

Free Subgroups of the Free Product of Cyclic Groups

By W. W. Stothers

Abstract. Two kinds of recurrence relation for the number of subgroups of finite index in a free product of finitely many cyclic groups are given. An asymptotic formula is obtained from the first of these relations.

We consider nontrivial free products of finite and infinite cyclic groups. This class comprises Fuchsian groups of genus zero which have parabolic elements, and the special case $C_2 * C_2$. It is known that such a group has free subgroups (i.e. subgroups which are free products of copies of C_∞); see [2]. When the group itself is free, all subgroups are free, and Hall, [3], has given a formula in the general case. We obtain the formula for the other cases, obtaining an asymptotic estimate in each case. Finally, we consider (formal) generating functions, and indicate the existence of another recurrence relation. For the simplest cases, we give the relations explicitly.

To avoid complicated notation, we consider a fixed group $G = C_{p_1} * C_{p_2} * \dots * C_{p_m}$, with $m \geq 2$, and each p_i is an integer (≥ 2) or is ∞ . We assume that p_1, \dots, p_s are finite, and the rest infinite. Unless $m = p_1 = p_2 = 2$, G is Fuchsian, and has hyperbolic measure (proportional to)

$$(1) \quad H = m - s - 1 + \sum_{i=1}^s (1 - p_i^{-1}).$$

This appears in our calculations.

1. The Recurrence Relation. To obtain all the subgroups, we use coset diagrams, defined in the following manner. We pick m distinct colors, c_1, \dots, c_m . A *diagram of order n* consists of n labelled vertices, together with colored, directed edges (including loops) such that:

- (a) each vertex has one edge of color c_i entering and one leaving ($i = 1, \dots, m$),
- (b) for $1 \leq i \leq s$, the edges of color c_i form polygons whose sizes each divide p_i ,
- (c) the entire diagram is connected.

For $1 \leq i \leq s$, a polygon with less than p_i sides is *degenerate*. We select one label (vertex) of a diagram as *special*. There is an equivalence relation among diagrams of order n obtained by permuting the nonspecial labels on the vertices. We have an obvious result:

PROPOSITION 1.1. *An equivalence class of diagrams of order n has $(n - 1)!$ members.*

By considering the effect of the generators of G on cosets of a subgroup of

Received September 14, 1977.

AMS (MOS) subject classifications (1970). Primary 20E30; Secondary 20H10, 10D05.

Copyright © 1978, American Mathematical Society

index n , and observing that an element of finite order in a subgroup will be the conjugate of a power of a generator.

THEOREM 1.2.(i) *There is a 1-1 correspondence between subgroups of index n in G and equivalence classes of diagrams of order n .*

(ii) *The free subgroups of index n correspond to the diagrams of order n with no degenerate polygons of any color.*

It is easy to refine the technique to describe all subgroups in more detail. Indeed, by using another color, we can include an account of the hyperbolic measure of the subgroup in the Fuchsian cases; see [7].

If $s \geq 1$, let d be the l.c.m. of p_1, \dots, p_s , and put $e_i = d/p_i$. When $s = 0$, we put $d = 1$.

COROLLARY 1.3. *If G has a free subgroup of index n , then $d|n$.*

PROOF. There is no problem if $s = 0$. If $s \geq 1$, the diagram must consist of complete p_i -gons, so that $p_i|d$. This holds for $1 \leq i \leq s$.

Let $M(n)$ be the number of free subgroups of index n in G .

We make the following definitions:

$$a_i(kd) = (kd)!/p_i^{ke_i}(ke_i)!, \quad i = 1, \dots, s,$$

and

$$a_i(kd) = (kd)!, \quad i > s.$$

For $1 \leq i \leq s$, $a_i(kd)$ gives the number of ways of joining kd vertices into nondegenerate p_i -gons. We also put

$$A(kd) = \left\{ \prod_{i=1}^m a_i(kd) \right\} / (kd)!$$

and

$$B(kd) = \prod_{i=2}^m a_i(kd).$$

THEOREM 1.4. *For $k \geq 1$,*

$$M(kd) = kdA(kd) - \sum_{j=1}^{k-1} A(jd)M((k-j)d).$$

Proof. Suppose that $s \geq 1$. We use the first kd integers as labels, with 1 as the special label. For a given set of ke_1 labelled, directed p_1 -gons, let $T(kd)$ be the number of diagrams of order kd which include these as the polygons of color c_1 . It is clear that

$$(2) \quad (kd - 1)!M(kd) = a_1(kd)T(kd).$$

If we take a fixed collection of p_1 -gons as above, then we can add polygons of the other colors in $B(kd)$ ways, respecting conditions (a) and (b) and with no degenerate polygons. The connected component which includes the vertex '1' will be a diagram

of order jd , with $1 \leq j \leq k$. A simple count now yields

$$(3) \quad T(kd) = B(kd) - \sum_{j=1}^{k-1} \binom{ke_1 - 1}{je_1} B(jd)T((k-j)d).$$

The result follows at once. If $s = 0$, the proof is similar but easier.

Note that the sum is void when $k = 1$, so that we have

COROLLARY 1.5. *G has a free subgroup of index d.*

Also, $kdA(kd)$ is an upper bound for $M(kd)$. By using this estimate in the sum on the left in 1.4, we obtain

COROLLARY 1.6.

$$kdA(kd) \geq M(kd) \geq kdA(kd) \left\{ 1 - \frac{1}{2} \sum_{j=1}^{k-1} \frac{A(jd)A((k-j)d)}{A(kd)} \right\}.$$

We note that the relation in 1.4 was obtained in a different way by Dey. It is referred to in [1], though not stated there.

2. The Asymptotic Formula. After Corollary 1.6, it is evident that we must find an upper bound for the sum

$$S(k) = \sum_{j=1}^{k-1} A(jd)A((k-j)d)/A(kd) = \sum_{j=1}^{k-1} b(j, k), \quad \text{say.}$$

LEMMA 2.1. *For $j \leq \frac{1}{2}(k-1)$, $b(j, k) \geq b(j+1, k)$.*

Proof. From the definitions,

$$(4) \quad \frac{b(j, k)}{b(j+1, k)} = \left\{ \frac{((k-j-1)d+1) \cdots ((k-j)d)}{(jd+1) \cdots ((j+1)d)} \right\}^{m-1} \cdot \prod_{i=1}^s \left\{ \frac{(je_i+1) \cdots ((j+1)e_i)}{((k-j-1)e_i+1) \cdots ((k-j)e_i)} \right\}.$$

Considerable simplification is possible since, for $r \leq e_i$,

$$\frac{(k-j-1)d + p_1 r}{jd + p_1 r} \cdot \frac{je_i + r}{(k-j-1)e_i + r} \geq 1.$$

Thus, the left-hand side of (4) is greater than one if $m > s$. When $m = s$, we can pair $m - 2$ factors from the first product on the right with the last $m - 2$ from the second product. Thus, it is enough to consider $m = s = 2$.

In this case, we can cancel all the e_1 terms as above. For the rest, either an e_2 term cancels or we can use the inequality,

$$\frac{(k-j-1)d + p_2 r - 1}{jd + p_2 r - 1} \cdot \frac{je_2 + r}{(k-j-1)e_2 + r} \geq 1,$$

which holds since $j \leq \frac{1}{2}(k-1)$. This always works since a term in the product involving d cannot cancel if it is adjacent to another which does cancel (recall that p_1 and p_2 are at least 2).

LEMMA 2.2. For $a = 1, 2$, and $k > a$, $b(a, k) = O(k^{-adH})$.

Proof. Applying (4) with $j = 0$, we get an upper bound for $b(1, k)$ by replacing $(k - 1)d + r$ by $(k - 1)d$, and $(k - 1)e_i + r$ by ke_i . Thus, there are constants K, K' with

$$b(1, k) \leq K \frac{k^{\sum e_i}}{(k - 1)^{d(m-1)}} \leq K' k^{-(d(m-1) - \sum e_i)} = K' k^{-dH}.$$

Another application gives the result for $a = 2$.

We observe that, as $p_i | d$ for each i , dH will be a positive integer unless $G = C_2 * C_2$. We treat this case separately below.

THEOREM 2.3. If $G \neq C_2 * C_2$, then there is a constant C such that

$$kdA(kd) \geq M(kd) \geq kdA(kd)\{1 - Ck^{-dH}\}.$$

Proof. By 2.1,

$$S(k) \leq 2b(1, k) + (k - 3)b(2, k).$$

By 2.2 and the observation immediately before the theorem,

$$(k - 3)b(2, k) = O(k^{1-2dH}) = O(k^{-dH}).$$

The result follows.

All of the factorials which appear in the definition of $A(kd)$ involve integers at least as large as k . Hence, we can apply Stirling's formula to obtain an asymptotic formula in more familiar terms, viz.

$$(5) \quad M(kd) \sim \frac{1}{2\pi} \left\{ \frac{(p_1 \cdots p_s)(2\pi kd)^{m-s}}{H} \right\}^{1/2} \frac{(kdH)!}{H^{kdH}}.$$

As an example, we consider the classical modular group, $C_2 * C_3$. Here, $m = s = 2$, $p_1 = 2, p_2 = 3$, so that $d = 6$ and $H = 1/6$. Now, (5) is

$$M(6k) = \frac{3}{\pi} 6^k k! \{1 + O(k^{-1})\}.$$

It requires a little thought to see that (5) is equivalent to the result for a free group obtained in [5]. As a comparison, the total number of subgroups in the nonfree cases (denoted by M_n), is rather greater. For the modular group, we have

$$M_{6k} = \frac{1}{2\pi e^{1/4}} 6^k k! \exp((6k)^{1/2} + (6k)^{1/3}) \{1 + O(k^{-1/6})\}.$$

The principal term is given in [5], the error term is implicit in [4].

Now assume that $G = C_2 * C_2$. The diagram for a free subgroup of index $2k$ in G will have $2k$ vertices and k distinct 2-gons of each of the two colors. If we replace each 2-gon by an uncolored edge, we obtain a figure in which each vertex has degree 2 (by (a)). It will be connected (by (c)), and so consists of a single cycle. The original diagram must have 2-gons of alternate colors (again by (a)), so that there

is precisely one unlabelled diagram. As all vertices are similarly situated, there is one equivalence class of diagrams of order $2k$ for each integer k , i.e. $M(2k) = 1$. In this case, $A(2j) = (2j)!/2^{2j}(j!)^2$, so that Theorem 1.4 yields the identity:

$$\sum_{j=0}^k (2j)!/2^{2j}(j!)^2 = (2k + 1)!/2^{2k}(k!)^2.$$

3. The Second Relation. For the modular group, diagrams were used in [6] to obtain a different recurrence relation connecting the $M(6k)$ (see Proposition 1.8).

Proceeding in a formal way, we shall show that there is an analogue of this result for each G , but that the result is a lot less elegant except in some special cases.

We put

$$f(x) = \sum_{k=0}^{\infty} A(kd)e^{kdx}, \quad g(x) = \sum_{k=1}^{\infty} M(kd)e^{kdx}.$$

Theorem 1.4 can be restated as

$$(6) \quad f'(x) = f(x)g(x).$$

Directly from the definition,

$$(7) \quad \left\{ \prod_{i=1}^s p_i^{e_i} (ke_i + 1) \cdots ((k + 1)e_i) \right\} A((k + 1)d) \\ = \{(kd + 1) \cdots ((k + 1)d)\}^{m-1} A(kd).$$

We imagine that all possible cancellation has been carried out, except that, when $m > s$, we leave a factor $k + 1$ on each side, we have

$$(8) \quad e^{-dx} P(D) \cdot Df(x) = Q(D)f(x),$$

where D is the operator d/dx , and $P(X), Q(X) \in \mathbf{Z}[X]$. It is to avoid problems at the origin that we make the change for $m > s$. Using (6), $f^{(n)}(x)$ is equal to $f(x)$ multiplied by a polynomial in $g(x), g'(x), \dots, g^{(n-1)}(x)$. Thus, (8) yields a relation involving $g(x)$ and its derivatives. On expanding in powers of e^x , we obtain a relation involving the $M(kd)$. In general, there does not seem to be a nice form for the relation, a direct approach involves partial Bell polynomials and Stirling numbers of the second kind.

To get an idea of the nature of the relation, we must consider the amount of cancellation in (7). If $m = s$, there are more $(k + 1)$ factors on the left than on the right, so complete cancellation is never possible. If $m > s$, then we must leave a factor $(k + 1)$ on each side. Thus, in either case, $Q(X)$ has degree at least $d(m - 1) - \sum e_i + 1 = dH + 1$. If $Q(X)$ has degree n , then the right-hand side of (8) will involve $f^{(n)}(x)$, but no higher derivatives. A simple argument shows that the equation obtained in derivatives of $g(x)$ will involve a term in $g^n(x)$, so that the relation contains an $(n - 1)$ -fold sum.

We will obtain a relatively simple relation only when $dH = 1$. We note that $dH =$

$d(m - 1) - \sum e_i$, and that $e_i \leq \frac{1}{2}d$, with equality only if $p_i = 2$. Thus, for $s = 0, d = 1$, and the only interesting case is $m = 2$, i.e. $C_\infty * C_\infty$. For $m > s > 0, dH \geq d(m - 1 - \frac{1}{2}s)$, so we have only $C_2 * C_\infty$ to consider. For $m = s, dH \geq d(\frac{1}{2}m - 1)$, so we must have $m \leq 3$. If $m = 3$, we must also have $d = 2$, so each p_i is 2, i.e. $C_2 * C_2 * C_2$. If $m = 2, dH = d - e_1 - e_2 = e_1(p_1 - 1) - e_2$. We might as well assume that $e_1 \geq e_2$, so we must have $p_1 \leq 3$. If $p_1 = 3$, then $e_1 = 1$, so we have $C_3 * C_3$. If $p_1 = 2, dH = e_1 - e_2$ and $d = 2e_1 = p_2e_2$, so that $p_2 \leq 4$, and we have the cases $C_2 * C_2, C_2 * C_3, C_2 * C_4$.

Except for $C_2 * C_2$, the relation is of the following form

$$(9) \quad M(kd) = a(k)M((k - 1)d) - \sum_{j=1}^{k-2} M(jd)M((k - j - 1)d),$$

with $a(k) = k + 1$ for $C_\infty * C_\infty, 2k + 1$ for $C_2 * C_\infty$, and dk for the other cases.

As usual, the situation for $C_2 * C_2$ is simpler. We have $f(x) = (1 - e^{2x})^{-\frac{1}{2}}$, and $g(x) = e^{2x}(1 - e^{2x})^{-1}$. The analogue of (9) is, of course, $M(2k) = M(2(k - 1)) (= 1)$.

As in [6], there are combinatorial arguments leading to (9). For example, for $G = C_2 * C_4$, we can get a relation for the $T(kd)$ by considering the number of diagrams with one square having a distinguished pair of vertices. The square can be removed, and the attached 2-gons repaired in an obvious way. From the relation with the $T(kd)$, we obtain one for the $M(kd)$ by using (2).

It seems reasonable to expect that there will be similar arguments for all groups, even when the result is more complicated than (9).

4. The Group $C_2 * C_2$. For $k \geq 0$, and p positive or infinite, let $\tau_p(k)$ be the number of homomorphisms from C_p to S_k , the symmetric group on k symbols. It is easy to adapt the proof of Theorem 1.4 to obtain a recurrence relation involving M_n and the relevant $\tau_{p_i}(k)$, see [5, (1), (12)]. For $C_2 * C_2$, we put $\alpha(k) = (\tau_2(k))^2/k!$. The relation is

$$(10) \quad k\alpha(k) = \sum_{j=0}^{k-1} \alpha(j)M_{k-j}.$$

In [5], the relations were used to estimate M_k , except in the present case. For $C_2 * C_2$, an appeal to the diagrams is effective:

PROPOSITION 4.1. For $k \geq 1$,

$$M_k = \begin{cases} k, & k \text{ odd,} \\ k + 1, & k \text{ even.} \end{cases}$$

Proof. As at the end of §2, a diagram for $C_2 * C_2$, which may now have degenerate polygons, i.e. loops, leads to a connected, 2-colorable graph of order k with each vertex of degree at most 2.

Ignoring colorability, such a graph must consist of a single cycle, or a single unbranched chain. For 2-colorability, the former arises only for k even. In this case,

exactly as before, we have one subgroup. In the case of a chain, there is one coloring if k is odd, and two if k is even. In the latter case, there is an obvious symmetry of order two. Thus, in either case, we get k subgroups from the chain graph. The result follows.

We put

$$F(x) = \sum_{k \geq 0} \alpha(k)e^{kx}, \quad G(x) = \sum_{k \geq 1} M_k e^{kx}.$$

By 4.1,

$$G(x) = \frac{e^x}{(1 - e^x)^2} + \frac{e^{2x}}{(1 - e^{2x})}.$$

By (10), $F'(x) = F(x)G(x)$, so that

$$(11) \quad F(x) = (1 - e^{2x})^{-1/2} \exp \left\{ \frac{e^x}{1 - e^x} \right\}.$$

Now, (11) can be used to obtain recurrence relations for the $\alpha(k)$. The most straightforward seems to be

$$(12) \quad \alpha(n) = \alpha(n - 1) + \alpha(n - 2) - \left(\frac{n - 2}{n} \right) \alpha(n - 3).$$

There do not appear to be relations for the " $\alpha(n)$ " for other groups, though there are more complex ones involving m th powers.

Finally, we note that, while we should expect a combinatorial argument for (12), none appears obvious.

Department of Mathematics
University Gardens
University of Glasgow
Glasgow G12 8QW, Scotland

1. I. M. S. DEY, "Schreier systems in free products," *Proc. Glasgow Math. Assoc.*, v. 7, 1967, pp. 61–79. MR 32 #5718.
2. R. H. FOX, "On Fenchel's conjecture about F -groups," *Mat. Tidsskr. B*, v. 1952, pp. 61–65. MR 14, 843.
3. M. HALL, JR., "Subgroups of finite index in free groups," *Canad. J. Math.*, v. 1, 1949, pp. 187–190. MR 10, 506.
4. L. MOSER & M. WYMAN, "Asymptotic expansions," *Canad. J. Math.*, v. 8, 1956, pp. 225–233. MR 19, 268.
5. M. NEWMAN, "Asymptotic formulas related to free products of cyclic groups," *Math. Comp.*, v. 30, 1976, pp. 838–846.
6. W. W. STOTHERS, "The number of subgroups of given index in the modular group," *Proc. Roy. Soc. Edinburgh*, v. 78A, 1977, pp. 105–112.
7. W. W. STOTHERS, "Subgroups of infinite index in the modular group," *Glasgow Math. J.*, v. 19, 1978, pp. 33–43.