrary constant* K *the probability that this procedure makes at least* $Kn \ln n$ *steps is less than* n^{-K}.

Proof: As we have already observed, at every step $t < Kn \ln n$ the process either fails or continues: states $\mathbf{u}_t$ and $\mathbf{v}_t$ are selected independently and uniformly at random from Q. The probability that $\mathbf{u}_t$ and $\mathbf{v}_t$ will coincide equals $\frac{1}{n}$. Thus, the probability that the process will not terminate within $Kn \ln n$ steps is less than $\left(1 - \frac{1}{n}\right)^{Kn \ln n} \leq n^{-K}$ □

So far we have proved that the probability of the existence of a long path $u_1 u_2 \dots u_t$ is rather low. Next, another question arises: how often do these states repeat in this path? In order to answer this question we need to obtain a certain information on a random path in a complete digraph — it is formulated below.

Lemma 3 *Let* $\mathbf{q}_1, \dots, \mathbf{q}_{Kn \ln n}$ *for some constant* K *be a random walk path in a complete digraph of size* n *then for any constant* $L, L > K$ *the probability that there is a vertex* $\mathbf{x}$ *such that* $|\{i \mid \mathbf{q}_i = \mathbf{x}\}| \geq L \ln n$ *is less than* $n^{1 - \frac{(L-K)^2}{6K}}$ *for a sufficiently large* n.

Proof: The expectation of $|\{i \mid \mathbf{q}_i = \mathbf{x}\}|$ for $bx \in Q$ equals to $\frac{1}{n} \times Kn \ln n = K \ln n$. So the Chernoff bound for the random variable $|\{i \mid \mathbf{q}_i = \mathbf{x}\}|$ gives (see for example [9])

$$\mathbf{P}\left(\Big||\{i \mid \mathbf{q}_i = \mathbf{x}\}| - K\ln n\Big| > \delta K \ln n\right) \leq 2e^{-\frac{\delta^2 K \ln n}{3}}. \quad (1)$$

Setting $\delta = \frac{L-K}{K}$ we get required inequality

$$\mathbf{P}\left(\Big||\{i \mid \mathbf{q}_i = \mathbf{x}\}| - K\ln n\Big| > (L-K)\ln n\right) \leq 2e^{-\frac{(L-K)^2 \ln n}{3K}} \leq n^{-\frac{(L-K)^2}{6K}}. \quad (2)$$

The last inequality holds for a sufficiently large n. Applying the union bound to all $\mathbf{x} \in Q$ we get the desired bound $n^{1-\frac{(L-K)^2}{6K}}$ and finish the proof. □

Now we are ready to prove the key lemma of the section.

Lemma 4 *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a random automaton such that $|Q| = n, |\Sigma| > 18 \ln n$ then for any two states $\mathbf{u} \in Q, \mathbf{v} \in Q$ the* VACUUM *procedure whp does not fail.*

Proof: Setting $K = 3$ in Lemma 2 we conclude that the VACUUM procedure will not terminate within $3n \ln n$ steps with the probability at most n^{-3}. It means that our procedure will finish with a word w, or with failure, with the probability at least $1 - n^{-3}$.

Setting $L = 18$ in Lemma 3 and using Lemma 1 we conclude that the probability that $\mathbf{u}_t$ or $\mathbf{v}_t$ will visit some state more than $18 \ln n$ times is less than $2n^{-23/2}$.

If there are $18 \ln n$ letters in our alphabet and there is a state x such that $|\{i \mid \mathbf{q}_i = \mathbf{x}\}| \geq 18 \ln n$ then the process will fail at the j-th step when we come to x for $(18n \ln n + 1)$-th time.

There are more than $18n \ln n$ letters, thus the probability that the process will fail is less than $2n^{-23/2}$.

There are only two possibilities not to find the word w before the $3n \ln n$-th step — to fail or to continue the process after this step, therefore the probability not to find the word w before the step $3n \ln n$ is at most $n^{-3} + 2n^{-23/2} \leq 3n^{-3}$. That means that the VACUUM procedure finishes with the probability $1 - 3n^{-3}$. The Lemma is proved. □

Proof Proof of Theorem 1.: Our Theorem 1 is easily derived from Lemma 4. Application of the union bound to all pairs of states $\mathbf{u}, \mathbf{v} \in Q$ finishes the synchronizability proof. The length of the reset word that is stated in the theorem is derived from the fact that every two states of the automaton may be synchronized within $3n \ln n$ steps. In order to synchronize the automaton we subsequently synchronize $(n-1)$ pairs. □

3 The proof of Theorem 2

Let us define one more procedure on automata, entitled EPIDEMIA — this algorithm works for automata with a 2-letter alphabet. It takes a random automaton $\mathcal{A} = (Q, \{a, b\}, \delta)$ and a state $\mathbf{x} \in Q$ and returns a set Q_2 of all the states from which $\mathbf{x}$ can be reached.

Let a state $\mathbf{q} \in Q$ have some illness and this illness can invertedly spread along the edges, i.e., if the state $\mathbf{q}$ is ill, then at a certain time all the states $\{\mathbf{u} \mid \mathbf{u}a = \mathbf{q} \vee \mathbf{u}b = \mathbf{q}\}$ will be ill, too. In these terms the aim of the procedure is to find all states that could be infected when only state x is initially ill.

INPUT: A random automaton $\mathcal{A} = (Q, \{a, b\}, \delta)$ and a state $\mathbf{x} \in Q$
OUTPUT: a set Q_2 of all the states from which $\mathbf{x}$ can be reached
METHOD:
let Q_0, Q_1, Q_2 be the subsets of Q
intialize $Q_0 = Q \setminus \{\mathbf{x}\}, Q_1 = \{\mathbf{x}\},\ Q_2 = \varnothing$
while $Q_1 \neq \varnothing$
  choose $\mathbf{q} \in Q_1$ arbitrary
  let $N = \{\mathbf{u} \in Q_0 \mid \mathbf{u}a = \mathbf{q}\ \vee \mathbf{u}b = \mathbf{q}\}$
  let $Q_0 = Q_0 \setminus N, Q_1 = (Q_1 \setminus \{\mathbf{q}\}) \cup N, Q_2 = Q_2 \cup \{\mathbf{q}\}$
return Q_2

Fig. 2: EPIDEMIA procedure

The algorithm works as follows. At each step of the algorithm we introduce 3 sets: Q_2 is the set of all states that are ill now and have already infected all their neighbours, Q_1 is the set of all states that are ill but have not infected their neighbours yet, Q_0 is the set of all states that are still healthy.

At the first step $Q_0 = Q \setminus \{\mathbf{x}\}, Q_1 = \{\mathbf{x}\},\ Q_2 = \varnothing$. At every step of the process we pick $\mathbf{q} \in Q_1$ arbitrarily and consider a set $N = \{\mathbf{u} \in Q_0 \mid \mathbf{u}a = \mathbf{q}\ \vee \mathbf{u}b = \mathbf{q}\}$ of all the healthy states that can be infected by $\mathbf{s}$. At this step we exclude N from Q_0 and include it into Q_1— from now on the states from this set are infected and may infect the new states at the following steps. State $\mathbf{q}$ is transferred to Q_2— from now on it is not dangerous for the healthy states. At some step Q_1 becomes empty: all the states that could be infected are infected. Q_2 is constructed. A formal description of the procedure is presented on Fig. 2. A step of the procedure is illustrated on Fig. 3.

We shall also need the following technical lemma.

Lemma 5 *For any letter a probability that there is a state $\mathbf{q}$ such that there are at least $n^{1/5}$ states $\mathbf{q}'$ for which $\mathbf{q}'a = \mathbf{q}$ is at most $e^{-cn^{1/5}}$ for some constant c.*

Proof: It is known that for any n, m we have

$$\binom{n}{m} \leq \left(\frac{ne}{m}\right)^m. \tag{3}$$

For a fixed $\mathbf{q}$ and a fixed set M of $n^{1/5}$ other states the probability that for all of them application of a letter a leads to $\mathbf{q}$ is less than

$$n^{-n^{1/5}} = e^{-n^{1/5} \ln n}. \tag{4}$$

There are less than

$$n\binom{n}{n^{1/5}} \leq n(n^{1-1/5}e)^{n^{1/5}} \leq e^{(\frac{4}{5}+o(1))n^{1/5} \ln n} \tag{5}$$

ways to choose $\mathbf{q}$ and M. By the union bound, the probability that such a set M and a state $\mathbf{q}$ exist is less than $e^{-(\frac{1}{5}n^{1/5}+o(1)) \ln n}$. □

Now we are ready to state the key lemma of this section.

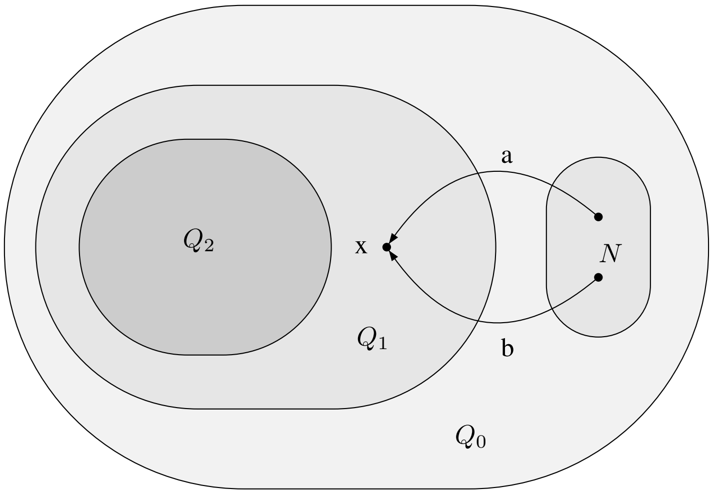

Fig. 3: One step of the EPIDEMIA procedure.

Lemma 6 *If $\mathcal{A} = (Q, \{a, b\}, \delta)$ is a random automaton over a two-letter alphabet and $\mathbf{x} \in Q$. Then there is a constant r, $0 < r < 1$, such that for sufficiently large n probability of the event "for any state $\mathbf{q} \in Q$ there is a word $w_{\mathbf{q}\to\mathbf{x}} \in \{a, b\}^*$ satisfying $\mathbf{q}w_{\mathbf{q}\to\mathbf{x}} = \mathbf{x}$" is greater than r.*

Proof: We consider a state $\mathbf{x} \in Q$ and compute the probability that it can be reached from any element of Q, i.e. the EPIDEMIA procedure with $\mathbf{x}$ on input returns $Q_2 = Q$. The computation may be divided into 3 parts:

- computation of the probability that the process will not terminate in the very beginning and at least $0.1n$ steps will be made;
- computation of the probability that the process will not terminate in the middle between $0.1n$-th and $0.9n$-th steps;
- computation of the probability that the process will not finish at the end before $|Q_2| = n$, i.e. if the EPIDEMIA makes $0.9n$ steps, then it will make n.

Let us start with the first probability. Execution of the EPIDEMIA procedure for a random automaton can be viewed as a Galton-Watson process. That is, at every step we have a population of species Q_1. One of them (namely $\mathbf{q}$) dies, but possibly leaves some offsprings N. The question of interest for us is the following: how many species will ever be born? We will use this model for the first $n/10$ steps of the procedure. Within this model at the step t the set N will be viewed as a set of all offsprings of $\mathbf{q}$. Note that if at the step $t < 0.1n$ we happened to have $|Q_1| > 0.2n$ then the process will not terminate by the step $0.1n$ and we will have at the step $|Q_1| \geq 0.1n$. Otherwise at the step t we have $|Q_2| + |Q_1| \leq 0.3n$ and consequently $|Q_0| > 0.7n$. Each state $\mathbf{q} \in Q_0$ with probability greater than $\frac{2}{n} - \frac{1}{n^2}$ will satisfy $\mathbf{q} \in N$. Therefore, expectation of the number of offspings at the step $t < 0.1n$ is at least $\frac{2}{n} \cdot 0.7n + o(1) \geq 1.3$. According to Lemma 8 when an expected number of offspings is more than 1 after $0.1n$ steps with at least constant probability we have a number of species at least ℓn for some constant $\ell > 0$.

Now consider the t-th step of the EPIDEMIA, where $t \in (0.1n, 0.9n)$. Let $Q_i(t)$ be Q_i at the t-th step and let us compute the expectation of the change of $|Q_0|, |Q_1|$ and $|Q_2|$:

$$\begin{aligned} \mathbf{E}\left(|Q_0(t+1)| - |Q_0(t)|\right) &= -2 \times \frac{|Q_0(t)|}{1 - |Q_2(t)|}, & (6)\\ \mathbf{E}\left(|Q_1(t+1)| - |Q_1(t)|\right) &= -1 + 2 \times \frac{|Q_0(t)|}{1 - |Q_2(t)|}, & (7)\\ \mathbf{E}\left(|Q_2(t+1)| - |Q_2(t)|\right) &= 1 & (8) \end{aligned}$$

So the change of Q_j at each step has constant expectation that can be expressed as a function of $Q_0(t), Q_1(t)$ and $Q_2(t)$. Since, according to Lemma 5, a degree of any variable exceeds $n^{1/5}$ with an exponentially small probability we have $\mathbf{P}\left(|Q_0(t+1) - Q_0(t)| > n^{1/5}\right) < n^{-3}$. We also observe that the functions in the right hand side of the equations are continuous and differentiable on the segment $[0.1, 0.9]$. Therefore, all conditions of the Wormald's theorem are met.

Applying the Wormald's theorem and denoting t/n by y we get the following system of differential equations in variables q_0, q_1 and q_2 corresponding to $|Q_0|, |Q_1|$ and $|Q_2|$, respectively.

$$\begin{aligned} \frac{dq_0}{dy} &= -2 \times \frac{|q_0(y)|}{1 - |q_2(y)|}, & (9)\\ \frac{dq_1}{dy} &= -1 + 2 \times \frac{|q_0(y)|}{1 - |q_2(y)|}, & (10)\\ \frac{dq_2}{dy} &= 1 & (11) \end{aligned}$$

or, shorter,

$$\begin{cases} \dot{q_0} = -\frac{2q_0}{1-q_2} \\ \dot{q_1} = -1 + \frac{2q_0}{1-q_2} \\ \dot{q_2} = 1 \end{cases} \tag{12}$$

It's easy to see that at the step t of the EPIDEMIA process we have $|Q_2(t)| = t$. Thus we are interested in the solution that has $q_2(y) = y$. Substituting the expression for q_2 into the first equation we get a linear differential equation and solve it for q_0. Once q_0 and q_2 are known q_1 can be found by integrating the right hand side of the second equation. Thus, we get a parameterized set of solutions

$$q_0 = (y-1)^2 c, \; q_1 = (2c-1)y - y^2 c + d, \; q_2 = y \tag{13}$$

with parameters c and d. By definition of q_i $q_0 + q_1 + q_2 = 1$, so $c + d = 1$. Obviously, $q_0 \geq 0$, so $c \geq 0$. Consequently, $0 \leq c \leq 1$ and an analysis of the quadratic function q_1 shows us that $q_1(0.9n) > 0$ and the process whp goes on for at least $0.9n$ steps reaching $|Q_2| = 0.9n$. Thus, we have shown that with constant probability we have the vertex $\mathbf{x}$ reachable from $0.9n$ vertices.

We finish the proof by showing that whp there is no set of size substantially less than n/e without outgoing edge. In terms of the EPIDEMIA it means that if at some step $|Q_0| < n/e$, the next step is possible, and finally we get $Q_2 = Q$.

Indeed, for an arbitrary set of size m ($m = n/c$ for some constant $c > e$) the probability that there are no outgoing edges equals to $(m/n)^{2m}$. There are $\binom{n}{m} \leq \left(\frac{ne}{m}\right)^m$ sets of size m. Applying the union bound we conclude that the probability that there is a set of size m with no outgoing edges is less than

$$\left(\frac{m}{n}\right)^{2m}\left(\frac{ne}{m}\right)^m = \left(\frac{me}{n}\right)^m \underset{n\to\infty}{\longrightarrow} 0. \tag{14}$$

□

To start proving Theorem 2 we need one more lemma. In proving it we use Chebushev inequality that holds for any random variable X and any real number k:

$$\mathbf{P}\left(|X - \mathbf{E}(X)| > k\sqrt{\mathbf{V}(X)}\right) \leq 1/k^2. \tag{15}$$

Lemma 7 *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a random automaton, such that $|Q| = n$, $|\Sigma| = n^\beta$, $\beta > 0.5$. Let Σ_1, Σ_2 be an arbitrary pair of sets such that $\Sigma \supseteq \Sigma_1 \cup \Sigma_2$, $\Sigma_1 \cap \Sigma_2 = \varnothing$, $|\Sigma_1| = |\Sigma_2| = n^\alpha$ for a real α satisfying $0.5 < \alpha < \beta$. Then, with high probability, a set of the triples $(a, b, \mathbf{q})$, $a \in \Sigma_1, b \in \Sigma_2$ such that*

$$\mathbf{q}a = \mathbf{q}b = \mathbf{q}, \tag{16}$$

contains more than $n^{2\alpha-1}$ elements.

Proof: Let us denote a set $\Sigma_1 \times \Sigma_2 \times Q$ by $\mathbf{T}$ and a random variable

$$|\{(a, b, \mathbf{q}) \in \mathbf{T} \mid \mathbf{q}a = \mathbf{q}b = \mathbf{q}\}| \tag{17}$$

by N. We shall use the Chebyshev inequality to prove that $N > 0$ whp.

At first we compute the expectation of N. The probability that a triple $(a, b, \mathbf{q}) \in \Sigma_1 \times \Sigma_2 \times Q$ satisfies (16) equals n^{-2}. There are $n^{2\alpha+1}$ triples thus we have

$$\mathbf{E}(N) = n^{2\alpha+1} \times n^{-2} = n^{2\alpha-1}. \tag{18}$$

Now we compute an upper bound of the variance of N. Since we have

$$\mathbf{V}(N) = \mathbf{E}\left(N^2\right) - \mathbf{E}(N)^2 \tag{19}$$

we need an upper bound for $\mathbf{E}\left(N^2\right)$. We define a random variable

$$\Delta_{(a,b,\mathbf{q})} = \begin{cases} 1, & \mathbf{q}a = \mathbf{q}b = \mathbf{q}, \\ 0, & otherwise \end{cases} \tag{20}$$

and compute

$$\begin{aligned}
\mathbf{E}\left(N^2\right) &= \mathbf{E}\left(\left(\sum_{(a,b,\mathbf{q})\in\mathbf{T}} \Delta_{(a,b,\mathbf{q})}\right)^2\right) \\
&= \sum_{\{(a_i,b_i,\mathbf{q}_i)\}_{i=1,2}} \mathbf{E}\left(\Delta_{(a_1,b_1,\mathbf{q}_1)}\cdot\Delta_{(a_2,b_2,\mathbf{q}_2)}\right) \\
&= \sum_{\{(a_i,b_i,\mathbf{q}_i)\}_{i=1,2}\in T^2,\mathbf{q}_1\neq\mathbf{q}_2} \mathbf{E}\left(\Delta_{(a_1,b_1,\mathbf{q}_1)}\cdot\Delta_{(a_2,b_2,\mathbf{q}_2)}\right) + \\
&\quad \sum_{a_1\neq a_2,b_1\neq b_2,\mathbf{q}} \mathbf{E}\left(\Delta_{(a_1,b_1,\mathbf{q})}\cdot\Delta_{(a_2,b_2,\mathbf{q})}\right) + \\
&\quad \sum_{a,b_1\neq b_2,\mathbf{q}} \mathbf{E}\left(\Delta_{(a,b_1,\mathbf{q})}\cdot\Delta_{(a,b_2,\mathbf{q})}\right) + \\
&\quad \sum_{a_1\neq a_2,b,\mathbf{q}} \mathbf{E}\left(\Delta_{(a_1,b,\mathbf{q})}\cdot\Delta_{(a_2,b,\mathbf{q})}\right) + \\
&\quad \sum_{a,b,\mathbf{q}} \mathbf{E}\left(\Delta_{(a,b,\mathbf{q})}\cdot\Delta_{(a,b,\mathbf{q})}\right).
\end{aligned}$$

Considering that $|\Sigma_1| = |\Sigma_2| = n^\alpha, |Q| = n$ we get

$$\mathbf{E}\left(N^2\right) = n^{4\alpha}n(n-1)n^{-4} + n^{2\alpha}(n^\alpha-1)^2nn^{-4} + 2n^{2\alpha}(n^\alpha-1)nn^{-3} + n^{2\alpha}nn^{-2} \tag{21}$$

and thus

$$\mathbf{E}\left(N^2\right) \le n^{4\alpha-2} + n^{4\alpha-3} + 2n^{3\alpha-2} + n^{2\alpha-1} \le \mathbf{E}\left(N\right)^2 + o(n) + \mathbf{E}\left(N\right). \tag{22}$$

So we have

$$\mathbf{V}\left(N\right) = \mathbf{E}\left(N^2\right) - \mathbf{E}\left(N\right)^2 \le \mathbf{E}\left(N\right) + o(n) \le 2\mathbf{E}\left(N\right). \tag{23}$$

The Chebyshev inequality in application to N, using the fact that $\mathbf{V}\left(N\right) \le 2\mathbf{E}\left(N\right)$ states that

$$\mathbf{P}\left(|N - \mathbf{E}\left(N\right)| > k\sqrt{2\mathbf{E}\left(N\right)}\right) \le 1/k^2. \tag{24}$$

Setting $k = \frac{\sqrt{\mathbf{E}(N)}}{2\sqrt{2}}$ and remembering that $\mathbf{V}\left(N\right) < 2\mathbf{E}\left(N\right), \mathbf{E}\left(N\right) = n^{2\alpha-1}$ we apply the Chebyshev inequality and get

$$\mathbf{P}\left(|N - \mathbf{E}\left(N\right)| > 0.5\mathbf{E}\left(N\right)\right) \le 8/\mathbf{E}\left(N\right) = o(1), \tag{25}$$

which implies $\mathbf{P}\left(N = 0\right) = o(1)$. □

Proof Proof of Theorem 2.: Let α be a real number satisfying $0.5 < \alpha < \min(2/3, 0.5+\varepsilon)$. Let us fix some sets of letters $\Sigma_1 \subseteq \Sigma, \Sigma_2 \subseteq \Sigma$ such that $|\Sigma_1| = |\Sigma_2| = n^\alpha, \Sigma_1 \cap \Sigma_2 = \varnothing$. Let L be the set of all triples $(a, b, \mathbf{x}), a \in \Sigma_1, b \in \Sigma_2, \mathbf{x} \in Q$ such that $\mathbf{x}a = \mathbf{x}, \mathbf{x}b = \mathbf{x}$. By Lemma 7 the set L whp contains more than $n^{2\alpha-1}$ elements. For any triple $(a, b, \mathbf{x}) \in L$ by Lemma 6 probability of event $\mathcal{S}(a, b, \mathbf{x})$ =“for any state $\mathbf{q} \in Q$ there is a word $w_{\mathbf{q}\to\mathbf{x}} \in \{a,b\}^*$ satisfying $w_{\mathbf{q}\to\mathbf{x}}\mathbf{q} = \mathbf{x}$" is greater than some constant r. Consequently expectation of the random variable

$$Z = |\{(a,b,\mathbf{x}) \mid \mathcal{S}(a,b,\mathbf{x}) \wedge (a,b,\mathbf{x}) \in L\}|. \tag{26}$$

is greater or equal to $rn^{2\alpha-1}$. In order to apply Chebyshev inequality and to show that whp $Z > 0$ we are going to prove that events $\mathcal{S}(a,b,\mathbf{x})$ are pairwise independent for triples $(a,b,\mathbf{x}) \in L$. And to prove that we show that whp for any pair of triples $(a_1,b_1,\mathbf{x}_1) \in L, (a_2,b_2,\mathbf{x}_2) \in L$ we have

$$a_1 \neq a_2 \wedge b_1 \neq b_2. \tag{27}$$

Note that $a_i \neq b_j$ because $\Sigma_1 \cap \Sigma_2 = \varnothing$.

We compute the probability that there are distinct triples $(a_1,b_1,\mathbf{x}_1),(a_2,b_2,\mathbf{x}_2)$ such that the statement $a_1 \neq a_2, b_1 \neq b_2$ does not hold and yet $(a_1,b_1,\mathbf{x}_1) \in L, (a_2,b_2,\mathbf{x}_2) \in L$, that is

$$\mathbf{x}_1 a_1 = \mathbf{x}_1 \wedge \mathbf{x}_1 b_1 = \mathbf{x}_1 \wedge \mathbf{x}_2 a_2 = \mathbf{x}_2 \wedge \mathbf{x}_2 b_2 = \mathbf{x}_2. \tag{28}$$

If distinct triples $(a_1,b_1,\mathbf{x}_1),(a_2,b_2,\mathbf{x}_2)$ do not satisfy condition $a_1 \neq a_2, b_1 \neq b_2$ they must satisfy one of the following:

1. $\mathbf{x}_1 = \mathbf{x}_2, a_1 = a_2, b_1 \neq b_2$,
2. $\mathbf{x}_1 = \mathbf{x}_2, a_1 \neq a_2, b_1 = b_2$,
3. $\mathbf{x}_1 \neq \mathbf{x}_2, a_1 = a_2, b_1 \neq b_2$,
4. $\mathbf{x}_1 \neq \mathbf{x}_2, a_1 \neq a_2, b_1 = b_2$,
5. $\mathbf{x}_1 \neq \mathbf{x}_2, a_1 = a_2, b_1 = b_2$.

For each condition C from this list we compute the probability of event "There are triples $(a_1,b_1,\mathbf{x}_1),(a_2,b_2,\mathbf{x}_2)$ that satisfy condition C and equation (28)".

To pick a pair of triples satisfying condition 1. we need to choose x_1, a_1, b_1 and b_2. So there are $n \cdot n^\alpha \cdot (n^{2\alpha} - 1) \leq n \cdot n^{3\alpha}$ pairs of triples satisfying condition 1. For those the equation (28) takes form

$$\mathbf{x}_1 a_1 = \mathbf{x}_1 \wedge \mathbf{x}_1 b_1 = \mathbf{x}_1 \wedge \mathbf{x}_1 b_2 = \mathbf{x}_1 \tag{29}$$

and its probability equals n^{-3}. Thus, the probability that there exists a pair of triples satisfying condition 1. and equation (28) can be bounded above by

$$nn^{3\alpha} \times n^{-3} = n^{3\alpha-2} \underset{n\to\infty}{\longrightarrow} 0. \tag{30}$$

Similar bounds for probabilities of conditions $2,\ldots,5$ equal $nn^{3\alpha} \times n^{-3}$, $n^2 n^{3\alpha} \times n^{-4}$, $n^2 n^{3\alpha} \times n^{-4}$, $n^2 n^{2\alpha} \times n^{-4}$, respectively, and it is easy to see that they all tend to 0 when n goes to infinity. Thus whp for any pair of distinct triples $(a_1,b_1,\mathbf{x}_1) \in L, (a_2,b_2,\mathbf{x}_2) \in L$ we have $a_1 \neq a_2, b_1 \neq b_2$.

So far we have proven that whp $|L| > n^{2\alpha-1}$ and for any $(a_1, b_1, \mathbf{x}_1) \in L, (a_2, b_2, \mathbf{x}_2) \in L$ we have $a_1 \neq a_2, b_1 \neq b_2$. The expectation of Z is at least $rn^{2\alpha-1}$ and it is a sum of pairwise independent random variables

$$I_{\mathcal{S}(a,b,\mathbf{x})} = \begin{cases} 1, \mathcal{S}(a,b,\mathbf{x}), \\ 0, \text{ otherwise.} \end{cases} \tag{31}$$

Similarly to Lemma 7 we can apply Chebyshev inequality and conclude that whp $Z > rn^{2\alpha-1}/2$. Thus whp $Z > 0$ and there is a triple $(a, b, \mathbf{x}) \in L$ such that for any state $\mathbf{q}$ there is a word $w_{\mathbf{q}\to\mathbf{x}} \in \{a, b\}^*$ satisfying $w_{\mathbf{q}\to\mathbf{x}}\mathbf{q} = \mathbf{x}$. Since $(a, b, \mathbf{x}) \in L, w_{\mathbf{q}\to\mathbf{x}} \in \{a, b\}$ we have $\mathbf{x}w = \mathbf{x}$. Then we consider a word $w_{Q\to\mathbf{x}}$ defined as follows: at the first step we take an arbitrary state $\mathbf{q}_0$ and set $w_{Q\to\mathbf{x}} = w_{\mathbf{q}_0\to\mathbf{x}}$, at the i-th step we take as a $\mathbf{q}_i$ one of the states remaining landed and set $w_{Q\to\mathbf{x}} = w_{Q\to\mathbf{x}}w_{\mathbf{q}_i\to\mathbf{x}}$. There are $n-1$ steps at most. By definition $w_{Q\to\mathbf{x}}$ is a reset word of the length at most $(n-1)^2$. □

4 Future Work

The results presented in this paper set new upper bounds for the number of letters required for a random automata to be synchronizing whp and to satisfy whp the Černý conjecture. The bounds still do not reach quantities that are to be expected considering the rareness of slowly synchronizing automata and the experimental results. We believe that an n state random automaton with an alphabet of size 2 is with high probability synchronizing and has a reset word of the length less than n.

Acknowledgements

We are grateful to Prof. M.V. Volkov for attracting our attention to the problem and several discussions on the topic, and to the anonymous reviewers for their remarks which have helped us make the article more accurate and clear.

References

[1] D. Achlioptas, Lower bounds for random 3-SAT via differential equations, Theoret. Comput. Sci. **265** (2001) 159–185.

[2] D. S. Ananichev, M. V. Volkov, Yu.I.Zaks, Synchronizing automata with a letter of deficiency 2, Theoret. Comput. Sci. **376** (2007) 30–41.

[3] S. Asmussen, H. Hering, Branching processes, Boston: Birkhäuser (1983).

[4] J. Černý, Poznámka k homogénnym eksperimentom s konečnými automatami, Matematicko-fyzikalny Časopis Slovensk. Akad. Vied, **14** (1964) 208–216 [in Slovak].

[5] D. Eppstein, Reset sequences for monotonic automata, SIAM J. Comput., **19** (1990) 500–510.

[6] B. Gertbakh, Epidemic process on a random graph: some preliminary results. J. Appl. Prob. **14** (1977) 427–438.

[7] P. M. Higgins, The range order of a product of i transformations from a finite full transformation semigroup, Semigroup Forum **37** (1988) 31–36.

[8] J. Jaworski, Epidemic processes on digraphs of random mappings, J. Appl. Probab. **36** (1999) 780–798.

[9] C.H. Papadimitriou, E. Koutsoupias, On the greedy algorithm for satisfiability, Information Processing Letters, **43** (1992) 53–55.

[10] J.-E. Pin, On two combinatorial problems arising from automata theory, Ann. Discrete Math. **17** (1983) 535–548.

[11] Raghavan P. Motwani R. *Randomized Algorithms*. Cambridge University Press, 1995.

[12] W. Samotij, A note on the complexity of the problem of finding shortest synchronizing words, in Proc. AutoMathA 2007, Automata: from Mathematics to Applications, Univ. Palermo (CD).

[13] N.C. Wormald, Differential equations for random processes and random graphs, Ann. Appl. Probab. **5(4)** (1995) 1217–1235.

5 Appendix

5.1 Chernoff's Bound

Let $B(p, n)$ be a random variable, that is the number of successes in n independent trials. If p is the probability of success in each trial, then the following inequality is known as Chernoff Bound [11]

$$\mathbf{P}\left(\left|\frac{B(p,n)}{n} - p\right| \leq \varepsilon\right) \leq 2e^{-\frac{\varepsilon^2 n}{3p}}. \tag{32}$$

5.2 Galton-Watson Process

A simple Galton-Watson Process[3] is a sequence of random variables $\{X_n\}$ which satisfies

$$X_n = \sum_{i=1}^{X_{n-1}} \xi, \tag{33}$$

where ξ is some predefined random variable. Galton-Watson Process was studied as a model of population survival. X_1 represents the size of the initial population and X_n is the size of the n-th generation. Distribution of the random variable ξ reflects the distribution of the number of offsprings of an individual.

The following statement was proven for the Galton-Watson process (see Proposition 1.2 and Corollary 1.6 in [3])

Lemma 8 *Let*

$$X_n = \sum_{i=1}^{X_{n-1}} \xi, X_1 > 0, \mathbf{E}(\xi) > 1. \tag{34}$$

Then there is a constant r such that $\mathbf{P}(X_n = 0) > r$ for all n.

5.3 Wormald's Theorem

One of the instruments of our analysis is the Wormald's theorem [13] that allows one to replace a probabilistic analysis of a combinatorial algorithm with an analysis of a deterministic system of differential equations.

All random processes are discrete time random processes. Such a process is a probability space Ω denoted by $(Q_0, Q_1, \ldots)$, where each Q_i takes values in some set S. Consider a sequence Ω_n, $n = 1, 2, \ldots$, of random processes. The elements of Ω_n are sequences $(q_0(n), q_1(n), \ldots)$ where each $q_i(n) \in S$. For the convenience's sake the dependance of n will usually be dropped from the notation. Asymptotics, denoted by the notation o and O, are for $n \to \infty$, but uniform over all other variables. For a random X, we say $X = o(f(n))$ *always* if $\max\{x|\mathbf{P}(X = x) \neq 0\} = o(f(n))$. An event occurs *almost surely* if its probability in Ω_n is $1 - o(1)$. We denote by S^+ the set of all $h_t = (q_0, \ldots, q_t)$, each $q_t \in S$ for $t = 0, 1 \ldots$. By H_t we denote the *history* of the processes, that is the $n \times (t+1)$-matrix with entries $Q_i(j), 0 \leq i \leq t, 1 \leq j \leq n$.

A function $f(u_1, \ldots, u_j)$ satisfies the *Lipschitz condition* on $D \subseteq \mathbb{R}^j$ if a constant $L > 0$ exists with the property that

$$|f(u_1, \ldots, u_j) - f(v_1, \ldots, v_j)| \leq L \sum_{i=1}^{j} |u_j - v_i| \tag{35}$$

for all $(u_1, \ldots, u_j)$ and $(v_1, \ldots, v_j)$ in D.

Theorem 3 (Wormald, [13]) *Let k be fixed. For $1 \leq \ell \leq k$, let $y^{(\ell)}\colon S^+ \to \mathbb{R}$ and $f_\ell\colon \mathbb{R}^{k+1} \to \mathbb{R}$, such that for some constant C and all ℓ, $|y^{(\ell)}| < Cn$ for all $h_t \in S^+$ for all n. Suppose also that for some function $m = m(n)$:*

(i) for all i and uniformly over all $t < m$, $\mathbf{P}\left(|Y_{t+1}^{(\ell)} - Y_t^{(\ell)}| > n^{1/5} \mid H_t\right) = o(n^{-3})$ always;

(ii) for all ℓ and uniformly over all $t < m$,
$\mathbf{E}(Y_{t+1}^{(\ell)} - Y_t^{(\ell)} \mid H_t) = f_\ell(t/n, Y_t^{(1)}/n, \ldots, y_t^{(k)}/n) + o(1)$ always;

(iii) for each ℓ the function f_ℓ is continuous and satisfies a Lipschitz condition on D, where D is some bounded connected open set containing the intersection of $\{(t, z^{(1)}, \ldots, z^{(k)}) \mid t \geq 0\}$ with some neighborhood of $\{(0, z^{(1)}, \ldots, z^{(k)}) \mid \mathbf{P}\left(Y_0^{(\ell)} = z^{(\ell)}n, 1 \leq \ell \leq k\right) \neq 0$ for some $n\}$.

Then:

(a) For $(0, \hat{z}^{(1)}, \ldots, \hat{z}^{(k)}) \in D$ the system of differential equations
$\dfrac{dz_\ell}{ds} = f_\ell(s, z_1, \ldots, z_k)$, $\ell = 1, \ldots, k$, has a unique solution in D for $z_\ell\colon \mathbb{R} \to \mathbb{R}$ passing through $z_\ell(0) = \hat{z}^{(\ell)}$, $1 \leq \ell \leq k$, and which extends to points arbitrarily close to the boundary of D.

(b) Almost surely $Y_t^{(\ell)} = nz_\ell(t/n) + o(n)$ uniformly for $0 \leq t \leq \min\{\sigma n, m\}$ and for each ℓ, where $z_\ell(s)$ is the solution in (a) with $\hat{z}^{(\ell)} = Y_0^{(\ell)}/n$, and $\sigma = \sigma(n)$ is the supremum of those s to which the solution can be extended.