Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки
Київ: НПУ імені М. П. Драгоманова. — 2013, № 14.— С. 46–54.

Finite cyclic self-similar groups

D. Vavdiyuk

Taras Shevchenko National University of Kyiv

Анотація. Наведено критерій скінченності для циклічної самоподібної групи автоморфізмів регулярного кореневого дерева. Обчислено число станів твірних елементів для певного класу скінченних самоподібних циклічних груп.

Abstract. A criterion for a cyclic self-similar group of automorphisms of a regular rooted tree to be finite is presented. It is calculated the number of states of generators for some class of finite self-similar cyclic groups.

Introduction

One of the natural problems concerning a residually finite group is to establish whether or not this group admits a faithful self-similar action on some regular rooted tree (e.g. [**1, 2**]). Much more difficult task is to describe all possible faithful self-similar actions of a given group.

We start to consider the last question for cyclic groups. The first result of the present paper gives a criterion for a cyclic self-similar group of automorphisms of a regular rooted tree to be finite (Theorem 1). After that we concentrate on case of finite cyclic self-similar groups. We assume that its generator cyclically permutes vertices connected with the root of the tree and estimates the number of its states. It is shown explicitly that this number varies between 1 and d, where d denotes the number of vertices connected with the root (Theorem 2).

1. Automorphism groups of rooted trees

Let $d \geq 2$ be a natural number. We consider a regular d-ary rooted tree T_d and fix a numeration of vertices, which start in the root. Then any automorphism g of the tree T_d can be uniquely expressed as:

$$g = (g_1, g_2, \ldots, g_d)\pi, \tag{1}$$

where $g_1, g_2, \ldots, g_d$ are some automorphisms of T_d and π is a permutation from the symmetric group S_d. These automorphisms are called *first level states* of the automorphism

E-mail: super_qwertyk@ukr.net

g. The *nth level states* are first level states of $(n-1)$th level states of the automorphism g, $n \geq 2$. The automorphism g itself is the *zero level state* of g. Presentation (1) is called the *wreath recursion* of g.

We can calculate the product of two automorphisms, which are presented as (1). Let $g, h \in AutT_d$, $g = (g_1, g_2, \ldots, g_d)\pi, h = (h_1, h_2, \ldots, h_d)\sigma$. Than their product equals

$$g \cdot h = (g_1, g_2, \ldots, g_d)\pi \cdot (h_1, h_2, \ldots, h_d)\sigma = (g_1 h_{\pi(1)}, \ldots, g_d h_{\pi(d)})\pi\sigma. \quad (2)$$

A subgroup G of the automorphisms group T_d is called *self-similar* if all states of arbitrary automorphism $g \in G$ belong to G ([**3, 4**]). The notation (1) is useful to define recurrently generators of finitely generated self-similar groups. Generators $g_1, \ldots, g_m$ of such a group satisfy the following wreath recursions:

$$\begin{array}{rcl} g_1 & = & (g_{11}, g_{12}, \ldots, g_{1d})\pi_1, \\ g_2 & = & (g_{21}, g_{22}, \ldots, g_{2d})\pi_2, \\ & \ldots & \\ g_m & = & (g_{m1}, g_{m2}, \ldots, g_{md})\pi_m, \end{array} \quad (3)$$

where $\pi_i \in S(X)$ and g_{ij} are words in the alphabet $\{g_1^{\pm 1}, \ldots, g_m^{\pm 1}\}$, $1 \leq i \leq m, 1 \leq j \leq d$.

2. Cyclic self-similar groups

We fix $X = \{1, 2, \ldots, d\}$ and denote the symmetric group on X by S_d. All groups are considered as subgroups of $AutT_d$.

Lemma 1. *Any cyclic self-similar group G can be generated by an element g having the following wreath recursion:*

$$g = (g^{\alpha_1}, g^{\alpha_2}, \ldots, g^{\alpha_d})\pi, \quad (4)$$

where $\alpha_1, \ldots, \alpha_d \in \mathbb{Z}, \pi \in S_d$.

Proof. The only generator g of a cyclic self-similar group G have a form

$$g = (g_1, g_2, \ldots, g_d)\pi,$$

where $g_i = h_1 h_2 \ldots h_{m_i}$ and $h_j = g^{\pm 1}$, $j \in \{1, \ldots, m_i\}$, $m_i \in \mathbb{N}$, $i \in X$. Let $deg(h_j)$ be the degree of h_j, i.e.:

$$deg(h_j) = \begin{cases} -1, \text{ when } h_j = g^{-1}, \\ \ \ 1, \text{ when } h_j = g. \end{cases}$$

Then $g_i = g^{\alpha_i}$, where $\alpha_i = \sum_{j=1}^{m_i} deg(h_j)$ and it satisfies conditions of lemma. □

Let an automorphism $g \in AutT_d$ is defined by (4) and a self-similar group G is generated by g. For arbitrary $i \in X$ we use the following notation:

(1) $O_\pi(i) = \{j \in X | \pi^n(i) = j, n \in \mathbb{N}\}$ (the orbit of i in π).

(2) $S(i) = \sum\limits_{s=1}^{|O_\pi(i)|} \alpha_{\pi^{s-1}(i)}$.

Proposition 1. *Let the permutation π is presented as a product of independent cycles $\pi = \pi_1\pi_2\ldots\pi_k$. Let $l(\pi_j)$ be the length of cycle π_j, where $j = 1, \ldots, k$. Then $l(\pi_j) = |O_\pi(i)|$, where $i = 1, \ldots, d$ and $\pi_j(i) \neq i$.*

Proof. Since $\pi = \pi_1\pi_2\ldots\pi_k$ is the product of independent cycles $O_\pi(i) = O_{\pi_j}(i)$ for $i = 1, \ldots, d$ and $\pi_j(i) \neq i$. It means that $\pi_s(i) = i$, for all $s = 1, \ldots, k$, $s \neq j$. Then

$$O_{\pi_j}(i) = \{\pi_j(i), \pi_j^2(i), \ldots\} = \{1, \pi_j(i), \ldots\ \pi_j^{l(\pi_j)-1}(i)\}.$$

Since $\pi_j^r \neq \pi_j^s$ if $r \neq s$, where $r, s \in \{1, \ldots, l(\pi_j) - 1\}$ then $|O_{\pi_j}(i)| = l(\pi_j)$. It means that $|O_\pi(i)| = l(\pi_j)$. □

Theorem 1. *A self-similar cyclic group G generated by an element g of the form (4) is finite if and only if $S(i)$ is divisible by $|O_\pi(i)|$ for all $i \in X$. In this case $|G| = n$, where n is the order of the permutation π.*

Proof. *Let $S(i)$ be divisible by $|O_\pi(i)|$ for all $i \in X$.*

The following equality is valid:

$$g^{|O_\pi(i)|}|_i = g^{S(i)}.$$

The order n of π is calculated as $n = lcm(|O_\pi(1)|, \ldots, |O_\pi(d)|)$, where the notation $lcm(\cdot, \ldots, \cdot)$ is used for the least common multiple. Since first level states of $g^{|O_\pi(i)|}|_i$ will be multiplied by g^{α_i} Proposition 1 implies that n is divisible by every $|O_\pi(i)|$, where $i = 1, \ldots, d$. Hence

$$g^n|_i = g^{\frac{n}{|O_\pi(i)|}S(i)} = (g^n)^{\frac{S(i)}{|O_\pi(i)|}}.$$

Then $g^n = \left((g^n)^{\frac{S(1)}{|O_\pi(1)|}}, \ldots, (g^n)^{\frac{S(d)}{|O_\pi(d)|}}\right) = 1$. Since the order of π is n the order of g is n too.

Let there exists $i = 1, \ldots, d$ such that $S(i)$ is not divisible by $|O_\pi(i)|$.

In this case we need to prove that the order of g is infinite. More precisely, we show that $g^k \neq 1$ for all $k \in \mathbb{N}$. Let $k = n^m q$, where $m \in \mathbb{N} \cup \{0\}$, $q \in \mathbb{N}$ and q is not divisible by n. We prove the statement by induction on m.

Basis of induction: $m = 0, k = n^0 q = q$.

$$g^k = g^q = (g^q|_1, \ldots, g^q|_d)\pi^q \neq 1, \text{ because of } \pi^q \neq 1.$$

We suppose that: $g^k = g^{n^m q} \neq 1$.

Inductive step:

$$g^k = g^{n^{m+1}q} = (g^n)^{n^m q} = (g^k|_1, \ldots, g^k|_d),$$

where

$$g^k|_i = g^{\frac{qS(i)}{|O_\pi(i)|}n^{m+1}}.$$

Let s be the maximum number such that $qS(i)^s$ is divisible by $|O_\pi(i)|^s$. The number satisfying this condition exists. In opposite case $q = 0$ and further q is divisible by n, which contradicts with the initial condition. We have the following

$$g^k|_{\underbrace{i\dots i}_{s+1}} = g^{\frac{qS(i)}{|O_\pi(i)|}n^{m+1}}|_{\underbrace{i\dots i}_{s}} = \dots = g^{\frac{qS(i)^s}{|O_\pi(i)|^s}n^{m+1}}|_i = g^{S(i)\frac{qS(i)^s}{|O_\pi(i)|^s}\frac{n}{|O_\pi(i)|}n^m} \neq 1.$$

Hence $g^k = g^{n^{m+1}q} \neq 1$. □

3. Finite cyclic self-similar groups

Let G be a cyclic self-similar group and g its generator defined by (4). Consider the case $\pi = (1, 2, \dots, d)$. Suppose that g satisfies conditions of Theorem 1, i.e. the group G is a cyclic group of order g. In the following propositions we prove that varying the initial definition of g one can achieve all possible numbers of states of g. The following notations will be used:

(1) Q for the set of all states of g;
(2) Q_i for sets of first level states of g^i, $i = 0, \dots, d-1$.

Proposition 2. *(1) If $g = (g, \dots, g)\pi$ then g has one state;*
(2) If

$$g = (1, \dots, 1)\pi, \text{ or}$$
$$g = (g^{-1}, \dots, g^{-1})\pi$$

then g has two states.

Proof. It is directly verified that:

(1) $Q = \{g\}$ and $|Q| = 1$;
(2) if $g = (1, \dots, 1)\pi$, then $Q = \{1, g\}$ and $|Q| = 2$,
if $g = (g^{-1}, \dots, g^{-1})\pi$, then $Q = \{g^{\pm 1}\}$ and $|Q| = 2$.

□

Proposition 3. *Let k be a positive integer such that $1 \leq k \leq \left[\frac{d+1}{2}\right]$. If*

$$g = (g^{k-1}, \underbrace{g^{-1}, \dots, g^{-1}}_{k-1}, \underbrace{1, \dots, 1}_{d-k})\pi$$

then g has $2k-1$ states.

Proof. Let $M = \{g^{-k+1}, \dots, g^{k-1}\}$. Direct calculations show that

$$g^{k-1} = (g, g^{-k+1}, \dots, g^{-1}, 1, \dots, 1, g, \dots, g^{k-1})\pi^{k-1}.$$

Hence $M \subseteq Q$.

On the contrary, for any r, $0 < r < d$:

$$g^r|_1 = \begin{cases} g^{k-r}, \text{ if } r < k, \\ 1, \text{ if } r \geq k. \end{cases}$$

For all $i = 2, \dots, k$:

$$g^r|_i = \begin{cases} g^{-k-1+i}, \text{ if } k+1-i < r < d+1-i, \\ g^{-r}, \text{ otherwise}. \end{cases}$$

For all $i = k+1, \dots, d$:

$$g^r|_i = \begin{cases} g^{k-r-i}, \text{ if } d+1-i \leq r \leq k+d-i, \\ 1, \text{ otherwise}. \end{cases}$$

These presentations of automorphisms show that for all $i = 1, \dots, d$ and $0 \leq r < d$, $g^r|_i \in M$. The last inclusion means that $Q \subseteq M$.

Hence $Q = M$ and $|Q| = 2k+1$. □

Proposition 4. *Let k be a positive integer such that $2 \leq k \leq \left[\frac{d-1}{2}\right]$. If*

$$g = (g^{-k}, \underbrace{g, \dots, g}_{k-2}, g^2, \underbrace{1, \dots, 1}_{d-k})\pi$$

then g has $2k$ states.

Proof. Let $M = \{1, g, g^{\pm 2}, \dots, g^{\pm k}, \}$.

Let $2 \leq r \leq k-2$:

$$g^r = (g^{-k+r-1}, \underbrace{g^r, \dots, g^r}_{k-r-1}, \underbrace{g^{r+1}, \dots, g^2}_{r}, \underbrace{1, \dots, 1}_{d-k-r+1}, \underbrace{g^{-k}, \dots, g^{-k+r-2}}_{r-1})\pi^r,$$

$$g^{k-1} = (g^{-2}, \underbrace{g^k, \dots, g^2}_{k-1}, \underbrace{1, \dots, 1}_{d-2k+2}, \underbrace{g^{-k}, \dots, g^{-3}}_{k-2})\pi^{k-1},$$

$$g^k = (1, \underbrace{g^k, \dots, g^2}_{k-1}, \underbrace{1, \dots, 1}_{d-2k+1}, \underbrace{g^{-k}, \dots, g^{-2}}_{k-1})\pi^k.$$

Then $Q_0 = \{1\} \subset M$.

$Q_1 = \{1\} \cup \{g, g^2\} \cup \{g^{-k}\} \subset M$.

$Q_r = \{1\} \cup \{g^2, \dots, g^{r+1}\} \cup \{g^{-k}, \dots, g^{-k+r-1}\} \subset M$.

$Q_{k-1} = Q_k = \{1\} \cup \{g^2, \dots, g^k\} \cup \{g^{-k}, \dots, g^{-2}\} \subset M$.

Therefore $Q_r \subset M$ for all $-k \leq r \leq -2$ because of

$$Q_{-i} = \{g^{-s} | g^s \in Q_i\}.$$

Furthermore,

$$\bigcup_{i=0}^{k} Q_i \cup \bigcup_{j=-k}^{-2} Q_j = M.$$

Then $Q = M$ and $|Q| = 2k$. □

Proposition 5. *Assume that d is odd, i.e. $d = 2d' + 1$ for some $d' \geq 1$. Let k be a positive integer such that $2 \leq k \leq d'$. If*

$$g = (\underbrace{1, \ldots, 1}_{d'-k+1}, g^{d'-k+2}, \underbrace{g, \ldots, g}_{2k-3}, g^{d'-k+2}, \underbrace{1, \ldots, 1}_{d'-k+1})\pi$$

then g has $2k$ states.

Proof. Let $M = \{1, g, g^{d'-k+2}, g^{d'-k+3}, \ldots, g^{d'+k-1}\}$.
In this case $Q_0 = \{1\}, Q_1 = \{1, g, g^{d'-k+2}\}$.
It is directly verified that $g^i|_2 = g^{i+1}$ for all $i = d' - k + 2, \ldots, d' + k - 2$.
Hence $M \subseteq Q$.

We need to prove that $Q \subseteq M$. More precisely, we need to show that $g^r|_i \in M$ for all $g^r \in M$ and $i = 1, \ldots, d$. Suppose that this statement does not hold. Then there exist $g^r \in M$ and $i = 1, \ldots, d$ such that $g^r|_i = g^s \notin M$. Then $r \neq 0$ for $Q_0 \subset M$. Also $r \neq 1$ for $Q_1 \subset M$. Then $d' - k + 2 \leq r \leq d' + k - 1$. As $g^s \notin M$ then $1 < s < d' - k + 2$ or $d' + k - 1 < s < d$. We have

$$g^s = g^r|_i = g|_i \cdot g|_{\pi(i)} \cdot g|_{\pi^2(i)} \cdot \ldots \cdot g|_{\pi^{r-1}(i)}.$$

1) If $g|_i = 1$ then $g|_{\pi(i)} = 1$ or $g|_{\pi(i)} = g^{d'-k+2}$.
2) If $g|_i = g$ then $g|_{\pi(i)} = g$ or $g|_{\pi(i)} = g^{d'-k+2}$.
3) If $g|_i = g^{d'-k+2}$ then $g|_{\pi^j(i)} = 1$, for all $j = 1, \ldots, 2d' - 2k + 2$ or $g|_{\pi^j(i)} = g$, for all $j = 1, \ldots, 2k - 3$.

We can apply these properties to g^s. Let $l = d' - k + 2$ then $l \leq r \leq l + 2k - 3$.
1) If $g|_i = 1$ then we have the following cases:

1.1) $s = \underbrace{0 + \ldots + 0}_{r} = 0$. In this case $s = 0$.

1.2) $s = \underbrace{0 + \ldots + 0}_{r-1} + l = l$. In this case $s = l$.

1.3) $s = \underbrace{0 + \ldots + 0}_{r-r_1-1} + l + \underbrace{1 + \ldots + 1}_{r_1}$,
where $1 \leq r_1 \leq 2k - 3$. In this case $l + 1 \leq s \leq l + 2k - 3$.

1.4) $s = \underbrace{0 + \ldots + 0}_{r-2k+1} + l + \underbrace{1 + \ldots + 1}_{2k-3} + l = 0$. In this case $s = 0$.

1.5) $s = \underbrace{0 + \ldots + 0}_{r_1} + l + \underbrace{1 + \ldots + 1}_{2k-3} + l + \underbrace{0 + \ldots + 0}_{r_2} = 0$,
where $r_1, r_2 \geq 1$ and $r_1 + r_2 = r - 2k + 1$. In this case $s = 0$.

2) If $g|_i = g$ then we have the following cases:

2.1) $s = \underbrace{1 + \ldots + 1}_{r}$. In this case $l \leq s \leq 2k - 3$.

2.2) $s = \underbrace{1 + \ldots + 1}_{r-1} + l$. In this case $2l - 1 \leq s \leq l + 2k - 3$.

2.3) $s = 1 + \ldots + 1 + l + 0 + \ldots + 0$. Same as 1.3).

2.4) $s = \underbrace{1 + \ldots + 1}_{r-2l} + l + \underbrace{0 + \ldots + 0}_{2l-2} + l = r$. In this case $s = r$.

2.5) $s = \underbrace{1 + \ldots + 1}_{r_1} + l + \underbrace{0 + \ldots + 0}_{2l-2} + l + \underbrace{1 + \ldots + 1}_{r_2} = r$,

where $r_1, r_2 \geq 1$ and $r_1 + r_2 = r - 2l$. In this case $s = r$.

3)If $g|_i = g^l$ then we have the following cases:

3.1) $s = l + 0 + \ldots + 0$. Same as 1.2).

3.2) $s = l + \underbrace{0 + \ldots + 0}_{2l-2} + l = 2l = r$. In this case $s = r$.

3.3) $s = l + 0 + \ldots + 0 + l + 1 + \ldots + 1$. Same as 2.4).

3.4) $s = l + 1 + \ldots + 1$. Same as 2.2).

3.5) $s = l + \underbrace{1 + \ldots + 1}_{2k-3} + l = 0$. In this case $s = 0$.

3.6) $s = l + 1 + \ldots + 1 + l + 0 + \ldots + 0$. Same as 1.4).

In all cases $g^s \in M$. We have a contradiction, then $Q \subseteq M$. It means that $Q = M$ and $|Q| = 2k$. □

Proposition 6. *An automorphism g has d states in each of the following cases:*

(1) $d = 2d' + 1$ for some $d' \geq 1$ and

$$g = (1, g, g^2, \ldots, g^{d-1})\pi;$$

(2) $d = 4d' - 2$ for some $d' \geq 1$ and

$$g = (g, g, g^2, g^2, \ldots, g^{\frac{d}{2}}, g^{\frac{d}{2}})\pi;$$

(3) $d = 4d'$ for some $d' \geq 1$ and

$$g = (1, g, g, g^2, g^2, \ldots, g^{\frac{d}{2}-1}, g^{\frac{d}{2}-1}, g^{\frac{d}{2}})\pi.$$

Proof. In all cases we prove that the group $G = \langle g \rangle$ is finite and $Q = \mathrm{G}$, where G is the set of elements of G. The inclusion $Q \subseteq \mathrm{G}$ follows from the definition of self-similar group. By Theorem 1 the group G is finite if and only if $S(i)$ is divisible by $|O_\pi(i)|$ for all $i = 1, \ldots, d$. Since π has the only one orbit we need to prove that $S(1)$ is divisible by $|O_\pi(1)| = d$. Consider each case separately.

(1) $S(1)$ is divisible by d.

$$S(1) = 0 + 1 + 2 + \ldots + d - 1 = \frac{(d-1) \cdot d}{2} = \frac{d \cdot (2d' + 1 - 1)}{2} = d \cdot d'.$$

Then G is finite.

We have $Q_1 = \{1, g, g^2, \dots, g^{d-1}\} = \mathrm{G}$ and $Q_1 \subseteq Q$. Then $\mathrm{G} \subseteq Q$ and $\mathrm{G} = Q$.

(2) $S(1)$ is divisible by d.

$$S(1) = 2 \cdot \left(1 + 2 + \ldots + \frac{d}{2}\right) = \frac{d}{2} \cdot \left(\frac{d}{2} + 1\right) = d \cdot \frac{d+2}{4} = d \cdot d'.$$

Then G is finite.

We have $Q_1 = \{g, g^2, \dots, g^{\frac{d}{2}}\}$. Since $g^2 \in Q_1$ we consider Q_2:

$$g^2 = (g^2, g^3, \dots, g^{d-1}, 1)\pi^2$$

and $Q_2 = \{1, g^2, g^3, \dots, g^{d-1}\}$. Hence $Q_1 \cup Q_2 = \mathrm{G}$ and $Q_1 \cup Q_2 \subseteq Q$. Then $\mathrm{G} \subseteq Q$ and $\mathrm{G} = Q$.

(3) $S(1)$ is divisible by d.

$$S(1) = \underbrace{0 + 1 + \ldots + \frac{d}{2} - 1}_{\text{odd}} + \underbrace{1 + 2 + \ldots + \frac{d}{2}}_{\text{even}} = \frac{\left(\frac{d}{2} - 1\right) \cdot \frac{d}{2}}{2} + \frac{\frac{d}{2} \cdot \left(\frac{d}{2} + 1\right)}{2} =$$

$$= \frac{\frac{d}{2} \cdot \left((\frac{d}{2} - 1) + (\frac{d}{2} + 1)\right)}{2} = d \cdot \frac{d}{4} = d \cdot d'.$$

Then G is finite.

We have $Q_1 = \{1, g, g^2, \dots, g^{\frac{d}{2}}\}$. Since $g^2 \in Q_1$ we consider Q_2:

$$g^2 = (g, g^2, \dots, g^{d-1}, g^{\frac{d}{2}+1})\pi^2$$

and $Q_2 = \{g, g^2, \dots, g^{d-1}\}$. Therefore $Q_1 \cup Q_2 = \mathrm{G}$ and $Q_1 \cup Q_2 \subseteq Q$. Then $\mathrm{G} \subseteq Q$ and $\mathrm{G} = Q$.

□

Now Propositions 2 – 6 imply the following assertion.

Theorem 2. *Let G be a finite self-similar cyclic group generated by an authomorphism g of the form (4), where $\pi = (1, \dots, d)$. There exists a set of values $\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ such that g has k states, where $1 \le k \le d$.*

4. Concluding remarks

It is natural to consider arbitrary permutation π of the vertices of the rooted tree and automorphisms generating finite cyclic self-similar groups which extend π. It is shown that for π being a long cycle all possible numbers of states for such automorphisms can be achieved. The question about possible numbers of states for automorphisms extending other permutations remains open.

References

[1] *Bartholdi L., Šuniḱ Z.* Some solvable automaton groups // Topological and Asymptotic Aspects of Group Theory. — 2006. — vol. 394. — P. 11–30.

[2] *Savchuk D., Vorobets Y.* Automata generating free products of groups of order 2 // Journal of Algebra. — 2011. — Vol. 336, no. 1. — P. 53 – 66.

[3] *Grigorchuk R. I., Nekrashevich V. V., Sushchanskii V. I.* Automata, dynamical systems and groups // Proceedings of the Steklov Institute of Mathematics. — 2000. — 231. — P. 128 – 203.

[4] Nekrashevych. V. *Self-similar groups.* volume 117 of Mathematical Surveys and Monographs. Amer. Math. Soc., Providence, RI, 2005.