HAL
open science

An analogue to Dixon's theorem for automaton groups

Thibault Godin

To cite this version:

Thibault Godin. An analogue to Dixon's theorem for automaton groups. Workshop on Analytic Algorithmics and Combinatorics (ANALCO), Conrado Martínez; Mark Daniel Ward, Jan 2017, Barcelone, Spain. hal-01378815

HAL Id: hal-01378815

https://inria.hal.science/hal-01378815

Submitted on 10 Oct 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

An analogue to Dixon's theorem for automaton groups

Thibault Godin*

IRIF, UMR 8243 CNRS, Univ. Paris Diderot Paris France
godin@liafa.univ-paris-diderot.fr

Abstract. Dixon's famous theorem states that the group generated by two random permutations of a finite set is generically either the whole symmetric group or the alternating group. In the context of random generation of finite groups this means that it is hopeless to wish for a uniform distribution – or even a non-trivial one – by drawing random permutations and looking at the generated group.
Mealy automata are a powerful tool to generate groups, including all finite groups and many interesting infinite ones, whence the idea of generating random finite groups by drawing random Mealy automata.
In this paper we show that, for a special class of Mealy automata that generate only finite groups, the distribution is far from being uniform since the obtained groups are generically a semi-direct product between a direct product of alternating groups and a group generated by a tuple of transpositions.

Keywords: Random Generation, Finite Groups, Automaton Groups, Random Permutations.

* The author is supported by the French *Agence Nationale pour la Recherche*, through the Project **MealyM** ANR-JCJC-12-JS02-012-01.

1 Introduction

The problem of random generation of finite groups was introduced by Netto in 1882 [25], who conjectured that two random elements of the symmetric group on k elements generate either the symmetric group or the alternating group with high probability when k goes to infinity. This was confirmed by Dixon in 1969 [8]. In this paper we study a different approach for this problem, using *Mealy automata*. More precisely, instead of drawing generators of a group, we draw a Mealy automaton next used to generate a group. In specific classes of automata we prove analogues to Dixon theorem: the limiting probability distributions on groups is formed by atoms of total weight 1.
In all the paper we denote by S_k the *symmetric group* over k elements, *i.e.* the group of the bijections of the set $\{1, \dots k\}$ (or equivalently the set of permutations on k symbols equipped with the multiplication), $|\sigma|$ the *order* of a permutation $\sigma \in S_k$, and $\mathrm{sgn}(\sigma)$ its *signature*. Moreover we say that A_k is the *alternating group*, that is the group of permutations of signature 1. If $g_1, \dots, g_i$ are elements of a group G then $\langle g_1, \dots, g_i \rangle$, called the *group generated* by $g_1, \dots, g_i$, is the smallest subgroup of G that contains $g_1, \dots g_i$. Finally we denote by $\leq$ the subgroup relation, by $\rtimes$ the (inner) semidirect product, by $\pi^\rho = \rho^{-1}\pi\rho$ the *conjugate* of π by ρ, by e the trivial permutation, and by lcm (*resp.* gcd) the function *lowest common multiple* (*resp.* smallest common multiple).

In 1969, Dixon proved the following theorem:

Theorem 1 (Dixon [8]). *Let σ and τ be two random permutations in S_k. Then*

$$\lim_{k\to\infty} \mathbb{P}\left(\langle \sigma, \tau \rangle = S_k \text{ or } A_k\right) = 1 \,.$$

In other terms the group generated by two random permutations is generically the biggest possible. The case where the generated group is A_k occurs when both permutations have signature 1.

The asymptotic in Theorem 1 has been gradually improved to $1 - 1/k - 1/k^2 - 4/k^3 - 23/k^4 - 171/k^5 \dots$[1] by Bovey and Williamson [6], Babai [3], and Dixon himself [9]. This theorem has also been extended to any finite simple group [19, 22]: pick two elements in a finite simple group, they generate the whole group with high probability.

This leaves open the problem of finding a suitable way to generate random finite groups. In this paper we examine a new model, that is, generating random finite groups via drawing random Mealy automata. More precisely we restrict ourselves to a class of automaton where every generated group is finite, the class of *automata with cycles without exit* [2, 26, 21]. Random generation of automata in this class has been studied by De Felice and Nicaud in [7].
In Section 2 we recall the definitions of Mealy automata, introduce the class of Mealy automata that we consider in the rest of the paper, and

[1] Sequence A113869 from OEIS [28].

prove some properties on the (finite) groups they generate. In Section 3 we show an analogue to Dixon's Theorem for cycle automata with 2 states, namely that, generically

$$\langle \; \overset{\sigma}{\underset{\tau}{\overset{1}{\bigcirc}\!\!\rightleftarrows\!\!\bigcirc\overset{2}{}}} \; \rangle = \begin{cases} \text{either } S_k \times S_k \,, \\ \text{or } (A_k \times A_k) \rtimes \langle(\pi,\pi)\rangle, \text{ with } \pi^2 = e \text{ and } \pi \neq e \\ \text{or } A_k \times A_k \,. \end{cases}$$

In Section 4 we extend this theorem to cyclic automata with any number of states. Section 5 is dedicated to the conclusion and some perspectives. Due to space constraints, several proofs are omitted but can be found in the appendix.

2 Mealy Automata

Mealy automata have been introduced by Mealy in [23] but have been widely used in (semi)group theory since Glushkov [16]. They have given numerous interesting groups, the most famous probably being the Grigorchuk group, that is an infinite torsion group with intermediate growth, solving both the Burnside problem and the Milnor problem [17, 18], along with many others. For a more complete introduction to the topic we refer the reader to the survey of Nekrashevych [24] or to the chapter of Bartholdi and Silva [4].

A *Mealy automaton* is a complete deterministic letter-to-letter transducer $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ where Q and Σ are finite sets respectively called the *stateset* and the *alphabet*, and $\delta = (\delta_i : Q \to Q)_{i\in\Sigma}$, $\rho = (\rho_q : \Sigma \to \Sigma)_{q\in Q}$ are respectively called the *transition* and *production* functions. These functions can be extended to words as follows: see $\mathcal{A}$ as an automaton with input and output tapes, thus defining mappings from input words over Σ to output words over Σ. Formally, for $q \in Q$, the map $\rho_q \colon \Sigma^* \to \Sigma^*$, extending $\rho_q \colon \Sigma \to \Sigma$, is defined recursively by:

$$\forall i \in \Sigma,\ \forall \boldsymbol{s} \in \Sigma^*, \qquad \rho_q(i\boldsymbol{s}) = \rho_q(i)\rho_{\delta_i(q)}(\boldsymbol{s}) \,. \tag{1}$$

We can also extend the map ρ to words of states $\boldsymbol{u} \in Q^*$ by composing the production functions associated with the letters of $\boldsymbol{u}$:

$$\forall q \in Q,\ \forall \boldsymbol{u} \in Q^*, \qquad \rho_{q\boldsymbol{u}} = \rho_{\boldsymbol{u}} \circ \rho_q \,. \tag{2}$$

A Mealy automaton is said to be *invertible* whenever ρ_q is a permutation of the alphabet for every $q \in Q$. It is called *reversible* whenever δ_i is a permutation of the stateset for every $i \in \Sigma$. Moreover an automaton is said to be *bireversible* whenever it is reversible (*i.e.* every input letter induces a permutation of the stateset) and every output letter induces a permutation of the stateset.
Examples of such automata are depicted in Figures 1 and 2.

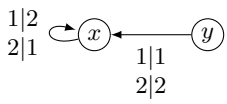

Fig. 1. An invertible non-reversible Mealy automaton (generating $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

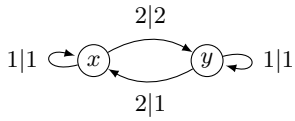

Fig. 2. A reversible non-invertible Mealy automaton (generating an infinite semigroup).

The production functions $\rho_q : \Sigma^* \to \Sigma^*$ of an automaton $\mathcal{A}$ generate a semigroup. Whenever $\mathcal{A}$ is invertible, one can define the *group generated by* $\mathcal{A}$:

$$\langle \mathcal{A} \rangle := \langle \rho_q | q \in Q \rangle = \langle \rho_{\boldsymbol{u}} : \Sigma^* \to \Sigma^* | \boldsymbol{u} \in Q^* \rangle \ .$$

The problem of deciding whether an automaton semigroup is finite was found undecidable by Gillibert [15]. For automaton groups the problem is still open. However some classes of automata are known to generate only finite or infinite groups. For instance automata that are invertible and reversible, but not bireversible generate only infinite groups [1]; while Antonenko [2] and Russyev [26] independently proved that automata with cycle without exit, *i.e.* automata where the underlying digraph consists in a directed graph where each cycle is a dead end (or equivalently a directed acyclic graph with eventually cycles and loops on the leaves), generate only finite groups, regardless of the production functions. This class is maximal in the sense that, for any automaton out of this class, there exist production functions such that the generated group is infinite [21].
In this paper we focus on the simplest of these later automata, namely those where the underlying digraph consists in a single cycle. We call the later *cyclic automata*, and draw the transitions $x \xrightarrow{\rho_x} y$ instead of $x \xrightarrow{i|\rho_x(i)} y$ when there is no ambiguity, see Figures 3 and 4 for examples.

For this class, the generated groups are finite, according to Antonenko and Russyev, but the simplicity of the structure allows us to be more precise:

Proposition 2. *Let $\mathcal{A}$ be an n-state k-letter cyclic automaton. Then $\langle \mathcal{A} \rangle \leq S_k^n$.*

Proof. Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$, with $Q = \{0, 1, \dots n-1\}$ and $|\Sigma| = k$. Consider the action of some state q on a word $\boldsymbol{s} = s_0 s_1 \dots s_\ell$, $s_i \in \Sigma$. Since the underlying graph is a cycle, up to renaming the states, we have $\delta_i(q) = q + 1 \bmod n$ for all $i \in \Sigma$. So $\rho_q(\boldsymbol{s}) = \rho_q(s_0) \dots \rho_{q+\ell \bmod n}(s_\ell)$. Hence ρ_q acts on $\boldsymbol{s}$ like the tuple

$$\left(\rho_q, \rho_{q+1 \bmod n}, \dots, \rho_{q+n-1 \bmod n}\right) .$$

The same holds for the other states, hence $\langle \mathcal{A} \rangle \leq S_k^n$. $\square$

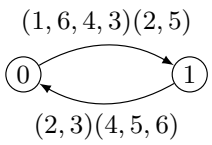

Fig. 3. A 2-state 6-letter cyclic automaton (generating S_6^2).

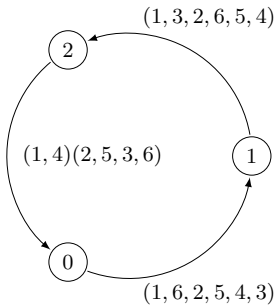

Fig. 4. A 3-state 6-letter cyclic automaton (generating $(A_6 \times A_6 \times A_6) \rtimes \langle(1, \pi, \pi)\rangle_c$ with the notations set below).

We have proved that

$$\langle \mathcal{A} \rangle = \langle (\rho_0, \rho_1, , \ldots, \rho_{n-1}), (\rho_1, \ldots, \rho_{n-1}, \rho_0), \ldots, (\rho_{n-1}, \rho_0, \ldots, \rho_{n-2}) \rangle \ .$$

In such case, we say that the group is *circularly generated* by the tuple $(\rho_1, \ldots, \rho_n)$ and write

$$\langle \mathcal{A} \rangle = \langle (\rho_0, \rho_1, \ldots, \rho_{n-1}) \rangle_c \ ,$$

where the subscript c stands for circular.
The multiplication law in $\langle \mathcal{A} \rangle$ can be seen as the usual multiplication of permutations extended componentwise to tuples.

Remark 3. The probability distribution on groups obtained by picking random cyclic automata is different from the one arising by picking random n-tuples of k-permutations. For instance, the probability of generating the trivial group is $1/k!^n$ in the first case, and $1/k!^{n^2}$ in the second case.

From now on we focus on groups that are circularly generated by a tuple of permutations. Likewise the case studied by Dixon, where two permutations were considered, their signatures impact the generated group. The easiest case arises when all permutations have signature 1, then no odd permutation can be generated by the tuple, hence $\langle \mathcal{A} \rangle \leq A_k^n$. To deal with this we mimic the notion of signature for tuples by defining, for any tuple $(\sigma_0, \ldots, \sigma_{n-1}) \in S_k^n$,

$$\mathrm{sgn}_\pi(\sigma_0, \ldots, \sigma_{n-1}) := (\pi^{\frac{1-\mathrm{sgn}(\sigma_0)}{2}}, \ldots, \pi^{\frac{1-\mathrm{sgn}(\sigma_{n-1})}{2}}) \ ,$$

where π is a transposition of S_k.

Then we obtain:

Proposition 4. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a n-state k-letter cyclic automaton with $Q = \{0, \ldots, n-1\}$. Then*

$$\langle \mathcal{A} \rangle = \langle (\rho_0, \ldots, \rho_{n-1}) \rangle_c \leq A_k^n \rtimes \langle sgn_\pi(\rho_0, \ldots, \rho_{n-1}) \rangle_c \ ,$$

where π is an arbitrary transposition of S_k.

In the following sections, we prove that, as for Dixon's theorem, the group circularly generated by $(\sigma_0, \ldots, \sigma_{n-1})$ is generically the biggest one, *i.e.* $A_k^n \rtimes \langle \mathrm{sgn}_\pi(\sigma_0, \ldots, \sigma_{n-1})\rangle_c$.

Note that the connectedness hypothesis (the fact that the automaton consists in a single cycle) matters. Indeed for a collection of cycles we get:

Proposition 5. *Let $I = \{1, \ldots, m\}$ and $\mathcal{A} = \bigsqcup_{i\in I} \mathcal{A}_i$ be the disjoint union of cyclic automata $\mathcal{A}_i$, each with n_i states, k_i letters, and transitions $\{\rho_{i,j}\}_{j<n_i}$. Then, putting $k = \max_i(k_i)$, we have*

$$\langle \mathcal{A}\rangle \leq A_k^{\mathrm{lcm}_I\,(n_i)} \rtimes E\,,$$

where $E \lesssim (\mathbb{Z}/2\mathbb{Z})^{\mathrm{lcm}_I\,(n_i)}$ has size at most 2^u, with

$$u = \sum_{j=1}^{m} (-1)^{j-1} \sum_{i_1<i_2<\ldots<i_j} \gcd(n_{i_1}, \ldots, n_{i_j})\,. \tag{3}$$

Example 6. If we have three automata, all of size 2, then Equation (3) gives

$$u = \underbrace{6-}_{\text{size 1}} \underbrace{(2+2+2)}_{\text{size 2}} \underbrace{+2}_{\text{size 3}} = 2\,.$$

If the sizes are $2, 3,$ and 5, we obtain $u = 10 - (1+1+1) + 1 = 8$. Hence we generate groups of size at most $|A_k|^{30} \times 2^8 = \frac{k!^{30}}{2^{22}}$.

This leads us to disprove the following conjecture from [20]: "the group generated by a bireversible n-state k-letter automaton is either infinite or of order less than or equal to $k!^n$". This conjecture fails, for instance, for the disjoint union of the automata from Figure 3 and 4 , which generates a group of order $34828517376000000 = 6!^6/4 > 6!^5$.

3 The 2-state Case

In this section we tackle the case of 2-state cyclic automata. Despite this limitation, most of the combinatorial complexity appears in this case which yet allows us to keep the proof easily readable.
In this section, $\mathcal{A}$ is a 2-state k-letter cyclic automaton with $\rho_0 = \sigma$ and $\rho_1 = \tau$.
The aim of this section is to prove the following :

Theorem 7. *Let $\mathcal{A}$ be a 2-state k-letter cyclic automaton. Then*

$$\begin{cases} \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq S_k \times S_k\right) & = 1/2\,, \\ \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq (A_k \times A_k) \rtimes \langle(\pi,\pi)\rangle\right) & = 1/4\,, \\ \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq A_k \times A_k\right) & = 1/4\,. \end{cases}$$

where π is an arbitrary transposition of S_k.

Remark 8. This is not a direct consequence of Dixon's theorem. Indeed one can apply Dixon's theorem to $S_k \times S_k$ – considering $G_D = \langle(\sigma,\tau),(\pi,\rho)\rangle$ – and get that G_D is asymptotically isomorphic to $S_k \times S_k$ with probability 3/8, to $S_k \times A_k$ with probability 3/8; $(A_k \times A_k) \rtimes \langle(\pi,\pi)\rangle$ with probability 3/16, or to $A_k \times A_k$ with probability 1/16.

In order to determine the generated group, we focus on the maximal subgroup of $\langle\mathcal{A}\rangle \leq S_k \times S_k$ where the first coordinate is e.

The following lemma allows us to conclude in a restricted number of cases:

Lemma 9. *For* $\gcd(|\sigma|,|\tau|) = 1$ *we have* $\langle\mathcal{A}\rangle = \langle\sigma,\tau\rangle \times \langle\sigma,\tau\rangle$.

However it is very unlikely that two permutations have relatively prime orders [12]. To prove Theorem 7 we use a theorem of Jordan (see [8]):

Theorem 10 (Jordan). *Let* $G \leq S_k$ *be a primitive group containing a cycle of prime length* $p \leq k-3$. *Then* G *is either the symmetric group* S_k *or the alternating group* A_k.

To apply this theorem we prove that we can find on the second coordinate a primitive group which contains a p-cycle.
The following proposition restricts the search of a subgroup to the search for a p-cycle.
We recall that the conjugacy classes in S_k are formed by the permutations with the same cycle structures. The same holds in A_k, and, if the cycle structure (including the cycles of length 1) consists only of cycles of odd length with no two cycles of same length, there are two conjugacy classes and we say that the conjugacy class *splits*, otherwise the elements with the same cycle structure form a single conjugacy class [27]. Using the notation $\pi^\rho = \rho^{-1}\pi\rho$ we hqve

Proposition 11. *Let* π *be a* p*-cycle of* S_k *with* p *prime and* $k \geq 5$, *then the groups* $G_\pi(S_k) = \langle\pi^\rho \mid \rho \in S_k\rangle$ *and* $G_\pi(A_k) = \langle\pi^\rho \mid \rho \in A_k\rangle$ *are primitive.*

The following easy but useful lemma shows that, if $A_k \leq \langle\sigma,\tau\rangle$ and there exists a p-cycle π such that $(e,\pi) \in \langle\mathcal{A}\rangle$, then the maximal subgroup of $\langle\mathcal{A}\rangle$ where the first component is e is isomorphic to either A_k or S_k.

Lemma 12. *Let* $(e,\pi) \in \langle\mathcal{A}\rangle$. *Then for any* $\rho \in \langle\sigma,\tau\rangle$ *we have* $(e,\pi^\rho) \in \langle\mathcal{A}\rangle$.

Hence if we find a cycle of prime length less than $k-3$ we will be able to conclude. The following lemma explains how to find such a permutation and contains the essence of the proof of Theorem 7.

Proposition 13. *Let* σ *and* τ *be two permutations of different orders and such that* $\langle\sigma,\tau\rangle = S_k$ *or* A_k. *Then there exists a* p*-cycle* π *(*p *prime) such that* $(e,\pi) \in \langle(\sigma,\tau)\rangle_c$.

Proof. Put $d = \gcd(|\sigma|, |\tau|)$. By construction $\left|\sigma^d\right|$ and $\left|\tau^d\right|$ are co-prime. Assume $\left|\tau^d\right| \neq e$: choose any prime number p that divides the order of τ^d (hence p does not divide the order of σ^d). Let a be the largest integer such that p^a divides $\left|\tau^d\right|$. Hence $\tau^{dp^{a-1}}$ has order pr, with $\gcd(p, r) = 1$, and $\sigma^{dp^{a-1}}$ has order co-prime with p (since it is the same order as σ^d). For simplicity we put $\hat{\tau} = \tau^{dp^{a-1}} \neq e$ and $\hat{\sigma} = \sigma^{dp^{a-1}}$.
Then $\langle \mathcal{A} \rangle \ni (\hat{\sigma}, \hat{\tau})^{\frac{|\hat{\sigma}||\hat{\tau}|}{p}} = ((\hat{\sigma}^{|\hat{\sigma}|})^{\frac{|\hat{\tau}|}{p}}, (\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|}) = (e, (\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|})$. Hence $\hat{\tau}^{\frac{|\hat{\tau}|}{p}}$ has order p by construction and, since $\gcd(|\hat{\sigma}|, p) = 1$, so has $(\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|} = \check{\tau}$.
Since $\check{\tau}$ has order p, it is a product $\prod_i \pi_i$ of ℓ disjoint p-cycles. For $\ell > 1$, we construct a p-cycle by considering the different cases:

1. Case $p \neq 2$. Let $\tilde{\tau}$ be the conjugate $\pi_1 \prod_{i \geq 2} \pi_i^{-1}$ of $\check{\tau}$. Hence $\langle \mathcal{A} \rangle \ni (e, \check{\tau})(e, \tilde{\tau}) = (e, \pi_1^2)$ and, since $\gcd(2, p) = 1$, π_1^2 is a p-cycle.
2. Case $p = 2$.
   (a) If $2\ell < k$. Then $\tilde{\tau} = \prod_{i \geq 0}(2i+1, 2i+2)$ and $\dot{\tau} = (1, k) \prod_{i \geq 0}(2i+1, 2i+2)$ are in the same conjugacy class as $\check{\tau}$, hence $\langle \mathcal{A} \rangle \ni (e, \tilde{\tau})(e, \dot{\tau}) = (e, (1, 2, k))$, whence we obtain a 3-cycle.
   (b) Otherwise $\tilde{\tau} = \prod_{i \geq 0}(2i+1, 2i+2)$ and $\dot{\tau} = (1, 4)(2, 3) \prod_{i \geq 2}(2i+1, 2i+2)$ satisfy $\tilde{\tau}\dot{\tau} = (1, 3)(2, 4)$ which reduces to the previous case (assuming $k > 4$).

□

We can now state our theorem:

Theorem 14. *Let σ and τ be two permutations of S_k, $k > 5$, of different orders and such that $\langle \sigma, \tau \rangle = S_k$ or A_k. Then*

$$\langle \; \overset{\sigma}{\underset{\tau}{\textcircled{1} \rightleftarrows \textcircled{2}}} \; \rangle = \begin{cases} S_k \times S_k & \textit{for } sgn(\sigma) \neq sgn(\tau), \\ (A_k \times A_k) \rtimes \langle (\pi, \pi) \rangle & \textit{for } sgn(\sigma) = sgn(\tau) = -1, \\ A_k \times A_k & \textit{for } sgn(\sigma) = sgn(\tau) = 1, \end{cases}$$

where π is an arbitrary transposition of S_k.

Proof. We apply Proposition 13. If the obtained p-cycle satisfies $p \leq k-3$ then we apply Theorem 10 and get that our group is one of the three described above.
Otherwise we can apply the same argument to σ and conclude, except in the six cases where (with $d = \gcd|\sigma|, |\tau|$) $(|\sigma|^d, |\tau|^d)$ is $((k-2)^a, (k-1)^b)$, $((k-1)^a, k^b)$, $((k-2)^a, k^b)$, $(1, (k-2)^b)$, $(1, (k-1)^b)$, or $(1, k^b)$, and $k = p$ is a prime greater than 5. Let us deal with the first three cases.
By taking the suitable powers of $(\sigma, \tau)^d$, we can assume $a = b = 1$ without loss of generality, and obtain the elements $(e, \hat{\sigma})$ and $(e, \hat{\tau})$ of $\langle \mathcal{A} \rangle$ with orders $p-2$ and $p-1$ (*resp.* $p-1$ and p, and $p-2$ and p). Then if the orders differ by one, we can construct $(e, (1, 2)) \in \langle \mathcal{A} \rangle$ by considering the product $(1, \ldots, p-2)(p-1, p-2, \ldots, 1)$ (*resp.* $(1, \ldots, p-1)(p, p-1, \ldots, 1)$), hence generating a group isomorphic to the direct product $\{e\} \times S_k$. If the difference is 2 then we use the same trick to get the 3-cycles. Since 3-cycles generate A_k we obtain $A_k \times A_k \leq \langle \mathcal{A} \rangle$.

In the last three cases we have $\sigma^d = 1$, with $d \leq 2$. For $d = 1$, $\langle \sigma, \tau \rangle \neq S_k, A_k$ which contradicts the hypothesis. For $d = 2$, we can assume that, up to renaming, $\tau = (1, 2)(3, \ldots, p)$. Hence we can get $(e, (1, \ldots, p-3, p-2))$ and $(e, (1, \ldots, p-3, p-1))$ in $\langle \mathcal{A} \rangle$. Then $(e, (1, \ldots, p-3, p-2))(e, (1, \ldots, p-3, p-1)) = (e, (1, 3, 5, \ldots, p-2)(2, 4, \ldots, p-3, p-1))$, so we can find a cycle of prime size smaller than $(p-1)/2$.
Finally, as $(\sigma, \tau) \in \langle \mathcal{A} \rangle$, by looking at its signature we show that the expected group is contained in $\langle \mathcal{A} \rangle$. We apply Proposition 4 as an upper bound and get the result. □

To prove Theorem 7 we use the convergence of the logarithm of the order of a random permutation to a (continuous) Gaussian limit law [11] to prove that two generic random permutations have different orders and Dixon's theorem to prove that they generate either A_k or S_k.
It would be interesting to compute a more precise asymptotic for this convergence. By Dixon's theorem we know that the probability for two random permutations to generate either S_k or A_k is $1 - 1/k + O(1/k^2)$. We are now interested in the probability for two random permutations to have the same order. It is clear that this probability admits $1/k^2$ for a lower bound (corresponding to the probability of drawing two k-cycles). A more precise lower bound is the probability that the permutations are conjugate, namely W_1/k^2 where $W_1 \approx 4.26340$ is an explicit constant, see [13] and [5]. Experimentally the probability that two random permutations have the same order seems to be of the same magnitude, hence we state the following conjecture:

Conjecture 15. Let σ, τ be two random permutations of S_k. Then

$$\lim_{k \to \infty} \mathbb{P}\left(|\sigma| = |\tau|\right) = \frac{K}{k^2} ,$$

with $W_1 \leq K \leq 12$.

Remark 16. The hypothesis "the permutations have different orders" is sufficient but not necessary: for instance, $\sigma = (1, 6, 7, 3, 12, 5)(2, 8)(9, 11)$ and $\tau = (1, 9, 8)(3, 5, 7, 6, 10, 11)(4, 12)$ satisfy $\mathrm{sgn}(\sigma, \tau) = (-1, 1)$ and $|\sigma| = |\tau| = 6$, but the generated group is $S_{12} \times S_{12}$, and other examples can be found for the other groups described.
On the other hand, one can find examples of a cyclic automaton with two permutations with the same order (generating either the symmetric or the alternating group), that generate none of the three expected groups. A necessary and sufficient, but yet ineffective, hypothesis would be that some product ρ of σ and τ has an order different from the order of ρ defined by applying $\sigma \mapsto \tau$ and $\tau \mapsto \sigma$ on $\rho \in \{\sigma, \tau\}^*$, and $A_k \leq \langle \sigma, \tau \rangle$.

Remark 17. This theorem, likewise Dixon's theorem, does not generalise to semigroups. Indeed to generate the whole transformation semigroup one need to pick at least two permutations, which is rare: the probability of drawing one permutation is $k!/k^k \sim_\infty \sqrt{2\pi k} e^{-k} \to_\infty 0$. Numerical simulations performed using GAP system [14] do not suggest any obvious convergence to a set of semigroups.

Using [10] we can also say a bit about another way of generating random groups:

Proposition 18. *Let σ and τ be two random permutations of S_k, $k \geq 5$. Let $\mathcal{A}$ be the disjoint union of two cyclic automata, with output functions σ and σ^{-1} for one, and τ and τ^{-1} for the other. Then, generically,*

$$\langle \mathcal{A} \rangle = \begin{cases} (A_k \times A_k) \rtimes \langle (\pi, \pi) \rangle & \textit{if one of the permutation is odd} \\ A_k \times A_k & \textit{otherwise.} \end{cases}$$

With π an arbitrary transposition.

Proof. We have $\langle \mathcal{A} \rangle = \langle (\sigma, \sigma^{-1}), (\tau, \tau^{-1}) \rangle_c$. It is a direct consequence of Dixon's theorem ($\langle \sigma, \tau \rangle = S_k, A_k$ generically) and Lemma 2.4 and Example 2.7 of [10], with the remark that $[A_k, A_k] = A_k$ for $k \geq 5$. □

In contrast, the group $\langle (\sigma, \tau^{-1}), (\sigma^{-1}, \tau) \rangle_c$ is equal to $\langle (\sigma, \tau^{-1}) \rangle_c$, and follows the behaviour described in Theorem 7.

4 Cyclic Automata with any Number of States

For the general case we need more conditions on the orders to find an isolated, prime-sized cycle. In order to conclude, we require that the tuple of the orders of the permutations has no periodic pattern.
Recall that a primitive word is a word that cannot be expressed as a power of a shorter word.

Proposition 19. *Let $(\sigma_i)_i$ be n permutations of S_k, $k \geq 7$, such that the tuple $(|\sigma_0|, \ldots, |\sigma_{n-1}|)$ is primitive and $\langle (\sigma_i)_i \rangle = S_k$ or A_k. Then there exists a prime-sized cycle π satisfying $(e, e, \ldots, e, \pi) \in \langle (\sigma_i)_i \rangle_c$.*

Now we have:

Theorem 20. *Let $\mathcal{A}_k$ be a random n-state k-letter cyclic automaton with output functions $(\sigma_0, \ldots, \sigma_{n-1})$. Then*

$$\lim_{k \to \infty} \mathbb{P}\Big(\langle \mathcal{A}_k \rangle = A_k^n \rtimes \langle sgn_\pi(\sigma_0, \ldots, \sigma_{n-1}) \rangle_c \Big) = 1 \,.$$

Proof. By Dixon's theorem we can assume that $\langle (\sigma_i)_i \rangle = S_k$ or A_k. If the tuple of orders is primitive then using Proposition 19 we get an element having a p-cycle on one coordinate and trivial permutations elsewhere, and, as in Theorem 14 we obtain the expected result. Now the probability that the tuple of orders is primitive is less than the probability that $|\sigma_0| = |\sigma_i|$ holds for some i, which goes to 0 as k goes to infinity, since n is fixed. □

Once again the signatures control the generated group, so we can deduce the probability of generating each group. Note that there is at most 2^n groups and that some of them are isomorphic.

5 Conclusion and Perspectives

We showed that the model of random cyclic automaton groups presents little diversity and hence cannot be used in order to provide an efficient model of random groups. The natural extension is now to deal with other types of Mealy automata. The closest step – the whole class of automata with cycles without exit – also seems to provide a Dixon-like property. One can prove another analogue to Dixon's Theorem in two other subclasses: paths ending with a loop and trees with loops on leaves.

Proposition 21. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be an n-state k-letter automaton with $Q = \{0, \dots, n-1\}$, such that $\delta_u(q) = \min(q+1, n-1), \forall q \in Q, u \in \Sigma$. Then*

$$\lim_{k\to\infty} \mathbb{P}\big(\langle \mathcal{A}_k \rangle = (A_k^{n-1} \times \langle \rho_{n-1} \rangle) \rtimes P\big) = 1\,,$$

where $P = \langle \{(sgn_\pi(\rho_i), \dots, sgn_\pi(\rho_{n-1}), \dots, sgn_\pi(\rho_{n-1}))\}_i \rangle$.

Proposition 22. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be an n-state k-letter automaton with Q labelled by words in $\{0, \dots, a-1\}^d$ (with a and d integers respectively called arity and depth of the automaton), such that $\delta_u(q_{x_0,\dots,x_i,x_{i+1}}) = q_{x_0,\dots,x_i}, \forall x_0, \dots x_{i+1} \in \{0, \dots, a-1\}^d, u \in \Sigma$. Then*

$$\lim_{k\to\infty} \mathbb{P}\big(\langle \mathcal{A}_k \rangle = (A_k^{n-1} \times P\big) = 1\,,$$

where $P = \langle \rho_{q_\epsilon} \rangle \rtimes \langle \{(sgn_\pi(\rho_{u_i u_{i-1} \dots}), \dots, sgn_\pi(\rho_{q_\epsilon}), \dots, sgn_\pi(\rho_{q_\epsilon}))\}_i \rangle$.

In particular, if the automaton $\mathcal{A}$ contains a cyclic automaton as a leaf, then generically $A_k \rtimes \langle \mathrm{sgn}_\pi(\sigma_1, \dots, \sigma_n) \rangle_c$ is a subgroup of $\langle \mathcal{A} \rangle$, preventing to generate small groups. This, in addition with numerical evidences, suggest that the class of automata with cycles without exit does not present interesting behaviour regarding random generation.
The more general classes of automata are more delicate to tackle since the finiteness problem is not yet known, however they present much more interesting behaviour since we no longer require a tree-like structure.

Besides, determining the probability that two permutations have the same order, which would provide asymptotics for our result, seems to be an interesting problem in its own.

Acknowledgements

I would like to thank Cyril Nicaud for the initial working session that lead to this paper. I am also grateful to my PhD supervisors, Ines Klimann and Matthieu Picantin for their patient listening and the proof reading of this work, and to Charles Paperman for the encouragements and remarks. I am also grateful to the anonymous reviewers for their careful reading and comments.
Finally, I am thankful to the many persons I bothered with the question *"what's the probability that two random permutations have the same orders?"*, in particular Vlady Ravelomanana, Nicolas Pouyanne, Guillaume Lagarde, Stefan-Christoph Virchow, Simon R. Blackburn, John R. Britnell, and Mark Wildon – thanks for your help.

References

1. A. Akhavi, I. Klimann, S. Lombardy, J. Mairesse, and M. Picantin, *On the finiteness problem for automaton (semi)groups*, Internat. J. Algebra Comput. **22** (2012), no. 6, 26p.
2. A. S. Antonenko, *On transition functions of Mealy automata of finite growth*, Matematychni Studii. **29** (2008), no. 1, 3–17.
3. L. Babai, *The probability of generating the symmetric group*, Journal of Combinatorial Theory, Series A **52** (1989), no. 1, 148 – 153.
4. L. Bartholdi and P. V. Silva, *Groups defined by automata*, CoRR **abs/1012.1531** (2010).
5. S. R. Blackburn, J.R. Britnell, and M Wildon, *The probability that a pair of elements of a finite group are conjugate*, J. London Math. Society **86** (2012), no. 3, 755–778.
6. J. D. Bovey and A. Williamson, *The probability of generating the symmetric group*, Bull. London Math. Soc. **10** (1978).
7. S. De Felice and C. Nicaud, *Random generation of deterministic acyclic automata using the recursive method*, Computer Science - Theory and Applications - 8th International Computer Science Symposium in Russia, CSR 2013, Ekaterinburg, Russia, June 25-29, 2013. Proceedings, 2013, pp. 88–99.
8. J. D. Dixon, *The probability of generating the symmetric group*, Mathematische Zeitschrift **110** (1969), no. 3, 199–205.
9. ———, *Asymptotics of generating the symmetric and alternating groups*, Electronic J. Comb (2005).
10. J. East and Th. E. Nordahl, *On groups generated by involutions of a semigroup*, Journal of Algebra **445** (2016), 136 – 162.
11. P. Erdos and P. Turan, *On some problems of statistical group theory iii*, Acta. Math. Acad. Sci. Hungar. **18** (1967), 309–320.
12. ———, *On some problems of statistical group theory v*, Acta. Math. Acad. Sci. Hungar. **1** (1971), 5–13.
13. P. Flajolet, E. Fusy, X. Gourdon, D. Panario, and N. Pouyanne, *A hybrid of darboux's method and singularity analysis in combinatorial asymptotics*, Electronic Journal of Combinatorics **13(1)** (2006), no. 1, 1–35.
14. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015.
15. P. Gillibert, *The finiteness problem for automaton semigroups is undecidable*, Internat. J. Algebra Comput. **24** (2014), no. 1, 1–9.
16. V. M. Glushkov, *The abstract theory of automata*, Russian Mathematical Surveys **16** (1961), no. 5, 1.
17. R. I. Grigorchuk, *On Burnside's problem on periodic groups*, Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 53–54.
18. ———, *On the Milnor problem of group growth*, Dokl. Akad. Nauk SSSR **271** (1983), no. 1, 30–33.
19. W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), no. 1, 67–87. MR 1065213
20. I. Klimann, J. Mairesse, and M. Picantin, *Implementing computations in automaton (semi)groups*, Implementation and Application of Automata (Nelma Moreira and Rogério Reis, eds.), Lecture Notes

in Computer Science, vol. 7381, Springer Berlin Heidelberg, 2012, pp. 240–252 (English).
21. I. Klimann and M. Picantin, *A characterization of those automata that structurally generate finite groups*, LATIN 2014: Theoretical Informatics - 11th Latin American Symposium, Montevideo, Uruguay, March 31 - April 4, 2014. Proceedings, 2014, pp. 180–189.
22. M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), no. 1, 103–113. MR 1338320
23. G. Mealy, *a method for synthesizing sequential circuits*, Bell System Tech. Jour. **34** (1955), 1045–1079.
24. V. Nekrashevych, *Self-similar groups*, Mathematical Surveys and Monographs, vol. 117, American Mathematical Society, Providence, RI, 2005.
25. E. Netto, *Substitutionstheorie und ihre Anwendung auf die Algebra*, 1882.
26. A. Russyev, *Finite groups as groups of automata with no cycles with exit*, Algebra and Discrete Mathematics **9** (2010), no. 1, 86–102.
27. W. R. Scott, *Group theory*, Dover Books on Mathematics, Dover Publications, 1964.
28. N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, 2016.

A Appendix

We present the omitted proofs. For coherence sake, we recall the statements using the same numerotation. To improve the legibility we add some intermediate results.

Proposition 4. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be a n-state k-letter cyclic automaton with $Q = \{0, \dots, n-1\}$. Then*

$$\langle \mathcal{A} \rangle = \langle (\rho_0, \dots, \rho_{n-1}) \rangle_c \leq A_k^n \rtimes \langle sgn_\pi(\rho_0, \dots, \rho_{n-1}) \rangle_c \,,$$

where π is an arbitrary transposition of S_k.

Proof. Let π be an arbitrary transposition of S_k. For $\sigma \in S_k$, we define

$$\hat{\sigma} = \begin{cases} \{\sigma\pi, \pi\} & \text{for } \operatorname{sgn}(\sigma) = -1 \,, \\ \{\sigma, e\} & \text{otherwise.} \end{cases}$$

The map $\sigma \mapsto \hat{\sigma}$ is clearly a bijection from S_k to $A_k \rtimes \langle \pi \rangle$. We can extend this bijection to tuples: A_k^n is a normal subgroup of S_k^n as it is a direct product of n normal subgroups of S_k, it is also the kernel of the morphism $\operatorname{sgn}_\pi \,:\, S_k^n \,\to\, \langle (\pi, e, e, \dots, e) \rangle_c$. Hence $S_k^n \simeq A_k^n \rtimes \langle (\pi, e, e, \dots, e) \rangle_c$ and

$$\begin{aligned} \langle \mathcal{A} \rangle \simeq & \langle \{ (\rho_0 \pi^{\frac{1-\operatorname{sgn}(\rho_0)}{2}}, \dots, \rho_{n-1} \pi^{\frac{1-\operatorname{sgn}(\rho_{n-1})}{2}}) \operatorname{sgn}_\pi(\rho_0, \dots \rho_{n-1}) \} \rangle_c \\ \leq & A_k^n \rtimes \langle \operatorname{sgn}_\pi(\rho_0, \dots, \rho_{n-1}) \rangle_c \,. \end{aligned}$$

□

We extend the notion of signature to tuple componentwise:

$$\mathrm{sgn}(\sigma_0, \ldots, \sigma_{n-1}) := (\mathrm{sgn}(\sigma_0), \ldots, \mathrm{sgn}(\sigma_{n-1})) \,.$$

Proposition 5. *Let $I = \{1, \ldots, m\}$ and $\mathcal{A} = \bigsqcup_{i \in I} \mathcal{A}_i$ be the disjoint union of cyclic automata $\mathcal{A}_i$, each with n_i states, k_i letters, and transitions $\{\rho_{i,j}\}_{j<n_i}$. Then, putting $k = \max_i(k_i)$, we have*

$$\langle \mathcal{A} \rangle \leq A_k^{\mathrm{lcm}_I\,(n_i)} \rtimes E \,,$$

where $E \lesssim (\mathbb{Z}/2\mathbb{Z})^{\mathrm{lcm}_I\,(n_i)}$ has size at most 2^u, with

$$u = \sum_{j=1}^{m} (-1)^{j-1} \sum_{i_1 < i_2 < \ldots < i_j} \gcd(n_{i_1}, \ldots, n_{i_j}) \,. \tag{3}$$

Proof. Similarly to Proposition 2, we show that every state $q_0^i \in \mathcal{A}_i$ acts like $(\rho_{i,1}, \ldots, \rho_{i,n_i-1}, \rho_{i,0}, \ldots, \rho_{i,n_i-1}, \ldots \rho_{i,0}, \ldots, \rho_{i,n_i-1})$, a tuple of size $\mathrm{lcm}_I(n_i)$ of permutations of S_k, hence

$$\langle \mathcal{A} \rangle \leq A_k^{\mathrm{lcm}_I\,(n_i)} \rtimes \langle \{\mathrm{sgn}_\pi(\rho_{i,0}, \ldots, \rho_{i,n_i-1}, \ldots \rho_{i,n_i-1})\}_{i \in I} \rangle_c \leq S_k^n \,.$$

Consider the elements of E: $\langle \mathrm{sgn}_\pi(\rho_{i,0}, \ldots, \rho_{i,n_i-1} \ldots \rho_{i,n_i-1}) \rangle_c$ is isomorphic to $\langle \mathrm{sgn}(\rho_{i,0}, \ldots, \rho_{i,n_i-1} \ldots \rho_{i,n_i-1}) \rangle \leq \langle (1, 0, \ldots, 1, 0, \ldots, 0) \rangle_c$, where the two last groups have additive laws. So the order of E is less than the order of the group circularly generated by tuples of periods n_i with only one entry 1 per period. This group has at most $2^{\sum n_i}$ elements: put $E_i = \langle \mathrm{sgn}(\rho_{i,0}, \ldots, \rho_{i,n_i} \ldots \rho_{i,n_i}) \rangle_c$ and $P_i = \langle (1, 0, \ldots, 1, 0, \ldots, 0) \rangle_c$ (where the tuple has length $\mathrm{lcm}_I(n_i)$, period n_i and one entry 1 in each periodic factor), then $|E_i| \leq |P_i| = 2^{n_i}$ and every element of E is a product of elements in E_i, hence $|E| \leq \prod_i |E_i| \leq \prod |P_i| = 2^{\sum n_i}$. In addition, tuples whose period divides both n_i and n_j belong to both P_i and P_j, hence are counted twice. By the inclusion-exclusion principle on the lowest common multiples of the periods we get the result. □

Lemma 9. *For $\gcd(|\sigma|, |\tau|) = 1$ we have $\langle \mathcal{A} \rangle = \langle \sigma, \tau \rangle \times \langle \sigma, \tau \rangle$.*

Proof. By Bezout lemma there exist $u, v \in \mathbb{N}$ such that $u\,|\sigma| + v\,|\tau| = 1$. Now $\langle \mathcal{A} \rangle \ni (\sigma, \tau)^{u|\sigma|} = (\sigma^{u|\sigma|}, \tau^{1-v|\tau|}) = (e, \tau)$. Likewise we get the elements $(e, \sigma), (\sigma, e)$ and (τ, e) whence $\langle \sigma, \tau \rangle \times \langle \sigma, \tau \rangle \leq \langle \mathcal{A} \rangle$. The other inclusion follows from Proposition 2. □

Proposition 11. *Let π be a p-cycle of S_k with p prime and $k \geq 5$, then the groups $G_\pi(S_k) = \langle \pi^\rho \mid \rho \in S_k \rangle$ and $G_\pi(A_k) = \langle \pi^\rho \mid \rho \in A_k \rangle$ are primitive.*

Proof. We only need to prove the second statement, which implies the first one. Recall that a primitive group is a transitive group that does not stabilise any partition of $\Sigma = \{1, \ldots, k\}$ (apart from the two trivial ones: the singleton partition and the partition of singletons). Let us prove first that $G_\pi(A_k)$ is transitive. Let $i, j \in \Sigma$. If the conjugacy class does not split then $(i, j, x_3, \ldots, x_p) = \pi^\rho$ for a suitable $\rho \in A_k$ and arbitrary x_ℓ's, and $\pi^\rho(i) = j$. Otherwise $p \geq 5$ and if $(i, j, x_3, \ldots, x_p) = \pi^\rho$,with $\rho \in S_k \setminus$

A_k is not in the same conjugacy class as π then $(i, j, x_3, \ldots, x_p, x_{p-1}) = (\pi^\rho)^{(p-1,p)} = \pi^{\rho(p-1,p)}$ is in the same conjugacy class since $\rho(p-1, p) \in A_k$. Hence $G_\pi(A_k)$ is transitive.
For primitivity, consider a partition $\Sigma_1, \ldots, \Sigma_a$ of Σ such that $i, j \in \Sigma_1$ and $\ell \notin \Sigma_1$. Then consider the cycle $\pi^\rho = (i, j, x_3, \ldots, x_{p-1}, \ell)$: as $\pi^\rho(i) = j \in \Sigma_1$ and $\pi^\rho(\ell) = i \in \Sigma_1$, the partition is not preserved. For $\rho \in A_k$ we get the result. Otherwise $\rho(1, 2) \in A_k$, so $(j, i, x_3, \ldots, x_{p-1}, \ell) \in G_\pi(A_k)$ and the same holds. □

Let $\overline{} : \{\sigma, \tau\}^* \to \{\tau, \sigma\}^*$ be the involutory morphism defined by $\overline{\sigma} = \tau$. Then for $\rho \in \{\sigma, \tau\}^*$, $(\rho, \overline{\rho}) \in \langle \mathcal{A} \rangle$ (after identifying words on $\{\sigma, \tau\}$ with permutation in S_k).

Lemma 12. *Let $(e, \pi) \in \langle \mathcal{A} \rangle$. Then for any $\rho \in \langle \sigma, \tau \rangle$ we have $(e, \pi^\rho) \in \langle \mathcal{A} \rangle$.*

Proof. Since $(\overline{\rho}, \rho) \in \langle \mathcal{A} \rangle$ and $\overline{\rho^{-1}} = \overline{\rho}^{-1}$, we have $(\overline{\rho}, \rho)^{-1}(e, \pi)(\overline{\rho}, \rho) = (e, \pi^\rho)$. □

To prove Proposition 19 we first present the case of three permutations, then generalise to an arbitrary number of them.

Proposition 23. *Let σ_0, σ_1 and σ_2 be three permutations of S_k, $k \geq 7$, that do not all have the same order and such that $\langle \sigma_0, \sigma_1, \sigma_2 \rangle$ is either S_k or A_k. Then there exists a prime-sized cycle π satisfying $(e, e, \pi) \in \langle (\sigma_0, \sigma_1, \sigma_2) \rangle_c$.*

Proof. Since the orders are different, there exist a prime p, an integer c, and a non-trivial subset of $\{\sigma_i\}_{i \in \{0,1,2\}}$ such that p^c divides each order of the elements in that subset. If it divides the order of only one permutation, we can apply the argument of Proposition 13. Otherwise, we can obtain, by taking the suitable power of a generator, the tuple (e, τ_1, τ_2) (and (τ_1, τ_2, e) by circularity). As in Proposition 13 we can create, by conjugation and multiplication, (e, ρ_1, α) (*resp.* (β, ρ_2, e)) for some p-cycle ρ_1 (*resp.* ρ_2). Moreover we can get that $|\alpha|$ (*resp.* $|\beta|$) is p^a for some integer a (*resp.* p^b for some b), so we have $(e, \rho_1, \alpha_{\rho_1})$ (*resp.* $(\beta_{\rho_2}, \rho_2, e)$) for any p-cycle ρ_1 (*resp.* ρ_2) in a certain conjugacy class under $\langle \sigma_0, \sigma_1, \sigma_2 \rangle$. Then we can multiply these tuples and obtain $(\beta_\pi, \pi, \alpha_\pi)$, where π is a cycle of size 3 (*resp.* 5 for $p = 3$), and the orders of α_π and β_π are powers of p. Then $(\beta_\pi, \pi, \alpha_\pi)^{|\alpha_\pi||\beta_\pi|} = (e, \hat{\pi}, e)$, where $\hat{\pi}$ is a 3-cycle (*resp.* 5-cycle), thus by conjugation (*resp.* multiplication and conjugation) we can get all 3-cycles, and finally able to generate A_k. The result follows. □

Proposition 19. *Let $(\sigma_i)_i$ be n permutations of S_k, $k \geq 7$, such that the tuple $(|\sigma_0|, \ldots, |\sigma_{n-1}|)$ is primitive and $\langle (\sigma_i)_i \rangle = S_k$ or A_k. Then there exists a prime-sized cycle π satisfying $(e, e, \ldots, e, \pi) \in \langle (\sigma_i)_i \rangle_c$.*

Proof. Since the tuple of orders is primitive there exists a prime p and an integer c such that p^c divides every element of a non-trivial subset of $\{|\sigma_i|\}_{i \in \{0,\ldots,n-1\}}$. Hence we get a tuple of permutations of orders p or 1. We can assume that each non-trivial permutation is surrounded by ones: consider $(\alpha_0, \ldots, \alpha_a, e, \pi_0, \ldots, \pi_s, e, \beta_0, \ldots, \beta_b)$ where

the π's have orders p and π_1 is a p-cycle, and its permuted-conjugated $(\beta'_b, \alpha'_0, \ldots, \alpha'_a, e, \pi'_0, \ldots, \pi'_s, e, \beta'_0, \ldots, \beta'_{b-1})$ where the π''s have orders p and π'_0 is a p-cycle such that $\pi_1\pi'_0$ has order r, with r a prime different from p, and $|\alpha_i| = |\alpha'_i|$ and $|\beta_i| = |\beta'_i|$. By multiplying these two tuples we get

$$\Delta = (\alpha_0\beta'_b, \alpha_1\alpha'_0, \ldots, \alpha_a\alpha'_{a-1}, \alpha'_a, \pi_0, \pi_1\pi'_0, \ldots, \pi_s\pi'_{s-1}, \pi'_s, \beta_0, \beta_1\beta'_0, \ldots, \beta_{b-1}\beta'_b)\,.$$

We remark that if a permutation α_i is trivial, then the corresponding coordinate in Δ has order p. Then by taking the suitable power we get a tuple $(\gamma_0, \ldots, \gamma_{a-1}, e, e, \rho_0, \ldots, \rho_{s-1}, e, e, \delta_0, \ldots, \delta_{b-1})$, where trivial coordinates remain trivial and every non-trivial permutation has order r, hence, by induction, we construct a tuple of permutations of prime order r, where each non-trivial permutation is surrounded by trivial permutations (note that if the original tuple is formed by one trivial permutation and a block of permutations of orders p, then using techniques similar to the one in Proposition 23 we reduce to this situation).This tuple might be non-primitive, but we can construct such a tuple for each prime greater than 2.

We now consider two cases: if $\exists \Pi = (\sigma_0, \ldots, \sigma_{n-1})^d = (\pi_0, \ldots, \pi_{n-1})$ a tuple with $|\pi_i| \in \{1, p\}$, p prime, such that the tuple of orders is primitive, then let Γ be a non-trivial tuple with the orders of the coordinate either 1 or p, and where two non-trivial permutations are consecutive (as constructed above). Since Π is aperiodic we can find a configuration were two non-trivial permutations of Γ face respectively a trivial permutation and a non-trivial one. Thus by multiplying and taking the suitable power, we get Γ_1 having the same properties as Γ and with strictly less non-trivial permutations. Hence we obtain $\Gamma_\infty \in \langle \mathcal{A} \rangle$ which contains exactly one p-cycle and trivial permutations.

If no such Π exists then, since the tuple of orders is aperiodic, there are two tuples Π_1, Π_2 having tuples of orders with non-multiple periods t_1, t_2 and such that the lowest common multiple of their periods is greater does not divide n (or equivalently is greater than n). Then can construct Γ as above for Π_1. Then, either Γ is aperiodic or t_1 does not divide its period, or t_1 divides its period. In the first case we can obtain a tuple Γ_1 having strictly less non-trivial permutations by multiplying Γ and Π_1 and taking the suitable power. In the second case t_2 does not divide the period of Γ and we apply the same argument using Π_2 instead of Π_1. By induction of this procedure we obtain Γ_∞ as described above. □

Proposition 21. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be an n-state k-letter automaton with $Q = \{0, \ldots, n-1\}$, such that $\delta_u(q) = \min(q+1, n-1), \forall q \in Q, u \in \Sigma$. Then*

$$\lim_{k\to\infty} \mathbb{P}\big(\langle \mathcal{A}_k \rangle = (A_k^{n-1} \times \langle \rho_{n-1} \rangle) \rtimes P\big) = 1\,,$$

where $P = \langle \{(sgn_\pi(\rho_i), \ldots, sgn_\pi(\rho_{n-1}), \ldots, sgn_\pi(\rho_{n-1}))\}_i \rangle$.

Proof. By definition of the automaton, q induces the transformation $(\rho_q, \rho_{q+1}, \ldots, \rho_{n-1}, \ldots, \rho_{n-1}, \ldots)$ on Σ^*. Hence

$$\langle \mathcal{A} \rangle \simeq \langle (\rho_0, \ldots, \rho_{n-1}), (\rho_1, \ldots, \rho_{n-1}, \rho_{n-1}), \ldots, (\rho_{n-1}, \ldots, \rho_{n-1}) \rangle\,,$$

whence the result by Dixon's theorem and conjugation. □

Hence the group has size $k!^{n-1} \times |\rho_{n-1}| \, / 2^{(\min_i (i | \{\mathrm{sgn}(\rho_{n-1-i})\}_i = \{-1,1\}) - 1)}$
In the same spirit, if the automaton is the disjoint union of linear automaton, then it is generically the direct product of symmetric or alternating groups.

Proposition 22. *Let $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ be an n-state k-letter automaton with Q labelled by words in $\{0, \ldots, a-1\}^d$ (with a and d integers respectively called arity and depth of the automaton), such that $\delta_u(q_{x_0,\ldots,x_i,x_{i+1}}) = q_{x_0,\ldots,x_i}, \forall x_0, \ldots x_{i+1} \in \{0, \ldots, a-1\}^d, u \in \Sigma$. Then*

$$\lim_{k \to \infty} \mathbb{P}\big(\langle \mathcal{A}_k \rangle = (A_k^{n-1} \times P\big) = 1 \, ,$$

where $P = \langle \rho_{q_\epsilon} \rangle \rtimes \langle \{(sgn_\pi(\rho_{u_i u_{i-1} \ldots}), \ldots, sgn_\pi(\rho_{q_\epsilon}), \ldots, sgn_\pi(\rho_{q_\epsilon}))\}_i \rangle$.

Proof. By definition of the automaton, $q_{u_0 u_1 \ldots u_i}$ induces the transformation $(\rho_{q_{u_0 u_1 \ldots u_i}}, \rho_{q_{u_0 u_1 \ldots u_{i-1}}}, \ldots, \rho_{q_\epsilon}, \ldots, \rho_{q-\epsilon}, \ldots)$ on Σ^*. Whence the result by Dixon's theorem and conjugaison. □