УДК 512.54

Є. В. Бондаренко[1], *к.ф.-м.н.*

Групи, породжені обмеженими автоматами без фінітарних станів

Встановлено алгоритмічний критерій скінченності груп, породжених обмеженими автоматами без нетривіальних фінітарних станів.

Ключові слова: автоматна група, обмежений автомат.

[1]Київський національний університет імені Тараса Шевченка, 01033, Київ, вул. Володимирська, 64, e-mail: ibond.univ@gmail.com.

I. V. Bondarenko[1], *PhD*

Groups generated by bounded automata without finitary states

We establish an algorithmic criterium for finiteness of groups generated by bounded automata without non-trivial finitary states.

Key Words: automaton group, bounded automaton.

[1]National Taras Shevchenko University of Kyiv, 01033, Kyiv, vul.Volodymyrska, 64, e-mail: ibond.univ@gmail.com.

Communicated by Prof. V. V. Kirichenko.

Introduction

The fundamental problem of the theory of automaton groups is the connection between the combinatorial structure of an automaton and the algebraic properties of the group it generates. Most of the algorithmic problems for automaton groups are open (and probably undecidable). In particular, it is not known how to check whether a group generated by a finite automaton is finite. One can hope for a positive result dealing with certain classes of automaton groups.

Studying cyclic structure of automata, S. Sidki in [7] introduced several classes of automata, and one of the most important of them are bounded automata. Interestingly, most of the studied automaton groups are generated by bounded automata, in particular, the famous Grigorchuk group. Moreover, bounded automata naturally appear in connection with fractal geometry [1]: An automaton group has post-critically finite limit space if and only if the generating automaton is bounded.

In this paper we study groups generated by bounded automata without non-trivial finitary states. This class happens to be more amenable to investigation and still contains many interesting groups like the Basilica group [4], Hanoi Towers group on three pegs [3], groups studied by P. Neumann [6], iterated monodromy groups of quadratic polynomials with periodic kneading sequence [5], etc. We give an algorithmic method to check when a group generated by a bounded automaton without non-trivial finitary states is finite.

1 Automorphisms of regular rooted trees

Let X be a finite alphabet with at least two letters. Let X^* be the free monoid freely generated by X. The elements of X^* are finite words $x_1x_2\dots x_n$ over X together with the empty word. We consider the set X^* as a rooted $|X|$-ary tree, where the empty word is the root of the tree and every vertex $v\in X^*$ is connected by an edge to vx for each $x\in X$.

Every automorphism $g\in \mathrm{Aut}(X^*)$ induces an automorphism $g|_v\in \mathrm{Aut}(X^*)$ for every $v\in X^*$ by the rule

$$g|_v(x)=y \text{ if } g(vx)=g(v)y \text{ for all } x,y\in X^*.$$

This automorphism is called the *state of g at v*. The states of the product are computed as

$$(g\cdot h)|_v=g|_v\cdot h|_{g(v)}$$

(we are using right actions: $gh(v)=h(g(v))$).

The permutation $\pi_g\in Sym(X)$ induced by g on X and the states of g at the letters $x\in X$ uniquely determine g by the relation

$$g(xv)=\pi_g(x)g|_x(v) \text{ for } x\in X \text{ and } v\in X^*.$$

Therefore one can represent automorphisms in the form: If $X=\{x_1,x_2,\dots,x_d\}$ then

$$g=(g|_{x_1},g|_{x_2},\dots,g|_{x_d})\pi_g,$$

which is the usual representation of elements of the permutational wreath product $\mathrm{Aut}(X^*)\cong$

$\mathrm{Aut}(X^*) \wr Sym(X)$. The multiplication of automorphisms written in this form is performed as follows

$$gh = (g|_{x_1}h|_{\pi_g(x_1)}, \ldots, g|_{x_d}h|_{\pi_g(x_d)})\pi_g\pi_h.$$

An automorphism $g \in \mathrm{Aut}(X^*)$ is called *finite-state* if the set of its states $S(g) = \{g|_v : v \in X^*\}$ is finite. Every finite-state automorphism g can be represented by a finite input-output automaton $A(g)$ over the alphabet X. The state set of $A(g)$ is the set $S(g)$ and there is an arrow $g|_v \to g|_{vx}$ labeled by $x|g(x)$ for every $x \in X$ and $v \in X^*$. Starting at the state g, the automaton $A(g)$ transforms a word $x_1x_2\ldots x_n$ into the word $g(x_1x_2\ldots x_n)$.

2 Bounded automorphisms

For an automorphism $g \in \mathrm{Aut}(X^*)$ define the numerical sequence

$$\theta_k(g) = |\{v \in X^k : g|_v \neq e\}| \quad \text{for } k \in \mathbb{N}.$$

A finite-state automorphism g is called *bounded* if the sequence $\theta_k(g)$ is bounded. The set of all bounded automorphisms forms a subgroup of $\mathrm{Aut}(X^*)$ called the *group of bounded automata*. Groups generated by bounded automata are precisely groups generated by all states of a finite collection of bounded automorphisms.

Bounded automorphisms can be characterized by the cyclic structure of corresponding automata as shown by S.Sidki [7]: A finite-state automorphism g is bounded if and only if any two different cycles in the automaton $A(g)$ are disjoint and not connected by a directed path except for loops at the trivial state (bounded automaton).

This description can be used to describe the structure of bounded automorphisms more precisely as follows. First, we need the notion of a finitary automorphism. An automorphism $g \in \mathrm{Aut}(X^*)$ is called *finitary* if the sequence $\theta_k(g)$ is eventually zero; in other words, there exists $k \in \mathbb{N}$ such that $g|_v = e$ for all $v \in X^k$. A bounded automorphism $g \in \mathrm{Aut}(X^*)$ is *circuit* if there exists a non-empty word $v \in X^*$ such that $g|_v = g$, i.e., g lies on a cycle in $A(g)$. Now, for any bounded automorphism g there exists $n \in \mathbb{N}$ such that for every $v \in X^n$ the state $g|_v$ is either circuit or finitary. Moreover, if g is a circuit automorphism then there exists $m \in \mathbb{N}$ such that $g|_v = g$ for a unique word $v \in X^m$ and $g|_u$ is finitary for every $u \in X^m$, $u \neq v$. Working with a finite collection of bounded automorphisms one can always assume that $n = m = 1$ by passing to a power of the alphabet.

In this paper we study the finiteness of groups generated by bounded automata without non-trivial finitary states. First, we make the following observation that reduces the problem to groups generated by all states of circuit automorphisms.

Lema 1. *Let $S \subset \mathrm{Aut}(X^*)$ be a finite collection of bounded automorphisms and S_c be all circuit states of automorphisms from S. Then the group generated by all states of elements from S is finite if and only the group generated by all states of elements from S_c is finite.*

Proof. Since the set S is finite, there exists $n \in \mathbb{N}$ such that for every $s \in S$ and $v \in X^n$ the state $s|_v$ is a state of an automorphisms from S_c. The statement follows. □

If a circuit automorphism g does not have non-trivial finitary states, then there exist $n \in \mathbb{N}$ and a word $u \in X^n$ such that

$$g|_u = g \quad \text{and} \quad g|_v = e \text{ for all } v \in X^n, v \neq u.$$

Passing to a power of the alphabet $X \leftarrow X^n$, g can be represented in the form

$$g = (e, \ldots, e, g, e, \ldots, e)\pi, \qquad (1)$$

where $\pi = \pi_g \in Sym(X)$ and the tuple on the right has precisely one non-trivial component equal to g.

Automorphisms of the form (1) we call *loop automorphisms*. More precisely, an automorphism $g \in \mathrm{Aut}(X^*)$ is a loop automorphism if there exists a letter $x = x_g \in X$ such that $g|_x = g$ and $g|_y = e$ for all $y \in X$, $y \neq x$. Every loop automorphism g is uniquely determined by the pair (x_g, π_g) using the rule: g acts on X as the permutation π_g and has states $g|_{x_g} = g$ and $g|_y = e$ for $y \in X, y \neq x_g$.

Remark 1. A group generated by all states of a finite collection of circuit automorphisms without non-trivial finitary states is isomorphic to a group generated by a finite collection of loop automorphisms (possibly over larger alphabet). Together with Lemma 1 this reduces the studied finiteness problem to groups generated by loop automorphisms.

The inverse of a loop automorphism is a loop automorphism, but the product of loop automorphisms may be not a loop automorphism, and therefore loop automorphisms do not form a group. Moreover, the product of loop automorphisms may be finitary.

Example 1. Consider the loop automorphisms

$$a = (e, e, e, a, e)(1, 2) \quad b = (e, e, e, e, b)(1, 3).$$

Then the product $abab$ is finitary:

$$abab = (e, e, e, e, e)(1, 3, 2).$$

The following examples demonstrate that many interesting groups are generated by loop automorphisms.

Example 2. The automorphism $a = (e, a)(0, 1)$ over the alphabet $X = \{0, 1\}$ is called the adding machine. The action of a on words over X corresponds to the addition of one in binary number system.

Example 3. The group over $X = \{1, 2, 3, 4\}$ generated by two automorphisms

$$a = (e, e, e, a)(1, 3)(2, 4) \quad b = (e, e, e, b)(3, 4)$$

is isomorphic to the Basilica group [4]. This group was the first example of an amenable but not subexponentially amenable group.

Example 4. The group over $X = \{1, 2, 3\}$ generated by automorphisms

$$a = (a, e, e)(2, 3)$$
$$b = (e, b, e)(1, 3)$$
$$c = (e, e, c)(1, 2)$$

is called the Hanoi Towers group on three pegs. This group models the classical Hanoi Towers game [3].

Example 5. Let $P < Sym(X)$ be a transitive permutation group. For every $x \in X$ and $\pi \in P$ with $\pi(x) = x$ define the loop automorphism associated to the pair (x, π):

$$g_{(x,\pi)} = (e, \dots, e, g_{(x,\pi)}, e, \dots, e)\pi.$$

The group generated by all such $g_{(x,\pi)}$ was studied by P.Neumann in [6] for the case when P is perfect.

3 Finiteness of groups generated by loop automorphisms

The next theorem gives an algorithmic method to check whether a group generated by loop automorphisms is finite.

Theorem 1. *Let $S \subset \mathrm{Aut}(X^*)$ be a finite set of loop automorphisms. The group $\langle S \rangle$ is finite if and only if for every non-empty subset $U \subset S$ the letters $\{x_s : s \in U\}$ do not belong to the same* ***non-trivial*** *orbit of the action of $\langle \pi_s : s \in U \rangle$ on X.*

Proof. The proof goes by induction on $n = |S|$.

In order to show the basis of induction ($n = 1$) we need to prove that a loop automorphism s has finite order if and only if x_s does not belong to a non-trivial orbit of π_s, i.e., $\pi_s(x_s) = x_s$. Indeed, if $\pi_s(x_s) = x_s$ then

$$s^k = (e, \dots, e, s^k, e, \dots, e)\pi_s^k$$

for all $k \in \mathbb{N}$ and the order of s is equal to the order of π_s. For the converse, let $\pi_s(x_s) \neq x_s$ and $k \geqslant 2$ be the length of the orbit of x_s. Then

$$s^k|_{x_s} = s \quad \text{and} \quad s^k(x_s) = x_s,$$

which imply that s has infinite order by standard inductive arguments. The case $n = 1$ is proved.

Suppose the statement holds for every system with $n - 1$ loop automorphisms and we consider a system S with n loop automorphisms. We can assume that every proper subset $U \subset S$ generates a finite subgroup; in particular, $s(x_s) = x_s$ for every $s \in S$. We need to prove that the group $G = \langle S \rangle$ is finite if and only if $\{x_s : s \in S\}$ does not belong to the same non-trivial orbit for $\langle \pi_s : s \in S \rangle$.

If all letters x_s for $s \in S$ belong to the trivial orbit $\{x\}$, then $x = x_s$ and $\pi_s(x) = x$ for all $s \in S$. Then the group G is finite as for the case $n = 1$ above.

Suppose $\{x_s : s \in S\}$ does not belong to the same orbit. Let y be any of x_s, $s \in S$, and let Y be the orbit of y. Then for every $x \in Y$ and $g \in G$ the state $g|_x$ is a product of generators $s \in S$ and their inverses such that $x_s \in Y$. The group generated by such generators is finite by our assumption. By the same reasons, every state $g|_x$ for $x \in X \setminus Y$ belongs to a finite group. Hence the group G is finite. The claim is proved in one direction.

For the converse, assume that $\{x_s : s \in S\}$ belongs to the same non-trivial orbit and let us prove that G is infinite. Fix any letter $x_1 \in \{x_s : s \in S\}$. We will prove that for every generator $s \in S$ there exists $h \in G$ such that

$$h|_{x_1} = s \text{ and } h(x_1) = x_1.$$

This property holds for every generator $s \in S$ such that $x_s = x_1$ (just take $h = s$ and recall our assumption). There exists a letter $x_2 \in \{x_s : s \in S\} \setminus \{x_1\}$ and an element $\pi = \pi_{s_1}^{k_1}\pi_{s_2}^{k_2}\ldots\pi_{s_m}^{k_m}$, $s_i \in S$, such that $\pi(x_1) = x_2$ and $\pi'(x_1) \notin \{x_s : s \in S\}$ for every prefix $\pi' = \pi_{s_1}^{k_1}\pi_{s_2}^{k_2}\ldots\pi_{s_l}^{k_l}$, $l < m$. Construct the element $g = s_1^{k_1}s_2^{k_2}\ldots s_m^{k_m}$ and notice that

$$g|_{x_1} = s_1^{k_1}|_{x_1} s_2^{k_2}|_{s_1^{k_1}(x_1)} \ldots s_m^{k_m}|_{s_1^{k_1}\ldots s_{m-1}^{k_{m-1}}(x_1)} = e.$$

Then for every generator $s \in S$ with $x_s = x_2$ we have

$$(gsg^{-1})|_{x_1} = s|_{x_2} = s \text{ and } (gsg^{-1})(x_1) = x_1.$$

In particular, for every $g \in \langle s : s \in S \text{ and } x_s \in \{x_1, x_2\}\rangle$ there exists $h \in G$ such that $h|_{x_1} = g$ and $h(x_1) = x_1$.

Further, there exists a letter $x_3 \in \{x_s : s \in S\} \setminus \{x_1, x_2\}$ and an element $\pi = \pi_{s_1}^{k_1}\pi_{s_2}^{k_2}\ldots\pi_{s_m}^{k_m}$, $s_i \in S$, such that $\pi(x_1) = x_3$ and $\pi'(x_1) \notin \{x_s : s \in S\} \setminus \{x_2\}$ for every prefix $\pi' = \pi_{s_1}^{k_1}\pi_{s_2}^{k_2}\ldots\pi_{s_l}^{k_l}$, $l < m$. Construct the element $g = s_1^{k_1}s_2^{k_2}\ldots s_m^{k_m}$ and notice that $g|_{x_1}$ is a product of generators s with $x_s = x_2$ and their inverses. Take an element $h \in G$ such that $h|_{x_1} = (g|_{x_1})^{-1}$ and $h(x_1) = x_1$. Then for every generator $s \in S$ with $x_s = x_3$ we have

$$(h^{-1}gsg^{-1}h)|_{x_1} = s|_{x_3} = s \text{ and}$$
$$(h^{-1}gsg^{-1}h)(x_1) = x_1.$$

In the same way we process all letters. As a result, we get that for every $g \in G = \langle S\rangle$ there exists $h \in G$ such that $h|_{x_1} = g$ and $h(x_1) = x_1$. This means that the homomorphism

$$St_G(x_1) \to G, \; g \mapsto g|_{x_1} \qquad (2)$$

is surjective. Since $St_G(x_1)$ is a proper subgroup of G (the orbit of x_1 is non-trivial), the group G is infinite. The statement is proved. □

Remark 2. If for a group G the homomorphism in (2) is surjective, the group is called *self-replicating* or recurrent (one usually assumes transitive action on X). We proved in the theorem that every infinite group generated by loop automorphisms is self-replicating.

Problem 1. Does the class of groups generated by loop automorphisms contain infinite periodic groups?

Problem 2. Does the class of groups generated by loop automorphisms contain groups of intermediate growth?

Problem 3. Is it true that a group generated by loop automorphisms has exponential growth if and only if it contains a free subsemigroup on two generators?

References

1. *Bondarenko I.V., Nekrashevych V.V.* Post-critically finite self-similar groups // Algebra Discrete Math. — 2003. — Vol. 4. — P. 21–32.

2. *Grigorchuk R.I., Nekrashevych V.V., Sushchanskyy V.I.* Automata, dynamical systems, and groups // Proc. Steklov Inst. Math. — 2000. — Vol. 231. — P. 134–214.

3. *Grigorchuk R.I., Šunić Z.* Asymptotic aspects of Schreier graphs and Hanoi Towers groups // C. R., Math., Acad. Sci. Paris — 2006. — Vol. 342. — P. 545–550.

4. *Grigorchuk R.I., Żuk A.* On a torsion-free weakly branch group defined by a three state automaton // Internat. J. Algebra Comput. — 2000. — Vol. 12. — P. 223–246.

5. *Nekrashevych V.* Self-similar groups / Nekrashevych V. — American Mathematical Society: Providence, RI, 2005. — 231 pp. — (Mathematical Surveys and Monographs 117).

6. *Neumann P.M.* Some questions of Edjvet and Pride about infinite groups // Illinois J. Math. — 1986. — Vol. 30. — P. 301–316.

7. *Sidki S.* Automorphisms of one-rooted trees: growth, circuit structure, and acyclicity // J. Math. Sci. (New York) — 2000. — Vol. 100. — P. 1925–1943.

Received: 10.11.2012