ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2023, **15** (2), 608–613
doi:10.15330/cmp.15.2.608-613

https://journals.pnu.edu.ua/index.php/cmp
Карпатськi матем. публ. 2023, Т.15, №2, С.608–613

Minimal generating sets in groups of p-automata

Lavrenyuk Y.V., Oliynyk A.S.[1]

For an arbitrary odd prime p, we consider groups of all p-automata and all finite p-automata. We construct minimal generating sets in both the groups of all p-automata and its subgroup of finite p-automata. The key ingredient of the proof is the lifting technique, which allows the construction of a minimal generating set in a group provided a minimal generating set in its abelian quotient is given. To find the required quotient, the elements of the groups of p-automata and finite p-automata are presented in terms of tableaux introduced by L. Kaloujnine. Using this presentation, a natural homomorphism on the additive group of all infinite sequences over the field $\mathbb{Z}_p$ is defined and examined.

Key words and phrases: finite automaton, p-automaton, minimal generating set.

[1] Taras Shevchenko National University of Kyiv, 64/13 Volodymyrska str., 01601, Kyiv, Ukraine
E-mail: ylavrenyuk@gmail.com (Lavrenyuk Y.V.), aolijnyk@gmail.com (Oliynyk A.S.)

Introduction

The problem to find a minimal genarating set of a given algebraic structure is well-known. In many cases it has useful positive solutions, say for vector spaces or free semigroups and groups. However, even to prove that a given group has a minimal generating set is in general a challenging task.

This paper can be regarded as a natural continuation of the first named author's research from [5], where for a wide class of groups splitting into a semidirect product the existence of minimal generating sets is shown. In particular, it allows to prove that the group of all finite automata over finite alphabet has a minimal generating set and therefore to solve a long-standing open problem formulated in [1]. This positive result in particular contrasts with negative ones for generic semigroups of finite automata [6].

For arbitrary odd prime p we consider groups of all p-automata and all finite p-automata. The latter group contains amalgamated free products of cyclic p-groups [9], certain HNN-extensions of free abelian groups [8, 10] and free non-abelian groups [7]. Applying method from [5], we show that both groups of all p-automata and of all finite p-automata possess minimal generating sets. Note that the case $p = 2$ is covered in [5]. The key ingredient of our proof for the group of all finite p-automata is a statement about the structure of its image under a natural homomorphism on the additive group of all infinite sequences over the field $\mathbb{Z}_p$.

УДК 512.54
2020 *Mathematics Subject Classification:* 20E08, 20E22.

The work of the second named author was partially supported by the grant 346300 for IMPAN from the Simons Foundation and the matching 2015-2019 Polish MNiSW fund.

The structure of the paper is following. In Section 1, we briefly recall required definitions and properties about groups of automata. For more details we refer to [2, 3, 6]. In Section 2, we construct minimal generating sets in groups of all p-automata and all finite p-automata. In Section 3, we formulate a few open problems arised during our research.

1 Preliminaries

Let X be a finite alphabet, $|\mathsf{X}| \geq 2$. The set

$$\mathsf{X}^* = \bigcup_{n=0}^{\infty} \mathsf{X}^n$$

of all finite words over X including the empty word Λ is a free monoid with basis X under concatenation. The Cayley graph of X^* with respect to X is a regular rooted tree $\mathcal{T}(\mathsf{X})$. For each $n \geq 0$ the set X^n is the nth level of this tree. The automorphism group $Aut\mathcal{T}(\mathsf{X})$ of the tree $\mathcal{T}(\mathsf{X})$ is an infinitely iterated wreath product of symmetric groups $Sym(\mathsf{X})$ on X, i.e.

$$Aut\mathcal{T}(\mathsf{X}) \simeq \wr_{n=1}^{\infty} Sym^{(n)}(\mathsf{X}), \qquad Sym^{(n)}(\mathsf{X}) \simeq Sym(\mathsf{X}), \ \ n \geq 1.$$

In particular, it means that $Aut\mathcal{T}(\mathsf{X})$ is profinite and contain Sylow subgroups.

An automaton $\mathcal{A}$ over X is a triple (Q, λ, μ) such that Q is a set, the set of states of $\mathcal{A}$, $\lambda : Q \times \mathsf{X} \to Q$ is the transition function and $\mu : Q \times \mathsf{X} \to \mathsf{X}$ is the output function of the automaton $\mathcal{A}$. The automaton $\mathcal{A}$ is called finite if the following equalities extend functions λ and μ to the set $Q \times \mathsf{X}^*$:

$$\lambda(q, \Lambda) = q, \quad \lambda(q, xw) = \lambda\big(\lambda(q, x), w\big),$$

$$\mu(q, \Lambda) = \Lambda, \quad \mu(q, xw) = \mu(q, x)\mu\big(\lambda(q, x), w\big),$$

where $q \in Q$, $x \in \mathsf{X}$, $w \in \mathsf{X}^*$. Automata over X gives a convenient way to define automorphisms from $Aut\mathcal{T}(\mathsf{X})$. Specifically, for every state $q \in Q$ the restriction of μ at q defines a mapping on X^*, that we denote by the same symbol q such that $q(w) = \mu(q, w)$, $w \in \mathsf{X}^*$.

A permutation $f : \mathsf{X}^* \to \mathsf{X}^*$ is an automorphism of $\mathcal{T}(\mathsf{X})$ if and only if there exist an automaton over X and its state q such that f coincides with the mapping q defined at this state. We denote the identity automorphism by e.

An automorphism $f \in Aut\mathcal{T}(\mathsf{X})$ is called finite state automorphism if there exist a finite automaton over X and its state q such that f coincides with the mapping q defined at this state. All finite state automorphisms of $\mathcal{T}(\mathsf{X})$ form a countable subgroup $FAut\mathcal{T}(\mathsf{X})$ of $Aut\mathcal{T}(\mathsf{X})$. An automorphism $f \in Aut\mathcal{T}(\mathsf{X})$ is called finitary, if there exists $m \geq 0$ such that f preserve letters in all words on all positions starting from m. It means that f can be defined by an automaton at some its state q such that for arbitrary word w of length m the transition function of this automaton maps q by w to a state that defines e. All finitary automorphisms of $\mathcal{T}(\mathsf{X})$ form a countable subgroup $FinAut\mathcal{T}(\mathsf{X})$ of $FAut\mathcal{T}(\mathsf{X})$.

Let $|\mathsf{X}| = p$ be an odd prime. We will identify X with the field $\mathbb{Z}_p$ of residues modulo p. A Sylow p-subgroup $\mathcal{K}_p$ of the group $Aut\mathcal{T}(\mathsf{X})$ can be characterized as follows. Let us denote by σ the mapping $x \mapsto x + 1$ on $\mathbb{Z}_p$, i.e. the cycle $(0\ 1\ \ldots\ p-1)$. An automaton over X is called p-automaton if for each its state the restriction of the output function at this state as a permutation on the alphabet is a power of σ. Then $\mathcal{K}_p$ consists of automorphisms defined at states of p-automata. Automorphisms defined at states of finite p-automata form a subgroup $\mathcal{FK}_p$ in $\mathcal{K}_p$. We call the group $\mathcal{K}_p$ as the group of p-automata and its subgroup $\mathcal{FK}_p$ as the group of finite p-automata. The subgroup of finitary automorphisms of $\mathcal{FK}_p$ is denoted by $Fin\mathcal{K}_p$.

Elements of $\mathcal{K}_p$ can be defined in terms of tableaux introduced by L. Kaloujnine. A tableau is a sequence

$$\left[\, a_0, a_1\left(x_1\right), \ldots, a_n\left(x_1, \ldots, x_n\right), \ldots\, \right], \tag{1}$$

where $a_0 \in \mathbb{Z}_p, a_n(x_1, \ldots, x_n) : \mathbb{Z}_p^n \to \mathbb{Z}_p, n \geq 1$.

For arbitrary word $w = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{Z}_p^m$, $m \geq 1$, its image under tableau (1) is the word $\left(\alpha_1 + a_0, \alpha_2 + a_1\left(\alpha_1\right), \ldots, \alpha_n + a_{m-1}\left(\alpha_1, \ldots, \alpha_{m-1}\right)\right)$. The residue of tableau (1) defined by the word w is the tableau

$$\left[\, a_m\left(\alpha_1, \ldots, \alpha_m\right), a_{m+1}\left(\alpha_1, \ldots, \alpha_m, x_1\right), \ldots, a_{m+n}\left(\alpha_1, \ldots, \alpha_m, x_1, \ldots, x_n\right), \ldots\, \right].$$

Tableau (1) defines an element from $\mathcal{FK}_p$ if and only if the set of all its residues is finite.

2 Minimal generating sets

The main result of the paper is the following assertion.

Theorem 1. *Groups $\mathcal{K}_p$ and $\mathcal{FK}_p$ contain minimal generating sets.*

Let $\mathbb{Z}_p^\infty$ be the vector space of all sequences over $\mathbb{Z}_p$. A sequence $(a_n, n \geq 0)$ is called ultimately periodic if there exist $k, l \geq 1$ such that $a_{n+l} = a_n$, $n \geq k$.

A sequence $(a_n, n \geq 0)$ is called finitary if there exists $k \geq 0$ such that $a_n = 0$, $n \geq k$.

Denote by $Fin\mathbb{Z}_p^\infty$ and $UP\mathbb{Z}_p^\infty$ the sets of all finitary and ultimately periodic sequences over $\mathbb{Z}_p$, respectively. Then $Fin\mathbb{Z}_p^\infty$ and $UP\mathbb{Z}_p^\infty$ are countable subspaces of $\mathbb{Z}_p^\infty$.

Consider the mapping $\pi : \mathcal{K}_p \to \mathbb{Z}_p^\infty$ such that for arbitrary $g \in \mathcal{K}_p$ defined by tableau (1) the image $\pi(g)$ has the form

$$\left(a_0, \sum_{\alpha_1 \in \mathbb{Z}_p} a_1(\alpha_1), \ldots, \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n} a_n(\alpha_1, \ldots, \alpha_n), \ldots \right).$$

Lemma 1 ([2]). *The mapping π is a surjective homomorphism. The kernel H of π coincides with the commutator subgroup $\left[\mathcal{K}_p, \mathcal{K}_p\right]$.*

Denote by π_1 the restriction of π on the subgroup $\mathcal{FK}_p$.

Lemma 2. *The homomorphism π_1 is a surjection on $UP\mathbb{Z}_p^\infty$. The kernel H_1 of π_1 contains the commutator subgroup $\left[\mathcal{FK}_p, \mathcal{FK}_p\right]$.*

Proof. Let $g \in \mathcal{FK}_p$. Assume that g is defined by tableau (1). Denote by $Q(g)$ the set of residues of g, including g. Let n be the cardinality of $Q(g)$, i.e. $Q(g) = \{g_1, \ldots, g_n\}$. We will show that all sequences $\pi_1(g_1), \ldots, \pi_1(g_n)$ are ultimately periodic.

Assume that g_i is defined by the tableau

$$[\, a_{i_0}, a_{i1}(x_1), \ldots, a_{in}(x_1, \ldots, x_n), \ldots], \quad i \geq n.$$

Denote by t_{ij} the number of states of g_i, defined by words of length 1, that equal to g_j, $1 \leq i, j \leq n$. Then $T = (t_{ij})_{i,j} = n$ is an $n \times n$ integer matrix. We will consider T as a matrix over $\mathbb{Z}_p$.

Let $\pi_1(g_i) = (b_{i0}, b_{i1}, \ldots, b_{in}, \ldots)$, $1 \leq i \leq n$. We will show by induction on m that

$$(b_{1m}, \ldots, b_{nm})^\top = T^m \cdot (a_{1m}, \ldots, a_{nm})^\top. \tag{2}$$

Since $(b_{10}, \ldots, b_{n0})^\top = (a_{10}, \ldots, a_{n0})^\top$, equality (2) holds for the case $m = 0$. For arbitrary i, $1 \leq i \leq n$, $m > 0$, definitions of π and T imply $b_{1m} = t_{i1}b_{1m-1} + \cdots + t_{in}b_{nm-1}$. Under inductive assumption for $m-1$ it implies the the required equality for m.

Since the matrix T is a matrix over a finite field the sequence $(T^m, m \geq 0)$ is ultimately periodic. Then equality (2) implies that all sequences $\pi_1(g_i)$, $1 \leq i \leq n$, are ultimately periodic as well.

On the other hand, for arbitrary sequence $(b_n, n \geq 0) \in UP\mathbb{Z}_p^\infty$, let us consider the tableau

$$[\,a_0, a_1(x_1), \ldots, a_n(x_1, \ldots, x_n), \ldots]$$

such that $a_0 = b_0$ and

$$a_n(x_1, \ldots, x_n) = \begin{cases} b_n, & \text{if } x_1 = \ldots = x_n, \\ 0, & \text{otherwise.} \end{cases}$$

Then this tableau defines a finite state automorphism g such that $\pi_1(g) = (b_n, n \geq 0)$. Hence, π_1 is a surjection on $UP\mathbb{Z}_p^\infty$.

The second statement of the lemma follows from Lemma 1. The proof is complete. □

Now we proceed with defining minimal generating sets of $\mathcal{K}_p$ and $\mathcal{FK}_p$. The construction is based on the approach presented in [5]. Consider the group $\mathcal{K}_p$.

Since every vector space contains a Hamel basis (see, e.g., [4]) all three spaces $\mathbb{Z}_p^\infty$, $Fin\mathbb{Z}_p^\infty$ and $UP\mathbb{Z}_p^\infty$ contain a basis. In particular, each basis is a minimal generating set of the additive group of the corresponding space.

Let I be a set of contunuum cardinality. Since the homomorphism π is surjective there exists a subset $\{s_{1i} : i \in I\} \in \mathcal{K}_p$ such that the set $\{\pi(s_{1i}) : i \in I\}$ is a basis of $\mathbb{Z}_p^\infty$. On the other hand, the commutator subgroup $[\mathcal{K}_p, \mathcal{K}_p]$ has continuum cardinality and we can use I to index its elements. Hence, $[\mathcal{K}_p, \mathcal{K}_p] = \{s_{2i} : i \in I\}$. Now for each $i \in I$ define $s_i \in \mathcal{K}_p$ such that s_i preserves the first two letters of each word w and for arbitrary $\alpha_1, \alpha_2 \in \mathbb{Z}_p$ its residue $s_i(\alpha_1, \alpha_2)$ on (α_1, α_2) satisfy the following condition

$$s_i(\alpha_1, \alpha_2) = \begin{cases} s_{1i}, & \text{if } \alpha_1 = \alpha_2 = 0, \\ s_{2i}, & \text{if } \alpha_1 = \alpha_2 = p-1, \\ e, & \text{otherwise.} \end{cases}$$

Let $\{g_i, i \geq 0\}$ be the set of finitary automorphisms such that g_0 is defined by the tableau $[\,1, 0, 0, \ldots, 0, \ldots]$ and for arbitrary $i \geq 1$ the automorphism g_i is defined by the tableau

$$[\,0, \ldots, 0, a_i(x_1, \ldots, x_i), 0, \ldots],$$

where

$$a_i(x_1, \ldots, x_i) = \begin{cases} 1, & \text{if } x_1 = \ldots = x_i = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Let $S = \{g_0, g_1\} \cup \{s_i : i \in I\}$.

Now proceed with the group $\mathcal{FK}_p$. Define the sequences

$$e_i = (e_{i0}, \ldots, e_{ij}, \ldots), \quad i \geq 0,$$

such that

$$e_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j, \end{cases} \quad i, j \geq 0.$$

Then we directly obtain the following assertion.

Lemma 3.

(i) The set $\{e_i : i \geq 0\}$ is a basis of the space $Fin\mathbb{Z}_p^\infty$.

(ii) There exists a countable set $\{f_i : i \geq 1\}$ of ultimately periodic sequences such that the union $\{e_i : i \geq 0\} \cup \{f_i : i \geq 1\}$ forms a basis of the space $UP\mathbb{Z}_p^\infty$.

Proof. The first statement is well-known and its proof is straightforward. Since the space $UP\mathbb{Z}_p^\infty$ is countable and contains periodic sequences of arbitrary least period the second statement follows. □

Lemma 4. *For each $i \geq 0$ the automorphism g_i has order p and $\pi_1(g_i) = e_i$.*

Proof. For each $i \geq 0$ the automorphism g_i defines a cyclic permutation of length p on the words of the form

$$(\underbrace{0, \ldots, 0}_{i}, \alpha_1, \ldots, \alpha_m), \quad m \geq 1,$$

and acts trivially on all other words. Hence, the order of g_i is p. The equality $\pi_1(g_i) = e_i$ immediately follows from the definitions of π_1 and g_i. □

Since the kernel of π_1, namely the subgroup H_1, is countable, we can enumerate its elements and obtain $H_1 = \{h_i : i \geq 0\}$.

Lemma 3 allows to choose a subset $\{t_i : i \geq 1\}$ of $\mathcal{FK}_p$ such that $\pi_1(t_i) = f_i$, $i \geq 1$.

Then define finite state automorphisms $r_{1i}, i \geq 0$, and $r_{2i}, i \geq 1$, such that they preserve the first two letters of each word w and for arbitrary $\alpha_1, \alpha_2 \in \mathbb{Z}_p$ their residues $s_{1i}(\alpha_1, \alpha_2), i \geq 0$, and $s_{2i}(\alpha_1, \alpha_2), i \geq 1$, on (α_1, α_2) satisfy the following conditions

$$s_{1i}(\alpha_1, \alpha_2) = \begin{cases} g_i, & \text{if } \alpha_1 = \alpha_2 = 0, \\ h_i, & \text{if } \alpha_1 = \alpha_2 = p - 1, \\ e, & \text{otherwise}, \end{cases} \quad i \geq 0,$$

and

$$s_{2i}(\alpha_1, \alpha_2) = \begin{cases} t_i, & \text{if } \alpha_1 = \alpha_2 = 0, \\ e, & \text{otherwise}, \end{cases} \quad i \geq 1,$$

respectively.

Let $R = \{g_0, g_1\} \cup \{r_{1i} : i \geq 0\} \cup \{r_{2i} : i \geq 1\}$.

Proof of Theorem 1. The sets S and R constructed above are minimal generating sets of the groups $\mathcal{K}_p$ and $\mathcal{FK}_p$, respectively. The proof uses lemmata proved above and it is solely the same as the proof of [5, Theorem 2] and we omit it. □

3 Open problems

Problem 1. Is it true that the kernel of the homomorphism π_1 coincides with the commutator subgroup $[\mathcal{FK}_p, \mathcal{FK}_p]$?

Problem 2. Is there an algorithm for effective enumeration of finite state automorphisms from the kernel of the homomorphism π_1?

References

[1] Chakan B., Gecheg F. *On a group of automatic permutations*. Cybernet. Systems Anal. 1965, **1**, 13–15. doi: 10.1007/BF01071419

[2] Grigorchuk R., Leonov Y., Nekrashevych V., Sushchansky V. *Self-similar groups, automatic sequences, and unitriangular representations*. Bull. Math. Sci. 2016, **6** (2), 231–285. doi:10.1007/s13373-015-0077-7

[3] Grigorchuk R., Nekrashevych V., Sushchansky V. *Automata, dynamical systems, and groups*. Proc. Steklov Inst. Math. 2000, **231**, 134–214.

[4] Heil C. A basis theory primer. In: Benedetto J., Czaja W., Okoudjou K. (Eds.) Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, 2011.

[5] Lavrenyuk Y. *The group of all finite-state automorphisms of a regular rooted tree has a minimal generating set*. Geom. Dedicata 2016, **183**, 59–67. doi:10.1007/s10711-016-0145-5

[6] Oliynyk A. *Finite state wreath powers of transformation semigroups*. Semigroup Forum 2016, **82** (3), 423–436. doi: 10.1007/s00233-011-9292-z

[7] Oliynyk A., Krenevych A. *Free groups defined by finite p-automata*. Researches Math. 2023, **31** (2), 49–55. doi: 10.15421/242314

[8] Oliynyk A., Prokhorchuk V. *On exponentiation, p-automata and HNN extensions of free abelian groups*. Algebra Discrete Math. 2023, **35** (2), 180–190. doi:10.12958/adm2132

[9] Prokhorchuk V. *Generation of amalgamated free products of cyclic groups by finite automata over minimal alphabet*. Theoret. Comput. Sci. 2021, **856**, 151–164. doi:10.1016/j.tcs.2020.12.036

[10] Prokhorchuk V. *On finite state automaton actions of HNN extensions of free abelian groups*. Carpathian Math. Publ. 2021, **13** (1), 180–188. doi:10.15330/cmp.13.1.180-188

Received 03.09.2023

Лавренюк Я.В., Олійник А.С. *Мінімальні системи твірних у групах p-автоматів* // Карпатські матем. публ. — 2023. — Т.15, №2. — С. 608–613.

Для довільного непарного простого числа p розглядаються групи всіх p-автоматів та всіх скінченних p-автоматів. Будуються мінімальні системи твірних як у групі всіх p-автоматів, так і в її підгрупі скінченних p-автоматів. Ключовим елементом доведення є техніка підняття, яка дозволяє конструювати мінімальну систему твірних у групі за умови, що мінімальну систему твірних задано у її абелевій факторгрупі. Для знаходження відповідної факторгрупи елементи груп p-автоматів та скінченних p-автоматів подаються у термінах таблиць, введених Л. Калужніним. З використанням цього подання визначається та досліджується природний гомоморфізм на адитивну групу всіх нескінченних послідовностей над полем $\mathbb{Z}_p$.

Ключові слова і фрази: скінченний автомат, p-автомат, мінімальна система твірних.