The sign of wreath product representations of finite groups

Jan-Christoph Schlage-Puchta

Abstract

Let G, H be finite groups. We asymptotically compute $|\mathrm{Hom}(G, H \wr A_n)|$, thereby establishing a conjecture of T. Müller.

Let G, H be finite groups. T. Müller[2] developed an enumerative theory of homomorphisms $\varphi : G \to H \wr S_n$, as $n \to \infty$, and asked to generalize this theory to other sequences of groups. In particular, he conjectured the following.

Conjecture 1. *Let G, H be a finite groups. Then we have for $n \to \infty$*

$$|\mathrm{Hom}(G, H \wr A_n)| = \Big(\frac{1}{1 + s_2(G)} + \mathcal{O}(e^{-cn^{1/|G|}})\Big)|\mathrm{Hom}(G, H \wr S_n)|,$$

where $s_2(G)$ is the number of subgroups of index 2 in G.

It is the aim of this note to proof this conjecture.

Theorem 1. *Conjecture 1 holds true for all finite groups G and H.*

One of the applications of wreath product representations is the recognition of finite index subgroups of infinite groups. Let Γ be an infinite group, Δ a subgroup of index n. The action of Γ on the cosets Γ/Δ by shift defines a homomorphism $\varphi : \Gamma \to S_n$. If in addition we know the number of lifts of φ to homomorphisms $\psi : \Gamma \to H \wr S_n$, we can compute $|\mathrm{Hom}(\Delta, H)|$. Doing so for different choices of H one can in certain situations gather sufficient information to reconstruct Δ. For Γ being a free product of cyclic groups of prime order this reconstruction was completed in [3], for free products of arbitrary finite groups in [5].

Received by the editors in November 2012 - In revised form in January 2014.
Communicated by M. Van den Bergh.
2010 *Mathematics Subject Classification* : 20E22, 20D60.

Comparing homomorphisms into $H \wr A_n$ with homomorphisms into $H \wr S_n$ gives information on the embedding of finite index subgroups in large groups. More precisely define for a subgroup Δ of a group Γ the core Δ^c as the normal subgroup $\bigcup_{\gamma\in\Gamma} \Delta^\gamma$. Then the case $H = 1$ of Theorem 1 implies that the probability that a random subgroup Δ of index n of a free product $\Gamma = G_1 * \ldots G_r$ of finite groups satisfies $\Gamma/\Delta^c \cong A_n$ converges to $\prod_{i=1}^r \frac{1}{1+s_2(G_i)}$. The case of general H yields that the property $\Gamma/\Delta^c \cong A_n$ and the isomorphism type of Δ are asymptotically independent. It would be interesting to generalize such considerations to arbitrary virtually free groups.

We now turn to the proof of the Theorem. We denote by π the canonical projection $H \wr S_n \to S_n$, and by ϵ the sign homomorphism $S_n \to C_2$. We view C_2 as $\{\pm 1\} \subseteq \mathbb{Z}$, that is, we write the group operation of C_2 multiplicatively, but allow for the addition of values as in $\mathbb{Z}$. Let $\varphi : G \to H \wr S_n$ be a homomorphism. Then $\epsilon \circ \pi \circ \varphi : G \to C_2$ has a kernel containing G^2G'. We denote the induced homomorphism $V = G/G^2G' \to C_2$ by $\overline{\varphi}$. To prove our theorem it is therefore sufficient to show that if $\varphi \in \mathrm{Hom}(G, H \wr S_n)$ is chosen at random, then the distribution of $\overline{\varphi}$ converges to a uniform distribution. This is certainly true if $s_2(G) = 0$, because then $G = G^2G'$. We shall therefore from now on assume that $s_2(G) > 0$, that is, V is a non-trivial elementary abelian 2-group. Then our claim is equivalent to the statement that for every non-trivial $v \in V$ we have

$$h_n^v(G,H) := \frac{1}{|\mathrm{Hom}(G, H \wr S_n)|} \sum_{\varphi\in\mathrm{Hom}(G,H\wr S_n)} \overline{\varphi}(v) \ll e^{-cn^{-1/|G|}},$$

where we identified C_2 with $\{\pm 1\} \subseteq \mathbb{Z}$.

We first compute the dependence of $h_n^v(G,H)$ on H.

Lemma 1. *Let G, H be finite groups, $\varphi : G \to S_n$ a transitive permutation representation, $\pi : H \wr S_n \to S_n$ the canonical projection. Then the number of homomorphisms $\psi : G \to H \wr S_n$ satisfying $\pi \circ \psi = \varphi$ equals $|H|^{n-1}$.*

Proof. This follows form the proof of [3, Proposition 1], more precisely the equality between [3, (8)] and [3, (9)]. ∎

Next we compute the generating series of $h_n^v(G,H)$.

Lemma 2. *We have*

$$\sum_{\nu\geq 0} \frac{h_n^v(G,H)}{n!} x^n = \exp\left(\sum_{k=1}^{|G|} \sum_{\psi:G\to S_k transitive} \overline{\psi}(v) \frac{|H|^{k-1}x^k}{k!} \right).$$

Proof. This is a weighted version of the exponential principle, see e.g. [6, Theorem 5.1.4]. We only have to show that if $\pi \circ \varphi$ decomposes as $\pi \circ \varphi = \bigoplus a_i\psi_i$, where the ψ_i are transitive permutation representations, then $\overline{\varphi}(v) = \prod \overline{\psi}(v)^{a_i}$. However, this follows immediately from the fact that ϵ is a homomorphism. ∎

To deal with the generating series we need a stability result similar to [4], note however, that here we do not require P_2 to be Hayman admissible. In fact it is easy to see that $\sum_{\nu\geq 0} \frac{h_n^v(G,H)}{n!} x^n$ is Hayman admissible if and only if $s_2(G) = 0$, which is precisely the case we are not interested in.

Lemma 3. *Let $P_1(x) = \sum_{\nu=1}^d a_\nu^{(1)} x^\nu$ be a polynomial with non-negative real coefficients, $a_d^{(1)} \neq 0$, and let $P_2 = \sum_{n=1}^d a_\nu^{(2)} x^\nu$ be a polynomial with complex coefficients satisfying $|a_\nu^{(2)}| \leq a_\nu^{(1)}$ for all $\nu \leq d$. Define the sequences $b_\nu^{(1)}, b_\nu^{(2)}$ by the relation $\sum_{\nu=0}^\infty \frac{b_\nu^{(i)}}{\nu!} x^\nu = e^{P_i(x)}$. Then either there exists some complex number ζ with $|\zeta| = 1$, such that $P_1(x) = P_2(\zeta x)$, or there is some $c > 0$ such that $|b_\nu^{(2)}| < e^{-c\nu^{1/d}} |b_\nu^{(1)}|$ for all ν sufficiently large.*

Proof. Let ρ_n be the unique real solution of the equation $\rho P'(\rho) = n$. It then follows from Hayman's theorem [1, Theorem I] that

$$b_n^{(1)} \sim \frac{\exp(P_1(\rho_n))}{\rho_n^n \sqrt{2\pi(\rho_n P_1'(\rho_n) + \rho_n^2 P''(\rho_n))}}.$$

We now express $b_n^{(2)}$ using Cauchy's integral formula as

$$b_n^{(2)} = \frac{1}{2\pi i} \int\limits_{\partial B_{\rho_n}(0)} \frac{\exp(P_2(z))}{z^{n+1}}\, dz$$

to obtain

$$\begin{aligned} |b_n^{(2)}| &\leq \frac{\max\limits_{|z|=\rho_n} |\exp(P_2(z)|}{\rho_n^n} \\ &\leq (\sqrt{2\pi}d + o(1))\rho_n^{d/2} \frac{\max\limits_{|z|=\rho_n} |\exp(P_2(z)|}{\exp(P_1(\rho_n))} b_n^{(1)} \\ &\ll n^{1/2} \frac{\max\limits_{|z|=\rho_n} |\exp(P_2(z)|}{\exp(P_1(\rho_n))} b_n^{(1)} \end{aligned}$$

where we used the fact that for $n \to \infty$ we have $\rho_n \sim cn^{1/d}$. Hence it suffices to show that either there is some ζ with $P_1(x) = P_2(\zeta x)$, or

$$\max_{|z|=\rho_n} \Re P_2(z) < P_1(\rho_n) - cn^{1/d}$$

for some $c > 0$. If there exists some ν with $|a_\nu^{(2)}| < a_\nu^{(1)}$, then this follows immediately from the triangle inequality. Define the function $f : [0, 2\pi] \to [0, \infty)$ by

$$f(\theta) = \max_{\substack{1 \leq \nu \leq d \\ a_\nu \neq 0}} |\nu\theta + \arg a_\nu^{(2)} \bmod 2\pi|,$$

where we normalize mod in such a way that it takes values in $[-\pi, \pi)$. Being continuous, this function either has a zero ξ, or it is uniformly bounded from below by some positive constant δ. In the first case we obtain $P_2(x) = P_1(e^{i\xi}x)$, while in the second we have

$$\begin{aligned} P_1(\rho_n) - \Re P_2(e^{i\theta}\rho_n) &= \sum_{\nu=1}^{d} \left(1 - \Re e^{i(\nu\theta + \arg a_\nu^{(2)})}\right) a_\nu^{(1)} \rho_n^\nu \\ &\geq (1 - \Re e^{i\delta}) \min_{\substack{1\leq\nu\leq d\\ a_\nu\neq 0}} a_\nu \rho_n^\nu \\ &\geq \left((1-\cos\delta) \min_{\substack{1\leq\nu\leq d\\ a_\nu\neq 0}} a_\nu\right) n^{1/d}. \end{aligned}$$

Hence in either case our claim follows. ■

We can now finish the proof of the theorem. We have to show that for $v \neq 0$ we have $h_n^v(G,H) \ll e^{-cn^{1/d}} h_n^0(G,H)$. We have

$$\left| \sum_{\psi:G\to S_k \text{transitive}} \overline{\psi}(v) \frac{|H|^{k-1}}{k!} \right| \leq \sum_{\psi:G\to S_k \text{transitive}} \frac{|H|^{k-1}}{k!}$$

for every k, hence we can apply Lemma 3 to find that either our claim holds true, or there exists some ζ with $|\zeta| = 1$, such that

$$\sum_{k=1}^{|G|} \sum_{\psi:G\to S_k \text{transitive}} \overline{\psi}(v) \frac{|H|^{k-1}x^k}{k!} = \sum_{k=1}^{|G|} \sum_{\psi:G\to S_k \text{transitive}} \frac{|H|^{k-1}(\zeta x)^k}{k!}.$$

Consider first the coefficient of x in these polynomials. There is only the trivial representation $G \to S_1 = 1$, hence the coefficient of x on both sides equals 1, and we conclude $\zeta = 1$.

Next we consider the coefficient of x^2. Let $\overline{U} < G/G^2G'$ be a subspace of codimension 1, which does not contain v, and U be the preimage of $\overline{U}$ under the canonical map $G \to G/G^2G'$. Then $\psi_0 : G \to G/U \cong S_2$ is a homomorphism, for which $\overline{\psi_0}(v) = -1$, and we conclude that

$$\Sigma_1 = \sum_{\psi:G\to S_2 \text{transitive}} \overline{\psi}(v) \frac{|H|}{2} < \sum_{\psi:G\to S_2 \text{transitive}} \frac{|H|}{2} = \Sigma_2,$$

say, while the equality $P_1(x) = P_2(\zeta x)$ implies that $\Sigma_1 = \zeta^2 \Sigma_2$. Clearly both Σ_1 and Σ_2 are real, and we conclude that $\zeta^2 = -1$. However, this contradicts the condition $\zeta = 1$ obtained from the coefficient of x, and our claim follows.

References

[1] W. K. Hayman, A generalization of Stirling's formula, *J. Reine Angew. Math.* **196** (1956), 67–95.

[2] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118–154.

[3] T. Müller, J.-C. Schlage-Puchta, Classification and statistics of finite index subgroups in free products, *Adv. Math.* **188** (2004), 1–50.

[4] T. Müller, J.-C. Schlage-Puchta, Asymptotic stability for sets of polynomials, *Arch. Math. (Brno)* **41** (2005), 151–155.

[5] T. Müller, J.-C. Schlage-Puchta, Statistics of isomorphism types in free products, *Adv. Math.* **224** (2010), 707–730.

[6] R. P. Stanley, *Enumerative combinatorics*, Vol. 2., Cambridge Studies in Advanced Mathematics, 62. Cambridge University Press, Cambridge, 1999.

Institut fuer Mathematik
Ulmenstr. 69, Haus 3
18057 Rostock
Germany
email : jan-christoph.schlage-puchta@uni-rostock.de