THE PROBABILITY OF GENERATING A FREE PRODUCT OF FINITE GROUPS

Nigel Boston

Department of Mathematics and CSL, University of Illinois, Urbana, IL 61801

0. Introduction.

A consequence of the Grushko-Neumann theorem is that if $H_1$ and $H_2$ are finite groups, then the free product $H = H_1 \ast H_2$ satisfies $d(H) = d(H_1) + d(H_2)$, where $d(G)$ denotes the minimal number of generators of a group $G$. Ribes and Wong [13] asked whether this holds in the category of profinite groups (in which case $H_1 \ast H_2$ is the profinite completion of the usual free product and $d(G)$ refers to topological generators). They showed that this is indeed the case if (and only if) the following fundamental question always has a positive answer. Given two finite groups, $H_1$ and $H_2$, is there a finite group $G$ containing and generated by them such that $d(G) = d(H_1) + d(H_2)$?

In [8] and [9], Lucchini shows that this sometimes fails. He does not obtain the best possible bound, which would be to show that if $G$ is a finite group generated by $s$ $r$-generated subgroups of pairwise coprime orders, then $d(G) \leq r + s - 1$. From this it follows that the corresponding free profinite product is $r + s - 1$-generated. This had been established in the prosolvable category by Kovács and Sim [5] (see also [7]), but was only conjectured in the general category.

In particular, if we let $m = \max(d(H_1), d(H_2))$, then we obtain a modified conjecture, that if $H_1$ and $H_2$ are finite groups of coprime order, then every finite group $G$ containing and generated by them satisfies $d(G) \leq m + 1$. Moreover, that there is indeed such a group $G$ with exactly $m + 1$ generators.

In this paper, we adopt an alternative approach, employing the probabilistic zeta function [1], [12]. We seek to describe $P(H_1 \ast H_2, s)$ for any given finite groups $H_1, H_2$. This typically does not converge for any value of $s$ but it can be handled as a formal Dirichlet series with a factorization into generalized Euler factors [1], say $P(H_1 \ast H_2, s) = F_1(s)^{r_1}F_2(s)^{r_2}...$. Our aim is to identify which terms arise in this factorization (also, their multiplicity, although that is less important).

The modified conjecture is then equivalent simply to: $F_i(m + 1) > 0$ for all generalized Euler factors of $P(H_1 \ast H_2, s)$. Moreover, $F_i(m) = 0$ for at least one generalized Euler factor. Below, we establish these for factors of a certain quotient

The author thanks Andrea Lucchini for generously sharing his preprints. He was partially supported by DMS 99-70184.
of $H_1 * H_2$ (the maximal metabelian quotient if $H_1$ and $H_2$ are abelian) and give some results for more general quotients.

1. Probabilistic zeta functions

In this section, we summarize the main results regarding probabilistic zeta functions. If $G$ is a profinite group (so in particular a finite group), then in [1], [12] a Dirichlet series $P(G, s)$ is defined which equals the measure of the subset of $G^s$ consisting of $s$-tuples (topologically) generating $G$. For certain groups $G$ this can be identically zero, whereas for other groups (the PFG groups) this is nonzero for some $s \in \mathbb{Z}^+$. As noted in [12], if $H_1$ and $H_2$ are nontrivial finite groups, one of which has order $> 2$, then $H_1 * H_2$ is not PFG. It is also noted, however, that finitely generated prosolvable groups are always PFG.

In all cases that $G$ is finitely generated, a formal Dirichlet series $P(G, s)$ can be defined as $\sum \mu(H)[G : H]^{-s}$ over all open subgroups of $G$, since there are finitely many such subgroups of any given index. Here, $\mu(H)$ denotes the Moebius function of the lattice of open subgroups of $G$, defined by $\sum_{H \geq K} \mu(H) = 0$ unless $K = G$, in which case the sum is 1. This formula gives $P(G, s)$ correctly in the cases when $G$ is PFG, and is also the limit of $P(G/N, s)$ for $G/N$ running over the finite quotients of $G$.

As explained in [1], $P(G, s)$ has a factorization into generalized Euler factors, corresponding to chief factors of $G$. In the case of $G$ prosolvable, these are of the form $1 - k p^{-s}$, where the chief factor is elementary abelian of order $p^n$. All such factors are known. For nonsolvable chief factors, i.e. isomorphic to $S^n$ for some nonabelian simple group $S$, certain possible Euler factors have been identified (see e.g. the calculation of $P(S^n, s)$ in [1] and of factors of $P(L_4, s)$ in [3]), but it is not known if this constitutes a complete list of possible Euler factors. In any case, there seems to be a short list of possibilities, which encourages us in the aim of this paper.

What is that aim? Let $\Sigma$ denote the set of Euler factors and $\Sigma_0$ denote the set of Euler factors corresponding to solvable chief factors. Let $H_1$ and $H_2$ be finite groups. We wish to identify those elements of $\Sigma$ (respectively $\Sigma_0$) that occur as factors of $P(H_1 * H_2, s)$ (respectively $P(G, s)$ with $G$ the maximal prosolvable quotient of $H_1 * H_2$). We will also find information on the multiplicities to which these terms arise. The former question is the more important one since, as noted in the introduction, the number of generators of $H_1 * H_2$ (respectively $G$) is determined once we know the Euler factors.

We get a complete description of $P(G/G''', s)$ for any choice of finite abelian groups $H_1, H_2$ (and a similar quotient for more general $H_1, H_2$). We then give some results on $P(G, s)$ and on $P(H_1 * H_2, s)$, in particular concentrating on the simplest case of $H_1 = C_2, H_2 = C_3$.

2. Metabelian quotients

Let $M = G/G''$ be the largest metabelian quotient of $H_1 * H_2$ if $H_1, H_2$ are abelian. Since the derived subgroup of $H_1 * H_2$ is free on $(|H_1| - 1)(|H_2| - 1)$ generators, we can describe $M$ explicitly [11]. Its derived subgroup $M'$ is free.
abelian on \((|H_1| - 1)(|H_2| - 1)\) generators (explicitly the commutators \((h, k)\) for \(1 \neq h \in H_1, 1 \neq k \in H_2\)), with \(M/M' \cong H_1 \times H_2\) acting on \(M'\) via the tensor product of augmentation representations. This extension splits. In the case that \(H_1, H_2\) are not necessarily abelian, we will still form this quotient of \(H_1 \ast H_2\) and call it \(M\).

This means that \(P(M, s) = P(H_1 \times H_2, s)\prod_p Q_p(s)\), where the factors \(Q_p(s)\) can be read off the semidirect product given by the tensor product of augmentation actions of \(H_1\) and \(H_2\) on a free \(\mathbb{F}_p\)-module on \((|H_1| - 1)(|H_2| - 1)\) generators. For instance, if \(H_1 = C_2\) and \(H_2 = C_3\), then to compute \(Q_p(s)\) we simply find \(P(K, s)\) where \(K = \langle a, b | a^2, b^3, (a, b)^p, (a, b^2)^p, ((a, b), (a, b^2)) \rangle\). The terms with \(p\) dividing \(|H_1||H_2|\) will be called modular, the rest ordinary. The ordinary factors are easier to compute.

Here are some examples: \(H_1 = C_2, H_2 = C_p\) (\(p\) odd). Then \(P(M, s) = \left(1 - 1/2^s\right)(1 - 1/p^s)/\zeta_K(s - 1)\), where \(K\) is the \(p\)th cyclotomic field \(\mathbb{Q}(\zeta_p)\) and \(\zeta_K\) is its zeta function. If \(H_2 = C_2\), we get the same result without the \(1 - 1/p^s\) factor.

If \(H_1 = C_2, H_2 = C_4\), then \(Q_p(s) = \left(1 - p/p^s\right)^3\) if \(p \equiv 1\) (mod 4), \(Q_p(s) = \left(1 - p/p^s\right)(1 - p^2/p^{2s})\) if \(p \equiv 3\) (mod 4), and \(Q_p(s) = 1\) if \(p = 2\). This comes e.g. from the fact that if \(p \equiv 3\) (mod 4), then the augmentation representation of \(C_4\) into \(GL(3, p)\) splits into one-dimensional and two-dimensional irreducible representations. Compare this with the case of \(H_1 = C_2\), \(H_2 = C_2 \times C_2\), when \(Q_p(s) = \left(1 - p/p^s\right)^3\) for all odd primes \(p\) (and \(= 1\) for \(p = 2\)), since the one-dimensional characters of \(C_2 \times C_2\) are all defined over \(\mathbb{F}_p\), whatever \(p\) is.

Thus, for \(H_1 = C_2, H_2 = C_4\), \(P(M, s) = \left(\text{finite factors}\right)/(\zeta_{\mathbb{Q}}(s - 1)/\zeta_{\mathbb{Q}}(s - 1))\), whereas for \(H_1 = C_2, H_2 = C_2 \times C_2\), \(P(M, s) = \left(\text{finite factors}\right)/(\zeta_{\mathbb{Q}}(s - 1))^3\). In general, the finite factors come from \(P(H_1 \times H_2, s)\) and modular \(Q_p(s)\). We obtain a complete description of the zeta function denominators by finding all ordinary \(Q_p(s)\).

**Theorem.** Suppose \(p\) is a prime that does not divide \(|H_1||H_2|\). Suppose that the tensor product of augmentation representations \(\rho_p : H_1 \times H_2 \to GL(d, p)\) \((d = (|H_1| - 1)(|H_2| - 1))\) decomposes into irreducible representations of degree \(d_1, \ldots, d_k\) \((\sum d_i = d)\). Then

\[
Q_p(s) = \prod_{i=1}^{k} (1 - p^{d_i}/p^{d_i s}).
\]

For example, let \(H_1 = C_2, H_2 = S_3\). Whatever \(p\) is, the representation \(\rho_p\) decomposes into one 1-dimensional and two 2-dimensional \(\mathbb{F}_p\)-representations. Thus for \(p \geq 5\), \(Q_p(s) = (1 - p/p^s)(1 - p^2/p^{2s})^2\) and so \(P(M, s) = \left(\text{finite factors}\right)/(\zeta_{\mathbb{Q}}(s - 1)/\zeta_{\mathbb{Q}}(2s - 2))^2\).

The modular factors are harder to obtain. For instance, for the previous example \((H_1 = C_2, H_2 = S_3)\), \(Q_2(s) = (1 - 4/4^s)(1 - 8/4^s)\) and \(Q_3(s) = (1 - 3/3^s)(1 - 9/3^s)\). These factors will be explained later.

**Theorem.** Whatever \(H_1\) and \(H_2\) are, \(P(M, s)\) always equals some finite factors divided by a finite product of zeta functions of cyclotomic fields evaluated at integer multiples of \(s - 1\).
Proof. Let $\rho : H_1 \times H_2 \to GL(d, \mathbb{Z}) \ (d = (|H_1| - 1)(|H_2| - 1))$ be the action of $M/M'$ on $M'$ (so the tensor product of augmentation representations). Then $\rho_p$ is $\rho$ composed with the mod $p$ map, for each $p$ not dividing $|H_1||H_2|$. Considering $\rho$ as a representation into $GL(d, C)$, we can decompose it into irreducible constitutents $\rho(i)$ $(1 \leq i \leq k)$. Then $\rho_p$ considered as a representation into $GL(d, \mathbb{F}_p)$ decomposes as $\rho(i)_p$ $(1 \leq i \leq k)$. Brauer’s theorem on splitting fields [4] tells us that the cyclotomic field $\mathbb{Q}(\mu_m)$, where $m$ is the exponent of $H_1 \times H_2$, is a splitting field for each $\rho(i)$. Let $K_i$ be the subfield that is the smallest splitting field for $\rho(i)$. Then its residue field at $p$ is a splitting field for $\rho(i)_p$. The $p$th Euler factor of the zeta function of $K_i$ is $(1 - 1/p^{i+})$, which, with $s$ replaced by $s - 1$, matches the factor $Q_p(s)$ in the last theorem.

Note that the ordinary factors certainly satisfy the modified conjecture. We now give a more detailed description of the modular factors ...

3. Further results on $P(H_1 \ast H_2, s)$

Let $H_1 = C_2$, $H_2 = C_3$, and $G$ be the maximal prosolvable quotient of $H_1 \ast H_2$. We are interested in the Dirichlet series $P(G, s)$ and the formal Dirichlet series $P(H_1 \ast H_2, s)$. The case of $P(G, s)$ is much more successful, although as we go deeper into the derived series, the awkward modular cases proliferate and cause problems. Since calculation of $P(C_2 \ast C_3, s)$ includes describing all $(2,3)$-generated groups, itself a major problem (see [6]), we have limited success in this case.

Computations give that $P(G, s) = (1 - 1/2^s)(1 - 1/3^s)(1 - 3/5^s)(1 - 4/7^s)(1 - 7/13^s)^2(1 - 9/17^s)^2(1 - 13/23^s)^2 ... = 1 - 1/2s - 4/3s - 8/4s + 4/6s - 14/7s + 8/8s - 15/9s + 32/12s - 26/13s + 14/14s + 16/16s + ...$, whereas $P(C_2 \ast C_3, s) = 1 - 1/2s - 4/3s - 8/4s - 5/5s - 2/6s - 42/7s - 16/8s - 78/9s - 255/10s - 286/11s - 418/12s - 1729/13s - 1918/14s - 4450/15s - 11416/16s + ... = (1 - 1/2s)(1 - 1/3s)(1 - 3/5s)(1 - 4/7s)^2P(A_5, s)(1 - 7/11^s)^2P(PSL(2, 7), s)^2P(A_7, s)^2P(PSL(2, 7), s)^2P(PSL(2, 8), s)^2P(A_9, s)^2P(A_9, s)^2 ...$, where $P(S_7, s) = P(C_2, s)P(A_7, s)$, $P(PGL(2, 7), s) = P(C_2, s)P(PSL(2, 7), s)$, $P(S_9, s) = P(C_2, s)P(A_9, s)$, $P(PSL(2, 8), s) = P(C_3, s)P(PSL(2, 8), s)$, ...

Families of solvable quotients of $C_2 \ast C_3$ of derived length $> 2$ can be obtained by taking extensions of solvable groups by smaller $(2,3)$-generated groups. For instance, the semidirect product $G_p$ of $C_p \times C_p$ by $S_3$ acting via its irreducible two-dimensional representation, has derived length 3. Its zeta function yields more factors of the form $(1 - p^2/p^{2s})$. In greater detail, we have

4. Minimal $d$-generated groups

We begin by following the argument of [9]. Assume that $G$ is minimal $d$-generated subject to being generated by $s$ $r$-generated subgroups of pairwise coprime order, say $H_1, ..., H_s$. Let $X$ be a nontrivial normal subgroup of $G$. Since $G/X$ can be generated by the subgroups $XH_1/X, ..., XH_s/X$, which are also $r$-generated and of pairwise coprime order, the minimality of $G$ implies that $d(G/X) \leq r + s - 1 < d(G)$. Thus, $G$ has the property that every proper quotient of it has strictly fewer generators than it has. In [2], such groups were classified. There is a finite group
Let $L$ be a group with a unique minimal normal subgroup $M$ and an integer $t$ such that $G \cong L_t$, where $L_t = \{(x_1, \ldots, x_t) \in L^t : x_1 \equiv \ldots \equiv x_t \mod M\}$. Moreover, $t \geq 2$, else by [9], $d(G) = d(L) = \max(2, d(L/M)) \leq r + s - 1$.

It therefore is of interest to concentrate on $P(L_t, d)$ for $t \geq 2$. Some work in this direction was done by [3].

**BIBLIOGRAPHY**

3. F.Dalla Volta, A.Lucchini, and F.Morini, On the probability of generating a minimal $d$-generated group, preprint.