NORTH-HOLLAND

Cogrowth of Groups and a Matrix of Redheffer

Stephen P. Humphries
Department of Mathematics
Brigham Young University
Provo, Utah 84602

Submitted by Richard A. Brualdi

ABSTRACT

We describe a relationship between the cogrowth function (and other similarly defined functions) of a presentation of a torsion-free group and the Riemann hypothesis. This relationship is determined using a certain matrix of Redheffer. © 1997 Elsevier Science Inc.

1. INTRODUCTION

Let

$$1 \to N \to F \xrightarrow{\varphi} G \to 1 \tag{1.1}$$

be a presentation for the group G where $F = \langle a_1, \dots, a_n \rangle$ is a free group of rank n. We call n the *rank of the presentation.* Put

$$A = \{a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}\}.$$

For $g \in G$, $c \in A$ we let $W(k, g, c)$ be the set of words w in F having freely reduced length k, which end (on the right) in c and which represent the element g of G [i.e., $\varphi(w) = g$]. Let $w(k, g, c) = |W(k, g, c)|$. The function

$$\Gamma(k) = \sum_{c \in A} w(k, \mathrm{id}_G, c)$$

LINEAR ALGEBRA AND ITS APPLICATIONS 265:101–117 (1997)

0024-3795/97/\$17.00
PII S0024-3795(96)00593-9

will be called the *cogrowth function* for this presentation. In the paper [5] we showed how the cogrowth function is related to the group matrix and group determinant studied by Dedekind and Frobenius [4]. This also allowed us to calculate the cogrowth functions in many cases, including most finitely generated abelian groups.

In this paper we show that if one can find the cogrowth function for a presentation, then one can also find other such functions. For example, let C_k denote the words in N of length k which are cyclically reduced, are not periodic, and have no base point; let c_k denote the cardinality of C_k. Then putting

$$(\Gamma(k))_m = (\Gamma(1), \Gamma(2), \dots, \Gamma(m))^T \quad \text{and} \quad (c_k)_m = (c_1, c_2, \dots, c_m)^T,$$

we show that (in the case where G is torsion-free) there is an infinite integral matrix $\mathfrak{M}$ (depending only on the degree n) such that if $\mathfrak{M}_m$ denotes the $m \times m$ principal submatrix of $\mathfrak{M}$, then for all $m > 0$ we have

$$(\Gamma(k))_m = \mathfrak{M}_m (c_k)_m. \tag{1.2}$$

Our main result shows that information about these functions translates into information about the Riemann hypothesis: For any $m > 0$ let $\mathfrak{R}_m$ denote (the transpose of) Redheffer's matrix of size m. This is the $m \times m$ which has ij entry 1 if either $i = 1$ or $j | i$. $\mathfrak{R}$ will be the corresponding infinite matrix. According to [7, 8] the Riemann hypothesis is equivalent to

$$\det \mathfrak{R}_m = O(m^{1/2+\varepsilon}) \qquad \text{for every} \quad \varepsilon > 0.$$

For results on det $\mathfrak{R}_m$ see [1, 9] and references therein.

Write $\mathfrak{R}_m = \mathfrak{D}_m + \mathfrak{L}_m$, where $\mathfrak{D}_m$ is the $m \times m$ lower triangular *division matrix* (the ij position is 1 if $j | i$ and is 0 otherwise) and $\mathfrak{L}_m = \mathfrak{R}_m - \mathfrak{D}_m$ is an $m \times m$ rank 1 strictly upper triangular matrix. Then in the torsion-free case the relation with cogrowth is given by the fact that

$$\mathfrak{M}_m = \mathfrak{N}_m \mathfrak{D}_m \mathfrak{F}_m = \mathfrak{N}_m (\mathfrak{R}_m - \mathfrak{L}_m) \mathfrak{F}_m. \tag{1.3}$$

Here $\mathfrak{F}_m$ is the diagonal matrix diag$(1, 2, \dots, m)$, and $\mathfrak{N}_m$ is a yet to be defined integer matrix. What we do is find a sequence of cogrowth functions of presentations of infinite torsion-free abelian groups and put them all together to give matrices. Suppose that Q_j is a sequence of presentations for torsion-free groups G_j with the same rank. Let $\Gamma_j(k)$ be the cogrowth functions and $c_{j,k}$ the corresponding c_k's for the presentations Q_j. For an integer $m \geqslant 1$ let $(\Gamma_j(k))_m$ be the $m \times m$ matrix whose ij entry is $\Gamma_j(i)$ and similarly for $(c_{j,k})_m$. Then (1.2) and (1.3) give

$$\left(\Gamma_j(k)\right)_m = \mathfrak{M}_m\left(c_{j,k}\right)_m = \mathfrak{R}_m\left(\mathfrak{R}_m - \mathfrak{L}_m\right)\mathfrak{F}_m\left(c_{j,k}\right)_m. \tag{1.4}$$

Putting this all together, we have

THEOREM 1.1. *Let $\mathfrak{Z}_m = (\Gamma_j(k))_m$ and $\mathfrak{C}_k = (c_{j,k})_m$ be the matrices as above for presentations Q_j of torsion-free groups G_j with the same degree. Then the Riemann hypothesis is true if and only if*

$$\frac{1}{m!\det \mathfrak{C}_m}\det\left(\mathfrak{R}_m^{-1}\mathfrak{Z}_m + \mathfrak{L}_m\mathfrak{F}_m\mathfrak{C}_m\right) = O\left(m^{1/2+\varepsilon}\right) \qquad \text{for every} \quad \varepsilon > 0.$$

In Section 3 we reinterpret the matrices $\mathfrak{R}_m^{-1}\mathfrak{Z}_m$ and $\mathfrak{L}_m\mathfrak{F}_m\mathfrak{C}_m$, giving them combinatorial significance similar to the numbers $\Gamma_j(k)$ and $c_{j,k}$, and so obtain a different formulation of Theorem 1.1 (see Theorem 3.1).

Theorem 1.1 might not appear too interesting except for the fact that one can actually calculate some of these determinants in certain circumstances:

EXAMPLE 1.2. For $j \geqslant 1$ we let P_j be the presentation of the infinite cyclic group

$$1 \to N_j \to F_3 \xrightarrow{\varphi_j} \mathbb{Z} \to 1,$$

where $F_3 = \langle a, b, c\rangle$, which is determined by

$$\langle a, b, c \mid b = a^j,\ c\rangle,$$

so that $\varphi_j(a) = 1$, $\varphi_j(b) = j$, and $\varphi_j(c) = 0$. Let $\Gamma_j(k)$ be its cogrowth function. Then we show

THEOREM 1.3. *For P_j as above we have*

$$\left|\det\left(\Gamma_j(k)\right)_m\right| = 2^m \cdot m!$$

and

$$\left|\det\left(c_{j,k}\right)_m\right| = 2^m.$$

We note that it is possible (using similar ideas) to prove results like Theorem 1.3 for other sequences of presentations, e.g., $\langle a, b, c, d \mid b = a^j, c, d \rangle$ or $\langle a, b, c, d \mid b = a^j, c = a^j, d \rangle$.

We prove Theorem 1.1 in Section 3 after some preliminaries in Section 2. In Section 4 we show the relationship between the $\Gamma(k)$ and the c_k in the situation where the group G of (1.1) is not torsion-free. In Section 5 we indicate the connection with geodesics on certain surfaces associated to covers with covering group N. In Section 6 we prove Theorem 1.3.

2. PRELIMINARY DEFINITIONS AND RELATIONS

Fix a presentation (1.1) with free group F of rank n. All words referred to will belong to F, and their *length* will be the freely reduced length relative to the fixed generating set $A = \{a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}\}$. A word is *cyclically reduced* if it is freely reduced and its first and last letters are not inverses of each other. Sometimes we shall consider "cyclically reduced words without base point." This will refer to the set (equivalence class) of all the cyclically reduced conjugates of the word (cf. free geodesics on surfaces).

LEMMA 2.1. *If w is a cyclically reduced word in F, then w can be written as $w = u^a$ where u is a nonperiodic word; here the positive integer a is uniquely determined by w, and u is determined uniquely as a cyclically reduced word.*

Proof. Suppose $w = u^a = v^b$, where we may assume

(1) $a \geqslant b$, and u and v are cyclically reduced and are not proper powers; and

(2) either $a \neq b$ or u is not a cyclic permute of v.

Think of w as being written around the perimeter of a circle. Then $w = u^a$ means that this circle has a rotational symmetry, $r(a)$ say, of order a; while $w = v^b$ means that this circle also has a rotational symmetry, $r(b)$ say, of order b. Thus the group $\langle r(a), r(b) \rangle$ of rotational symmetries of w has order $c = \operatorname{lcm}(a, b)$ and is cyclic. If $c > a$, then u is a proper power and we have a contradiction; thus $c = a$. If $c = a > b$, then $b \mid a$ and so v is a proper power of a cyclic permute of u, another contradiction. Thus $a = b$, and the result follows. ∎

We will also need

LEMMA 2.2. *If w is a nontrivial, cyclically reduced word in F, then there are exactly $2n-2$ choices of $b \in A$ such that bwb^{-1} is freely reduced (as written) and, more generally, there are exactly $(2n-2)(2n-1)^{p-1}$ choices of $b_1, \ldots, b_p \in A$ such that $b_p \cdots b_1 w b_1^{-1} \cdots b_p^{-1}$ is freely reduced as written.*

DEFINITION 2.3. Let C_k denote the words in N of length k which are cyclically reduced, are not periodic, and have no base point.

Let P_k denote the words in N of length k which are cyclically reduced, are periodic, and have no base point. Let $P_{k,q}$ denote the words in P_k which have period q.

Let P_k' denote the words in N of length k which are cyclically reduced, are periodic, have no base point, and are proper powers of elements of $C_{k'}$ for some k'. Let $P_{k,q}'$ denote the words in P_k' which have period q.

Let P_k'' denote the words in N of length k which are cyclically reduced, are periodic, have no base point, and are not powers of elements of $C_{k'}$ for any k'. Let $P_{k,q}''$ denote the words in P_k'' which have period q.

Let E_k denote the words in N of length k which are cyclically reduced and which have no base point.

Let $\tilde{C}_k$, $\tilde{P}_k$, etc. denote the same sets except that the words now have a base point. Let c_k, p_k, $\tilde{c}_k$, $\tilde{p}_k$, etc. denote the cardinalities of C_k, P_k, $\tilde{C}_k$, $\tilde{P}_k$, etc.

Let $C_k(g)$, $\tilde{C}_k(g)$, $P_k(g)$, $\tilde{P}_k(g)$, etc. denote the same sets except that the words (in F) now represent the element $g \in G$.

Given these definitions, we have

LEMMA 2.4. *The following equations relate these variables:*

$$p_k = p_k' + p_k'',$$

$$p_{k,q} = p_{k,q}' + p_{k,q}'',$$

$$p_k = \sum_{\substack{q \mid k \\ q \neq k}} p_{k,q}' + p_{k,q}'',$$

$$p_{k,q}' = c_q \qquad \text{if} \quad q \mid k,$$

$$p'_k = \sum_{\substack{d|k \\ d \neq k}} c_d,$$

$$\tilde{p}'_{k,q} = qc_q \qquad \text{if} \quad q|k,$$

$$\tilde{p}_k = \sum_{\substack{q|k \\ q \neq k}} qp'_{k,q} + qp''_{k,q},$$

$$e_k = c_k + p_k,$$

$$\tilde{e}_k = \tilde{c}_k + \tilde{p}_k,$$

$$\tilde{c}_k = kc_k,$$

$$\tilde{p}'_k = \sum_{\substack{d|k \\ d \neq k}} dc_d.$$

By partitioning the set of all words in N of length k into four disjoint sets according as they are or are not periodic and cyclically reduced, one thus obtains

LEMMA 2.5.

$$\Gamma(k) = \tilde{c}_k + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \tilde{c}_m(2n-2)(2n-1)^{(k-m-2)/2} + \tilde{p}_k$$

$$+ \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \tilde{p}_m(2n-2)(2n-1)^{(k-m-2)/2}$$

$$= kc_k + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} mc_m(2n-2)(2n-1)^{(k-m-2)/2} + \sum_{\substack{d|k \\ d \neq k}} dc_d$$

$$+ \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \sum_{\substack{d|m \\ d \neq 1, m}} dc_d(2n-2)(2n-1)^{(k-m-2)/2} + \tilde{p}''_k$$

$$+ \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \tilde{p}''_m(2n-2)(2n-1)^{(k-m-2)/2}.$$

We write the above as $\Gamma(k) = Z_k + J_k$, where

$$Z_k = kc_k + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} mc_m(2n-2)(2n-1)^{(k-m-2)/2} + \sum_{\substack{d|k \\ d \neq k}} dc_d$$

$$+ \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \sum_{\substack{d|m \\ d \neq 1, m}} dc_d(2n-2)(2n-1)^{(k-m-2)/2}$$

and

$$J_k = \tilde{p}''_k + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \tilde{p}''_m(2n-2)(2n-1)^{(k-m-2)/2}. \tag{2.1}$$

LEMMA 2.5. *If G has no elements of finite order, then $\tilde{p}''_k = 0$ for all k and also $J_k = 0$ for all k. In particular, $\Gamma(k) = Z_k$ for all k.*

3. PROOF OF THEOREM 1.1

Let $\mathfrak{R}$ be the following infinite lower triangular matrix:

$$\begin{pmatrix}
1 & & & & & & & & & \\
0 & 1 & & & & & & & & \\
y & 0 & 1 & & & & & & & \\
0 & y & 0 & 1 & & & & & & \\
xy & 0 & y & 0 & 1 & & & & & \\
0 & xy & 0 & y & 0 & 1 & & & & \\
x^2y & 0 & xy & 0 & y & 0 & 1 & & & \\
0 & x^2y & 0 & xy & 0 & y & 0 & 1 & & \\
x^3y & 0 & x^2y & 0 & xy & 0 & y & 0 & 1 & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix},$$

where $y = 2n - 2$ and $x = 2n - 1$. Let $\mathfrak{R}_m$ be the principal $m \times m$ submatrix of $\mathfrak{R}$. Since $\mathfrak{R}$ is lower triangular, it is locally invertible, and in fact one easily sees that

$$\mathfrak{N}^{-1} = \begin{pmatrix} 1 \\ 0 & 1 \\ -y & 0 & 1 \\ 0 & -y & 0 & 1 \\ -y & 0 & -y & 0 & 1 \\ 0 & -y & 0 & -y & 0 & 1 \\ -y & 0 & -y & 0 & -y & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Thus from Lemma 2.5 we see that if $(c_q)_m = (c_1, \dots, c_m)$ and $(Z_q)_m = (Z_1, \dots, Z_m)$ are the corresponding m-vectors, then we have

$$\begin{aligned} (Z_q)_m &= \mathfrak{N}_m \mathfrak{D}_m \mathfrak{F}_m (c_q)_m \\ &= \mathfrak{N}_m (\mathfrak{R}_m - \mathfrak{L}_m) \mathfrak{F}_m (c_q)_m \\ &= \mathfrak{N}_m \mathfrak{R}_m \mathfrak{F}_m (c_q) - \mathfrak{N}_m \mathfrak{L}_m \mathfrak{F}_m (c_q)_m \end{aligned}$$

and so

$$\mathfrak{N}_m^{-1} (Z_q)_m = \mathfrak{R}_m \mathfrak{F}_m (c_q)_m - \mathfrak{L}_m \mathfrak{F}_m (c_q)_m.$$

Now if $G^{(j)}$, $j = 1, \dots,$ is a sequence of presentations for torsion-free groups having the same degree n, then we get $m \times m$ matrices

$$\mathfrak{Z}_m = \left(Z_q^{(j)}\right) \text{ and } \mathfrak{C}_m = \left(c_q^{(j)}\right), \qquad j,\, q = 1, \dots, m.$$

Thus

$$\mathfrak{R}_m \mathfrak{F}_m \mathfrak{C}_m = \mathfrak{N}_m^{-1} \mathfrak{Z}_m + \mathfrak{L}_m \mathfrak{F}_m \mathfrak{C}_m,$$

and so taking determinants gives

$$m! \det \mathfrak{R}_m \det \mathfrak{C}_m = \det\left(\mathfrak{N}_m^{-1} \mathfrak{Z}_m + \mathfrak{L}_m \mathfrak{F}_m \mathfrak{C}_m\right). \tag{3.1}$$

From (3.1) and Lemma 2.5 we get the proof of Theorem 1.1. ∎

Note that since G is torsion-free, Lemma 2.4 gives $\mathfrak{F}_m \mathfrak{C}_m = (\tilde{c}_q^{(j)})_m$ and $\mathfrak{R}_m^{-1} \mathfrak{Z}_m = \mathfrak{D}_m \mathfrak{F}_m \mathfrak{C}_m = (\tilde{e}_q^{(j)})_m$, and so Theorem 1.1 can also be stated as

THEOREM 3.1. *The Riemann hypothesis is true if and only if*

$$\frac{1}{m!\det \mathfrak{C}_m} \det\left[\left(\tilde{e}_q^{(j)}\right)_m + \mathfrak{L}_m\left(\tilde{c}_q^{(j)}\right)_m\right] = O(m^{1/2+\varepsilon}) \qquad \textit{for every} \quad \varepsilon > 0.$$

4. THE NON-TORSION-FREE CASE

We now consider J_k. We note that

$$p''_{k,q} = \sum_{\substack{g \in G \setminus \{\mathrm{id}\} \\ |g| = q}} c_{k/q}(g) \quad \text{and} \quad p''_k = \sum_{g \in G \setminus \{\mathrm{id}\}} \sum_{m|k} c_m(g),$$

where $|g|$ is the order of g and we recall that $c_m(g)$ is the number of cyclically reduced words of length m which represent g, are not periodic, and have no base point.

We will indicate how to proceed in the non-torsion-free case in the following:

EXAMPLE 4.1. We choose the presentation $\langle a, b | a^2, ab \rangle$ with $n = 2$; from (2.1) we see that $J_k = 0$ if k is odd and

$$J_k = \frac{k}{2} c_{k/2}(a') + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \frac{m}{2} c_{m/2}(a') 2 \times 3^{(k-m-2)/2}$$

if k is even, and so if $(J_q)_m = (J_1, J_2, \ldots, J_m)$ and $(c_q(a'))_m = (c_1(a'), c_2(a'), \ldots, c_m(a'))$ are the m-vectors, and

$$\mathfrak{S}_m = \begin{pmatrix} 0 & \cdots & & & & \\ 1 & 0 & \cdots & & & \\ 0 & 0 & \cdots & & & \\ 0 & 1 & 0 & \cdots & & \\ 0 & 0 & 0 & 0 & \cdots & \\ 0 & 0 & 1 & 0 & \cdots & \\ 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{pmatrix}$$

is an $m \times m$ matrix (the only nonzero entries being in the $(2i, i)$ positions), then

$$(J_q)_m = \mathfrak{R}_m \mathfrak{G}_m \mathfrak{D}_m \mathfrak{F}_m(c_q(a'))_m.$$

Here $a' = \varphi(a)$. Thus from Lemma 2.5 we get

$$(\Gamma(q))_m = \mathfrak{R}_m \mathfrak{D}_m \mathfrak{F}_m(c_q)_m + \mathfrak{R}_m \mathfrak{G}_m \mathfrak{D}_m \mathfrak{F}_m(c_q(a'))_m. \quad (4.1)$$

Now a similar argument to that used to calculate $\Gamma(k)$ (Lemma 2.5) allows us to find $\Gamma(k)(a')$. We first get relations

LEMMA 4.2.

$$p_k(a') = p'_k(a') + p''_k(a'),$$

$$p'_k(a') = 0,$$

$$p''_{k,q}(a') = \begin{cases} c_q(a') & \text{if } k/q \text{ is odd}, \\ 0 & \text{otherwise}, \end{cases}$$

$$p_k(a') = p''_k(a') = \sum_{\substack{q=1 \\ k/q \text{ odd}}}^{k-2} c_q(a'),$$

$$e_k(a') = c_k(a') + p_k(a').$$

This gives

LEMMA 4.3.

$$\Gamma(k)(a') = kc_k(a') + \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} mc_m(2n-2)(2n-1)^{(k-m-2)/2}$$
$$+ \sum_{\substack{d|k,\ d \neq k \\ k/d \text{ odd}}} dc_d(a')$$
$$+ \sum_{\substack{m=1 \\ m \equiv k \bmod 2}}^{k-2} \sum_{\substack{d|m,\ d \neq 1, m \\ m/d \text{ odd}}} dc_d(a')(2n-2)(2n-1)^{(k-m-2)/2}.$$

Lemma 4.3 then shows that

$$(\Gamma(q)(a'))_m = \mathfrak{R}_m(\mathfrak{I}_m - \mathfrak{G}_m)\mathfrak{D}_m\mathfrak{F}_m(c_q(a'))_m,$$

where $\mathfrak{I}_k$ is the $k \times k$ identity matrix, which in turn gives (since $\mathfrak{I}_k - \mathfrak{G}_k$ is invertible)

$$(c_q(a')) = \mathfrak{F}_k^{-1}\mathfrak{D}_k^{-1}(\mathfrak{I}_k - \mathfrak{G}_k)^{-1}\mathfrak{R}_k^{-1}(\Gamma(q)(a')).$$

Substituting for $(c_q(a'))$ in (4.1) now gives

$$(\Gamma(q)) = \mathfrak{R}_k\mathfrak{D}_k\mathfrak{F}_k(c_q) + \mathfrak{R}_k\mathfrak{G}_k(\mathfrak{I}_k - \mathfrak{G}_k)^{-1}\mathfrak{R}_k^{-1}(\Gamma(q)(a')),$$

from which we can find $(c_q)_m$ for the presentation $\langle a, b | a^2, a = b\rangle$; specifically this gives the sequence

1, 4, 18, 116, 810, 5880, 44,220, 341,484, 2,690,010, 21,522,228,

174,336,264, 1,426,403,748, 11,767,874,940, 97,764,009,000,

817,028,131,140, 6,863,037,256,208, ...,

where (starting at 0) we have only listed the even terms (the odd terms being 0).

One can do lots of other examples like this; however, the details are tedious and unenlightening to write down.

5. CONNECTION WITH GEODESICS ON SURFACES

We now represent the free group $F = \langle a_1, \dots, a_n\rangle$ in the presentation (1.1) as a Schottky group generated by hyperbolic elements, which we also call $a_1, \dots, a_n$ [2]; these generators give an action of F on hyperbolic space with fundamental domain a regular $2n$-gon with $2n$ vertices at infinity, as shown in Figure 1 for the case $n = 2$, where we draw the Poincare disc model for 2-dimensional hyperbolic space $\mathbf{H}^2$. In general we will have the n axes of the hyperbolic generators $a_1, \dots, a_n$ all crossing pairwise. See Figure 1, where $a = a_1$, $b = a_2$. In general the quotient surface $\mathbf{H}^2/F$ has genus $[n/2]$ and has one cusp point. The surface $\mathbf{H}^2/N$ is thus a cover of $\mathbf{H}^2/F$ with covering group $G = F/N$. For example for the presentation

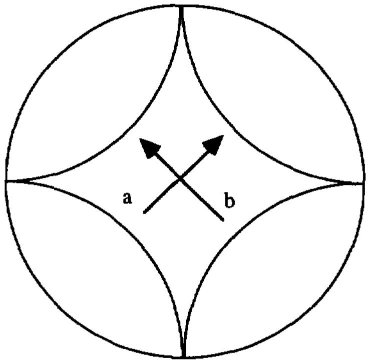

FIG. 1.

$\langle a, b \mid a^2, a = b \rangle$ considered above, the quotient $\mathbf{H}^2/N$ is a twice punctured torus. The presentation

$$\langle a_1, \ldots, a_n \mid a_1 = \cdots = a_n, a_1^2 \rangle$$

of C_2 gives a surface of genus $n - 1$ with two cusp points.

Consider an arbitrary presentation (1.1), and let v_k be the number of oriented geodesics of length k on the surface $\mathbf{H}^2/N$; here length is relative to the generators for the free group F. Now a closed geodesic on $\mathbf{H}^2/N$ is represented uniquely as a free homotopy class, which in turn is represented as a cyclically reduced word in N without base point; note that this word is not a proper power of an element of N. Conversely, any cyclically reduced word without base point in N which is not a proper power of a word in N determines a closed geodesic in $\mathbf{H}^2/N$.

Note that a closed geodesic is thus only represented by a periodic word $w = u^r$ if $\varphi(u) = g \in G$ where g has order r. Thus we have

LEMMA 5.1.

$$v_k = c_k(\mathrm{id}) + \sum_{g \in G \setminus \{\mathrm{id}\}} \sum_{\substack{q \mid k \\ |g| = k/q}} c_q(g) = \sum_{g \in G} \sum_{\substack{q \mid k \\ |g| = k/q}} c_q(g).$$

EXAMPLE 5.2. Lemma 5.1 now allows us to find v_k for the presentation $\langle a, b | a^2, a = b \rangle$; we get the sequence (starting at $k = 1$)

0, 8, 0, 18, 0, 124, 0, 810, 0, 5928, 0, 44,220, 0, 341,796, 0, 2,690,010, 0, 21,524,412, 0, 174,336,264, 0, 1,426,419,852, 0, 11,767,874,940, ...

6. PROOF OF THEOREM 1.3

Let

$$P_\infty = \langle a, b, c \mid ab = ba,\ c \rangle.$$

Then P_∞ is a presentation for $\mathbb{Z} \times \mathbb{Z}$. Let $\Gamma_\infty(k)$ be its cogrowth function. Note that for each k we have

$$\lim_{j \to \infty} \Gamma_j(k) = \Gamma_\infty(k).$$

Suppose that $\Gamma_\infty(k) = a_k$ for $k > 0$. Proposition 6.1 (below) shows that the infinite matrix $\mathfrak{Z} = (\Gamma_j(k))$, where j is the column index and k is the row index, has the form

$$\begin{pmatrix} a_1 & a_1 & a_1 & a_1 & a_1 & a_1 & \cdots \\ a_2+4 & a_2 & a_2 & a_2 & a_2 & a_2 & \cdots \\ * & a_3+6 & a_3 & a_3 & a_3 & a_3 & \cdots \\ * & * & a_4+8 & a_4 & a_4 & a_4 & \cdots \\ * & * & * & a_5+10 & a_5 & a_5 & \cdots \\ * & * & * & * & a_6+12 & a_6 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where $a_1 = 2$, $a_2 = 2$, $a_3 = 10$, $a_4 = 50$, etc. It is easily seen [by subtracting the $(m-1)$th row from the mth, then the $(m-2)$th row from the $(m-1)$th, etc.] that if this matrix is truncated to the principal $m \times m$ matrix $\mathfrak{Z}_m$, then $\det \mathfrak{Z}_m = (-1)^{m+1}\, 2 \times 4 \times 6 \times \cdots \times 2m$ and so we have proved Theorem 1.3.

PROPOSITION 6.1. *For all $k, j > 0$ we have*

(i) $\Gamma_j(k) = \Gamma_m(k)$ *if* $k \leqslant m, j$.
(ii) $\Gamma_j(j+1) = \Gamma_j(j) + 2(j+1)$.

Proof. (i): For $j \in \{1, 2, \ldots\} \cup \{\infty\}$ let $W_j(k)$ be the set of words in the kernel N_j of the presentation P_j of length k, so that $\Gamma_j(k) = \mathrm{card}(W_j(k))$. We prove (i) by showing that if $k \leqslant j$, then $W_j(k) = W_\infty(k)$.

Let $w \in W_j(k)$ have α letters equal to a, β letters equal to b, γ letters equal to c, α' letters equal to a^{-1}, β' letters equal to b^{-1}, and γ' letters equal to c^{-1}. We will show that $\alpha = \alpha'$ and $\beta = \beta'$, from which it follows that $w \in W_\infty(k)$. Then the nonnegative integers $\alpha, \beta, \dots$ satisfy

$$k = \alpha + \beta + \gamma + \alpha' + \beta' + \gamma', \tag{6.1}$$

$$\alpha + j\beta - \alpha' - j\beta' = 0. \tag{6.2}$$

Equation (6.1) comes from the fact that w has length k, while (6.2) comes from the fact that $w \in N_j$. Now replacing w by w^{-1} replaces α by α', α' by α, β by β', etc., and so with no loss of generality we may assume that $\beta \geqslant \beta'$. Note further from (6.2) that $\alpha = \alpha'$ if and only if $\beta = \beta'$. Thus we may now assume that $\beta > \beta'$, in order to get a contradiction. Solving (6.2) for α' and substituting into (6.1) gives

$$j \leqslant j(\beta - \beta') < j(\beta - \beta') + 2\alpha + \beta + \beta' + \gamma + \gamma' = k \leqslant j,$$

a contradiction. This proves (i).

(ii): We show that the only words in $W_j(j+1)$ that are not in $W_\infty(j+1)$ are the $2(j+1)$ words

$$a^r b a^s \quad \text{with} \quad r, s \leqslant 0 \text{ and } r + s = -j$$

and

$$a^r b^{-1} a^s \quad \text{with} \quad r, s \geqslant 0 \text{ and } r + s = j.$$

Let $w \in W_j(j+1)$ with α, β, etc. as above. Again we can, without loss, assume that $\beta \geqslant \beta'$. Then we have

$$j + 1 = \alpha + \beta + \gamma + \alpha' + \beta' + \gamma',$$

$$\alpha + j\beta - \alpha' - j\beta' = 0,$$

which gives

$$j(\beta - \beta') + 2\alpha + \beta + \beta' + \gamma + \gamma' = j + 1.$$

From this equation we see that if $\beta > \beta'$, then the only solution is

$$\beta = 1, \qquad \beta' = 0, \qquad \alpha = \gamma = \gamma' = 0, \quad \text{and} \quad \alpha' = j,$$

as required. If $\beta = \beta'$, then $\alpha = \alpha'$ and so $w \in W_\infty(j+1)$, as required. ∎

This completes the proof of Theorem 1.3.

We now indicate how to calculate the cogrowth function $\Gamma_j(k)$. For $j, m \geqslant 0$ we let $P_{j,m}$ be the presentation

$$1 \to N_{j,m} \to F_3 \to \mathbb{Z} \to 1,$$

where $F_3 = \langle a, b, c \rangle$, determined by

$$\langle a, b, c \mid b = a^j,\ a^m,\ c \rangle$$

of the infinite cyclic group $\mathbb{Z}$. Let $\Gamma_{j,m}(k)$ be its cogrowth function.

LEMMA 6.2. *Let $j, k > 0$; then for all $m \geqslant k$ we have*

$$\Gamma_{j,2m(j+1)}(k) = \Gamma_j(k).$$

Proof. Let $W_{j,m}(k)$ be the set of words in the kernel $N_{j,m}$ of the presentation $P_{j,m}$ of length k, so that $\Gamma_{j,m}(k) = \operatorname{card}(W_{j,m}(k))$. Let α, β, etc. be as in the proof of Proposition 6.1. Then we have the following two equations:

$$k = \alpha + \beta + \gamma + \alpha' + \beta' + \gamma', \tag{6.3}$$

$$\alpha + j\beta - \alpha' - j\beta' = [2m(j+1)]\,p \tag{6.4}$$

for some integer p. We aim to show that $p = 0$, from which the result will follow. Note that by (6.3) we see that

$$|\alpha|, |\beta|, |\alpha'|, |\beta'| \leqslant k.$$

Then by (6.4) we have

$$\begin{aligned} |2m(j+1)p| &= |\alpha + j\beta - \alpha' - j\beta'| \\ &\leqslant |\alpha| + j|\beta| + |\alpha'| + j|\beta'| \\ &< k + jk + k + jk \\ &= 2k(j+1) \\ &\leqslant 2m(j+1), \end{aligned}$$

which gives a contradiction if $p \neq 0$. ∎

We take the case $m = k$ of the above lemma in order to calculate $\Gamma_j(k) = \Gamma_{j,2k(j+1)}(k)$. Using the techniques used in [5] for calculating the cogrowth of infinite abelian groups (see [5, Theorem 1.2 and Section 5]), we get that $\Gamma_n(k)$ is equal to

$$\sum_{j=1}^{2k(n+1)} \frac{1}{5\sqrt{n_1}} \left[n_2^k - n_3^k - 2n_2^k \cos^2\left(\frac{nj\pi}{2k(n+1)}\right) \right.$$
$$-2n_3^k \cos^2\left(\frac{nj\pi}{2k(n+1)}\right) + 3n_3^k\sqrt{n_1} + 3n_2^k\sqrt{n_1}$$
$$\left. +2n_3^k \cos^2\left(\frac{j\pi}{2k(n+1)}\right) - 2n_2^k \cos^2\left(\frac{j\pi}{2k(n+1)}\right)\right], \tag{6.5}$$

where

$$n_1 = \cos^4\left(\frac{j\pi}{2k(n+1)}\right) - \cos^2\left(\frac{j\pi}{2k(n+1)}\right) - 1$$
$$+ 2\cos^2\left(\frac{j\pi}{2k(n+1)}\right)\cos^2\left(\frac{nj\pi}{2k(n+1)}\right)$$
$$- \cos^2\left(\frac{nj\pi}{2k(n+1)}\right) + \cos^4\left(\frac{nj\pi}{2k(n+1)}\right),$$
$$n_2 = 2\cos^2\left(\frac{j\pi}{2k(n+1)}\right) - 1 + \cos^2\left(\frac{nj\pi}{2k(n+1)}\right) - 2\sqrt{n_1},$$
$$n_3 = 2\cos^2\left(\frac{j\pi}{2k(n+1)}\right) - 1 + \cos^2\left(\frac{nj\pi}{2k(n+1)}\right) + 2\sqrt{n_1}.$$

We note that $n_1 = 0$ gives the trigonometric diophantine equation

$$\cos\left(\frac{j\pi}{2k(n+1)}\right) + \cos\left(\frac{nj\pi}{2k(n+1)}\right) + 1 = \pm\sqrt{5}$$

which has no solutions for integral j, k, and n by [6, Theorem 4], which is proved using results of Conway and Jones [3]. Thus $n_1 \neq 0$.

One can now expand the expression (6.5) as we did in similar examples in [5] to get $\Gamma_n(k)$ as a multisum of rational multiples of binomial coefficients.

REFERENCES

1 W. Barrett, R. Forcade, and A. Pollington, On the spectral radius of a (0, 1) matrix related to Merten's function, *Linear Algebra Appl.* 107:151–159 (1988).
2 A. Beardon, *On the Geometry of Discrete Groups*, Graduate Texts in Math. 91, Springer-Verlag.
3 J. H. Conway and A. J. Jones, Trigonometric diophantine equations (on vanishing sums of roots of unity), *Acta Arith.* XXX:229–240 (1976).
4 T. Hawkins, The origins of the theory of group characters, *Arch. Hist. Exact Sci.* 7:142–170 (1971).
5 S. P. Humphries, Cogrowth of groups and the Dedekind-Frobenius group determinant, *Math. Proc. Cambridge Philos. Soc.*, 121, (1997), pp. 193–217.
6 J. C. Parnami, M. K. Agrawal, and A. R. Rajwade, On some trigonometric diophantine equations of the type $\sqrt{n} = c_1 \cos \pi d_1 + \cdots + c_\lambda \cos \pi d_\lambda$, *Acta Math. Acad. Sci. Hungar.* 37:423–432 (1981).
7 R. M. Redheffer, Eine explizit lösbare Optimierungsaufgabe, *Internat. Schriftenreihe Numer. Math.* 36 (1977).
8 E. C. Titchmarsh, *The Theory of the Riemann Zeta Function*, Oxford U.P., Oxford, 1951.
9 R. C. Vaughan, On the eigen-values of Redheffer's matrix I, in *Number Theory with an Emphasis on the Markoff Spectrum* (A. Pollington and W. Moran, Eds.), Lecture Notes in Pure and Appl. Math. 147, Dekker, New York, 1993, pp. 283–296.

Received 3 October 1995; final manuscript accepted 10 October 1996