Res. Math. **31**(2), 2023, p. 49–55
doi:10.15421/242314

ISSN (Print) 2664-4991
ISSN (Online) 2664-5009

UDK 512.54

A. P. Krenevych*, **A. S. Oliynyk****

* Taras Shevchenko National University of Kyiv, Volodymyrska 60, 01601 Kyiv, Ukraine. *E-mail: krenevych@knu.ua*

** Taras Shevchenko National University of Kyiv, Volodymyrska 60, 01601 Kyiv, Ukraine. *E-mail: aolijnyk@gmail.com*

Free groups defined by finite p-automata

Abstract. For every odd prime p we construct two p-automata with 14 inner states and prove that the group genertaed by 2 automaton permutations defined at their states is a free group of rank 2.
Key words: finite automaton, p-automaton, free group

Анотація. Для кожного непарного простого p ми будуємо два p-автомати з 14 внутрішніми станами та доводимо, що група, породжена 2 автоматними перестановками, визначеними в їхніх станах, є вільною групою рангу 2.
Ключові слова: скінченний автомат, p-автомат, вільна група

MSC2020: Pri 20E08 Sec 20E22, 20E26

1. Introduction

Explicit constructions of finite automata that define free non-abelian groups is an interesting topic in modern geometric group theory. This direction was initiated in [1] where brilliant constructions of automata were presented but the complete proof was found later in [11]. Among others, original examples of automata that define free groups appeared in [3, 6, 12, 10, 2, 9] and other papers.

In this note for an odd prime p we consider finite p-automata, i.e. finite automata over an alphabet of cardinality p such that at every their state a power of a fixed cycle of length p on the alphabet is defined. We present two p-automata both with 14 inner states such that the group generated by permutation defined at 2 their states is a free group of rank 2.

The paper is organized as follows. In Section 2 we briefly recall preliminary definitions on finite automata and automaton permutation. For details one can refer to [4] and [7, 8]. In Section 3 we present the main result and in Section 4 we mention its generalization and computations with a presented construction executed with developed Python scripts.

2. Finite automata and groups defined by automata

Let X be a finite set, called alphabet, $|X| \geq 2$. 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 set X^+ of all non-empty words over X is a free subsemigroup of X^*. The length of a word $w \in \mathsf{X}^*$ will be denoted by $|w|$.

A finite automaton $\mathcal{A}$ over X is a triple (Q, λ, μ) such that Q is a finite set, the set of states, $\lambda : Q \times \mathsf{X} \to Q$ is the transition function and $\mu : Q \times \mathsf{X} \to \mathsf{X}$ is the output function of the automaton $\mathcal{A}$.

Functions λ and μ admit recursive extensions to the set $Q \times \mathsf{X}^*$, defined by the rules

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

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

where $q \in Q$, $x \in \mathsf{X}$, $w \in \mathsf{X}^*$. 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

$$q(w) = \mu(q, w), \quad w \in \mathsf{X}^*.$$

A permutation $f : \mathsf{X}^* \to \mathsf{X}^*$ is called finite automaton permutation over X 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 automaton permutations over X form a countable residually finite group under superposition denoted by $FGA(\mathsf{X})$. A finite automaton is called permutational if at every its state the output function defines a permutation on the alphabet. Each finite automaton permutation $g \in FGA(\mathsf{X})$ is defined by some finite permutational automaton $\mathcal{A}$ at some state q.

Let (G, X) be a permutation group. A finite automaton over X is called G-automaton if at every its state the output function defines a permutation from G. All finite automaton permutations defined by G-automata form a subgroup of $FGA(\mathsf{X})$ called finite state wreath power of (G, X). If (G, X) is a regular cyclic group of order p for a prime p then G-automaton is called p-automaton.

3. Constructions of free groups

Let p be an odd prime. Consider the alphabet $\mathsf{X} = \{0, 1, \ldots, p-1\}$. The elements of X will be treated as digits in positional numeral system with base p. It allows for to define a surjective mapping

$$\pi : \mathsf{X}^+ \to \mathbb{N} \cup \{0\}$$

by the rule

$$\pi(x_0 \dots x_m) = \sum_{i=0}^{m} x_i p^i, \quad x_0, \dots, x_m \in \mathsf{X}, m \geq 0.$$

For arbitrary $m \geq 1$ the restriction of π on the set X^m defines a one-to-one correspondence between X^m and the set of integers $\{0, 1, \dots, p^m - 1\}$. Note, that for each integer k from this set the corresponding word over X is a representation of the number k in a positional numeral system with base p where the rightmost symbol is the most significant digit.

Denote by σ the cycle $(p-1 \dots 10)$ of length p on X. Then

$$\sigma(x) = (x-1) \bmod p, \quad x \in \mathsf{X}.$$

Define automata $\mathcal{A} = (Q_a, \psi_a, \lambda_a)$ and $\mathcal{B} = (Q_b, \psi_b, \lambda_b)$ over X. Both sets of states Q_a and Q_b contain 14 elements, i.e.

$$Q_a = \{a_1, \dots, a_{14}\}, \quad Q_b = \{b_1, \dots, b_{14}\}.$$

Transition functions ψ_a and ψ_b are defined by Table 1 and Table 2 correspondingly.

ψ_a	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}
0	a_2	a_4	a_1	a_5	a_4	a_8	a_1	a_9	a_4	a_1	a_1	a_{13}	a_{12}	a_1
1	a_3	a_{12}	a_1	a_7	a_{12}	a_8	a_1	a_{10}	a_{12}	a_1	a_1	a_{13}	a_{12}	a_1
x	a_3	a_{12}	a_1	a_6	a_{12}	a_8	a_1	a_{11}	a_{12}	a_1	a_1	a_{14}	a_{12}	a_1

Tab. 1. Transition function of automaton $\mathcal{A}$, $x \in \mathsf{X}$, $x \neq 0, 1$

ψ_b	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}
0	b_3	b_4	b_1	b_7	b_4	b_8	b_1	b_{10}	b_4	b_1	b_1	b_{13}	b_{12}	b_1
1	b_2	b_{12}	b_1	b_5	b_{12}	b_8	b_1	b_9	b_{12}	b_1	b_1	b_{13}	b_{12}	b_1
x	b_3	b_{12}	b_1	b_6	b_{12}	b_8	b_1	b_{11}	b_{12}	b_1	b_1	b_{14}	b_{12}	b_1

Tab. 2. Transition function ψ_a of automaton $\mathcal{B}_p$, $x \in \mathsf{X}$, $x \neq 0, 1$

Output functions λ_a and λ_b are defined by equalities

$$\lambda_a(x, a_i) = \begin{cases} (x-1) \bmod p, & \text{if } i = 5 \text{ or } i = 10 \\ x & \text{otherwise} \end{cases},$$

$$\lambda_b(x, b_i) = \begin{cases} (x-1) \bmod p, & \text{if } i = 5 \text{ or } i = 10 \\ x & \text{otherwise} \end{cases}.$$

The definition immediately implies that permutations on X defined at states a_5, a_{10} of $\mathcal{A}$ and at states b_5, b_{10} of $\mathcal{B}$ are σ, and trivial at all other states. It means that both automata $\mathcal{A}$ and $\mathcal{B}$ are p-automata.

Lemma 1. *For arbitrary $n \geq 1$, $m \in \mathbb{Z}$ and words $u = x_0 u_{e_0} \dots u_{e_{n-1}} \in \mathsf{X}^{n+1}$ and $v = v_0 v_{e_0} \dots v_{e_{n-1}} \in \mathsf{X}^{n+1}$ such that $v = u^g$ the following equalities hold: $v_0 = x_0$ and*

$$\sum_{k=0}^{n-1} \psi_X(v_{e_k}) 2^k = \left(\sum_{k=0}^{n-1} \psi_X(u_{e_k}) 2^k + m \right) \bmod 2^n.$$

Denote by $G_p(a_1, b_1)$ the group generated by finite automaton permutations defined in states a_1 and b_1 of automata $\mathcal{A}_p$ and $\mathcal{B}_p$ correspondingly.

The main result of the paper is the following

Theorem 1. *The group $G_p(a_1, b_1)$ is a free group of rank 2.*

In order to prove this theorem we need some additional statements.

Lemma 2. *Let $u, v, w \in \mathsf{X}^2$, $u \neq 00$, $v \neq 10$. Then*

$$u^{a_1} = u, \quad v^{b_1} = v, \quad w^{a_1} = w, \quad w^{b_1} = w.$$

Proof. Directly follows from the definition of automata $\mathcal{A}_p$ and $\mathcal{B}_p$.

Lemma 3. *Let $x_1, \dots, x_m \in \mathsf{X}$, $y_1, \dots, y_m \in \mathsf{X}$, $m \geq 1$, and $k \in \mathbb{Z}$. Assume that*

$$\pi(x_1 \dots x_m) - k = \pi(y_1 \dots y_m) \bmod p.$$

Then the following equalities hold:

$$(000x_1 \dots 0x_m)^{a_1^k} = 000y_1 \dots 0y_m, \tag{3.1}$$

$$(1011x_1 \dots 1x_m)^{a_1^k} = 101y_1 \dots 1y_m. \tag{3.2}$$

Proof. We prove equality (3.1), the proof of equality (3.2) is entirely the same. It is sufficient to consider the case $k = 1$. The general statement then will follow by induction.

Definition of the automaton $\mathcal{A}$ directly implies the equalities

$$(000x_1 \dots 0x_m)^{a_1} = 00(0x_1 0x_2 \dots 0x_m)^{a_4} = 000((x_1 - 1) \bmod p)(0x_2 \dots 0x_m)^{a_i},$$

where

$$i = \begin{cases} 4, & \text{if } x_1 = 0 \\ 12 & \text{otherwise} \end{cases}.$$

Then there are two cases. The first case is $x_1 = \dots = x_m = 0$. In this case

$$(000x_1 \dots 0x_m)^{a_1} = 000((x_1 - 1) \bmod p) \dots 0((x_m - 1) \bmod p)$$

and equality (3.1) holds. In the opposite case let i be the least number such that $x_i \neq 0$, $1 \leq i \leq m$. Then

$$(000x_1 \dots 0x_m)^{a_1} = 000((x_1 - 1) \bmod p) \dots 0((x_i - 1) \bmod p)(0x_{i+1} \dots 0x_m)^{a_{12}}.$$

Since $(0xw)^{a_{12}} = 0xw^{a_{12}}$ for arbitrary $x \in \mathsf{X}$, $w \in \mathsf{X}^*$, equality (3.1) holds as well.

Lemma 4. *Let k be a non-negative integer and $w = x_1 \dots x_m \in \mathsf{X}^*$, $m \geq 1$, be a word such that $\pi(w) = k$. Then for arbitrary $x \in \mathsf{X}$, $x \neq 0, 1$, the following equalities hold:*

$$(000x_1 \dots 0x_m xx11)^{a_1^{k+1}} = 00\,\underbrace{(0p-1)\dots(0p-1)}_{m}\,xx10, \tag{3.3}$$

$$(101x_1 \dots 1x_m xx01)^{b_1^{k+1}} = 10\,\underbrace{(1p-1)\dots(1p-1)}_{m}\,xx00. \tag{3.4}$$

Proof. Since proofs of both equalities are quite similar we prove equality (3.3) only.

Equalities

$$\pi(x_1 \dots x_m) - k = 0 = \pi(\underbrace{0 \dots 0}_{m})$$

and Lemma 3 imply

$$(000x_1 \dots 0x_m xx11)^{a_1^{k}} = 00\,\underbrace{(00)\dots(00)}_{m}(xx11)^{a_{12}^{k}} = 00\,\underbrace{(00)\dots(00)}_{m}\,xx11.$$

Then

$$(000x_1 \dots 0x_m xx11)^{a_1^{k+1}} = (00\,\underbrace{(00)\dots(00)}_{m}\,xx11)^{a_1} =$$

$$(00\,\underbrace{(0p-1)\dots(0p-1)}_{m}\,xx(11)^{a_8} = 00\,\underbrace{(0p-1)\dots(0p-1)}_{m}\,xx10.$$

The proof is complete.

Using similar arguments we obtain

Lemma 5. *Let k be a non-negative integer and $w = x_1 \dots x_m \in \mathsf{X}^*$, $m \geq 1$, be a word such that $\pi(w) = p^m - k$. Then for arbitrary $x \in \mathsf{X}$, $x \neq 0, 1$, the following equalities hold:*

$$(000x_1 \dots 0x_m xx1p-1)^{a_1^{-k-1}} = 0001\,\underbrace{(00)\dots(00)}_{m-1}\,xx10, \tag{3.5}$$

$$(101x_1 \dots 1x_m xx0p-1)^{b_1^{-k-1}} = 1010\,\underbrace{(10)\dots(10)}_{m-1}\,xx00. \tag{3.6}$$

Proof of Theorem 1. We need to show that every reduced word in alphabet $\{a_1, b_1\}$ defines a non-trivial automaton permutation (see [5, Proposition 1.9]). By Lemma 3 both automaton permutations a_1 and b_1 have infinite order. Then up to conjugacy it is sufficient to show that for arbitrary non-zero integers $k_1, k_2, \dots, k_{2r-1}, l_{2r}$, $r \geq 1$, the product

$$g = a_1^{k_1} b_1^{k_2} \dots a_1^{k_{2r-1}} b_1^{k_{2r}},$$

is nontrivial.

For numbers $k_1, k_2, \ldots, k_{2r-1}, l_{2r}$ consider words

$$u_1 = x_{11} \ldots x_{1m_1}, u_2 = x_{21} \ldots y_{2m_2}, \ldots,$$

$$u_{2r-1} = x_{2r-11} \ldots x_{2r-1m_{2r-1}}, u_{2r} = x_{2r1} \ldots x_{2rm_{2r}}$$

such that

$$\pi(u_1) = |k_1|-1, \pi(u_1) = |k_2|-1, \ldots, \pi(u_{2r-1}) = |k_{2r-1}|-1, \pi(u_{2r}) = |k_{2r}|-1.$$

Using these words we construct a word w, such that $w^g \neq g$. Let $x \in \mathsf{X}$, $x \neq 0, 1$, and

$$x_i = \begin{cases} 1, & \text{if } k_i > 0 \\ p-1, & \text{if } k_i < 0 \end{cases}, \quad 1 \leq i \leq 2r.$$

Define words

$$v_1 = 0x_{11} \ldots 0x_{1m1}, \quad v_2 = 1x_{21} \ldots 1x_{2m_2}, \ldots,$$

$$v_{2r-1} = 0x_{2r-11} \ldots 0x_{2r-1m2r-1}, \quad v_{2r} = 1x_{2r1} \ldots 1x_{2rm_{2r}}.$$

Consider the word

$$w = 00v_1xx1x_1v_2xx0x_2 \ldots v_{2r-1}xx1x_{2r-1}v_{2r}xx1x_{2r}.$$

Applying Lemma 4, Lemma 5 and Lemma 2 we obtain by induction

$$w^{a_1^{k_1}} = (00v_1xx)^{a_1^{k_1}}10v_2xx0x_2 \ldots v_{2r-1}xx1x_{2r-1}v_{2r}xx1x_{2r},$$

$$w^{a_1^{k_1}b_1^{k_2}} = (00v_1xx1x_1v_2xx)^{a_1^{k_1}b_1^{k_2}}00 \ldots v_{2r-1}xx1x_{2r-1}v_{2r}xx1x_{2r}, \ldots$$

$$w^{a_1^{k_1}b_1^{k_2}\ldots a_1^{k_{2r-1}}} = (00v_1xx1x_1v_2xx0x_2 \ldots v_{2r-1}xx)^{a_1^{k_1}b_1^{k_2}\ldots a_1^{k_{2r-1}}}10v_{2r}xx1x_{2r},$$

$$w^{a_1^{k_1}b_1^{k_2}\ldots a_1^{k_{2r-1}}b_1^{2r}} =$$

$$(00v_1xx1x_1v_2xx0x_2 \ldots v_{2r-1}xx10v_{2r}xx1x_{2r-1})^{a_1^{k_1}b_1^{k_2}\ldots a_1^{k_{2r-1}}b_1^{2r}}10.$$

Hence $w^g \neq w$. The proof is complete.

4. Generalizations and further computations

The construction of a free group of rank 2 defined by p-automata described in Section 3 can be naturally generalized on the case of a free group of rank r, $r > 2$. However, the number of states of corresponding p-automata grows as r does and the proof becomes overloaded with technical details.

We developed Python scripts in order to provide further computations with finite automaton permutations a_1 and b_1. For a given reduced word g in $\{a_1, b_1\}$ we calculated the least lengths of a word over X not fixed by g. For a given reduced word g in $\{a_1, b_1\}$ and $k \geq 1$ we computed the number of words from X^k not fixed by g.

References

1. *Aleshin S. V.*: A free group of finite automata. Vestnik Moskov. Univ. Ser. I Mat. Mekh. 1983; 4: pp. 12–14.
2. *Bondarenko I., Kivva B.*: Automaton groups and complete square complexes. Groups Geom. Dyn. 2022; 16: pp. 305–332. doi:10.4171/ggd/649
3. *Brunner A.M., Sidki S.*: The generation of $\mathrm{GL}(n, \mathbf{Z})$ by finite state automata. Internat. J. Algebra Comput. 1998; 8: pp. 127–139. doi:10.1142/S0218196798000077
4. *Grigorchuk R.I., Nekrashevych V.V., Sushchanskii V.I.*: Automata, Dynamical Systems, and Groups. Proceedings of the Steklov Institute of Mathematics 2000; 231: pp. 128–203.
5. *Lyndon R.C., Schupp P.E.*: Combinatorial group theory. Springer-Verlag, 1977.
6. *Oliynyk A.*: Free products of finite groups and groups of finitely automatic permutationss. Proceedings of the Steklov Institute of Mathematics 2000; 231: pp. 323–331.
7. *Oliynyk A.*: Finite state wreath powers of transformation semigroups. Semigroup Forum. 2011; 82: pp. 423–436. doi:10.1007/s00233-011-9292-z
8. *Oliynyk A., Prokhorchuk V.*: On exponentiation, p-automata and HNN extensions of free abelian groups. Algebra Discrete Math. 2023; 35: pp. 180–190. doi:10.12958/adm2132
9. *Oliynyk A., Prokhorchuk V.*: On a finite state representation of $GL(n, \mathbb{Z})$. Algebra Discrete Math. 2023; 36: pp. 74–84. doi:10.12958/adm2158
10. *Steinberg B., Vorobets M., Vorobets, Y.*: Automata over a binary alphabet generating free groups of even rank. Internat. J. Algebra Comput. 2011; 21: pp. 329–354. 10.1142/S0218196711006194
11. *Vorobets M., Vorobets, Y.*: On a free group of transformations defined by an automaton. Geom. Dedicata. 2007; 124: pp. 237–249. doi:10.1007/s10711-006-9060-5
12. *Vorobets M., Vorobets, Y.*: On a series of finite automata defining free transformation groups. Groups Geom. Dyn. 2010; 4: pp. 377–405. doi:10.4171/GGD/87

Received: 12.11.2023. *Accepted:* 22.12.2023