On the Probability of Being Synchronizable

Mikhail V. Berlinkov(✉)

Institute of Mathematics and Computer Science,
Ural Federal University, 620000 Ekaterinburg, Russia
m.berlinkov@gmail.com

Abstract. We prove that a random automaton with n states and any fixed non-singleton alphabet is synchronizing with high probability. Moreover, we also prove that the convergence rate is exactly $1 - \Theta(\frac{1}{n})$ as conjectured by Cameron [4] for the most interesting binary alphabet case.

1 Synchronizing Automata

Suppose $\mathcal{A}$ is a complete deterministic finite automaton whose input alphabet is A and whose state set is Q. The automaton $\mathcal{A}$ is called *synchronizing* if there exists a word $w \in A^*$ whose action *resets* $\mathcal{A}$, that is, w leaves the automaton in one particular state no matter at which state in Q it is applied: $q.w = q'.w$ for all $q, q' \in Q$. Any such word w is called a *reset word* of $\mathcal{A}$. For a brief introduction to the theory of synchronizing automata we refer reader to the survey [13].

Synchronizing automata serve as transparent and natural models of error-resistant systems in many applications (coding theory, robotics, testing of reactive systems) and also reveal interesting connections with symbolic dynamics and other parts of mathematics. We take an example from [1]. Imagine that you are in a dungeon consisting of a number of interconnected caves, all of which appear identical. Each cave has a common number of one-way doors of different colors through which you may leave; these lead to passages to other caves. There is one more door in each cave; in one cave the extra door leads to freedom, in all the others to instant death. You have a map of the dungeon with the escape door identified, but you do not know in which cave you are. If you are lucky, there is a sequence of doors through which you may pass which takes you to the escape cave from any starting point.

The result of this paper is very positive; we prove that for an uniformly at random chosen dungeon (automaton) there is a life-saving sequence (reset word) with probability $1 - O(\frac{1}{n^{0.5c}})$ where n is the number of caves (states) and c is the number of colors (letters). Moreover, we prove that the convergence rate is tight for the most interesting 2-color case, thus confirming Peter Cameron's conjecture from [4]. Up to recently, the best results in this direction were much weaker: in [10] was proved that random 4-letter automata are synchronizing with probability p for a specific constant $p > 0$; in [9] was proved that if a random automaton with n states has at least $72 \ln(n)$ letters then it is almost surely synchronizing. Recently, Nicaud [8] has shown (independently) by a different

S. Govindarajan and A. Maheshwari (Eds.): CALDAM 2016, LNCS 9602, pp. 73–84, 2016.
DOI: 10.1007/978-3-319-29221-2_7

method that a random n-state automaton with 2 letters is synchronizing with probability $1 - O(n^{-\frac{1}{8}+o(1)})$. Our results give a much better convergence rate.

2 The Probability of Being Synchronizable

Let Q stand for $\{1, 2, \dots n\}$ and Σ_n for the probability space of all unambiguous maps from Q to Q with the uniform probability distribution. Throughout this section let $\mathcal{A} = \langle Q, \{a, b\}\rangle$ be a random automaton, that is, maps a and b are chosen independently at random from Σ_n.

The *underlying digraph* of $\mathcal{A} = \langle Q, \Sigma\rangle$ is a digraph denoted by $UG(\mathcal{A})$ whose vertex set is Q and whose edge multiset is $\{(q, q.a) \mid q \in Q,\ a \in \Sigma\}$. In other words, the underlying digraph of an automaton is obtained by erasing all labels from the arrows of the automaton. Given a letter $x \in \Sigma$, the underlying digraph of x is the underlying digraph of the automaton $\mathcal{A}_x = \langle Q, \{x\}\rangle$ where the transition function is the restriction of the original transition function to the letter x. Clearly each directed graph with n vertices and constant out-degree 1 corresponds to the unique map from Σ_n whence we can mean Σ_n as the probability space with the uniform distribution on all directed graphs with constant out-degree 1.

Theorem 1. *The probability of being synchronizable for 2-letter random automata with n states equals $1 - \Theta(\frac{1}{n})$.*

Proof. Since synchronizing automata are necessary weakly connected, the following lemma gives the lower bound of the theorem.

Lemma 1. *The probability that $\mathcal{A}$ is not weakly connected is at least $\Omega(\frac{1}{n})$.*

Proof. Let us count the number of automata having exactly one *disconnected loop*, that is the state having only (two) incoming arrows from itself. Such automata can be counted as follows. We first choose the state p of a disconnected loop in n ways. The transitions for this state is defined in the unique way. The number of ways to define transitions for any other state q is

$$1(n-2) + (n-2)(n-1) = n(n-2)$$

because if a maps q to q then b can map q to any state except $\{p, q\}$; if a doesn't map q to $\{p, q\}$ then b can map q to any state except $\{p, q\}$. Thus the probability of being such automata is equal

$$\frac{n(n(n-2))^{n-1}}{n^{2n}} = \frac{1}{n}(1 - \frac{2}{n})^{n-1} = \Theta(\frac{1}{n}).$$

Now we turn to the proof of the upper bound. For this purpose, we need some knowledge about the structure of the underlying graphs of a random mapping. The underlying digraph $UG(x)$ of any mapping $x \in \Sigma_n$ consists of one or more (weakly) connected components called *clusters*. Each cluster has a unique cycle, and all other vertices of this cluster are located in trees rooted on this cycle.

Lemma 2. *With probability $1 - o(\frac{1}{n^4})$, a random digraph from Σ_n has at most $5 \ln n$ clusters.*

Proof. Let ν_n denote the number of clusters for a random digraph. It is proved in [11, Theorem 1] that if $n, N \to +\infty$ such that $0 < \gamma_0 \leq \gamma = \frac{N}{\ln n} \leq \gamma_1$ where γ_0, γ_1 are constants; then uniformly for $\gamma \in [\gamma_0, \gamma_1]$

$$P(\nu_n = N) = \frac{e^{\phi(\gamma)}}{\sqrt{\pi \ln n}} n^{\phi(\gamma)}(1 + o(1)),$$

where $\phi(\gamma) = \gamma(1 - \ln 2\gamma) - 0.5$ for $\gamma \neq 0.5$. It is also known that the function $p(N) = P(\nu_n = N)$ has a unique maximum, which is achieved for $N = 0.5 \ln n(1 + o(1))$. Since also $\nu_n \leq n$, we get

$$P(\nu_n > 5 \ln n) < nP(\nu_n = [5 \ln n]) = o(\frac{1}{n^4}).$$

For convenience, by the term *whp* (with high probability) we mean "with probability $1 - O(\frac{1}{n})$". Call a set of states $K \subseteq Q$ *synchronizable* if it can be mapped to one state by some word. In contrast, a pair of states $\{p, q\}$ is called a *deadlock* if $p.s \neq q.s$ for each word s.

First we aim to show that for proving that $\mathcal{A}$ is synchronizing whp, it is enough to find whp for each letter a large synchronizable set of states which is completely defined by this letter. Given $x \in \{a, b\}$, we define S_x to be the set of *big* clusters of $UG(x)$, i.e., the clusters containing more than $n^{0.45}$ states and define T_x to be the complement of S_x, or equivalently, T_x is the set of *small* clusters of $UG(x)$, i.e., the clusters containing at most $n^{0.45}$ states. Since S_x and T_x are completely defined by x, both are independent of the other letter.[1] Due to Lemma 2, whp there are at most $5 \ln n$ clusters in $UG(x)$, whence whp T_x contains at most $5 \ln(n) n^{0.45}$ states. Given a set of clusters X, denote by $\widehat{X}$ the set of states in the clusters of X.

Theorem 2. *If $\widehat{S_a}$ and $\widehat{S_b}$ are synchronizable, then $\mathcal{A}$ is synchronizing whp.*

Proof. First, we need the following useful remark.

Remark 1. If a pair $\{p, q\}$ is independent of one of the letters, it is a deadlock with probability $O(\frac{1}{n^{1.02}})$.

Proof. Suppose $\{p, q\}$ is chosen independently of a. Then the set $R = \{p.a, q.a, p.a^2, q.a^2\}$ is independent of b whence also of $\widehat{T_b}$. If $p.a = q.a$ or $p.a^2 = q.a^2$ the pair $\{p, q\}$ is not a deadlock. Therefore, we can assume that there are (probably equal) states $r_1 \in \{p.a, q.a\}$ and $r_2 \in \{p.a^2, q.a^2\}$ which belong to $\widehat{T_b}$ (because $\widehat{S_b}$ is synchronizable). If $|R| = 4$ then $r_1 \neq r_2$. Since r_1, r_2 are independent of $\widehat{T_b}$, this happens with probability $\frac{1}{|\widehat{T_b}|(|\widehat{T_b}|-1)} \in O(\frac{1}{n^{1.02}})$.

[1] Here and below by independence of two objects $O_1(\mathcal{A})$ and $O_2(\mathcal{A})$, we mean the independence of the events $O_1(\mathcal{A}) = O_1$ and $O_1(\mathcal{A}) = O_2$ for each instances O_1, O_2 from the corresponding probability spaces.

If $|R| = 3$ then a maps two states from $\{p, q, p.a, q.a\}$ to one state. Since $\{p, q\}$ is independent of a and the images of different states by a are chosen independently and uniformly at random from Q, this happens with probability $O(\frac{1}{n})$. Furthermore, r_1 has to belong to $\widehat{T_b}$ whence the probability of this case is $O(\frac{1}{n})O(\frac{1}{|\widehat{T_b}|}) \in O(\frac{1}{n^{1.02}})$. Finally, in the case $|R| = 2$, we have that $p.a \in \{p, q\}, q.a \in \{p, q\}$. This happens with probability $O((\frac{2}{n-2})^2) = O(\frac{1}{n^{1.02}})$. The remark follows.

Now let us bound the probability that $\mathcal{A}$ is not synchronizing. If this is the case, $\mathcal{A}$ possesses some deadlock pair $\{p, q\}$. Given a state r, denote by c_r the cycle of the cluster containing r in $UG(a)$ and by s_r the length of this cycle. Denote also by $c_{r,i}$ the i-th state on the cycle c_r for some order induced by the cycle c_r, i.e., $c_{r,i}.a = c_{r,i+1 \mod s_r}$. Let d be the g.c.d. of s_p and s_q. Then for some $0 \le x < d$ and all $0 < k_1, k_2, 0 \le i \le d-1$, the pairs

$$\{c_{p,(i+k_1 d) \mod s_p}, c_{q,(x+i+k_2 d) \mod s_q}\} \text{ are deadlocks.} \tag{1}$$

It follows that in each of these pairs at least one of the states belongs to $\widehat{T_b}$.

Case 1. $c_p = c_q$, that is, p and q belong to the same cluster. Since $\{p, q\}$ is a deadlock, in this case $s_p = s_q = d > 1$ and by (1) at least half of the states of c_p belongs to $\widehat{T_b}$. The probability that a satisfies such configuration is at most

$$O(\frac{1}{n}) + 5\ln n 2^d (\frac{|\widehat{T_b}|}{n})^{\lceil 0.5d \rceil} \le O(\frac{1}{n}) + 20 \ln n \frac{1}{n^{\lceil 0.5d \rceil 0.54}}.$$

Indeed, first due to Lemma 2, whp there is at most $5\ln n$ ways to choose the cluster c_p, then we choose $\lceil 0.5d \rceil$ states of c_p (in at most 2^d ways) which belong to $\widehat{T_b}$ with probability at most $(|\widehat{T_b}|/n)^{\lceil 0.5d \rceil}$.

If $d > 2$ then $\lceil 0.5d \rceil \ge 2$ and we are done. If $d = 2$, due to Lemma 2 whp there are at most $5\ln n$ cycles of size 2 in $UG(a)$, each containing one pair. Since this set of pairs is defined by a, these pairs are independent of b. Due to Remark 1 one of these pairs is a deadlock with probability at most $5\ln n/n^{1.02} = O(\frac{1}{n})$. Since $\{p, q\}$ is one of these pairs, it is not a deadlock whp.

Case 2. c_p and c_q are different. Since k_1, k_2 are arbitrary in (1), for each $i \in \{0, 1, \dots d-1\}$ either $c_{p,(i+k_1 d) \mod s_p} \in \widehat{T_b}$ for all k_1 or $c_{q,(x+i+k_2 d) \mod s_q} \in \widehat{T_b}$ for all k_2. Thus the probability of such configuration is at most

$$O(\frac{1}{n}) + (25\ln^2 n) d \sum_{k=0}^{d-1} \binom{d}{k} (\frac{|\widehat{T_b}|}{n})^{\frac{ks_1 + (d-k)s_2}{d}}. \tag{2}$$

Indeed, first due to Lemma 2, whp we choose clusters c_p, c_q in at most $25\ln^2 n$ ways, then we choose x in d ways, and for some $k \in \{0, 1, \dots d-1\}$ we choose k-subset $I_p \subseteq \{0, 1, \dots d-1\}$ in $\binom{d}{k}$ ways such that $c_{p,(i+k_1 d) \mod s_q} \in \widehat{T_b}$ for all k_1 and $i \in I_p$, meanwhile choosing the corresponding set $I_q = \{0, 1, \dots d-1\} \backslash I_p$. Since S_b is independent of a, the probability that the corresponding states from the cycles belong to $\widehat{T_b}$ equals $(\frac{|\widehat{T_b}|}{n})^{\frac{ks_1+(d-k)s_2}{d}}$. The maximum of (2) is achieved for $s_1 = s_2 = d$ and equals

$$(25\ln^2 n)d\sum_{k=0}^{d-1}\binom{d}{k}(\frac{|\widehat{T_b}|}{n})^d \leq (25\ln^2 n)d2^d n^{-0.54d}$$

up to a $O(\frac{1}{n})$ term. In the case $d > 1$, we get

$$25\ln^2 n\sum_{d=2} n^{0.45}d2^d n^{-0.54d} = o(\frac{1}{n}).$$

In the case $d = 1$, by Lemma 2 whp there are at most $5\ln n$ cycles of size 1 in $UG(a)$. Hence there are at most $25\ln^2 n$ pairs from these cycles independent of b. In this case the proof is the same as for $d = 2$ in Case 1.

In view of Theorem 2, it remains to prove that $\widehat{S_a}$ and $\widehat{S_b}$ are synchronizable whp. For this purpose, we use the notion of the *stability* relation introduced by Kari [7]. A pair of states $\{p, q\}$ is called *stable*, if for every word u there is a word v such that $p.uv = q.uv$. The *stability* relation, given by the set of stable pairs, is stable under the actions of the letters and complete whenever $\mathcal{A}$ is synchronizing. It is also transitive whence its reflexive closure is a congruence on Q.

Given a pair $\{p, q\}$, either $\{p, q\}$ in one a-cluster or the states p and q belong to different a-clusters. In the latter case, we say that $\{p, q\}$ *connects* these a-clusters. Suppose there exists a *large* set Z_a of distinct pairs that are stable independently of a; that is, $|Z_a| \geq n^{0.4}$ and the map b alone suffices to witness the stability. Consider the graph $\Gamma(S_a, Z_a)$ with the set of vertices S_a, and there is an edge between two clusters if and only if some pair from Z_a connects them.

The underlying idea of the two following combinatorial lemmas is that if we have many pairs chosen independently of a given random mapping from Σ_n, whp they cannot satisfy any non-trivial partition or coloring stable under the action of this mapping.

Lemma 3 (see [2] for the proof). *If such Z_a exists then whp $\Gamma(S_a, Z_a)$ is connected. If additionally all cycle pairs of one of the clusters from S_a are stable then $\widehat{S_a}$ is synchronizable.*

Lemma 4 (see [2] for the proof). *If such Z_a exists then whp there is a cluster from S_a whose cycle is stable.*

Due to above lemmas, by Theorem 2 it remains to prove that whp there exists Z_a and Z_b. The crucial step for this is to find a stable pair completely defined by one of the letters whence independent of the other one. For this purpose, we reuse ideas from Trahtman's solution [12] of the famous Road Coloring Problem. A subset $A \subseteq Q$ is called an F-clique of $\mathcal{A}$, if it is a set of maximum size such that each pair of states from A is a deadlock. It follows from the definition that all F-cliques have the same size. First, we need to reformulate [12, Lemma 2] for our purposes.

Lemma 5. *If A and B are two distinct F-cliques such that $A \backslash B = \{p\}, B \backslash A = \{q\}$ for some states p, q; Then $\{p, q\}$ is a stable pair.*

Proof. Arguing by contradiction, suppose there is a word u such that $\{p.u, q.u\}$ is a deadlock. Then $(A \cup B).u$ is an F-clique because all pairs are deadlocks. Since $p.u \neq q.u$, we have $|A \cup B| = |A| + 1 > |A|$ contradicting maximality of A.

Given a digraph $g \in \Sigma_n$ and an integer $c > 0$, call a *c-branch* of g any subtree of a tree of g with the root of height c. For instance, the trees are exactly 0-branches. Let T be a highest c-branch of g and h be the height of the second by height c-branch. Let us call the *c-crown* of g the (probably empty) forest consisting of all the states of height at least $h+1$ in T. For example, the digraph g presented on Fig. 1 has two highest 1-branches rooted in states $6, 12$. Without the state 14, the digraph g would have the unique highest 1-branch rooted at state 6, having the state 8 as its 1-crown.

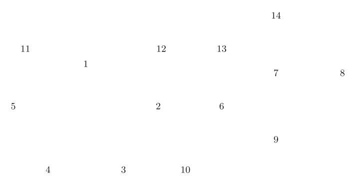

Fig. 1. A digraph with a one cycle and a unique highest tree.

The following theorem is an analogue of Theorem 2 from [12] for 1-branches instead trees and a relaxed condition on the connectivity of $\mathcal{A}$.

Theorem 3. *Suppose the underlying digraph of the letter a has a unique highest 1-branch T and its 1-crown is reachable from an F-clique F_0. Denote by r the root of T and by q the predecessor of the root of the tree containing T on the a-cycle. Then $\{r, q\}$ is stable and independent of b.*

Proof. Let p be some state of height h in T which is reachable from an F-clique F_0. Since p is reachable from F_0, there is another F-clique F_1 containing p. Since F_1 is an F-clique, there is a unique state $g \in F_1 \cap T$ of maximal height $h_1 \geq h+1$. Let us consider the F-cliques $F_2 = F_1.a^{h_1 - 1}$ and $F_3 = F_2.a^L$ where L is the least common multiplier of all cycle lengths in $UG(a)$. By the choice of L and F_2, we have that

$$F_2 \backslash F_3 = \{g.a^{h_1 - 1}\} = \{r\} \text{ and } F_3 \backslash F_2 = \{q\}.$$

Hence, by Lemma 5 the pair $\{r, q\}$ is stable. Since this pair is completely defined[2] by the unique 1-branch of a and the letters are chosen independently, this pair is independent of b.

[2] The reason why we consider 1-branches instead of trees is that the state r would not be completely defined by the unique highest tree of a.

Once we have got a one stable pair which is independent of one of the letters, it is possible to get a lot of such pairs for each of the letters.

Theorem 4 (see Sect. 3 for the proof). *Whp for each letter $x \in \{a, b\}$ of $\mathcal{A}$, there is a set of at least $n^{0.4}$ distinct stable pairs independent of x.*

The proof of the above theorem result is mainly based on repeatedly referring to the following fact. Given a set $D \subset Q$ and a stable pair $\{p, q\}$ independent of some letter $c \in \Sigma$, $\{p, q\}.c$ is also the stable pair independent of the other letter and $p, q \notin D$ with probability $1 - O(\frac{|D|}{n})$. However, some accuracy is required when using this argument many times.

Due to Theorems 2, 4 and Lemmas 3, 4, it remains to show that we can use Theorem 3, that is, whp the underlying graph of one of the letters has a unique 1-branch and some high height vertices of this 1-branch are accessible from F-cliques (if F-cliques exist). The crucial idea in the solution of the Road Coloring Problem [12] was to show that each *admissible* digraph can be *colored* into an automaton satisfying the above property (for trees) and then use Theorem 3 to reduce the problem. In order to apply Theorem 3, we need the following analogue of the combinatorial result from [12] for the random setting.

Theorem 5 (Theorem 12 [3]). *Let $g \in \Sigma_n$ be a random digraph, $c > 0$, and H be the c-crown of g having r roots. Then $|H| > 2r > 0$ with probability $1 - \Theta(1/\sqrt{n})$, in particular, a highest c-branch is unique and higher than all other c-branches of g by 2 with probability $1 - \Theta(1/\sqrt{n})$.*

The proof of the above theorem has been moved to the separate paper [3] because it is rather mathematical than computer science result and hopefully could have independent importance.

Since the letters of $\mathcal{A}$ are chosen independently, the following corollary of Theorem 5 is straightforward.

Corollary 1. *Whp the underlying digraph of one of the letters (say a) satisfies Theorem 5.*

In order to use Theorem 3 and thus complete the proof of Theorem 1, it remains to show that the 1-crown of the underlying graph of a is accessible from F-cliques of $\mathcal{A}$. Let us call a *subautomaton* a strongly connected component of $\mathcal{A}$ closed under the actions of the letters. Since each F-clique can be mapped to some minimal (by inclusion) subautomaton, the following statement completes the proof of Theorem 1.

Theorem 6. *The 1-crown of the underlying digraph of a intersects with each minimal subautomaton whp.*

Proof. The following lemma can be obtained as a consequence of [5, Theorem 3] but we present the proof here for the self completeness.

Lemma 6. *For each constant $q > 1$ the number of states in each subautomaton of $\mathcal{A}$ is at least n/qe^2 whp.*

Proof. The probability that there is a subautomaton of size less than n/qe^2 is bounded by

$$\sum_{i=1}^{n/qe^2} \binom{n}{i} (\frac{i}{n})^{2i} \leq \sum_{i=1}^{n/qe^2} \frac{(1-\frac{i}{n})^i}{(1-\frac{i}{n})^n} (\frac{i}{n})^i \leq \sum_{i=1}^{n/qe^2} (\frac{ei}{n})^i. \tag{3}$$

Indeed, there are $\binom{n}{i}$ ways to choose some subset T of i states; the probability that arrows for both letters leads a state to the chosen set T is $(\frac{i}{n})^2$.

For $i \leq n/qe^2$, we get that

$$\frac{(\frac{e(i+1)}{n})^{i+1}}{(\frac{ei}{n})^i} \leq \frac{e(i+1)}{n}(1+\frac{1}{i})^i \leq \frac{e^2(i+1)}{n} \leq \frac{1}{q}.$$

Hence the sum (3) is bounded by the sum of the geometric progression with the factor $1/q$ and the first term equals $\frac{e}{n}$. The lemma follows.

Let $g \in \Sigma_n$ and H be the 1-crown of g. Let n_1 and n_2 be the number of root and non-root vertices in H respectively. Due to Corollary 1, one of the letters (say a) satisfies Theorem 5 whp, that is, $n_2 > n_1$ for $g = UG(a)$ whp. By Lemma 6, we can choose some $r < \frac{1}{e^2}$ such that whp there are no subautomaton of size less than rn. Therefore there are at least $\Theta(n^{2n})$ of automata satisfying both constraints. Arguing by contradiction, suppose that among such automata there are more than n^{2n-1} automata $\mathcal{A}$ such that their 1-crown does not intersect with some minimal subautomaton of $\mathcal{A}$. Denote this set of automata by L_n. For $1 \leq j < d$ denote by $L_{n,d,j}$ the subset of automata from L_n with the 1-crown having exactly d vertices and j roots. By the definitions,

$$\sum_{d=2}^{(1-r)n} \sum_{j=1}^{0.5d} |L_{n,d,j}| = |L_n|. \tag{4}$$

Given an integer $rn \leq m < (1-r)n$, let us consider the set of all m-states automata whose letter a has a unique highest 1-branch which is higher by 1 than the second one. Due to Theorem 5 there are at most $O(m^{2m-0.5})$ of such automata. Denote this set of automata by K_m. By $K_{m,j}$ denote the subset of automata from K_m with exactly j vertices in the 1-crown. Again, we have

$$\sum_{j=1}^{m-1} |K_{m,j}| = |K_m|. \tag{5}$$

Each automaton from $L_{n,d,j}$ can be obtained from $K_{m,j}$ for $m = n-(d-j)$ as follows. Let us take an automaton $\mathcal{B} = (Q_b, \Sigma)$ from $K_{m,j}$ with no subautomaton of size less than rn. First we append a set H_b of $d-j$ states to the set H_b to every possible positions, in at most $\binom{n}{d-j}$ ways. The indices of the states from H_b are shifted in compliance with the positions of the inserted states, that is, the index q is shifted to the amount of chosen indices $z \leq q$ for H_b. Next, we choose an arbitrary forest on d vertices and j roots which belong to the 1-crown of $\mathcal{B}$ in at most jd^{d-j-1} ways. Thus we have completely chosen the action of the letter a.

Next we choose some minimal subautomaton M of $\mathcal{B}$ and redefine arbitrarily the image by the letter b for all states from $Q_b \backslash M$ to the set $Q_b \cup H_b$ in $n^{m-|M|}$ ways. Within this definition, all automata from $K_{m,j}$ which differs only in the images of the states from $Q_b \backslash M$ by the letter b can lead to the same automaton from $L_{n,d,j}$. Given a subautomaton M, denote such class of automata by $K_{m,j,M}$. There are exactly $m^{m-|M|}$ automata from $K_{m,j}$ in each such class. Since $|M| \geq rn$ and M is minimal, $\mathcal{B}$ can appear in at most $1/r$ of such classes.

Thus we have completely chosen both letters and obtained each automaton in $L_{n,d,j}$. Thus for the automaton $\mathcal{B}$ and one of its minimal subautomaton M of size $z \geq rn$, we get at most

$$\binom{n}{d-j} jd^{d-j-1} n^{m-z}$$

automata from $L'_{n,d,j}$ each at least m^{m-z} times, where $L'_{n,d,j}$ is the set of automata containing $L_{n,d,j}$ without the constraint on the size of minimal subautomaton. Notice that we get each automaton from $L_{n,d,j}$ while $\mathcal{B}$ runs over all automata from $K_{n-(d-j),j}$ with no subautomaton of size less than rn. Thus we get that

$$|L_{n,d,j}| \leq \sum_{z=rn}^{n} \sum_{a,M,|M|=z} \sum_{\mathcal{B} \in K_{m,j,M}} \frac{\binom{n}{d-j} jd^{d-j-1} n^{m-z}}{m^{m-z}}. \tag{6}$$

Since each automaton $\mathcal{B} \in K_{m,j}$ with no minimal subautomaton of size less than rn appears in at most $1/r$ of $K_{m,j,M}$, we get

$$|L_{n,d,j}| \leq \frac{1}{r} |K_{m,j}| \max_{rn \leq z \leq m} \frac{\binom{n}{d-j} jd^{d-j-1} n^{m-z}}{m^{m-z}} = \frac{1}{r} |K_{m,j}| \frac{\binom{n}{d-j} jd^{d-j-1} n^{m-rn}}{m^{m-rn}}. \tag{7}$$

Using (4) and (5), we get

$$\begin{aligned} |L_n| &= \frac{1}{r} \sum_{d=2}^{(1-r)n} \sum_{j=1}^{0.5d} |K_{m,j}| \frac{\binom{n}{d-j} jd^{d-j-1} n^{m-rn}}{m^{m-rn}} \\ &\leq \frac{1}{r} \sum_{d=2}^{(1-r)n} \max_{j \leq 0.5d} |K_m| \frac{\binom{n}{d-j} jd^{d-j} n^{m-rn}}{m^{m-rn}}. \end{aligned} \tag{8}$$

Using Stirling's approximation

$$x! = (\frac{x}{e})^x \sqrt{2\pi x} O(1) \text{ and } (1 - \frac{x}{k})^k = e^x O(1),$$

we get

$$\binom{n}{d-j} j d^{d-j} = O(1)\frac{n^n j d^{d-j}}{(d-j)^{d-j}(n-(d-j))^{n-(d-j)}}$$
$$= O(1)\frac{j n^{d-j}}{(1-\frac{j}{d})^{d-j}(1-\frac{d-j}{n})^{n-(d-j)}} \leq O(1) j n^{d-j} e^d \tag{9}$$

Using that $|K_m| = O(m^{2m-0.5})$ from (8), we get

$$|L_n| \leq O(1)\sum_{d=2}^{(1-r)n} \max_{j \leq 0.5d} m^{2m-0.5} j n^{d-j} e^d (\frac{n}{m})^{m-rn}$$
$$\leq O(1)\sum_{d=2}^{(1-r)n} \max_{j \leq 0.5d} (n-d+j)^{n-d+j+rn-0.5} j e^d n^{(1-r)n}$$
$$\leq O(1)\sum_{d=2}^{(1-r)n} (n-0.5d)^{(1+r)n-0.5(d+1)} d e^d n^{(1-r)n}$$
$$\leq O(1)\sum_{d=2}^{(1-r)n} d n^{2n-0.5(d+1)} e^{d(0.5-r)} (1-\frac{0.5d}{n})^{-0.5(d+1)} \leq O(1)\sum_{d=2}^{(1-r)n} e^{f(d)}, \tag{10}$$

where

$$f(d) = \ln d n^{2n-0.5(d+1)} e^{d(0.5-r)} (1-\frac{0.5d}{n})^{-0.5(d+1)}$$
$$= 0.5(2\ln d + (4n-(d+1))\ln n + d(1-2r) + 2\ln(1-0.5d)(d+1)). \tag{11}$$

For the derivative of $f(d)$, we get

$$f'(d) = 0.5(\frac{2}{d} - \ln n + (1-2r) + 2\ln(1-\frac{0.5d}{n}) + \frac{d+1}{n-\frac{0.5d}{n}}.$$

Thus for n big enough, we have that $f'(d) < -1$ for all $d \geq 2$. Hence the sum (10) is bounded by the doubled first term of the sum, which is equal to $O(1)n^{2n-1.5}$. This contradicts $|L_n| \geq \Theta(n^{2n-1})$ and the theorem follows.

3 Searching for Stable Pairs

Lemma 7. *If $\mathcal{A}$ has a stable pair $\{p, q\}$ independent of b; then for any constant $k > 0$ whp there are k distinct stable pairs independent of a and only $2k$ transitions by b have been observed.*

Proof. Consider the chain of states $p.b, q.b, \ldots p.b^{k+1}, q.b^{k+1}$. Since $\{p, q\}$ is independent of b, the probability that all states in this chain are different is

$$(1-\frac{2}{n})(1-\frac{3}{n})\ldots(1-\frac{2(k+1)}{n})(1-\frac{2k+3}{n}) \geq (1-\frac{2(k+2)}{n})^{2(k+1)} = 1-O(\frac{1}{n}).$$

Since $\{p, q\}$ is independent of b, all states in this chain are independent of a.

Lemma 8. *If for some* $0 < \epsilon < 0.125$ *the automaton* $\mathcal{A}$ *has* $k = [\frac{1}{2\epsilon}] + 1$ *stable pairs independent of* b*; then whp there are* $n^{0.5-\epsilon}$ *stable pairs independent of* a *and at most* $kn^{0.5-\epsilon}$ *transitions by* a *have been observed.*

Proof. Let $\{p, q\}$ be one of these c stable pairs. Consider the chain of states

$$p, q, p.b, q.b, \ldots p.b^{n^{0.5-\epsilon}}, q.b^{n^{0.5-\epsilon}}.$$

Since $\{p, q\}$ is independent of b, the probability that all states in this chain are different is

$$(1-\frac{2}{n})(1-\frac{3}{n})\ldots(1-\frac{2n^{0.5-\epsilon}}{n})(1-\frac{2n^{0.5-\epsilon}+1}{n}) \geq (1-\frac{2n^{0.5-\epsilon}}{n})^{2n^{0.5-\epsilon}} = 1-O(\frac{1}{n^{2\epsilon}}).$$

Since these c stable pairs are independent of b, for $k = [\frac{1}{2\epsilon}] + 1$ the probability that there is such a pair $\{p, q\}$ is at least $1 - O(\frac{1}{n^{2k\epsilon}}) = 1 - O(\frac{1}{n})$. Again, all states in the chain are independent of a.

Theorem 4. *Whp for each letter* $x \in \{a, b\}$ *of* $\mathcal{A}$*, there is a set of at least* $n^{0.4}$ *distinct stable pairs independent of* x*, and only* $O(n^{0.4})$ *transitions have to be observed.*

Proof. By Corollary 1 and Theorem 6, there is a letter (say a) in the automaton $\mathcal{A}$ satisfying Theorem 3. Hence, there is a stable pair independent of b. Thus if we subsequently apply Lemma 7 for b and Lemma 8 for a, we get that there are $n^{0.5-\epsilon}$ stable pairs independent of b and only $O(n^{0.5-\epsilon})$ transitions by b have been observed. It remains to notice that we can do the same for the letter b if we additionally use Lemma 7 for a.

4 Conclusions

Theorem 1 gives an exact order of the convergence rate for the probability of being synchronizable for 2-letter automata up to the constant factor. One can easily verify that the convergence rate for t-size alphabet case ($t > 1$) is $1 - O(\frac{1}{n^{0.5t}})$ because the main restriction appears for the probability of having a unique 1-branch for some letter. Thus the first open question is about the tightness of the convergence rate $1 - O(\frac{1}{n^{0.5t}})$ for the t-letter alphabet case.

Since only weakly connected automata can be synchronizing, the second natural open question is about the convergence rate for random weakly connected automata of being synchronizable. Especially, binary alphabet is of certain interest because the lower bound for this case appears from a non-weakly connected case. We suppose exponentially small probability of not being synchronizable for this case and $\Theta(\frac{1}{n^{k-1}})$ for random k letter automata.

In conclusion, let us briefly remark that following the proof of Theorem 1 we can decide, whether or not a given n-state automaton $\mathcal{A}$ is synchronizing in linear expected time in n. Notice that the best known deterministic algorithm (basically due to Černý [6]) for this problem is quadratic on the average and in the worst case.

The author is thankful to Mikhail Volkov for permanent support in the research and also to Cyril Nicaud, Dominique Perrin, Marie-Pierre Béal and Julia Mikheeva for their interest and useful suggestions about the presentation of the current paper.

References

1. Araújo, J., Bentz, W., Cameron, P.: Groups synchronizing a transformation of non-uniform kernel. Theor. Comp. Sci. **498**, 1–9 (2013)
2. Berlinkov, M.: On the probability of being synchronizable (2013). arXiv:1304.5774
3. Berlinkov, M.: Highest trees of random mappings (2015). arXiv:1504.04532
4. Cameron, P.J.: Dixon's theorem and random synchronization. arXiv:1108.3958
5. Carayol, A., Nicaud, C.: Distribution of the number of accessible states in a random deterministic automaton. In: Leibniz International Proceedings in Informatics (LIPIcs), STACS 2012, vol. 14, pp. 194–205 (2012)
6. Černý, J.: Poznámka k homogénnym eksperimentom s konečnými automatami. Matematicko-fyzikalny Časopis Slovensk. Akad. Vied **14**(3), 208–216 (1964) (in Slovak)
7. Kari, J.: Synchronization and stability of finite automata. J. Univers. Comp. Sci. **2**, 270–277 (2002)
8. Nicaud, C.: Fast synchronization of random automata (2014). arXiv:1404.6962
9. Skvortsov, E., Zaks, Y.: Synchronizing random automata. Discrete Math. Theor. Comput. Sci. **12**(4), 95–108 (2010)
10. Skvortsov, E., Zaks, Y.: Synchronizing random automata on a 4-letter alphabet. J. Math. Sci. **192**, 303–306 (2013)
11. Timashov, A.: Asymptotic expansions for the distribution of the number of components in random mappings and partitions. Discrete Math. Appl. **21**(3), 291–301 (2011)
12. Trahtman, A.: The road coloring problem. Israel J. Math. **172**(1), 51–60 (2009)
13. Volkov, M.V.: Synchronizing automata and the Černý conjecture. In: Martín-Vide, C., Otto, F., Fernau, H. (eds.) LATA 2008. LNCS, vol. 5196, pp. 11–27. Springer, Heidelberg (2008)