On the divisibility of \( \# \text{Hom}(\Gamma, G) \) by \( |G| \)

Cameron Gordon
University of Texas at Austin
gordon@math.utexas.edu

Fernando Rodriguez-Villegas
University of Texas at Austin
villegas@math.utexas.edu

January 26, 2013

Abstract
We extend and reformulate a result of Solomon on the divisibility of the title. We show, for example, that if \( \Gamma \) is a finitely generated group, then \(|G|\) divides \( \# \text{Hom}(\Gamma, G) \) for every finite group \( G \) if and only if \( \Gamma \) has infinite abelianization. As a consequence we obtain some arithmetic properties of the number of subgroups of a given index in such a group \( \Gamma \).

1 Introduction
Let \( G \) be a finite group. For any non-negative integer \( g \) and a fixed \( z \in G \) consider the set

\[
U_z := \{ (x_1, y_1, \ldots, x_g, y_g) \in G^{2g} \mid [x_1, y_1] \cdots [x_g, y_g] = z \},
\]

where \([x, y] := xyx^{-1}y^{-1}\). We have \(3\)

\[
\#U_z = \sum_{\chi} \left(\frac{|G|}{\chi(1)}\right)^{2g-1} \chi(z),
\]

where the sum is over all irreducible characters of \( G \) (formulas of this sort were already known to Frobenius).

In particular, for \( z = 1 \) we obtain

\[
\#U_1 = |G| \sum_{\chi} \left(\frac{|G|}{\chi(1)}\right)^{2g-2} \chi(1).
\]

Since \( \chi(1) \) divides \(|G|\) for every \( \chi \), it follows that \(|G|\) divides \( \#U_1 \) when \( g > 0 \). The purpose of this note is to give a more direct proof of a generalization of this observation.

We may interpret \( U_1 \) as the set \( \text{Hom}(\pi_1(\Sigma_g), G) \) of homomorphisms of the fundamental group of a Riemann surface \( \Sigma_g \) of genus \( g \) to \( G \). The question is then the following. Given a finitely generated group \( \Gamma \), say, when do we have that \(|G|\) divides \( \text{Hom}(\Gamma, G) \) for every finite group \( G \)? It turns out that the answer is quite simple: precisely when \( \Gamma \) has an infinite abelianization (see Corollary 3.3).

As it happens, the answer to our question is buried in a paper of Solomon’s [4], which was the main motivation for the present note. Solomon’s proof assumes that \( \Gamma \) has positive deficiency (i.e., has a presentation with strictly more generators than relations), but it is easy to see that it can be made to apply more
generally to any group with infinite abelianization. However, his proof is lengthy and somewhat hard to 
read; the proof we give is short and, we hope, more perspicuous. Solomon deduces his result from a more 
general statement about homomorphisms from a free group to $G$ that send specified elements into specified 
conjugacy classes. As an immediate corollary to our theorem we get a generalization of this in which the 
free group is replaced by any group whose abelianization is infinite.

2 $G$-torsors

Let $G$ be a finite group. A $G$-set $X$ is a set $X$ on which $G$ acts. We denote by $X/G$ the set of orbits under the 
action. Let $G$ be the bundle of groups $\text{Stab}_G(x)$ on $X$. A $G$-torsor of $X$ is a surjective map of sets $\pi : Y \to X$, 
for some set $Y$, such that each fiber $Y_x$ is a principal homogeneous space for $\text{Stab}_G(x)$. In other words, there 
is an action of $\text{Stab}_G(x)$ on $Y_x$ for every $x \in X$ such that for any fixed $y \in Y_x$ the map 
$$
\text{Stab}_G(x) \to Y_x 
$$
$$
s \mapsto sy
$$
is a bijection. It is worth stressing that we do not require a global action of $G$ on $Y$ inducing the action of 
$\text{Stab}_G(x)$ on $Y_x$.

We will write $\#$ for the cardinality of a set and reserve $|\cdot|$ for the order of a group.

Lemma 2.1. Let $X$ be a $G$-set and $\pi : Y \to X$ a $G$-torsor. Then 
(i) $X$ is finite if and only if $Y$ is finite.
(ii) In this case, $\# Y = \#(X/G)$. In particular $\# Y = |G|$ is an integer or, equivalently, $|G|$ divides $\# Y$.

Proof. The first assertion (i) is clear since $G$ is finite. As for (ii) note that 
$$
\# Y = \sum_{x \in X} \# Y_x = \sum_{x \in X} |\text{Stab}_G(x)|.
$$

Since $|\text{Stab}_G(x)|$ is constant on orbits in $X/G$ we can group terms in the sum by orbits. The contribution to 
the sum of an orbit $[x]$ is then $|[x]| |\text{Stab}_G(x)| = |G|$. Hence 
$$
\# Y = \sum_{[x]} |G| = |G| \cdot #(X/G).
$$

and the lemma is proved. \hfill \Box

3 Homomorphisms

Let $\Gamma$ be a group. The set $X := \text{Hom}(\Gamma, G)$, where $G$ is a finite group, is then finite if $\Gamma$ is a finitely 
generated. The group $G$ acts on $X$ by conjugation. The quotient $\# \text{Hom}(\Gamma, G)/|G|$ that we are interested in 
can be thought of as a weighted count of homomorphisms from $\Gamma$ to $G$. Namely,

$$
\frac{1}{|G|} \# \text{Hom}(\Gamma, G) = \sum_{[\phi]} \frac{1}{|\text{Stab}_G(\phi)|},
$$

where $[\phi]$ runs through the $G$-orbits of $\text{Hom}(\Gamma, G)$.

We also have an action of $\text{Aut}(\Gamma)$ on $X$ by 
$$
\phi^\sigma(\gamma) := \phi(\sigma^{-1} \gamma), \quad \sigma \in \text{Aut}(\Gamma), \quad \phi \in X, \quad \gamma \in \Gamma.
$$

Fix $\sigma \in \text{Aut}(\Gamma)$ and let $X_\sigma := \text{Hom}_\sigma(\Gamma, G) \subseteq \text{Hom}(\Gamma, G)$ be the subset of $\phi \in X$ which are fixed by $\sigma$ 
up to conjugation by $G$. The two actions, of $G$ and $\text{Aut}(\Gamma)$, on $X$ clearly commute. In particular, the action 
of $\text{Aut}(\Gamma)$ passes to the quotient $X/G$ and $X_\sigma$ is a $G$-set.
Let $\Gamma \rtimes_{\sigma} \mathbb{Z}$ be the semidirect product of $\Gamma$ and $\mathbb{Z}$ induced by the map $\mathbb{Z} \to \text{Aut}(\Gamma)$ that takes 1 to $\sigma$. A homomorphism $\Phi \in \text{Hom}(\Gamma \rtimes_{\sigma} \mathbb{Z}, G)$ is uniquely determined by the pair $(\phi, g)$, where $\phi := \Phi_\Gamma$ and $g \in G$ is the image of $(1, 1) \in \Gamma \rtimes_{\sigma} \mathbb{Z}$. The necessary and sufficient condition for $(\phi, g)$ to arise from a $\Phi$ in this way is

$$\phi''(\gamma) = g\phi(\gamma)g^{-1}, \quad \gamma \in \Gamma.$$

In particular, $\phi \in \text{Hom}_{\sigma}(\Gamma, G)$. It follows that if we fix one pair $(\phi, g)$ then the set of all other pairs $(\phi, g')$ are given by setting $g' = gs$ with $s \in \text{Stab}_G(\phi)$. We may hence define an action of $\text{Stab}_G(\phi)$ on these pairs by setting $s \cdot (\phi, g) := (\phi, gs^{-1})$. This proves the following.

**Proposition 3.1.** With the above notation for any finite group $G$ the map

$$\text{Hom}(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) \to \text{Hom}_{\sigma}(\Gamma, G)$$

given by restriction is a $G$-torsor of $\text{Hom}_{\sigma}(\Gamma, G)$.

Combining Proposition 3.1 with Lemma 2.1 we obtain the following corollary

**Corollary 3.2.** If $\Gamma \rtimes_{\sigma} \mathbb{Z}$ is finitely generated then

(i) $\text{Hom}_{\sigma}(\Gamma, G)$ is finite,

(ii) moreover,

$$\frac{1}{|G|} \# \text{Hom}(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) = \#(\text{Hom}_{\sigma}(\Gamma, G)/G).$$

We should point out that for a finitely generated group $\tilde{\Gamma}$ to be isomorphic to a $\Gamma \rtimes_{\sigma} \mathbb{Z}$ for some $\Gamma$ and $\sigma$ is equivalent to having infinite abelianization. If $\tilde{\Gamma}$ has finite abelianization $A$ then picking, say, $G = \mathbb{Z}/p\mathbb{Z}$ with $p$ a prime not dividing $|A|$ we see that $|G|$ does not always divide $\# \text{Hom}(\tilde{\Gamma}, G)$. We have proved the following.

**Corollary 3.3.** A finitely generated group $\Gamma$ has the property that $|G|$ divides $\# \text{Hom}(\Gamma, G)$ for every finite group $G$ if and only if it has infinite abelianization.

We can extend the previous results as follows. Let $C_i$ be an indexed collection of (not necessarily distinct) conjugacy classes in $G$, and let $S_i$ be a collection of subsets of $\Gamma$. Let $\text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) \subseteq \text{Hom}(\Gamma \rtimes_{\sigma} \mathbb{Z}, G)$ consist of those homomorphisms $\Phi$ such that $\Phi(S_i) \subseteq C_i$ for all $i$. Define $\text{Hom}'_{\sigma}(\Gamma, G) \subseteq \text{Hom}_{\sigma}(\Gamma, G)$ similarly and let $\pi'$ be the restriction of $\pi$ to $\text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G)$.

**Theorem 3.4.** The map $\pi'$ takes $\text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G)$ to $\text{Hom}'_{\sigma}(\Gamma, G)$ and

$$\pi' : \text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) \to \text{Hom}'_{\sigma}(\Gamma, G)$$

is a $G$-torsor of $\text{Hom}'_{\sigma}(\Gamma, G)$.

**Proof.** Note that $\text{Hom}'_{\sigma}(\Gamma, G)$ is indeed a sub-$G$-set of $\text{Hom}_{\sigma}(\Gamma, G)$ since the $C_i$ are conjugacy classes and $\text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) = \pi^{-1}(\text{Hom}'_{\sigma}(\Gamma, G))$. Now the claim follows from Proposition 3.1.

As before we obtain

**Corollary 3.5.** Let $\Gamma \rtimes_{\sigma} \mathbb{Z}$ be finitely generated. Then

$$\frac{1}{|G|} \# \text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G) = \#(\text{Hom}'_{\sigma}(\Gamma, G)/G).$$

**Remark 3.6.** The fact that $|G|$ divides $\# \text{Hom}'(\Gamma \rtimes_{\sigma} \mathbb{Z}, G)$ when $\Gamma \rtimes_{\sigma} \mathbb{Z}$ is a free group of rank $n$, the conjugacy classes $C_i$ are indexed by $1, 2, \ldots, m$ with $m < n$, and each $S_i$ is a singleton is the main result of [4].
4 Examples

We illustrate some of the issues concerning the ratio \( \# \text{Hom}'(\tilde{\Gamma}, G)/|G| \) with a few examples.

1. Take \( \tilde{\Gamma} \) to be the free group \( F \) in \( k-1 \) generators given as \( \langle x_1, \ldots, x_k \mid x_1 \cdots x_k = 1 \rangle \) for some \( k > 1 \) and \( S_i = \{ x_i \} \) for \( i = 1, 2, \ldots, k \). Fix a finite group \( G \) and conjugacy classes \( C_1, \ldots, C_k \) of \( G \) and let \( \text{Hom}'(F, G) \) be as above. In general there is no reason to expect \( \# \text{Hom}'(F, G) \) to be divisible by \( |G| \), though the denominator of the quotient is often much smaller than \( |G| \).

By a formula extending (1.0.2) we have

\[
\frac{\# \text{Hom}'(F, G)}{|G|} = \sum_{\chi} \frac{\chi(1)^2}{|G|} \prod_{i=1}^{k} f_\chi(C_i),
\]

where the sum is over all irreducible characters of \( G \) and for a conjugacy class \( C \) we define

\[
f_\chi(C) := \frac{\# C \chi(x)}{\chi(1)}, \quad x \in C.
\]

It is known that \( f_\chi(C) \) is an algebraic integer.

For example, take \( G = S_n \), the symmetric group in \( n \) letters, and let \( C_i \), for \( i = 1, 2, \ldots, k \), be the conjugacy class of an \( n \)-cycle \( \rho := (1 \cdots n) \). The irreducible characters \( \chi_1 \) of \( S_n \) are parametrized by partitions \( \lambda \) of \( n \) and \( \chi_1(\rho) = (-1)^{\lambda} \) if \( \lambda = (n-r, 1, \ldots, 1) \) is the \( r \)-th hook and \( \chi_1(\rho) = 0 \) otherwise.

A short calculation then shows that

\[
\frac{1}{|G|} \# \text{Hom}'(F, G) = \frac{1}{n^2} \sum_{r=0}^{n-1} (-1)^r r!(n-r-1)! k^{k-2},
\]

which is typically not an integer; for example, for \( k = 2 \) it equals \( n^{-1} \). In fact, for \( k > 2 \) this quantity is an integer unless \( n \) is a prime not dividing \( k-1 \), in which case the denominator equals \( n \). (We thank J. Gunther for showing us a proof of this fact.)

2. In the previous example take \( k = 4 \) and \( G = \text{SL}_2(\mathbb{F}_q) \) for some \( q = p^r \) with \( p > 2 \) a prime. For simplicity pick \( C_i \), for \( i = 1, \ldots, 4 \), to be the conjugacy class of a diagonal matrix with eigenvalues \( \lambda_i, \lambda_i^{-1} \in \mathbb{F}_q^* \). Then using the known description of the irreducible characters of \( G \) we find after some calculation that in this case

\[
\frac{1}{|G|} \# \text{Hom}'(F, G) = q^2 + 4q + 1 + a \frac{q^2}{q-1},
\]

where

\[
a := \frac{1}{2} \# \{ (e_1, \ldots, e_4) \in (\pm 1)^4 \mid \lambda_1^{e_1} \cdots \lambda_4^{e_4} = 1 \}.
\]

If \( q \) is sufficiently large there will be a choice of eigenvalues \( \lambda_1, \ldots, \lambda_4 \) such that \( a = 0 \), in which case \( \# \text{Hom}'(F, G)/|G| = q^2 + 4q + 1 \) is polynomial in \( q \). In fact, with this choice of generic eigenvalues the action of \( G \) by conjugation on \( \# \text{Hom}'(F, G) \) is actually free explaining the divisibility. (See [1] for more details.)

3. Consider the group \( \tilde{\Gamma} := \langle u_1, \ldots, u_n, z_1, \ldots, z_k \mid w(u_1, \ldots, u_n) \cdot z_1 \cdots z_k = 1 \rangle \), where \( n \geq 1 \) and \( w \) is an arbitrary word in \( u_1, \ldots, u_n \) that belongs to the commutator of the free group \( \langle u_1, \ldots, u_n \rangle \). Pick a non-trivial homomorphism \( \psi : \tilde{\Gamma} \to \mathbb{Z} \) with \( \psi(z_i) = 0 \) for \( i = 1, 2, \ldots, k \) and let \( \Gamma := \ker \psi \). Take \( S_i = \{ z_i \} \) for \( i = 1, 2, \ldots, k \) and pick arbitrary conjugacy classes \( C_1, \ldots, C_k \) in \( G \). Then by Corollary 3.3 \( |G| \) divides \( \# \text{Hom}'(\tilde{\Gamma}, G) \). Concretely, the number of solutions to the equation

\[
w(u_1, \ldots, u_n) \cdot z_1 \cdots z_k = 1, \quad u_i \in G, \quad z_i \in C_i
\]

is divisible by \( |G| \) for any finite group \( G \). If we take \( k = 0 \) and \( w = [x_1, y_1] \cdots [x_g, y_g] \) this yields the case of a Riemann surface (1.0.3) considered in the introduction.
Consider for example, $w = x^2y^2x^{-2}y^{-2}$ and $G = \text{PSL}_2(\mathbb{Z})$. Then the values of $s_h(w)\chi(1)$ for the different irreducible characters (computed using Magma) and their sum are as follows

$$1 + 29/6 + 29/6 + 551/33 + 547/33 + 296/15 + w + w' = 112,$$

where $w, w' \in \mathbb{Q}(\sqrt{5})$ are the roots of

$$3025x^2 - 146190x + 1766236 = 0.$$

(The corresponding character dimensions $\chi(1)$ are 1, 5, 5, 10, 10, 11, 12, 12.)

While testing this question numerically we discovered that for some words, for example $w = x^2yxy^2$, it did indeed seem that $s_h(w)\chi(1) \in \mathbb{Z}$ for all $\chi$. It turns out not difficult to show why. Consider more generally $w = x^{-m}y^nx^{-1}$ (take $m = -2, n = 1$ and replace $x$ by $xy$ to obtain a conjugate of the word $x^2yxy^2$ just mentioned). The resulting group $\hat{\Gamma}$ is called a Baumslag–Solitar group.

Let $V$ be an irreducible representation of $G$ over $\mathbb{C}$ with character $\chi$. For a fixed $u \in G$ let

$$U := \frac{1}{|G|} \sum_{y \in G} yuy^{-1} \in \text{End}(V).$$

It is easy to check that $U$ preserves the $G$ action on $V$. Hence by Schur’s lemma it must be of the form $y\text{id}_V$. Computing traces we find that $\gamma = \chi(u)/\chi(1)$. Setting $u = x^m$ and computing the trace of $x^{-m}U$ we finally find that

$$\chi(1)s_h(w) = \langle \Psi^m\chi, \Psi^m\chi \rangle,$$

where $(\alpha, \beta) := 1/|G| \sum_{x \in G} \alpha(x)\beta(x)$ is the standard inner product of class functions and $\Psi^m(x) := x(x^m)$ is the $m$-th Adams operations on (virtual) characters. In particular, $\chi(1)s_h(w)$ is an integer for all $\chi$.

More directly, if $n = 1$ we can count the solutions to $xyy^{-1} = x^m$ with $x, y \in G$ as follows. Group the solutions according to the conjugacy class $C$ of $x$. This class must satisfy $C^m = C$ and contributes precisely $|G|$ to the total since for fixed $x \in C$ we have that $y$ lies in a coset of the centralizer of $x$. Hence in this case

$$\frac{1}{|G|} \# \text{Hom}(\hat{\Gamma}, G) = \#(C^m = C).$$

For example, for $G = \text{SL}_2(\mathbb{F}_p)$ it is not hard to verify that when $m$ is even this number equals

$$1 + \delta_p(m) + \frac{1}{2} \sum_{\varepsilon_1, \varepsilon_2 = \pm 1} \gcd(p + \varepsilon_1, m + \varepsilon_2) - 1,$$

where $\delta_p(m) = 2$ if $m$ is a square modulo $p$ and is zero otherwise.
5 Subgroups

It is a consequence of the exponential formula in combinatorics that for a finitely generated group $\tilde{\Gamma}$ we have

$$F(x) := \sum_{n \geq 0} \frac{\# \text{Hom}(\Gamma, S_n)}{n!} = \exp\left(\sum_{n \geq 1} \frac{u_n(\tilde{\Gamma}) x^n}{n}\right),$$

where $u_n(\tilde{\Gamma})$ denotes the number of subgroups of $\tilde{\Gamma}$ of index $n$ (see for example [2],[5]). By Corollary 5.3 if $\tilde{\Gamma}$ has infinite abelianization then the series on the left hand side has integer coefficients and hence may be written as an infinite product

$$F(x) = \prod_{n \geq 1} (1 - x^n)^{-v_n(\tilde{\Gamma})},$$

for certain integers $v_n(\tilde{\Gamma})$. Comparing the two expressions we find that

$$u_n = \sum_{d \mid n} d v_d$$  \hspace{1cm} (5.0.5)

and by Möbius inversion

$$v_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) u_d.$$  \hspace{1cm} (5.0.6)

As before we can write $\tilde{\Gamma} = \Gamma \rtimes \mathbb{Z}$ and by Corollary 5.2 we get

$$F(x) = \sum_{n \geq 0} \frac{\#(\text{Hom}_{\sigma}(\Gamma, S_n)/S_n)}{n!} x^n.$$  \hspace{1cm}

We can interpret the $n$-th coefficient of this series as the number of isomorphism classes of $\sigma$-equivariant actions of $\Gamma$ on a set of $n$ elements. It follows that the exponents $v_n(\Gamma)$ count the number of such actions which are indecomposable (i.e., transitive). In particular, $v_n(\Gamma)$ is a non-negative integer.

If $\sigma$ is trivial, equivalently if $\tilde{\Gamma} = \Gamma \times \mathbb{Z}$ is a direct product, then isomorphism classes of transitive actions of $\Gamma$ on $n$ objects corresponds to conjugacy classes of subgroups of $\Gamma$ of index $n$. (This interpretation of $v_n(\tilde{\Gamma})$ appears as exercise 5.13 (c) in [5] with a different suggested proof.)

From (5.0.5), we obtain the following.

**Proposition 5.1.** Let $\tilde{\Gamma}$ be a finitely generated group with infinite abelianization and let $u_n := u_n(\tilde{\Gamma})$ be its number of subgroups of index $n$. Then for every prime number $p$ we have

$$u_{p^{k+1}} \equiv u_{p^k} \mod p^{k+1}.$$  \hspace{1cm}

Here is a short table of the numbers $u_n$ in the case of $\tilde{\Gamma} = \pi_1(S_g)$, the fundamental group of a genus $g$ Riemann surface,

| $g \backslash n$ | 1 | 2 | 3 | 4 | 5 |
|-----------------|---|---|---|---|---|
| 1               | 1 | 3 | 4 | 7 | 6 |
| 2               | 1 | 15| 220|5275|151086|
| 3               | 1 | 63| 7924|2757307|2081946006|
| 4               | 1 | 255|281740|1542456475|2975792813886|
| 5               | 1 | 1023|10095844|882442672507|429988374084026406|

and the corresponding numbers $v_n$.
\begin{tabular}{|c|c|c|c|c|c|}
\hline
$g\backslash n$ & 1 & 2 & 3 & 4 & 5 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 7 & 73 & 1315 & 30217 \\
3 & 1 & 31 & 2641 & 689311 & 416389201 \\
4 & 1 & 127 & 93913 & 385614055 & 5973474562777 \\
5 & 1 & 511 & 3365281 & 22061067871 & 85997674816805281 \\
\hline
\end{tabular}

References

[1] T. Hausel, E. Letellier and F. Rodriguez Villegas, *Arithmetic harmonic analysis on character and quiver varieties* (to appear in Duke Math. J.)

[2] A. D. Mednykh, *On the solution of the Hurwitz problem on the number of nonequivalent coverings over a compact Riemann surface* (Russian) Dokl. Akad. Nauk SSSR 261 (1981), 537–542.

[3] J.-P. Serre, *Topics in Galois theory* Research Notes in Mathematics, 1 A K Peters, Ltd., Wellesley, MA, 2008

[4] L. Solomon, *The solution of equations in groups* Arch. Math. 20 (1969) 241–247

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