

Shift automorphisms of finite order

Venu Addepalli and Edward C. Turner

ABSTRACT. We study automorphisms of free groups—called *shift automorphisms*—for which the images of a particular element form a free basis. We view them as free group analogues of basic rational canonical blocks for linear transformations on a vector space. Our focus in this paper is a classification of shift automorphisms of finite order.

§1) Introduction and preliminaries

In what follows, $F(x_1, \dots, x_n)$ denotes the free group on the basis $\{x_1, \dots, x_n\}$, abbreviated F_n when convenient, and F denotes a free group of unspecified finite rank. An element $w \in F_n$ can be considered a function of n variables from a free group of rank n to itself by substitution in the natural way—functional notation will be used when this is the point of view (so, for example, if $w = x_2x_1x_3$ then $w(x_2^{-1}, x_1^2, x_1x_2) = x_1^2x_2^{-1}x_1x_2$).

DEFINITION 1. If $w \in F(x_1, x_2, \dots, x_n)$, then α_w is the shift automorphism defined by

$$\alpha_w : x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_{n-1} \longrightarrow x_n \longrightarrow w.$$

More generally, $\alpha \in \text{Aut}(F)$ is a shift automorphism with shift generator u if $\{u, \alpha(u), \dots, \alpha^{n-1}(u)\}$ is a basis for F . Furthermore, $w \in F(x_1, x_2, \dots, x_n)$ is the shift representing word for α relative to u if

$$\alpha^n(u) = w(u, \alpha(u), \dots, \alpha^{n-1}(u)).$$

We denote the shift representing word for α relative to the generator u by $w_{\alpha, u}$.

Thus, x_1 is a shift generator for α_w and w is a shift representing word for α_w relative to x_1 . Furthermore, up to a change of basis, all shift automorphisms are of this form. For any word w , the prescription above determines an endomorphism which we also denote by α_w .

Basic facts:

- (1) One can decide algorithmically whether an automorphism $\alpha \in \text{Aut}(f_n)$ has finite order.

Any automorphism of finite order of F_n is induced by a homeomorphism of a graph of rank n . Such a graph can be chosen to have at most $3n - 3$ edges. Considering the permutation of the edges, such a homeomorphism has order dividing $(3n - 3)!$.

- (2) The endomorphism α_w is an automorphism if and only if $w = ux_1^{\pm 1}v$, where u and v are in the subgroup $F(x_2, \dots, x_n)$. This is because F_n is Hopfian and α_w is surjective if and only if the set $\{x_2, \dots, x_n, w\}$ Nielsen reduces to the standard basis $\{x_1, x_2, \dots, x_n\}$ [LS, p4].
- (3) For each i , x_i is a shift generator for α_w with shift generating word

$$w_{\alpha_w, x_i} = w \text{ for all } i.$$

In fact, $\alpha_w^k(x_1)$ is a shift generator for all $k \in \mathbb{Z}$ with shift generating word

$$w_{\alpha_w, \alpha_w^k(x_1)} = w.$$

More generally, if u is a generator for α_w , then so is $\alpha_w^k(u)$ for all $k \in \mathbb{Z}$: such generators will be considered equivalent.

- (4) The shift automorphisms α_w and α_v are conjugate in $Aut(F(x_1, \dots, x_n))$ if and only if there is a shift generator u for α_w with shift representing word

$$\alpha_w^n(u) = v(u, \alpha_w(u), \dots, \alpha_w^{n-1}(u)).$$

If $\varphi^{-1}\alpha_w\varphi = \alpha_v$, then $\alpha_w(\varphi(x_i)) = \varphi(\alpha_v(x_i)) = \varphi(x_{i+1})$ for $i < n$ and $\alpha_w(\varphi(x_n)) = \varphi(w(x_1, \dots, x_n)) = w(\varphi(x_1), \dots, \varphi(x_n))$.

- (5) Define \tilde{w} to be the word whose letters are those of w in reverse order: e.g.,

$$\widetilde{x_1x_2^{-1}x_3} = x_3x_2^{-1}x_1.$$

Otherwise stated,

$$\tilde{w} = (w(x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}))^{-1}.$$

Then α_w and $\alpha_{\tilde{w}}$ are conjugate in $Aut(F(x_1, \dots, x_n))$ since

$$\alpha_w^n(x_1^{-1}) = \tilde{w}(x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}).$$

In other words, x_1^{-1} is a shift generator for α_w for which the shift representing word is \tilde{w} ; i.e., $w_{\alpha_w, x_1^{-1}} = \tilde{w}$.

Some Examples

- 1) Clearly, the only shift automorphism of F_n of order n is α_{x_1} :

$$\alpha_{x_1} : x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_n \rightarrow x_1.$$

Furthermore, the generators and their inverses $x_i^{\pm 1}$ are all shift generators all with representing word x_1 . It is an exercise to show that these are the *only* shift generators for α_{x_1} : thus α_{x_1} is conjugate to no other shift automorphism.

- 2) For any $w \in F_n$, x_1^{-1} is a shift generator for α_w with representing word

$$\tilde{w} = (w(x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}))^{-1},$$

$$(\tilde{w} = w \text{ backwards; e.g., } \widetilde{x_1x_2^{-1}x_3} = x_3x_2^{-1}x_1).$$

Thus α_w and $\alpha_{\tilde{w}}$ are conjugate.

- 3) Suppose $w = x_n^{-1}x_{n-1}^{-1} \dots x_1^{-1} \in F_n$. Then α_w has order $n+1$. E.g, for $\alpha_{x_3^{-1}x_2^{-1}x_1^{-1}}$;

$$\begin{aligned} x_1 &\rightarrow x_2 \rightarrow x_3 \rightarrow \\ &\rightarrow x_3^{-1}x_2^{-1}x_1^{-1} \rightarrow x_1x_2x_3 \cdot x_3^{-1}x_2^{-1} = x_1 \end{aligned}$$

In this case, x_1x_2 is also a shift generator with representing word $x_3^{-1}x_1^{-1}x_4^{-1}x_2^{-1}$. Similarly, the following are all conjugate (and are conjugate to no other shift automorphisms):

$$\begin{array}{cc} \alpha_{x_4^{-1}x_3^{-1}x_2^{-1}x_1^{-1}} & \alpha_{x_1^{-1}x_2^{-1}x_3^{-1}x_4^{-1}} \\ \alpha_{x_3^{-1}x_1^{-1}x_4^{-1}x_2^{-1}} & \alpha_{x_2^{-1}x_4^{-1}x_1^{-1}x_3^{-1}} \end{array}$$

- 4) For $w = x_n^{-1}x_{n-1}^{-1} \cdots x_1^{-1}$ the shift automorphism α_w is conjugate to exactly $\frac{1}{2}\varphi(n+1)$ pairs of shift automorphisms whose representing words are obtained by permuting the letters of w .

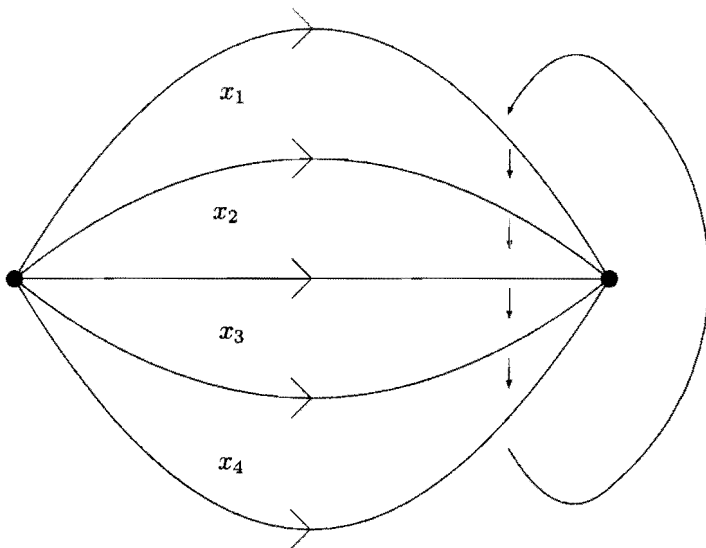
More precisely, if $\gcd(k, n+1) = 1$, then the words

$$x_1x_2 \cdots x_k \quad \text{and} \quad x_k^{-1} \cdots x_2^{-1}x_1^{-1}$$

are shift generators for $\alpha_{x_n^{-1}x_{n-1}^{-1} \cdots x_1^{-1}}$. The corresponding representing words are permutations of w . Two such words determine the same permutation if and only if

$$k \equiv \pm k' \pmod{n+1}.$$

There are no other shift generators. Shown below is a homeomorphism of a graph that induces $\alpha_{x_4^{-1}x_3^{-1}x_2^{-1}x_1^{-1}}$. The elements x_1, \dots, x_4 are the clockwise loops in the regions they label.



§2) Graph representations

Suppose α is an automorphism of finite order n of a free group which is induced by the homeomorphism h (acting without inversions) of the finite graph Γ , considered as an action of $G = \mathbb{Z}_n$ on Γ . (Note that we always consider \mathbb{Z}_n with a specified generator.) Stabilizers of vertices and edges are denoted G_v and G_e respectively, and orbits by $G \cdot v$ and $G \cdot e$. Then the following entities can be defined:

- (1) the quotient graph $\bar{\Gamma}$ with the projection $p : \Gamma \rightarrow \bar{\Gamma}$;

(2) for each vertex $v \in \Gamma$,

$$\nu(v) \equiv |G \cdot v| = [G; G_v]$$

and for each edge $e \in \Gamma$

$$\nu(e) \equiv |G \cdot e| = [G; G_e];$$

(3) for each edge $e \in \Gamma$

$$\delta_i(e) \equiv |G \cdot e|/|G \cdot i(e)| = |G_{i(e)}|/|G_e|,$$

and

$$\delta_t(e) \equiv |G \cdot e|/|G \cdot t(e)| = |G_{t(e)}|/|G_e|;$$

(4) a minimal spanning tree $\bar{T} \subset \bar{\Gamma}$;

(5) a tree $\tilde{T} \subset \Gamma$ which is a lift of

\bar{T} (i.e., $p(\tilde{T}) = \bar{T}$ and p is (1-1) on edges) with the associated splitting $j: \bar{T} \rightarrow \tilde{T}$ defined on the sets of vertices and edges so that $j(i(p(e))) = i(e)$;

(6) a minimal spanning tree $T \subset \Gamma$ so that $\tilde{T} \subset T$ and for each edge e , the edges in $(\mathbb{Z}_n \cdot e) \cap T$ are the first few images of e under h ;

(7) for each edge $e \in \Gamma$,

$$\eta_e \equiv \min\{k|h^k(tj(p(e))) \in \tilde{T}\}.$$

These numbers are all integers satisfying the conditions that

- a) $\nu(v), \nu(e), \delta_i(e)$ and $\delta_t(e)$ are divisors of n ,
- b) $\nu(*) = 1$,
- c) $\nu(e) = \delta_i(e)\nu(i(e)) = \delta_t(e)\nu(t(e))$,
- d) $0 \leq \eta(e) \leq \nu(t(e))$.

The numbers $\nu(v), \nu(e), \delta_i(e), \delta_t(e)$ and $\eta(e)$ are constant on orbits in Γ and so can be considered as defined on $\bar{\Gamma}$.

The action of g on Γ is *reduced* if no edge orbit is a forest. We will always assume that actions are reduced—for if a particular edge orbit is a forest, the components can be collapsed to points to produce an action on a graph with fewer edges representing the same automorphism. If the action is reduced then for each edge e which is not a loop, $\delta_i(e) > 1$ and $\delta_t(e) > 1$.

DEFINITION 2. A completed \mathbb{Z}_n -graph is a graph Γ with directed tree $\tilde{T} \in \Gamma$ with source $*$, taken as the basepoint, and a reduced action of \mathbb{Z}_n on Γ fixing the basepoint $*$ so that \tilde{T} contains exactly one edge from each orbit and the initial vertices of edges of \tilde{T} contain exactly one vertex from each orbit. The associated numbers $\nu(v), \nu(e), \delta_i(e), \delta_t(e)$ and $\eta(e)$ are defined as above.

A completed \mathbb{Z}_n quotient graph is a graph $\bar{\Gamma}$ with a minimal spanning tree \bar{T} a basepoint $\bar{*}$, a number n and

$\nu(v)$ for each vertex and $\nu(e), \delta_i(e), \delta_t(e)$

and $\eta(e)$ for each edge satisfying condition a)–d) above.

DEFINITION 3. The graph complexity of an automorphism α of order n is the smallest number of edges in a completed \mathbb{Z}_n quotient graph representing α .

We will denote completed graphs and completed \mathbb{Z}_n quotient graphs by Γ and $\bar{\Gamma}$ respectively when context avoids confusion. When considering a particular example of a completed quotient graph and the associated completed \mathbb{Z}_n -graph, we will

denote the quotient edges by letters (e.g., a, b, c, \dots), the corresponding edges of \tilde{T} with subscript 0 (e.g., a_0, b_0, c_0, \dots) and the successive images under g with increasing subscripts (e.g., $a_1 = g(a_0), a_2 = g^2(a_0), \dots$). (Note: The edge $e \in \bar{\Gamma}$ is covered by $e_k, 0 \leq k < \nu_e$. Furthermore, the number of edges in $\Gamma \setminus \tilde{T}$ covering the edge $e \in \bar{\Gamma}$ is $\nu(e)$ if $e \notin \bar{T}$ and $\nu(e) - \nu(t(e))$ if $e \in \bar{T}$.)

PROPOSITION 1. *A completed \mathbb{Z}_n -graph determines a completed quotient graph and conversely. Every automorphism of a free group of finite order is represented by a completed \mathbb{Z}_n -graph.*

Proof of Proposition 1: The first statement is straightforward. The second follows from the theorem of Culler [Cu]. \square

Note that the information that determines a completed \mathbb{Z}_n -graph also determines a basis for $\pi_1(\Gamma, *)$ —namely the basis associated to the maximal tree T which is defined to be \tilde{T} with the first few images of each edge added to form a spanning tree.

We can use these notions to prove a version of the theorem of McCool characterizing automorphisms of finite order of a free group. The use of Culler's Theorem (proven after the publication of McCool's theorem) simplifies the argument considerably. This theorem can be considered an analog of the rational canonical form representation of a linear transformation.

THEOREM 1. *Suppose Γ and $\bar{\Gamma}$ are a completed \mathbb{Z}_n -graph and the corresponding completed \mathbb{Z}_n quotient graph with all the associated terms as described above. Suppose α is the automorphism of F_r (with basis S determined by T) induced by the generator of \mathbb{Z}_n . Then there is a basis S for F_r that can be expressed in terms of the edges e of $\bar{\Gamma}$ as*

$$S = \bigcup_{e \in \bar{\Gamma}} S(e), \quad S(e) = \{E_0, E_1, \dots, E_{k(e)-1}\}$$

where

$$\begin{aligned} k(e) &= \nu(e) - \nu(t(e)) & \text{for } e \in \bar{T}, \\ k(e) &= \nu(e) & \text{for } e \notin \bar{T}, \end{aligned}$$

so that α has the following form.

a) For each edge $e \in \bar{\Gamma}$, $\alpha(E_i) = E_{i+1}$ for $0 \leq i < k(e) - 1$.

b) If $e \in \bar{T}$ and c is the edge of \tilde{T} so that $i(e) = t(e)$, then

$$\alpha(E_{k(e)-1}) = E_{\nu(e)-2\nu(t(e))}^{-1} \cdots E_{\nu(t(e))}^{-1} E_0^{-1} C_0 C_{\nu(i(e))} \cdots C_{\nu(e)-\nu(i(e))}.$$

c) If $e \notin \bar{T}$ and c and d are the edges of \tilde{T} so that $i(e) = t(c)$ and $t(e) = t(d)$, then

$$\alpha(E_{k(e)-1}) = C_{\nu(e)-\nu(i(e))} \cdots C_{\nu_1(e)} C_0 E_0 D_{\eta_e} \cdots D_{\eta_e + \nu(e) - \nu(t(e))}.$$

Proof: Let $g: \Gamma \rightarrow \Gamma$ be the generator of \mathbb{Z}_n . For each edge $e \in \bar{\Gamma}$, let $e_0 = j(e)$ be the edge of $\tilde{T} \in \Gamma$ covering it, $e_j = g^j(e_0)$ and $\gamma_{i(e)}$ be the path in \tilde{T} from $*$ to $i(e)$ (so in particular, $\gamma_{i(e_0)} = \gamma_{i(c_0)} c_0$). Then define

- (1) $E_0 = \gamma_{i(e_0)} e_0 g^{\nu(t(e))} (\overline{e_0 \gamma_{i(e_0)}})$ if $e \in \bar{T}$,
- (2) $E_0 = \gamma_{i(e_0)} e_0 g^{-\eta(e)} (\overline{\gamma_{g^{\eta_e}(t(e_0))}})$ if $e \notin \bar{T}$,
- (3) $E_i = g^i(E_0)$ (for all i), and

(4) $S(e) = \{E_0, E_1, \dots, E_{k(e)-1}\}$, $k(e)$ as above.

Condition a) is clear. If $e \in \bar{T}$, then

$$\begin{aligned} E_0 E_{\nu(t(e))} \cdots E_{\nu(e)-\nu(t(e))} &= \gamma_{i(e_0)} e_0 g^{\nu(e)}(\bar{e}_0 \overline{\gamma_{i(e_0)}}) \\ &= \gamma_{i(c_0)} c_0 g^{\nu(e)}(\bar{c}_0 \overline{\gamma_{i(c_0)}}) \\ &= \gamma_{i(c_0)} c_0 g^{\delta_{i(e)} \nu(t(c))}(\bar{c}_0 \overline{\gamma_{i(c_0)}}) \\ &= C_0 C_{\nu(t(c))} \cdots C_{\nu(e)-\nu(t(c))}. \end{aligned}$$

from which b) follows.

If $e \notin \bar{T}$, let $v' = g^{\eta(e)}(t(e_0))$: then

$$\begin{aligned} E_{\nu(e)} &= g^{\nu(e)}(\gamma_{i(e_0)}) e_0 g^{\nu(e)-\eta(e)}(\overline{\gamma_{v'}}) \\ &= (g^{\nu(e)}(\gamma_{i(e_0)}) \overline{\gamma_{i(e_0)}}) \cdot (\gamma_{i(e_0)} e_0 g^{-\eta(e)}(\overline{\gamma_{v'}})) \\ &\quad \cdot g^{-\eta(e)}((\gamma_{v'} g^{\nu(e)}(\overline{\gamma_{v'}})) \\ &= (g^{\delta_{i(e)} \nu(t(e))}(\gamma_{i(c_0)} c_0) \bar{c}_0 \overline{\gamma_{i(c_0)}}) \cdot E_0 \cdot g^{-\eta(e)}(\gamma_{i(d_0)}) d_0 g^{\delta_{i(e)} \nu(t(d))}(\bar{d}_0 \overline{\gamma_{v'}}) \\ &= \overline{C_{\nu(e)-\nu(i(e))}} \cdots \overline{C_{\nu(i(e))}} \overline{C_0} E_0 D_{-\eta(e)} D_{-\eta(e)+\nu(i(e))} \cdots D_{-\eta(e)+\nu(e)-\nu(i(e))}. \end{aligned}$$

It only remains to show that S is a basis. The elements of S correspond to the edges of $\Gamma \setminus T$ (albeit not in the usual way), so the cardinality is correct. It is straightforward to use the equations above to show inductively that S generates. \square

§3) Matrix results

In this section we prove the matrix results that will be applied in the next two sections. Consider the following sequence of maps, where θ assigns the outer class to an automorphism, μ gives the matrix representing the abelianization of an outer class (relative to the given basis) and χ assigns the characteristic polynomial to an integral matrix.

$$\text{Aut}(F_n) \xrightarrow{\theta} \text{Out}(F_n) \xrightarrow{\mu} \text{GL}(n, \mathbb{Z}) \xrightarrow{\chi} \mathbb{Z}[t]$$

where

$$\alpha \mapsto \bar{\alpha} \mapsto M_\alpha \mapsto \chi_\alpha(t).$$

The maps θ and μ are well known to be (1-1) on finite subgroups (in other words to have torsion free kernels)—the kernel of θ is free and the kernel of μ is torsion free by [BT]. The polynomial $\chi(\alpha) = \chi_\alpha(t) = \det(tI - M_\alpha)$ —which we call the *characteristic polynomial of α* —is the usual characteristic polynomial of the matrix M_α and depends only on the conjugacy class of α . (In arguing about the factors of $\chi(\alpha)$, we may as well consider the coefficients as rational numbers so that the standard theory of linear algebra over a field can be used. It is straightforward to check that all the results we use hold over \mathbb{Z} as well.) If α has finite order k , then so does M_α and by the Cayley-Hamilton Theorem, the minimal polynomial of M_α is a divisor of $t^k - 1$: therefore the minimal polynomial is a product of distinct cyclotomic polynomials corresponding to divisors of k . In the case of a shift automorphism, the minimal polynomial is $\chi_\alpha(t)$.

We begin with some notation. All vectors $v \in \mathbb{Z}^n$ are assumed to be integral column vectors and matrices $M \in \text{GL}(n, \mathbb{Z})$ act by multiplying on the left.

DEFINITION 4. If $p(t) = t^k + c_{k-1}t^{k-1} + \dots + c_1t + c_0 \in \mathbb{Z}[t]$, then the associated companion matrix is

$$C_p = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -c_{k-1} \end{pmatrix}$$

More generally,

$$C_{p_1, p_2, \dots, p_k} = \begin{pmatrix} C_{p_1} & 0 & \dots & 0 \\ 0 & C_{p_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_{p_k} \end{pmatrix}.$$

If B is a matrix of the appropriate size, then

$$C_{p_1, p_2; B} = \begin{pmatrix} C_{p_1} & B \\ 0 & C_{p_2} \end{pmatrix}.$$

If $v_1, v_2, \dots, v_k \in \mathbb{Z}^n$, then (v_1, v_2, \dots, v_k) is the $n \times k$ matrix whose columns are the v_i 's. Furthermore,

$$L_{v, M} = (v, Mv, \dots, M^{n-1}v).$$

The vector c is a cyclic vector for the matrix M if the columns of $L_{c, M}$ form a basis for \mathbb{Z}^n and M is said to be a cyclic matrix if there exists a cyclic vector for M .

Note that if α is a shift automorphism, then $M_\alpha = C_{X_\alpha}$ and is in particular cyclic.

LEMMA 1. The vector c is a cyclic vector for $M \in Gl(n, \mathbb{Z})$ if and only if $\det(L_{c, M}) = \pm 1$. Furthermore, if there exists a polynomial $r \in \mathbb{Z}[t]$ such that

- (1) $\deg(r) < n$,
- (2) $r(0) = \pm 1$,
- (3) there exists a prime p so that

$$r(M) \cong 0 \pmod{p}$$

then M is not cyclic.

Proof: The first statement is clear. Suppose $r(t) = \sum_{k=0}^{n-1} r_k t^k$ is a polynomial with the stated properties and v is any vector. Properties (1) and (2) imply that $r(M)(v) = \pm v + \sum_{k=1}^{n-1} r_k M^k v$ —in other words, we can replace the first column of $L_{v, M}$ with $\pm r(M)v$ without changing its determinant. Then (3) implies that this determinant is a multiple of p : it follows that v is not a cyclic vector for M . \square

LEMMA 2. Suppose $n_1 = de$, $1 \leq d, e < n_1$, and

$$p_1(t) = \frac{t^{n_1} - 1}{t^d - 1} \quad \text{and} \quad p_2(t) = t^{n_2} - 1.$$

Suppose B is an integral matrix such that $\Sigma B \cong 0 \pmod{p}$ for some prime $p \mid e$, where ΣB is the sum of all the entries in B . Then the matrices C_{p_1, p_2} and $C_{p_1, p_2; B}$ are non-cyclic.

Proof: Let $q_2(t) = \frac{p_2(t)}{t-1}$ and $q_1(t) = \frac{p_1(t)-e}{t-1}$ (note that $p_1(1) = e$). We show that \mathcal{C}_{p_1, p_2} and $\mathcal{C}_{p_1, p_2; B}$ are not cyclic by showing that the polynomial

$$r(t) = \frac{p_1(t)p_2(t)}{t-1} = p_1(t)q_2(t)$$

satisfies the conditions of Lemma 1 for both \mathcal{C}_{p_1, p_2} and $\mathcal{C}_{p_1, p_2; B}$ for any prime divisor p of e . Conditions (1) and (2) are clear.

Claim:

$$r(\mathcal{C}_{p_1, p_2}) = \begin{pmatrix} r(\mathcal{C}_{p_1}) & 0 \\ 0 & r(\mathcal{C}_{p_2}) \end{pmatrix}$$

and

$$r(\mathcal{C}_{p_1, p_2; B}) = \begin{pmatrix} r(\mathcal{C}_{p_1}) & q_1(\mathcal{C}_{p_1})Bq_2(\mathcal{C}_{p_2}) \\ 0 & r(\mathcal{C}_{p_2}) \end{pmatrix}.$$

Furthermore, $q_1(\mathcal{C}_{p_1})Bq_2(\mathcal{C}_{p_2}) \cong 0 \pmod{p}$.

Proof of Claim: Now $p_1 \mid r$ so that $r(\mathcal{C}_{p_1}) = 0$ and $(t-1) \mid p_1(t) \pmod{p}$ so that $r(\mathcal{C}_{p_2}) \cong 0 \pmod{p}$.

Block matrix manipulations show that

$$\begin{aligned} r(\mathcal{C}_{p_1, p_2; B}) &= p_1(\mathcal{C}_{p_1, p_2; B})q_2(\mathcal{C}_{p_1, p_2; B}) \\ &= \begin{pmatrix} 0 & B_1 \\ 0 & p_1(\mathcal{C}_{p_2}) \end{pmatrix} \begin{pmatrix} q_2(\mathcal{C}_{p_1}) & B_2 \\ 0 & q_2(\mathcal{C}_{p_2}) \end{pmatrix} \\ &\cong \begin{pmatrix} 0 & B_1q_2(\mathcal{C}_{p_2}) \\ 0 & 0 \end{pmatrix} \pmod{p} \end{aligned}$$

where

$$B_1 = \sum_{k=1}^{e-1} \sum_{\ell=0}^{k-1} \mathcal{C}_{p_1}^\ell B \mathcal{C}_{p_2}^{k-1-\ell}.$$

Now

$$(\mathcal{C}_{p_2} - I)q_2(\mathcal{C}_{p_2}) = 0 \implies \mathcal{C}_{p_2}^k q_2(\mathcal{C}_{p_2}) = q_2(\mathcal{C}_{p_2}) \quad \text{for all } k,$$

so that

$$\begin{aligned} B' &= B_1q_2(\mathcal{C}_{p_2}) = \sum_{k=1}^{e-1} \sum_{\ell=0}^{k-1} \mathcal{C}_{p_1}^\ell B \mathcal{C}_{p_2}^{k-1-\ell} q_2(\mathcal{C}_{p_2}) \\ &= \left(\sum_{k=1}^{e-1} \sum_{\ell=0}^{k-1} \mathcal{C}_{p_1}^\ell B \right) q_2(\mathcal{C}_{p_2}). \end{aligned}$$

Furthermore,

$$(t-1) \sum_{k=1}^{e-1} \sum_{\ell=0}^{k-1} t^\ell = \sum_{k=1}^{e-1} (t^{jd-1} - 1) = p_1(t) - e$$

so that

$$\sum_{k=1}^{e-1} \sum_{\ell=0}^{k-1} t^\ell = q_1(t). \text{ Thus } B' = q_1(\mathcal{C}_{p_1})Bq_1(\mathcal{C}_{p_2}).$$

Considering the product $q_1(\mathcal{C}_{p_1})(\mathcal{C}_{p_1} - I) = 0$, we see that the columns of $q_1(\mathcal{C}_{p_1})$ are all the same—i.e., $q_1(\mathcal{C}_{p_1}) = D(\text{all } 1\text{'s})$ for some diagonal matrix D —and direct calculation shows that $q_2(\mathcal{C}_{p_2}) = (\text{all } 1\text{'s})$ are 1's. Thus

$$q_1(\mathcal{C}_{p_1})Bq_1(\mathcal{C}_{p_2}) = D(\text{all } 1\text{'s})B(\text{all } 1\text{'s}) = D(\text{all } \Sigma B\text{'s}).$$

The result follows. \square

LEMMA 3. Suppose $\nu_1 \mid n_1$ and $\nu_2 \mid n_2$, and

$$p_1(t) = \frac{t^{n_1} - 1}{t^{\nu_1} - 1} \quad \text{and} \quad p_2(t) = \frac{t^{n_2} - 1}{t^{\nu_2} - 1}$$

and $\gcd(\frac{n_1}{\nu_1}, \frac{n_2}{\nu_2}) \neq 1$.

Suppose B is an integral matrix such that $\Sigma B \cong 0 \pmod{p}$ for some prime $p \mid e$, where

ΣB is the sum of all the entries in B . Then the matrices C_{p_1, p_2} and $C_{p_1, p_2; B}$ are non-cyclic.

Proof: Let $e_1 = \frac{n_1}{\nu_1}, e_2 = \frac{n_2}{\nu_2}, p$ be any prime divisor of $e = \gcd(e_1, e_2)$ and let

$$q_1(t) = \frac{p_1(t) - e_1}{t - 1} \quad \text{and} \quad q_2(t) = \frac{p_2(t)}{t - 1}.$$

Then all the arguments of Lemma 2 hold when interpreted modulo p . □

§4) Graph complexity one and two

In this section we describe all shift automorphisms of geometric complexity 1 or 2.

THEOREM 2. All automorphisms of finite order n and geometric complexity 1 are shift automorphisms. They are described in terms of the quotient graph $\bar{\Gamma}$, which has a single edge a corresponding to the orbit $\{a_i \mid 1 \leq i \leq n\}$, as follows.

- 1) The edge a is a loop with $\nu(a) = n$. Then $x_1 = a_1$ is a shift generator with representing word x_1 : i.e.,

$$\alpha \cong \alpha_{x_1}.$$

The generators and their inverses are shift generators.

- 2) The edge a has two endpoints, the basepoint v_0 and $w \neq v_0$; furthermore, $\nu(w) = 1$ and $\nu(a) = n$. Then $x_1 = a_1 a_2^{-1}$ is a shift generator with representing word $x_1^{-1} x_2^{-1} \cdots x_{n-1}^{-1}$;

i.e.,

$$\alpha \cong \alpha_{x_{n-1}^{-1} x_{n-2}^{-1} \cdots x_1^{-1}}.$$

The words $x_1 x_2 \cdots x_k$ and their inverses for $\gcd(k, n) = 1$ are shift generators.

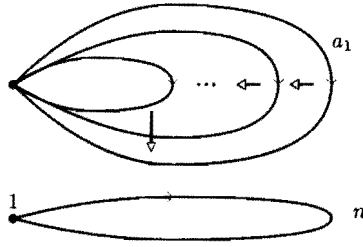
- 3) The edge e has two endpoints, the basepoint v_0 and $w \neq v_0$; furthermore, $\nu(w) = d \neq 1$ and $\nu(e) = n$. Then

$$\begin{array}{c} \uparrow \\ n \cdot \downarrow \end{array} \quad \alpha = \alpha_{x_{n-d+1}^{-1} x_{n-2d+1}^{-1} \cdots x_1^{-1}}.$$

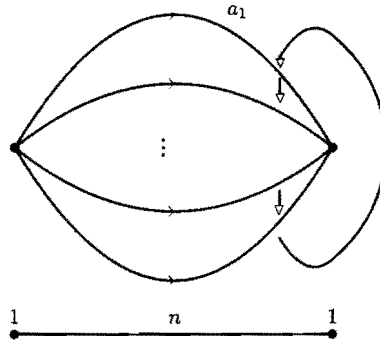
Note: With some more work, one can show that the shift generators described in the theorem are all the shift generators.

Proof of Theorem 2: The three possibilities of the theorem are illustrated below. In each case, there are n edges a_1, \dots, a_n , the first edge a_1 is labeled and $g(a_i) = a_{i+1} \pmod{n}$.

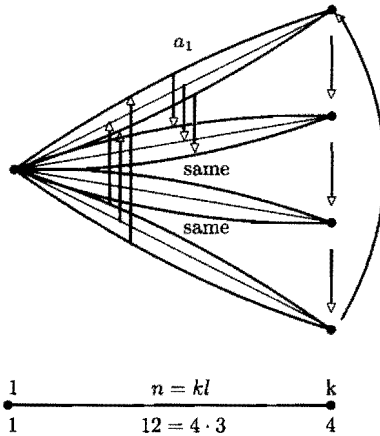
1) α_{x_n}



2) $\alpha_{x_{n-1}^{-1}x_{n-2}^{-1}\dots x_1^{-1}}$



3) $\alpha_{x_5^{-1}x_1^{-1}}$



(Check: $\alpha_{x_5^{-1}x_1^{-1}}$ has order 12 in $Aut(F_8)$:

$$\begin{aligned}
 &x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow x_4 \rightarrow x_5 \rightarrow x_6 \rightarrow x_7 \rightarrow x_8 \rightarrow x_5^{-1}x_1^{-1} \\
 &\rightarrow x_6^{-1}x_2^{-1} \rightarrow x_7^{-1}x_3^{-1} \rightarrow x_8^{-1}x_4^{-1} \rightarrow x_1x_5x_5^{-1} = x_1.)
 \end{aligned}$$

Proof of Theorem 2: The quotient graph is either a loop or an edge with two different endpoints.

If the quotient $\bar{\Gamma}$ is a loop, then Γ is clearly a bouquet of circles and the action of g is to permute the loops cyclically, leading to Case 1. Since reduced products are mapped to reduced products, it is easy to verify that the only shift generators are the free generators and their inverses.

If the quotient $\bar{\Gamma}$ is an edge with endpoints v_0 (the basepoint) and w with $\nu(w) = 1$, then we have the picture of Example 2 above. Then

$$\alpha : a_1 a_2^{-1} \rightarrow \cdots \rightarrow a_{n-1} a_n^{-1} \rightarrow a_n a_1^{-1} = (a_{n-1} a_n^{-1})^{-1} \cdots (a_1 a_2^{-1})^{-1}.$$

Thus $x_1 = a_1 a_2^{-1}$ is a generator with representing word $x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1}$.

If $\bar{\Gamma}$ is an edge with vertices v_0 , the basepoint, and w with $\nu(w) = d \neq 1$, then we have the picture of Example 3 above.

Then

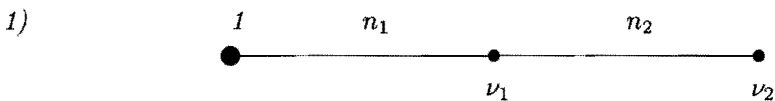
$$\begin{aligned} \alpha & : a_1 a_{d+1}^{-1} \rightarrow a_2 a_{d+2}^{-1} \cdots a_{d+1} a_{2d+1}^{-1} \rightarrow \cdots \rightarrow a_{n-d+1} a_1^{-1} \\ & = (a_{n-2d+1} a_{n-d+1}^{-1})^{-1} \cdots (a_1 a_{d+1}^{-1})^{-1}. \end{aligned}$$

Thus $x_1 = a_1 a_{d+1}^{-1}$ is a shift generator with representing word

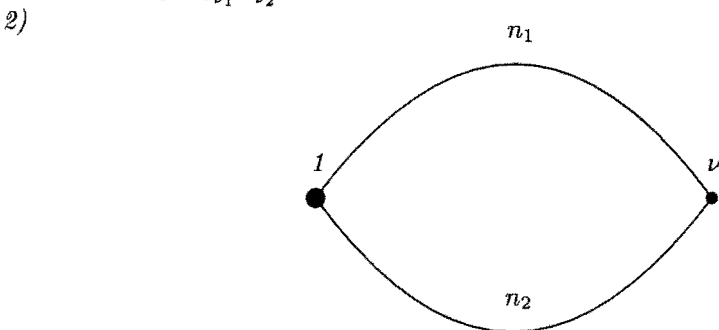
$$x_{n-d+1}^{-1} x_{n-2d+1}^{-1} \cdots x_{d+1}^{-1} x_1^{-1}.$$

□

THEOREM 3. *All shift automorphisms of finite order and geometric complexity 2 are realized by graph homeomorphisms whose quotients are of the following types.*

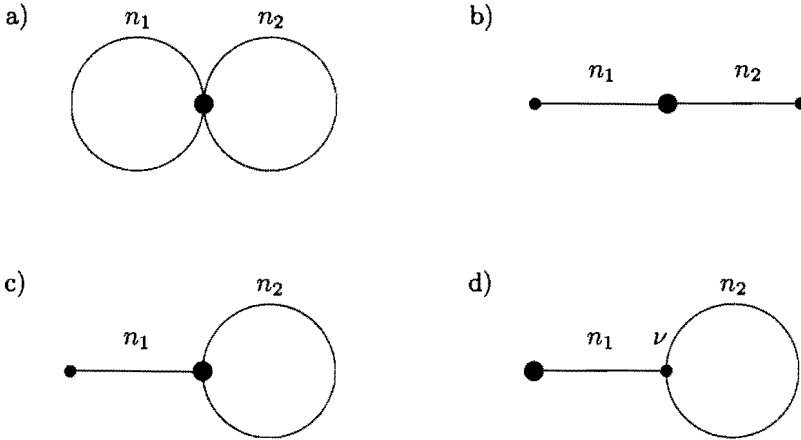


where $\gcd(\frac{n_1}{\nu_1}, \frac{n_2}{\nu_2}) = 1$.



where $\gcd(\frac{n_1}{\nu}, \frac{n_2}{\nu}) = 1$.

Proof: Besides the topological types of quotients described in the statement to the theorem, we have the following possibilities for two edge quotients (the placement of the basepoint being important).



The proof involves showing that none of these can be realized by shift automorphisms, and that for the types described in the theorem, shift automorphisms occur only when the given greatest common divisor conditions are satisfied. Cases a), b) and c) are easy to dispense with: in each case, the matrix associated with the natural basis is block diagonal with two blocks that are companion matrices. But a shift automorphism has such a representation with a single block—the uniqueness part of the rational canonical form theorem shows that these three cases are not shift automorphisms.

In case d), the corresponding matrix M_α is C_{p_1, p_2} or $C_{p_1, p_2, B}$ (notation as in Lemma 2 with $\nu = d$), depending on whether $\nu = 1$ or $\nu = d \neq 1$. In either case, Lemma 2 shows that M_α does not have a cyclic vector and so α is not a shift automorphism.

Now consider Case 1) of the theorem. Relative to the natural basis, we have

$$\chi_\alpha(t) = \left(\frac{t^{n_1} - 1}{t^{\nu_1} - 1} \right) \cdot \left(\frac{t^{n_2} - 1}{t^{\nu_2} - 1} \right) = p_1(t)p_2(t)$$

and

$$M_\alpha = \begin{pmatrix} C_{p_1} & B \\ 0 & C_{p_2} \end{pmatrix}$$

where $B = (0 \mid 0 \mid \cdots \mid c_B)$, c_B the column matrix with entries 1 in rows $1, \nu + 1, \dots, n_2 - \nu_1 + 1$ and 0 in the remaining positions. If $\gcd(\frac{n_1}{\nu_1}, \frac{n_2}{\nu_2}) \neq 1$, then Lemma 3 applies to show that α is not a shift automorphism. If, on the other hand, $\gcd(\frac{n_1}{\nu_1}, \frac{n_2}{\nu_2}) = 1$, then $x_1 = a_1 b_1 g^{\nu_2} (b_1^{-1} a_1^{-1})$ is a shift generator.

Now consider Case 2) of the theorem. Relative to the natural basis, we have

$$\chi_\alpha(t) = \left(\frac{t^{n_1} - 1}{t^{\nu_1} - 1} \right) (t^{n_2} - 1) = p_1(t)p_2(t)$$

and

$$M_\alpha = \begin{pmatrix} C_{p_1} & B \\ 0 & C_{p_2} \end{pmatrix}$$

where $B = (0 \mid 0 \mid \cdots \mid c_B)$, c_B the column matrix with entries 1 in rows $1, \nu + 1, \dots, n_2 - \nu_1 + 1$ and 0 in the remaining positions. In the case that $\gcd(\frac{n_1}{\nu_1}, \frac{n_2}{\nu_2}) \neq 1$,

then Lemma 2 applies to show that α is not a shift automorphism. If $\gcd(\frac{\nu_1}{\nu_1}, \frac{\nu_2}{\nu_2}) = 1$, then $x_1 = a_1 b_1^{-1}$ is a shift generator. \square

§5) Shift automorphisms of prime power order

From the remarks at the beginning of §3, we know that the polynomial $\chi(t)$ for a shift automorphism of finite order n is a product of distinct cyclotomic polynomials corresponding to divisors of n .

Example: Suppose α has order 20. Since the divisors of 20 are 1, 2, 4, 5, 10, 20 and

$$\begin{aligned} t^{20} - 1 &= c_1(t)c_2(t)c_4(t)c_5(t)c_{10}(t)c_{20}(t) \\ &= (t-1)(t+1)(t^2+1) \cdot \\ &\quad (t^4+t^3+t^2+t+1) \cdot \\ &\quad (t^4-t^3+t^2-t+1) \cdot \\ &\quad (t^8+t^6+t^4+t^2+1) \end{aligned}$$

$\chi_\alpha(t)$ will be a product of some subset of

$$\{c_1(t), c_2(t), c_4(t), c_5(t), c_{10}(t), c_{20}(t)\}.$$

Since α has order 20 and not some factor of 20, the set of subscripts has greatest common divisor 20.

The main results of this section are the following.

THEOREM 4. *There exists a shift automorphism α with $\chi_\alpha(t) = c_n(t)$ if and only if n is a power of a prime.*

THEOREM 5. *If α is a shift automorphism of order $n = p^m$, p a prime, then for some $k < m$,*

$$\chi_\alpha(t) = c_{p^{k+1}}(t) \cdots c_{p^m}(t),$$

the product of the top $m - k$ cyclotomic factors of $t^n - 1$. All such products are realized as characteristic polynomials of shift automorphisms of order n .

Note that

$$c_{p^{k+1}}(t) \cdots c_{p^m}(t) = \frac{t^{p^m} - 1}{t^{p^k} - 1} = 1 + t^{p^k} + t^{p^{2k}} + \cdots + t^{p^m - p^k}.$$

We begin with the following observation.

LEMMA 4. *If the shift automorphism α of finite order n is realized by the homeomorphism $g : \Gamma \rightarrow \Gamma$ (fixing the base point) and $\chi_\alpha(t)$ has ℓ irreducible factors, then $\Gamma/\langle g \rangle$ has at most ℓ edges. This is in particular the case if*

$$\chi_\alpha(t) = c_{d_1}(t)c_{d_2}(t) \cdots c_{d_\ell}(t)$$

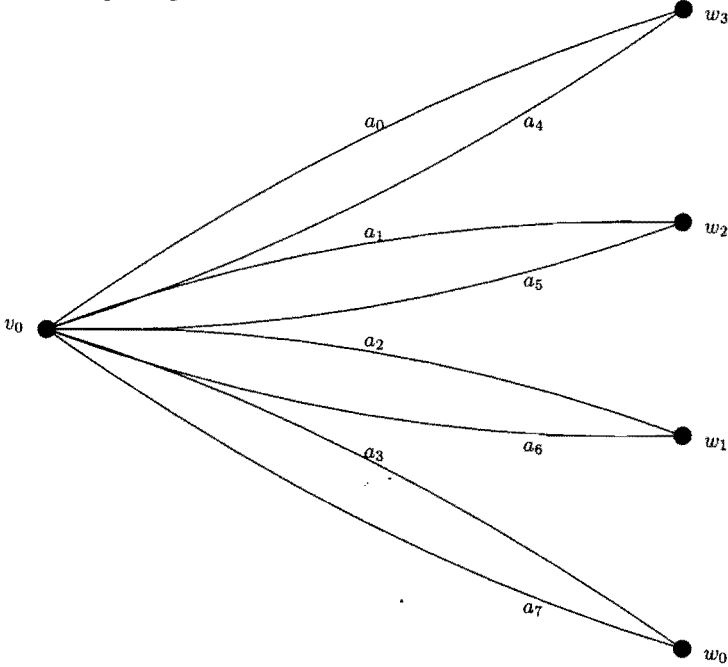
for divisors $\{d_1, \dots, d_\ell\}$ of n .

Proof: The representation of Theorem 1 shows that the matrix M_α is upper block triangular with one block for each edge of $\Gamma/\langle g \rangle$. Therefore the polynomial $\chi_\alpha(t)$ has a factorization with ℓ factors of degree 1 or more. The second part follows from the fact that cyclotomic polynomials are irreducible. \square

Proof of Theorem 4: Suppose $n = p^m$, p a prime: we describe explicitly a shift automorphism α with $\chi_\alpha(t) = c_{p^m}(t)$. Define Γ to be the graph, shown below for $n = 2^3$, with p^m directed edges $\{a_0, a_1, \dots, a_{p^m-1}\}$ all with initial vertex v_0 and $p^m - p^{m-1}$ terminal vertices $\{w_0, w_1, \dots, w_{p^m-p^{m-1}}\}$. Let g be the homeomorphism

$$g(v_0) = v_0, \quad g(w_i) = w_{i+1}, \quad g(a_i) = a_{i+1},$$

where the subscripts of the w 's are interpreted modulo $p^m - p^{m-1}$ and the subscripts of the a 's are interpreted modulo p^m . Let α be the induced automorphism of the free group of rank $p^m - p^{m-1}$.



It is straightforward to check the following.

- a) The automorphism α is a shift automorphism for which a shift generator is $x_1 = a_0 a_{p^{m-1}}^{-1}$; i.e., the set

$$S_{x_1} = \{x_1, \alpha(x_1), \dots, \alpha^{p^m - p^{m-1} - 1}(x_1)\}$$

is a basis for $F_{p^m - p^{m-1}}$.

- b) The corresponding shift representing word is

$$W_{(\alpha, x_1)} = x_1^{-1} x_{p^{m-1}+1}^{-1} x_{2p^{m-1}+1}^{-1} \cdots x_{(p-1)p^{m-1}+1}^{-1}.$$

- c) The characteristic polynomial of α is

$$\chi_\alpha(t) = t^{(p-1)(p^m-1)} + t^{(p-2)(p^m-1)} + \cdots + t^{p^m-1} + 1 = c_{p^m}(t).$$

(Recall that $c_{p^m}(t) = c_p(t^{p^{m-1}})$.)

For the converse, suppose

- $\alpha : F_r \rightarrow F_r$,
- $\alpha^n = id$,
- $\chi_\alpha(t) = c_n(t)$,
- α is induced by the homeomorphism $g : \Gamma \rightarrow \Gamma$.

By Lemma 4, the quotient $\Gamma/\langle g \rangle$ has one edge, and so is either a loop or a single edge. Furthermore, Γ has n edges which are permuted cyclically by g . By rank considerations, $r = \varphi(n)$ where $\varphi(n)$ is the Euler totient function (the degree of $\chi(t)$). It is easy to deal with the case of a loop: since the action of g must fix the base point, the fact that there is a single vertex orbit means that there is a single vertex. Thus Γ is a circle and the action of g is a cyclic permutation of the loops. Then $\chi_\alpha(t) = t^n - 1$.

Now suppose $\Gamma/\langle g \rangle$ is an edge with vertices \bar{v}_0 (the basepoint) and $\bar{w}_0 \neq \bar{v}_0$. The number of vertices in the orbit corresponding to \bar{w}_0 is d for some divisor of n ($d = \nu(\bar{w}_0)$ in the terminology of §2). A maximal tree in Γ thus has d edges and

$$r = \varphi(n) = n - d.$$

Thus $n - \varphi(n)$ is a divisor of n . The following simple claim finishes the proof of the theorem.

Claim: *The following are equivalent:*

- a) $n - \varphi(n)$ divides n ,
- b) n is a power of a prime.

Proof: If $n = p^r$, p a prime, then $n - \varphi(n) = p_1^{r-1}$ is a divisor of n .

For the reverse implication, it suffices to assume that n is square-free since the fraction $\frac{n}{n-\varphi(n)}$ does not depend on the exponents of the prime factors. Now

$$n = p_1 \cdots p_k \implies n - \varphi(n) = p_1 \cdots p_k - (p_1 - 1) \cdots (p_k - 1).$$

This is a divisor of n if and only if it equals a product, say $p_1 \dots p_\ell$, of the factors of n . This is equivalent to the equality

$$(*) \quad (p_1 - 1) \cdots (p_k - 1) = p_1 \cdots p_\ell (p_{\ell+1} \cdots p_k - 1).$$

But the first ℓ terms on the left are less than the first ℓ terms on the right, and for the remaining factors,

$$\begin{aligned} (p_{\ell+1} - 1) \cdots (p_k - 1) &< (p_{\ell+1}) \cdots (p_{k-1})(p_k - 1) \\ &= p_{\ell+1} \cdots p_k - p_{\ell+1} \cdots p_{k-1} < p_{\ell+1} \cdots p_k - 1. \end{aligned}$$

Thus equation (*) is impossible since the left-hand side is less than the right-hand side. □

This concludes the proof of Theorem 4. □

Proof of Theorem 5: Consider the graph Γ with a base point v_0 , a family of p^k vertices $\{w_0, w_1, \dots, w_{p^k-1}\}$ and a family of p^m edges $\{a_0, a_1, \dots, a_{p^m-1}\}$ with a homeomorphism $g: \Gamma \rightarrow \Gamma$ so that:

- a) the edge a_i joins v_0 to $w_{i'}$, where i' is the reduction of i modulo p^k ,
- b) $g(a_i) = a_{i+1}$, i considered modulo p^m ,
- c) $g(w_j) = w_{j+1}$, j considered modulo p^k ,

Then $x_1 = a_0 a_{p^k}^{-1}$ is a shift generator with representing word

$$W_{(\alpha, x_1)} = x_1^{-1} x_{p^k+1}^{-1} \cdots x_{p^m+1}^{-1}$$

and characteristic polynomial

$$\chi_\alpha(t) = \frac{t^{p^m} - 1}{t^{p^k} - 1}.$$

This proves the second part of Theorem 5.

Now suppose α is an automorphism of order p^m of a free group of rank r . Then since $\chi_\alpha(t)$ divides $t^{p^m} - 1$,

$$\chi_\alpha(t) = c_{p^{k_1}}(t)c_{p^{k_2}}(t) \cdots c_{p^{k_s}}(t)$$

for some $k_1 < k_2 < \cdots < k_s$. Furthermore, $k_s = p^m$ since α has order $n = p^m$ and not some lower power of p .

We need to show that if for some subscript i , $k_i + 1 < k_{i+1}$, then the matrix M_α does not have a cyclic vector and so can't be the matrix associated with a shift automorphism. The following fact about cyclotomic polynomials will be needed.

Claim: *Suppose p is a prime.*

- a) *Modulo p , $c_{p^m}(t)$ is a multiple of $c_p(t)c_{p^2}(t) \cdots (t)c_{p^{m-1}}(t) = \frac{t^{p^{m-1}} - 1}{t - 1}$.*
- b) *If $s < r$, then the matrix $c_{p^s}(C_{c_{p^r}(t)})$ is invertible as an integral matrix.*

Proof of Claim:

First note that

$$s^{p-1} + s^{p-2} + \cdots + s + 1 = (s - 1)(s^{p-2} + 2s^{p-3} + \cdots + (p-2)s + (p-1)) + p$$

so that $s - 1$ divides $s^{p-1} + s^{p-2} + \cdots + s + 1$ modulo p . Thus $t^{p^{m-1}} - 1$ divides $c_{p^m}(t) = t^{p^{m-1}(p-1)} + t^{p^{m-1}(p-2)} + \cdots + t^{p^{m-1}} + 1$ modulo p . But

$$t^{p^{m-1}} - 1 = (t - 1)c_{p^1}(t) \cdots c_{p^{m-1}}(t)$$

proving a).

Since $c_{p^s}(t)$ divides $t^{p^s} - 1$, it suffices to show that $C_{c_{p^r}(t)}^{p^s} - I$ is invertible: i.e., that 1 is not an eigenvalue of $C_{c_{p^r}(t)}^{p^s}$. But the p^s th powers of the primitive p^r th roots of 1 are all eigenvalues $C_{c_{p^r}(t)}^{p^s}$, each with multiplicity p^s . Since the number of them is the dimension of $C_{c_{p^r}(t)}^{p^s}$, 1 is not an eigenvalue. Thus $c_{p^s}(C_{c_{p^r}(t)})$ is invertible as a matrix over the field of rationals. But its determinant is ± 1 , so its inverse is integral. This establishes b). \square

Returning to the proof of Theorem 5, suppose α is represented by the graph homeomorphism $g : \Gamma \rightarrow \Gamma$. We show that if $\bar{\Gamma}$ has one edge, then the condition on the characteristic polynomial is satisfied and that it is not possible for $\bar{\Gamma}$ to have two or more edges for a shift automorphism of this type.

Case 1: If $\bar{\Gamma}$ has only one edge which is a loop (see Case 1 of Theorem 2), then

$$\chi_\alpha(t) = t^{p^m} - 1 = c_{p^0}(t)c_{p^1}(t) \cdots c_{p^m}(t)$$

with all powers appearing.

Case 2: If $\bar{\Gamma}$ has only one edge which is not a loop, and the vertex orbit other than the base point has only one vertex (see Case 2) of Theorem 2), then

$$\chi_\alpha(t) = \frac{t^{p^m} - 1}{t - 1} = c_{p^1}(t)c_{p^2}(t) \cdots c_{p^m}(t)$$

with all powers except the 0^{th} appearing.

Case 3: If $\bar{\Gamma}$ has only one edge and the vertex orbit other than the base point has more than one vertex (see Case 3) of Theorem 2), then

$$\chi_\alpha(t) = \frac{t^{p^m} - 1}{t^{p^k} - 1} = c_{p^{k+1}}(t)c_{p^{2(k+1)}}(t) \cdots c_{p^m}(t)$$

Case 4: If $\bar{\Gamma}$ has more than one edge, then it follows that M_α is similar to a matrix M'_α in upper block triangular form:

$$M'_\alpha = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}.$$

If the characteristic polynomial of A_i is $m_i(t)$, then $\chi_\alpha(t) = m_2(t)m_1(t)$. Therefore $\chi_\alpha(M'_\alpha) = m_2(M'_\alpha)m_1(M'_\alpha) = 0$ and

$$\begin{pmatrix} m_2(A_1) & B' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & B'' \\ 0 & m_1(A_2) \end{pmatrix} = \begin{pmatrix} 0 & m_2(A_1)B'' + B'm_1(A_2) \\ 0 & 0 \end{pmatrix} = 0.$$

Thus $m_2(A_1)B'' + B'm_1(A_2) = 0$. Now

$$m_1(t)m_2(t) = \chi_\alpha(t) = c_{p^{k_1}}(t)c_{p^{k_2}}(t) \cdots c_{p^m}(t),$$

so that $c_{p^m}(t)$ divides either $m_1(t)$ or $m_2(t)$ but not both. Suppose $c_{p^m}(t)$ divides $m_1(t)$ but not $m_2(t)$. Then $m_2(A_1)$ is invertible by part b) of the Claim and $m_1(A_2) = 0 \pmod{p}$ by part a) of the Claim. Thus $B'' = 0 \pmod{p}$. In this case, $m_1(M'_\alpha) = 0 \pmod{p}$, and the result follows from Lemma 1. A similar argument works if $c_{p^m}(t)$ divides $m_2(t)$ but not $m_1(t)$. □

§6) Two generator one relator groups

Observation: *The HNN extension H_w of F_n determined by the shift automorphism α_w is a two generator, one relator group; namely*

$$\begin{aligned} H_w &= \langle x_1, x_2, \dots, x_n, t \mid tx_it^{-1} = x_{i+1} \text{ for } 1 \leq i < n, tx_nt^{-1} = w \rangle \\ &\cong \langle x, t \mid t^n xt^{-n} = w(x_1, tx_1t^{-1}, \dots, t^{n-1}x_1t^{-(n-1)}) \rangle. \end{aligned}$$

Note that the total exponent of t in the relator is 0.

This observation raises the question as to which two generator one relator groups correspond to shift automorphisms. The following addresses this question.

Consider the group $G = \langle x, y \mid R \rangle$ and the swap that replaces x with $z = xy$. Then the total exponent vector of R changes by $(a, b) \rightarrow (a, b - a)$. Thus we can apply the Euclidean algorithm to the pair (a, b) repeatedly to get a pair $(d, 0)$ with associated changes on the groups that generate them. So we can assume that $G = \langle x, t \mid R \rangle$ where t has total exponent 0 in R . Now write

$$R = R'(t^{k_1}xt^{-k_1}, t^{k_2}xt^{-k_2}, \dots, t^{k_r}xt^{-k_r})$$

with $k_1 = \min(k_1, k_2, \dots, k_r)$ and $k_r = \max(k_1, k_2, \dots, k_r)$. Then

$$R = t^{k_1}R'(x, txt^{-1}, \dots, t^{k_r-k_1}xt^{-k_r+k_1})t^{-k_1}$$

and R can be replaced by its conjugate $R'(x, txt^{-1}, \dots, t^{k_r-k_1}xt^{-k_r+k_1})$. Then this presentation of G displays it as an appropriate H_w if x and $t^{k_r-k_1}xt^{-k_r+k_1}$ each appear exactly once in $R'(x, txt^{-1}, \dots, t^{k_r-k_1}xt^{-k_r+k_1})$.

THEOREM 6. *If α is a shift automorphism of finite order and geometric complexity 1, then the corresponding HNN extension is one of the following:*

$$i) \langle x, t \mid t^n x = xt^n \rangle, \quad ii) \langle x, t \mid x^k = t^n \rangle \quad \text{where } k \text{ divides } n.$$

Proof: Theorem 2 gives representatives for all such automorphisms for which the conversion to two-generator one-relator form is straight forward. Case 1 leads to $\langle x, t \mid t^n x = xt^n \rangle$ in which x is the first generator and t is the stable variable. Cases 2 and 3 lead to $\langle x, t \mid (t^\ell x^{-1})^k = t^n \rangle$, where $\ell = \nu$, $k = \frac{n}{\nu}$, x is the inverse of the first generator and t is the stable letter. (In case 2, $\nu = 1$.) Replacing the generating pair $\{x, t\}$ with $\{t^\ell x, t\}$ gives $\langle x, t \mid x^k = t^n \rangle$. \square

Examples:

- 1) *The HNN extension corresponding to a shift automorphism of complexity 1 and order 12 is one of the following:*

$$\begin{aligned} \langle x, t \mid x^2 = t^{12} \rangle, & \quad \langle x, t \mid x^3 = t^{12} \rangle, & \quad \langle x, t \mid x^4 = t^{12} \rangle, \\ \langle x, t \mid x^6 = t^{12} \rangle, & \quad \langle x, t \mid x^{12} = t^{12} \rangle, & \quad \langle x, t \mid t^{12}x = xt^{12} \rangle. \end{aligned}$$

These six groups are all different since their abelianizations have different orders of torsion.

- 2) *The HNN extension corresponding to a shift automorphism of complexity 1 and order 13 is one of the following:*

$$\langle x, t \mid x^{13} = t^{13} \rangle, \quad \langle x, t \mid t^{13}x = xt^{13} \rangle. \dots$$

Again these groups are different since their abelianizations have different torsion. This example follows easily from [DS].

References

- [BT] Baumslag, G. and Taylor, T. *The centre of groups with one defining relator*, Math. Annalen **175** (1968), 315-319.
- [Cu] Culler, M., *Finite groups of automorphisms of a free group*, Contemporary Math.: Contributions to group theory (Appel, K.I., Ratcliffe, J.G., Schupp, P.E. eds.), vol 33, (1984), 197-208.
- [DS] Dyer, J.L and Scott, G.P., *Periodic automorphisms of free groups* Comm. in Algebra **3** (1975), 195-201.
- [KPS] Karrass, A, Pietrowski, A. and Solitar, D. *Finitely generated groups with a free subgroup of finite index*, J. Austral. Math. Soc. **16** (1973), 458-466.
- [K] Krstić, S., *Actions of finite groups on graphs and related automorphisms of free groups*, J. Algebra **124** (1989), 119-138.
- [LS] Lyndon, R. and Schupp, P.E., *Combinatorial group theory*, Springer-Verlag, Berlin, 1977.

- [M] McCool, J. *A characterization of periodic automorphisms of a free group*, Trans. AMS **260** (1980), 309–318.
- [MKS] Magnus, W., Karrass, A. and Solitar, D., *Combinatorial group theory*, Wiley, New York, 1966.
- [S] Serre, J.P., *Trees*, Springer-Verlag, Berlin, 1980.

42 HARVEST RIDGE RD, SELKIRK, NY 12158

DEPT. OF MATH, UNIVERSITY AT ALBANY, ALBANY, NY 12222

E-mail address: `ted@math.albany.edu`