On the probabilistic zeta function for finite groups

John Shareshian
California Institute of Technology
Pasadena, CA 91125
email: shareshi@cco.caltech.edu

August 20, 1999

Abstract

Let G be a finite group, and define the function

$$P(G,s) := \sum_{H \leq G} \frac{\mu(H,G)}{[G:H]^s},$$

where μ is the Möbius function on the subgroup lattice of G. The function $P(G,s)$ is the multiplicative inverse of a zeta function for G, as described in [Ma] and [Bo]. In [Bo], Boston conjectured that $P'(G,1) = 0$ if G is nonabelian simple. We will prove a generalization of this conjecture, showing that $P'(G,1) = 0$ unless $G/O_p(G)$ is cyclic for some prime p.

In [Ma] and [Bo], respectively, A. Mann and N. Boston examined the function

$$P(G,s) = \sum_{H} \frac{\mu(H)}{[G:H]^s}$$

where the sum runs over the set of subgroups of finite index in a finitely generated profinite group G, and μ is the Möbius function on the poset of such subgroups. Here, and in the rest of this paper, $\mu(H)$ means $\mu(H,G)$. In [Bo], it was conjectured that $P'(G,1) = 0$ when G is a nonabelian finite simple group. Exponentiating both sides of the equality allows one to write this conjecture as follows.

Conjecture 1 (Boston) *Let G be a nonabelian finite simple group. Then*

$$\prod_{H \leq G} [G:H]^{\frac{\mu(H)}{[G:H]}} = 1.$$

In what follows, I'll prove a generalization of this conjecture, which will imply that the conclusion of the conjecture holds for any finite group G such that there is no prime p with $G/O_p(G)$ cyclic. The proof involves examining Boston's conjecture one prime at a time. This idea was suggested by Richard Lyons, whom I thank for that suggestion and for his encouragement. I thank Nigel Boston and Avinoam Mann for their helpful comments, and I thank the anonymous referee for clarifying the history of the study of $P(G, s)$.

From now on, every group G will be assumed to be finite.

Definition 2 *Let G be a group and let $\{p_1, \ldots, p_k\}$ be the set of prime divisors of $|G|$. Define the rational numbers $\alpha_1, \ldots, \alpha_k$ by*

$$\prod_{H \leq G} [G : H]^{\frac{\mu(H)}{[G:H]}} = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

A formula for α_i will be determined from which the next result will follow.

Proposition 3 *If $G/O_{p_i}(G)$ is not cyclic then $\alpha_i = 0$.*

The first step is to get a crude formula for α_i directly from the definition. Fix from now on a prime $p = p_i$ and let $\alpha = \alpha_i$. For a positive integer m, we denote by m_p the largest power of p dividing m.

Definition 4 *1. For $H \leq G$ set $a_p(H) = log_p(|H|_p)$.*

2. For $1 \leq a \leq a_p(G)$ set $\Gamma_a(G) = \{H \leq G; a_p(H) = a\}$.

3. For $1 \leq a \leq a_p(G)$ define $f_a(G) = \sum_{H \in \Gamma_a(G)} |H|\mu(H)$.

The next proposition follows from the definition by an easy calculation.

Proposition 5 $\alpha = \frac{a_p(G)}{|G|} \sum_{H \leq G} |H|\mu(H) - \frac{1}{|G|} \sum_{a=1}^{a_p(G)} a f_a(G)$.

Now we'll calculate the two sums in the difference above. The first term was examined by P. Hall in [Ha], where he defined the Möbius function μ and proved the Möbius inversion formula in order to show, among other things, that if n is a positive integer then $P(G, n)$ gives the probability that a randomly chosen ordered n-tuple $(g_1, \ldots, g_n)$ from G satisfies $G = \langle g_1, \ldots, g_n \rangle$. The proposition below is a special case of that result.

Proposition 6 *Let ϕ be Euler's function. Then*

$$\sum_{H\le G}|H|\mu(H)=\begin{cases}\phi(|G|) & \text{if } G \text{ is cyclic}\\ 0 & \text{otherwise}\end{cases}$$

The second sum in Proposition 5 will be determined by calculating each $f_a(G)$.

Definition 7 *Fix a with $1\le a\le a_p(G)$.*

1. *Set $\Delta_a(G)=\{R\le G:|R|=p^a\}$ and $\Delta_a^*(G)=\{R\in\Delta_a(G):R\trianglelefteq G\}$.*
2. *For $R\in\Delta_a(G)$ set $\Omega(R)=\{H\le G:R\in Syl_p(H)\}$.*

Lemma 8 *Let R be a nontrivial p-subgroup of G. Then*

$$\sum_{H\in\Omega(R)}|N_H(R)|\mu(H)=\begin{cases}\sum_{H\in\Omega(R)}|H|\mu(H), & R\trianglelefteq G\\ 0, & \text{otherwise.}\end{cases}$$

Proof: If $R\trianglelefteq G$ then $N_H(R)=H$ for all $H\in\Omega(R)$ and the claim of the lemma holds, so assume $N_G(R)<G$. Note that for $H\le G$ we have $H\in\Omega(R)$ if and only if $N_H(R)\in\Omega(R)$. Indeed, if $P\in Syl_p(H)$ strictly contains R, then so does $N_P(R)\le N_H(R)$. Let $\Omega^*(R)=\{L\in\Omega(R):R\trianglelefteq L\}$. It follows from the above argument that

$$\sum_{H\in\Omega(R)}|N_H(R)|\mu(H)=\sum_{L\in\Omega^*(R)}|L|\sum_{H\cap N_G(R)=L}\mu(H).$$

Fix $L\in\Omega^*(R)$. Since $N_G(R)\ne G$, it follows from Weisner's Theorem (see for example Corollary 3.9.3 of [St]) that

$$\sum_{H\cap N_G(R)=L}\mu(H)=0,$$

and the lemma follows. □

Corollary 9 *For $1\le a\le a_p(G)$,*

$$f_a(G)=\sum_{R\in\Delta_a^*(G)}\sum_{H\in\Omega(R)}|H|\mu(H).$$

Proof: By Sylow's Theorem, we have

$$f_a(G) = \sum_{R\in\Delta_a(G)} \sum_{H\in\Omega(R)} |N_H(R)|\mu(H).$$

The corollary now follows immediately from Lemma 8. □

Now we can prove Proposition 3. By Propositions 5 and 6, it suffices to show that if $G/O_p(G)$ is not cyclic then $f_a(G) = 0$ for $1 \le a \le a_p(G)$. If $a > a_p(O_p(G))$ then $\Delta_a^*(G) = \emptyset$ and $f_a(G) = 0$ by Corollary 9. If $a = a_p(O_p(G))$ then $\Delta_a^*(G) = \{O_p(G)\}$ and by Corollary 9 we have

$$f_a(G) = \sum_{H\in\Omega(O_p(G))} |H|\mu(H).$$

Set $\overline{G} = G/O_p(G)$ and let $\overline{\mu}$ be the Möbius function on the subgroup lattice of $\overline{G}$. Also, let $\Xi(\overline{G})$ be the set of subgroups of $\overline{G}$ whose order is not divisible by p. Then

$$\sum_{H\in\Omega(O_p(G))} |H|\mu(H) = |O_p(G)| \sum_{\overline{H}\in\Xi(\overline{G})} |\overline{H}|\overline{\mu}(\overline{H}).$$

Since $\overline{G}$ is not cyclic, Proposition 6 gives

$$\sum_{\overline{H}\in\Xi(\overline{G})} |\overline{H}|\overline{\mu}(\overline{H}) = -\sum_{\overline{H}\notin\Xi(\overline{G})} |\overline{H}|\overline{\mu}(\overline{H}).$$

Now Sylow's theorem gives

$$\sum_{\overline{H}\notin\Xi(\overline{G})} |\overline{H}|\overline{\mu}(\overline{H}) = \sum_{b=1}^{a_p(\overline{G})} \sum_{\overline{R}\in\Delta_b(\overline{G})} \sum_{\overline{K}\in\Omega(\overline{R})} |N_{\overline{K}}(\overline{R})|\overline{\mu}(\overline{K}).$$

Since $O_p(\overline{G}) = 1$,

$$\sum_{\overline{K}\in\Omega(\overline{R})} |N_{\overline{K}}(\overline{R})|\overline{\mu}(\overline{K}) = 0$$

for each nontrivial p-subgroup $\overline{R} \le \overline{G}$ by Lemma 8. Thus $f_a(G) = 0$ for $a = a_p(O_p(G))$. We now proceed by downwards induction on a, so we assume that $a < a_p(O_p(G))$ and that if $Q \in \Delta_b^*(G)$ with $a < b$ then $\sum_{H\in\Omega(Q)} |H|\mu(H) = 0$. By Corollary 9 we have

$$f_a(G) = \sum_{R\in\Delta_a^*(G)} \sum_{H\in\Omega(R)} |H|\mu(H).$$

Fix $R \in \Delta_a^*(G)$ and set $\tilde{G} = G/R$. Let $\tilde{\mu}$ be the Möbius function on the subgroup lattice of $\tilde{G}$. Since $\overline{G}$ is not cyclic, neither is $\tilde{G}$. Using the same arguments we used when examining $a = a_p(O_p(G))$, we see that to show that $\sum_{H\in\Omega(R)} |H|\mu(H) = 0$ it suffices to show that if $\tilde{Q}$ is a nontrivial normal p-subgroup of $\tilde{G}$ then $\sum_{\tilde{H}\in\Omega(\tilde{Q})} |\tilde{H}|\tilde{\mu}(\tilde{H}) = 0$. Let Q be the full preimage of $\tilde{Q}$ in G. Then $Q \in \Delta_b^*(G)$ for some $b > a$, and by inductive hypothesis we have

$$|R| \sum_{\tilde{H}\in\Omega(\tilde{Q})} |\tilde{H}|\tilde{\mu}(\tilde{H}) = \sum_{H\in\Omega(Q)} |H|\mu(H) = 0.$$

This completes the proof of Proposition 3. If $G/O_p(G)$ is cyclic for some prime p, then G is solvable and $P(G, s)$ is quite well understood (see Section 3 of [Bo]).

References

[Bo] N. Boston, *A probabalistic generalization of the Riemann zeta function*, Analytic Number Theory, Proceedings of a Conference in Honor of Heini Halberstam, vol. 1, Progress in Mathematics Volume 138, Birkhäuser, Boston, 1996.

[Ha] P. Hall, *The Eulerian functions of a finite group*, Quart. J. Math. **7** (1936), 134-151.

[Ma] A. Mann, *Positively generated finite groups*, Forum Math. **8** (1996), 429-459.

[St] R.P. Stanley, Enumerative Combinatorics, vol. 1, Wadsworth and Brooks/Cole, 1986.