# The Asymptotic Genus of a Group

Daniel Frohardt
Robert Guralnick
Kay Magaard

October 25, 2006

## Introduction

As in [Gur], we define the genus of a finite permutation group $G$ to be the minimal genus of a Riemann surface $X$ such that $G \cong \mathrm{Mon}(X, \phi)$ where $\phi : X \to P^1(C)$ is a covering of the extended complex plane by $X$. It is known that if $G$ has a nonabelian composition factor $S$ that is not an alternating group, then the genus of $G$ goes to infinity as $|S|$ does. In the present paper we consider a larger class of groups and obtain asymptotic lower bounds for the relative genus, that is, the ratio of the genus to the degree. This generalizes results appearing in [Gur] and [FM.comp].

Let $X$ be a compact Riemann surface of genus $g$, and let $\phi : X \to P^1(C)$ be an $n$-cover. The monodromy group $\mathrm{Mon}(X, \phi)$ is a transitive permutation group of degree $n$. It is realized by the action of $\pi_1(P^1(C) \setminus B)$ on the image $\phi^*(\pi_1(X \setminus A))$ where $B$ is the set of branch points in $P^1(C)$, $A = \phi^{-1}(B)$, and $\phi^*$ is the embedding of $\pi_1(X \setminus A)$ into $\pi_1(P^1(C) \setminus B)$ induced by $\phi$. If $G = \mathrm{Mon}(X, \phi)$, then $G$ contains nontrivial elements $x_1, \ldots, x_r$ such that

1. $G = \langle x_1, \ldots, x_r \rangle$.
2. $x_1 \cdot x_2 \cdot \ldots \cdot x_r = 1$.
3. $\sum \mathrm{Ind}(x_i) = 2(n + g - 1)$.

Note that $\mathrm{Ind}(x)$ is the permutation index of $x$, which is just $n - \mathrm{Orb}(x)$ where $\mathrm{Orb}(x)$ is the number of orbits of $\langle x \rangle$.

For convenience, say that $\underline{x} = (x_1, \ldots, x_r)$ is a generating tuple for $G$ when (1) and (2) hold.

If $\underline{x}$ is a generating tuple for $G$ and $\Omega$ is a transitive $G$-set, then the *genus of the system* $(G, \Omega, \underline{x})$ is the value of $g$ such that

$$\sum \mathrm{Ind}(x_i) = 2(|\Omega| + g - 1)$$

where $\mathrm{Ind}(x_i)$ is the index of $x_i$ as a permutation of $\Omega$.

If $\Omega$ is a transitive $G$-set, then $g(G, \Omega)$, the genus of the action of $G$ on $\Omega$ is defined to be the smallest value of the genus of $(G, \Omega, \underline{x})$ for $\underline{x}$ a generating tuple of $G$.

The Riemann Existence Theorem states that if $G$ is a permutation group of degree $n$ containing elements $x_i$ satisfying (1)–(3) then there is a Riemann surface $X$ of genus $g$ such that $G \cong \mathrm{Mon}(X, \phi)$ for some $n$-covering $\phi : X \to P^1(C)$. The genus of a finite group can therefore be described in purely group theoretic terms. It is the smallest value of $g(G, \Omega)$ where $\Omega$ is a tranistive $G$-set. We can define the *primitive* genus of $G$ to be the minimal value of $g(G, \Omega)$ where $\Omega$ is a primitive $G$-set.

The natural actions of the symmetric groups and cyclic groups are genus 0 actions. However, it is known [FM.comp] that for each non-negative integer $g$ there is a finite set $\mathcal{E}(g)$ of simple groups such that if $G$ is a group of genus $g$ and $S$ is a nonabelian composition factor of $G$ then either $S$ is an alternating group or $S \in \mathcal{E}(g)$.

The purpose of this paper is to show that for primitive actions, $g/n$, the ratio of the genus to the degree, must asymptotically be at least 1/84 if $G$ is required to have a non-abelian composition factor that is not an alternating group. More specifically, we prove the following.

**Theorem** *For every $\epsilon > 0$ there is an integer $n$ such that if $G$ is a noncyclic group and $F^*(G)$ is neither an alternating group nor a product of alternating groups, then*

$$g(G, \Omega) > \left(\frac{1}{84} - \epsilon\right) |\Omega|$$

*for every primitive faithful $G$-set $\Omega$ of degree at least $n$*

The assumption of primitivity is necessary. See Section 5.

# 1 Notation

Set $\underline{d} = (d_1, \ldots, d_r)$ where $d_i = o(x_i)$ and

$$A(\underline{d}) = \sum_{i=1}^{r} \frac{d_i - 1}{d_i}.$$

From the Cauchy-Frobenius Formula, we have

$$\frac{g}{n} = \frac{1}{2}(A(\underline{d}) - 2) + \frac{1}{n} - \frac{1}{2} \sum_{i=1}^{r} \frac{1}{d_i} \sum_{y \in \langle x_i \rangle^\sharp} \mathrm{fpr}(y) \tag{1}$$

where $\mathrm{fpr}(y)$ is the fixed point ratio of $y$, that is, $|\mathrm{Fix}(y)|/n$, where $\mathrm{Fix}(y)$ is the set of points of $\Omega$ fixed by $y$. For convenience, we shall use $f(x)$ to denote the fixed point ratio of $x$.

The point of the analysis is to show that the contribution of the fixed point ratios to the right hand side of (1) is asymptotically bounded above by $\frac{1}{2}(A(\underline{d})-2) - \frac{1}{84}$.

**Definition** *Write* $A \succeq B$ *[or* $B \preceq A$*] if for every* $\epsilon > 0$ *there is an* $n_0$ *such that* $A \geq B - \epsilon$ *whenever* $n > n_0$*.*

In this notation, the Main Theorem states that $g/n \succeq 1/84$.

Say that $G$ is a linear group provided that either $G \subseteq GL(V)$ or $G \subseteq PGL(V)$ for some vector space $V$.

**Definition** *For* $V$ *a finite dimensional vector space over* $\mathbf{F}$ *and* $x \in GL(V)$*, set* $v(x) = \min(\{\dim_{\mathbf{F}}[V, \lambda x] \mid \lambda \text{ is a scalar in}) \mathbf{F}\})$*.*

Since $v(\lambda y) = v(y)$ for all $\lambda \in Z(GL(V))$, this induces a function on $PGL(V)$, also denoted $v$. The function $v$ defined on linear groups is analogous to the index function defined on permutation groups.

## 2 Primitive Actions

Let $G$ be a primitive permutation group of degree $n$ with point stabilizer $M$. Let $F = F^*(G)$, the generalized Fitting subgroup of $G$. By the Aschbacher-O'Nan-Scott Theorem (see [KurSte], 6.6.12), one of the following is true. We follow the breakdown in [GurTho].

1. (Affine action) [GT case A] $F$ is an elementary abelian $p$-group for some prime $p$.
2. (Diagonal action) [GT case B] $F = N_1 \times N_2$ where $N_1$ and $N_2$ are isomorphic, simple, and normal in $G$, and $F \cap M \cong N_1$.
3. $F = K_1 \times \ldots \times K_t$ where $K_1$ is simple, $G$ permutes $\{K_i\}$ transitively by conjugation, and one of the following is true.
   (a) (Twisted wreathed product action) [GT case C1] $t > 1$ and $F \cap M = 1$.
   (b) (Wreathed product action) [GT case C2] $t > 1$, $F \cap M \neq 1$, and $F \cap K_1 = 1$.
   (c) (Almost simple action) [part of GT case C3] $t = 1$.
   (d) (Product action) [part of GT case C3] $t > 1$, and If $M_0 = N_M(K_1)$, $G_0 = K_1 M_0$, and $\overline{G}_0 = G_0/C_{G_0}(K_1)$, then $\overline{M}_0$ is a maximal subgroup of $\overline{G}_0$.

## 2.1 Fixed Point Analysis

The purpose of this subsection is to prove the following.

**Lemma 1** *For every $\epsilon > 0$, there is an $n_0$ such that if $n > n_0$ and $x \in G^\sharp$, then one of the following holds.*

1. *$G$ is cyclic.*

2. *$F$ is a direct product of (one or more) alternating groups.*

3. *$f(x) < \epsilon$.*

4. *There is a homomorphic image $\widehat{G}$ of $G$ such that*

   (a) *$\widehat{G}$ is a linear group over $\mathbf{F}_p$,*

   (b) *$\widehat{G}$ is not cyclic, dihedral, or isomorphic to $A_4$, $S_4$, or $A_5$,*

   (c) *$\widehat{x} \neq 1$, and*

   (d) *$f(x) < p^{-v(\widehat{x})} + \epsilon$.*

5. *$(G, M)$ is a diagonal action and one of the following holds.*

   (a) *$f(x) \leq 1/3600$ and $x$ induces a nontrivial permutation of index at most $\log_{60}(1/\epsilon)$ on the set $\mathcal{K}(F)$ of components of $F$.*

   (b) *$f(x) \leq 1/60$ and $x$ induces a transposition on $\mathcal{K}(F)$.*

Proof. We consider in turn the cases of the Aschbacher-O'Nan-Scott Theorem. Without loss, assume that $x \in M$.

In the affine case, we may assume that $G$ is noncyclic. We have $n = p^t$ for some prime $p$ and some positive integer $t$. $F$ is a regular normal subgroup of order $p^t$ and $G = FM$. Letting $V = F$, we have a map $\phi : G \to GL(V)$ with $\phi(G) \cong G/V \cong M$. We have $|\mathrm{Fix}(x)| = |C_V(\phi(x))| \leq p^{t-v(\phi(x))}$. Thus, $f(x) \leq p^{-v(\phi(x))}$.

In particular, $f(x) \leq 1/p$ for $x \in G^\sharp$. We claim that if $G/F$ is cyclic, dihedral or of type $A_4$, $S_4$, or $A_5$, then $f(x) \to 0$ as $n \to \infty$. If $G/H$ is cyclic, then $f(x) \leq 1/n$ for all $x \in G^\sharp$. If $G/H$ is dihedral, then $|\mathrm{Fix}(x)| \leq |V|^{1/2}$ for all $x \in G^\sharp$. The action of $G/V$ must be irreducible, so the rank $t$ of $V$ is bounded if $G/H$ is of types $A_4, S_4$ or $S_5$, and $p \to \infty$ as $n = p^t \to \infty$. The claim follows, and the conclusion of the lemma holds in the affine case.

Suppose $(G, M)$ is a diagonal action. Then

1. $F^*(G) = N_1 \times N_2$ where $N_1$ and $N_2$ are isomorphic, nonabelian simple, normal subgroups of $G$.

2. $M \cap F^*(G) = D$ and $M = N_G(D)$.

3. The projections $\pi_i : N_1 \times N_2 \to N_i$, $i = 1, 2$ become isomorphisms when restricted to $D$.

4. $G = MN_2$.

$N_2$ is thus a set of right coset representatives of $M$ in $G$, and the action of $M$ on $\Omega$ is isomorphic to the action of the almost simple group $M$ on $D = F^*(M)$ by conjugation. We have $|\mathrm{Fix}(x)| = |C_D(x)|$, so $f(x) = 1/[D : C_D(x)]$. In particular, if $f(x) \geq 1/m$ for some positive integer $m$, then $D$ is isomorphic to a subgroup of $\mathrm{Sym}(m)$, so $|D| \leq m!$. This implies that

$$\max\left(\{f(x) \ \mid \ x \in G^\sharp\}\right) \to 0 \text{ as } n \to \infty.$$

Now suppose that $(G, M)$ is a wreathed product action. Then

1. $F^*(G) = N_1 \times \ldots \times N_s$
2. $M$ acts transitively on $\{N_1, \ldots, N_s\}$
3. $F \cap M = (N_1 \cap M) \times \ldots \times (N_s \cap M)$
4. For every $E \in \mathcal{K}(N_i)$ the mapping $N_i \cap M \to E$ with $x \mapsto \pi_E(x)$ is an $N_M(E)$-isomorphism, $i = 1, \ldots, s$.
5. $N_M(K)/C_M(K) = KN_M(K)/C_M(K)$
6. $|\Omega| = (k^{t-1})^s$ where $t$ is the number of components $E$ in $\mathcal{K}(N_i)$ and $k = |E|$, for each such $E$

Consider first the special case $s = 1$. Let $\pi_i, i = 1, \ldots, t$ be the projection of $N_1$ onto $E_{1i}$ and let $\widetilde{\pi}_i : N_1 \to E$ be the composition of $\pi_i$ with the isomorphism $E_i \to E$ so that $M \cap N_1 = \{a \in N_1 \ \mid \ \widetilde{\pi}_i(a) = \widetilde{\pi}_1(a) \text{ for all } i\}$.

The map $\widetilde{\pi} : M \cap N_1 \to E$, defined to be the common value of $\widetilde{\pi}_i$ for all $i$, is thus an isomorphism.

The group $E_2 \times \ldots \times E_t$ is a complement to $M$ in $G$. The action of $x \in M \cap N_1$ on $\Omega$, or more generally of $x \in \cap_j N_M(E_j)$ which is almost simple of type $E$, is permutation isomorphic to the product action of $\widetilde{\pi}(x)$ on $E_2 \times \ldots \times E_t$ by conjugation. Thus $|\mathrm{Fix}(x)| = |C_E(\widetilde{\pi}(x))|^{t-1}$, so

$$f(x) = |(\widetilde{\pi}(x))^E|^{-(t-1)}.$$

Since either $t \to \infty$ or $k \to \infty$ as $|\Omega| = k^{t-1} \to \infty$, it follows that $f(x) \to 0$ as $|\Omega| \to \infty$.

Let $x \in M$, and let $\overline{x}$ be the image of $x$ in $\mathrm{Sym}_s$. If $\overline{x}$ fixes a point, say 1, in $\{1, \ldots, s\}$, then for every orbit $\{i_1, \ldots, i_u\}$ of $\overline{x}$, $i_j > 1$ for all $j$, the projections $\pi_{i_j}(a)$, $j = 2, \ldots, u$, are determined by $\pi_{i_1}(a)$. This implies that $|\mathrm{Fix}(x)| \leq k^{\mathrm{Orb}(\overline{x})-1}$, so $f(x) \leq k^{-\mathrm{Ind}(\overline{x})}$. In particular,

$$f(x) \leq \begin{cases} 1/60 & \text{for all } x \\ 1/3600 & \text{if } x \text{ does not induce a transposition on } \{1, \ldots, s\}. \end{cases}$$

If $\overline{x}$ has no fixed points on $\{1, \ldots, r\}$, then $|\mathrm{Fix}(x)| \leq k^{\mathrm{Orb}(\overline{x})} \leq k^{t/2}$. This implies that $f(x) \leq k^{1-t/2}$. If $t > 2$, then $f(x) \to 0$ as $|\Omega| \to \infty$. (Recall that if $t$ is bounded, then $k \to \infty$.) If $t = 2$, then $x^2 \in N_M(E_1)$ and $f(x) \leq f(x^2)$, so $f(x) \to 0$ as $\Omega \to 0$ unless $x^2 = 1$. We may therefore assume that $x^2 = 1$. Setting $x = x_0\tau$ for $x_0 \in M_1$ and $\tau$ a transposition, we have $x_0^2 = 1$. The action of $x$ on $\Omega$ is equivalent to the action on $E$ defined by $b \mapsto b^{-x_0}$. Thus the fixed points of $x$ on $\Omega$ are in one-to-one correpondence with the elements $b$ of $E$ with $b = b^{-x_0}$. Since $x_0^2 = 1$. $b = b^{-x_0}$ if and only if $(bx_0)^2 = 1$. Thus $|\mathrm{Fix}(x)| = 1 + |\mathrm{Inv}(\mathrm{Aut}(E))|$. This implies that

$$f(x) \to 0 \text{ as } |\Omega| \to \infty.$$

NEED TO CONSIDER: the case $s > 1$.

Suppose $(G, M)$ is an almost simple action. In view of CFSG, it suffices to assume that $G$ is of Lie type. It follows from results of Liebeck-Saxl [LieSax] and Liebeck-Shalev [LieSha] that either $f^* \to 0$ as $n \to \infty$ or $G$ has a subspace action over a field of bounded order.

We may therefore assume that $G$ is a linear group with module $V$ over $\mathbf{F}_p$. The following theorem, which is the main result of [FM.grass], applies.

**Theorem 2 (Grassmannian Theorem)** *There is a real-valued function $\epsilon_1$, defined on the set of finite vector spaces such that $\epsilon_1(V) \to 0$ as $|V| \to \infty$ and if $V$ is the module for a subspace action of $G$ then*

$$\mathrm{fpr}(y) \leq p^{-v(y)} + \epsilon_1(V) \text{ for all } y \in G.$$

Since $|V| \to \infty$ as $n \to \infty$ (4) must hold.

Suppose $(G, M)$ is a product action. It suffices to assume that $F$ is a direct product of linear groups. $G$ acts on the product $\Omega_1 \times \ldots \times \Omega_t$.

If $x$ stabilizes each $\Omega_i$, then $\mathrm{Fix}_\Omega(x) = \prod \mathrm{Fix}_{\Omega_i}(x)$, and $f(x) = \prod f_i(x_i)$, where $f_i$ is the fixed point ratio of the restriction $x_i$ of $x$ to $\Omega_i$. Since $f_i(x) < p^{-v_i(x_i)} + \epsilon_i$, it follows that $f(x) < p^{-\sum v_i(x_i)} + \epsilon^*$ where $\epsilon^* \to 0$ as $n \to \infty$. If $W_i$ is an eigenspace of maximal dimension for $x_i$ acting on $V_i$, then $\otimes W_i$ is an eigenspace for $x$ acting on $V = \otimes V_i$. This implies that $v(x) \leq \mathrm{codim}_V W = \sum \mathrm{codim}_{V_i} W_i = \sum v(x_i)$. Therefore $f(x) < p^{-v(x)} + \epsilon^*$.

We claim that if $x$ permutes $\{\Omega_i\}$ nontrivially, then $f(x) \to 0$ as $n \to 0$.

Let $k = |\Omega_1|$. Then $n = k^t$. If $x$ permutes $\{\Omega_i\}$ nontrivially, then $f(x) \leq k^{-\mathrm{Ind}(x^*)}$ where $x^*$ is the permutation $x$ induces on $\{\Omega_i\}$. In particular $f(x) \leq k^{-1} \leq 1/7$.

Suppose $s$ elements of the tuple $\underline{x}$ act nontrivially on $\{\Omega_i\}$. If $s > 4$, then the contribution from these elements to the right side of (1) is at least $\frac{1}{2}\left(\frac{5}{2} \cdot \frac{6}{7}\right) > 85/42$. We may therefore assume that $s \leq 4$.

If $s = 4$, then

Ir $s = 3$, then Bound $r$ (hence, also, $s$), by using that all ratios are at most $1/2$ and the permutation ratios are at most $1/7$.

Use argument of GT, p. 338, paragraph 2, to bound number of components once $s \leq 4$.

GAP

Suppose $(G, M)$ is a twisted wreath product action. $M \cap F^*(G) = 1$.

GAP

$n = k^t$ where $k = |N_1|$. Every $x \in M^\sharp$ must permute $\{N_i\}$ nontrivially and $f(x) \le k^{-\mathrm{Ind}(x^*)}$, as in the previous analysis.

## 2.2 Reduction to the linear case

In view of (1), we have:

**Lemma 3** *If $f^*$ is the largest fixed point ratio of a nontrivial element of $G$, then*

$$\frac{g}{n} > \frac{1}{2}\Big(A(\underline{d})(1 - f^*) - 2\Big).$$

**Lemma 4** *If $(G, M)$ is a diagonal action, then $g/n \succeq 1/84$.*

Proof. We have $f(x) \le 1/60$ for all $x$ and $f(x) \le 1/3600$ if $x$ does not have order 2. Furthermore $f(x) \to 0$ if the permutation index of $x$ acting on the components is unbounded.

By straightforward computation, if $\underline{d}$ is not of type $(2,3,7), (2,3,8), (2,3,9)$, or $(2,4,5)$ then $A(\underline{d})(1 - 1/60) > 85/42$. It therefore suffices to assume that $\underline{d}$ is one of the types listed.

If $\underline{d} = (2,3,7)$ then $G$ is necessarily perfect, so $G$ is generated by at most 3 conjugates of $x_i$, $i = 1,2,3$. This implies that $\mathrm{Ind}(x_i) \ge (n-1)/3$ for all $i$, so $f(x_i) \to 0$ as $n \to \infty$.

If $\underline{d} = (2,3,8), (2,3,9)$, or $(2,4,5)$, then (1) and the conditions on $f(x_i)$ imply that $g/n \ge 1/84$. $\square$

## 2.3 The function $\theta$

**Lemma 5** *$r \le 8$ and*

$$\frac{g}{n} \succeq \frac{1}{2}A(\underline{d}) - 2 - \sum_{i=1}^{r} \theta_i$$

*where*

$$\theta_i = \theta(x_i) = \frac{1}{d_i}(1 + \sum_{y \in \langle x_i \rangle^\sharp} p^{-v(y)}).$$

Proof. Set $\Xi(\underline{x}) = A(\underline{d}) - 2 - \sum_{i=1}^{r} \theta_i$.

Then

$$\sum_i \frac{1}{d_i} \sum_{y \in \langle x_i \rangle^\sharp} f(y) \le \left( \sum_i \frac{1}{d_i} \sum_{y \in \langle x_i \rangle^\sharp} p^{-v(y)} \right) + A(\underline{d})\epsilon_1(V).$$

It follows that
$$\frac{g}{n} \geq \frac{1}{2}\Xi(\underline{x}) + \frac{1}{n} - \frac{1}{2}A(\underline{d})\epsilon_1(V) \tag{2}$$

We have $p^{-v(y)} \leq 1/2$ for all $y \in G^\sharp$, so $\Xi(\underline{x}) \geq A(\underline{d}) - 2 - \sum \frac{d_i - 1}{2d_i} = A(\underline{d})/2 - 2$. Evidently, $r/2 \leq A(\underline{d}) \leq r$. Therefore $\Xi(\underline{x}) \geq (r-8)/4$ and $\frac{1}{2}A(\underline{d})\epsilon_1(V) \leq r\epsilon_1(V)$. It follows that $\frac{g}{n} \geq \frac{r-8}{4} + \frac{1}{n} - r\epsilon_1(V) = (\frac{1}{4} - \epsilon_1(V))r - 2 + \frac{1}{n}$. If $r > 8$ then $g/n \succeq 1/8$ because $|V| \to \infty$ as $n \to \infty$, so we may assume that $r \leq 8$.

Now (2) implies that $\frac{g}{n} \geq \frac{1}{2}\Xi(\underline{x}) + \frac{1}{n} - 4\epsilon_1(V)$. The statement now follows easily. □

# 3 Bounding $\sum p^{-v(y)}$ in terms of $\underline{d}$ and $p$

To bound $g/n$ from below, it suffices to bound $\sum \theta_i$ from above. We do this by obtaining lower bounds on key values of $v(y)$.

## 3.1 Basic bounds

The most salient bounds on $v(y)$ are those that depend only on the order of $y$ and the prime $p$. For $d \geq 2$ and $p$ a prime, let $\mu_*(d,p)$ be the smallest positive integer $e$ such that there is an $\mathbf{F}_p$-vector space $V$ and a linear operator $x$ of order $d$ on $V$ such that $[V,x]$ has dimension $e$. This establishes the following

**6** *If $y$ has order $d$, then $v(y) \geq \mu_*(d,p)$.*

For each proper divisor $m$ of $d_i$, the group $\langle x_i \rangle$ contains exactly $\phi(d_i/m)$ elements of order $d_i/m$ where $\phi$ is the Euler $\phi$-function. Consequently,

$$\sum_{y \in \langle x_i \rangle^\sharp} p^{-v(y)} = \sum_{m | d_i, m < d_i} \phi(\frac{d_i}{m}) p^{-v(x_i^m)} \leq \sum_{m | d_i, m < d_i} \phi(\frac{d_i}{m}) p^{-\mu_*(\frac{d_i}{m}, p)}.$$

Setting
$$\zeta_0(d,p) = \frac{1}{d}\left(1 + \sum_{m | d, m < d} \phi(\frac{d}{m}) p^{-\mu_*(\frac{d}{m}, p)}\right)$$
we have

**7** $\theta(x_i) \leq \zeta_0(d_i, p)$.

The following bounds for $\zeta_0(d,p)$ will be used later.

**Lemma 8** *1.* $\zeta_0(d,p) \leq \frac{1}{d}\left(1 + (d-1)\frac{1}{p}\right) = \frac{1}{d} + \frac{1}{p} - \frac{1}{dp}$.

2. $\zeta_0(d,p) \le \dfrac{3}{d} + \dfrac{1}{25}$.

3. *If* $d \ge 50$ *then* $\zeta_0(d,p) \le 1/10$.

Proof. The first statement is an immediate consequence of the definition since $p^{-\mu_*(\frac{d}{m},p)} \le 1/p$ whenever $m < d$.

For $k = 1, 2, \ldots$, let $\mathcal{M}(p,k) = \{m \mid \mu_*(m,p) = p^{-k}\}$, the set of exponents $m$ for which $\mu_*(m,p) = p^{-k}$.

Set $M(p,k) = \sum_{m \in \mathcal{M}(p,k)} \phi(m)$ and $N(p,k) = \sum_{1 \le \ell \le k} M(p,\ell)$. Then $M(p,k)$ is an upper bound for the number of elements $y$ in a cyclic group with $o(y)$ belonging to $\mathcal{M}(p,k)$. Thus, for every positive integer $h$,

$$\zeta_0(d,p) \le \frac{1}{d}\left(1 + \sum_{k=1}^{h} M(p,k)p^{-k} + (d-1-N(p,h))p^{-(h+1)}\right). \qquad (3)$$

If $v(y) = 1$ for an element $y$ acting on an $F_p$-vector space, then either $y$ is a transvection, of order $p$, or $o(y)$ divides $p-1$. Therefore $N(p,1) = M(p,1) = \phi(p) + \phi(p-1) = 2p-3$ since such elements exist for all such orders. In particular, (3) with $h = 1$ shows that $\zeta_0(d,p) < \frac{1}{d}\left(1 + \frac{2p-3}{p} + \frac{d}{p^2}\right)$. This implies that $\zeta_0(d,p) < 3/d + 1/p^2$. We may therefore suppose $p < 5$.

By inspection, $\mathcal{M}(3,2) = \{4,6,8\}$, $\mathcal{M}(2,2) = \{3,4\}$, $\mathcal{M}(2,3) = \{6,7\}$, and $\mathcal{M}(2,4) = \{5,8,12,14,15\}$. This implies that $M(3,2) = 8$, $M(2,2) = 4$, $M(2,3) = 8$, and $M(2,4) = 26$. Applying (3) with $h = 2$ when $p = 3$ and $h = 5$ when $p = 2$ yields the result.

The last statement is a special case. $\square$

## 3.2 Bounds from Scott's Theorem

We obtain better bounds for $\sum \theta_i$ using Scott's Theorem [Scott] on linear groups in conjunction with elementary properties of generators and relations.

**Theorem 9 (Scott)** *Suppose* $H = \langle h_i \rangle$, $\prod h_i = 1$, *and* $H$ *acts on* $V$ *with* $V = [V,H]$. *Then* $\sum v(h_i) \ge 2 \dim V$.

To state the property of generators and relations we introduce some terminology. For the $r$-tuple $\underline{e}$ of positive integers, set

$$G(\underline{e}) = \langle g_i \mid g^{e_i} = 1, \prod g_i = 1 \rangle,$$

the group on $r$ generators with $r+1$ relations. Then, by [Mag], $G(\underline{e})$ is finite if and only if $A(\underline{e}) < 2$.

**Definition** *The tuple* $\underline{e}$ *is spherical if* $A(\underline{e}) < 2$. *The tuple* $\underline{d}$ *is hyperbolic if* $A(\underline{d}) > 2$.

The following fact about generators and relations is well-known. See, for example [Mag].

**Theorem 10 (Magnus)** *Let $\underline{e}$ be a spherical tuple. Then $G(\underline{e})$ has order at most $\dfrac{2}{(2-A(\underline{e}))}$. Furthermore, one of the following is true.*

1. *$G(\underline{e})$ is cyclic.*
2. *$G(\underline{e})$ is dihedral.*
3. *$G(\underline{e}) \cong A_4$, $S_4$, or $A_5$.*

The following key result is a consequence of the two previous theorems.

**Lemma 11** *If $\underline{e}$ is a spherical $r$-tuple and $C_k(\underline{e}) = \dfrac{2}{(2-A(\underline{e}))e_i}$, then*

$$\sum C_i(\underline{e}) v(x_i^{e_i}) \geq 2 \dim V.$$

Proof. Let $H$ be the normal closure $H$ of $\langle x_i^{e_i}, i = 1, \ldots, r\rangle$ in $G$. Then $G/H$ is a homomorphic image of $G(\underline{e})$, so $|G/H| \leq \frac{2}{2-A(\underline{e})}$, and either $G/H$ is solvable or $G/H \cong A_5$. Under the assumption on composition factors of $G$, the preimage $\widehat{H}$ of $H$ in $\widehat{G}$ must act on $V$ with $V = [V, \widehat{H}]$. By the argument of [FM.comp], $H$ has a generating tuple consisting of $C_1(\underline{e})$ conjugates of $x_1^{e_1}$, $C_2(\underline{e})$ conjugates of $x_2^{e_2}$, ..., and $C_r(\underline{e})$ conjugates of $x_r^{e_r}$. The result now follows from Theorem 9. □

**Corollary 12** *Suppose $\underline{e}$ is a spherical $r$-tuple and $\mathcal{S}$ is a subset of $\{1, \ldots, r\}$, such that the following conditions hold for some subset $\mathcal{K} \subseteq \{1, \ldots, r\}$.*

1. *$|\mathcal{K}| \leq 1$ and $C_k(\underline{e}) = 1$ for $k \in \mathcal{K}$.*
2. *$e_j = d_j$ for all $j \notin \mathcal{S} \cup \mathcal{K}$*

*Set $D = \sum_{i \in \mathcal{S}} C_i(\underline{e})$ Then $v(x_i^{e_i}) \geq \dfrac{\dim V}{D}$ for some $i$ in $\mathcal{S}$. In particular, if $\underline{e}$ and $\underline{d}$ are constant on $\mathcal{S}$, $e$ is the common value of $e_i$, $i \in \mathcal{S}$, and $C$ is the common value of $C_i(\underline{e})$, $i \in \mathcal{S}$ then $v(x_i^e) \geq \dfrac{\dim V}{C|\mathcal{S}|}$ for some $i$ in $\mathcal{S}$.*

Proof. Let $C_i = C_i(\underline{e})$. Since $v(1) = 0$ we have

$$\sum_{i \in \mathcal{S}} C_i v(x_i)^{e_i} + \sum_{k \in \mathcal{K}} C_k v(x_k)^{e_k} \geq 2 \dim V.$$

By assumption on $\mathcal{K}$, $\sum_{k \in \mathcal{K}} C_k v(x_k)^{e_k} \leq \dim V$. Therefore $\sum_{i \in \mathcal{S}} C_i v(x_i)^{e_i} \geq \dim V$, whence $v(x_i)^{e_i} \geq \dim V / \sum_{j \in \mathcal{S}} C_j$ for some $i \in \mathcal{S}$. □

We apply this to obtain an asymptotic upper bound for $\sum \theta_i$, by omitting the contributions of elements $y$ with $v(y)$ large.

Fix a positive integer $N$ and set $\mathcal{E}(\underline{d}) = \{(\underline{e}, \mathcal{S}) \mid \underline{e}$ is spherical, $\underline{e}$ and $\underline{d}$ are constant on $\mathcal{S}$ and there is a set $\mathcal{K}$ of cardinality at most 1 such that $C_k(\underline{e}) = 1$ for $k \in \mathcal{K}$, and $e_j = d_j$ and $C_j(\underline{e}) < N$ for $j \notin \mathcal{S} \cup \mathcal{K}\}$. Then $\mathcal{E}(\underline{d})$ consists of the pairs $(\underline{e}, \mathcal{S})$ meeting the conditions for the second conclusion in Corollary 12.

$J_i(\underline{d}) = \{h \mid e_i = h$ and $i$ is the largest element of $\mathcal{S}$ for some $(\underline{e}, \mathcal{S}) \in \mathcal{E}(\underline{d})\}$.

For $J$ a set of proper divisors of $d$, set

$$\tilde{\theta}(d, p, J) = \frac{1}{d}\left(1 + \sum_{m|d, m<d, m \notin J} \phi(\frac{d}{m}) p^{-\mu_*(\frac{d}{m}, p)}\right).$$

**Lemma 13** $\sum \theta(x_i) \preceq \sum \tilde{\theta}(d_i, p, J_i(\underline{d}))$.

Proof. We have $\sum \theta(x_i) = A(\underline{d}) + X$ where

$$X = \sum_i \frac{1}{d_i} \sum_{m|d_i, m<d_i} \phi(\frac{d_i}{m}) p^{-v(x_i^m)}.$$

If $U(m, a) = \{i \in \{1, \ldots, r\} \mid d_i = ma\}$ and $Y(m, a) = \sum_{i \in U(m,a)} p^{-v(x_i^m)}$, then

$$\begin{aligned} X &= \sum_m \sum_{a \geq 2} \sum_{i, d_i = ma} \frac{1}{ma} \phi(a) p^{-v(x_i^m)} \\ &= \sum_m \sum_{a \geq 2} \frac{\phi(a)}{ma} \sum_{i, d_i = ma} p^{-v(x_i^m)} \\ &= \sum_m \sum_{a \geq 2} \frac{\phi(a)}{ma} Y(m, a). \end{aligned}$$

Set $\mathcal{S}(m, a) = \{S \mid S \subseteq U(m, a)$ and $(\underline{e}, S) \in \mathcal{E}(\underline{d})$ for some $\underline{e}$ with $e_s = m, s \in S\}$ and $Z(m, a) = \{z \in U(m, a) \mid z$ is the largest element of $S$ for some $S \in \mathcal{S}(m, a)\}$. We claim that

$$Y(m, a) \leq |U(m, a) \setminus Z(m, a)| \cdot p^{-\mu_*(a)} + \epsilon_5$$

where $\epsilon_5 \to 0$ as $n \to \infty$.

To establish the claim, note that $\mathrm{Sym}(U(m, a))$ acts on $\mathcal{S}(m, a)$, so for the purposes of computing $Y(m, a)$ if suffices to assume that $v(x_i^m)$ is increasing on $U(m, a)$. Setting $K = Nr \geq N|\mathcal{S}(m, a)|$, under this assumption, we have $v(x_i^m) \geq \dim V/K$ for $i \in Z(m, a)$. Therefore

$$\begin{aligned} \sum_{i \in U(m,a)} p^{-v(x_i^m)} &= \sum_{i \in U(m,a) \setminus Z(m,a)} p^{-v(x_i^m)} + \sum_{i \in Z(m,a)} p^{-v(x_i^m)} \\ &\leq |U(m, a) \setminus Z(m, a)| p^{-\mu_*(a)} + |Z(m, a)| p^{-\dim V/K}. \end{aligned}$$

The claim now follows because $\dim V \to \infty$ as $n \to \infty$. Note that $p$ is bounded.

The statement is an easy consequence. □

### 3.3 Bounds on $\tilde{\theta}$

**Lemma 14** *Suppose $\tilde{\theta} = \tilde{\theta}(d, p, J)$.*

1. *If $\tilde{\theta} > 3/8$, then one of the following is true.*
   (a) $d = 2$ *and* $\tilde{\theta} \leq 3/4$.
   (b) $d = 3$ *and* $\tilde{\theta} \leq 5/9$.
   (c) $d = 4$ *and* $\tilde{\theta} \leq 1/2$.
2. *If $1 \in J$ and $\tilde{\theta} > 1/4$, then one of the following is true.*
   (a) $d \leq 3$ *and* $\tilde{\theta} = 1/d$.
   (b) $d = 4$ *and* $\tilde{\theta} \leq 3/8$.
   (c) $d = 6$ *and* $\tilde{\theta} \leq 1/3$.
3. *If $1, 2 \in J$ and $\tilde{\theta} > 5/24$, then one of the following is true.*
   (a) $d \leq 4$ *and* $\tilde{\theta} = 1/d$.
   (b) $d = 6$ *and* $\tilde{\theta} \leq 1/4$.
4. *If $1, 2, 3 \in J$ and $\tilde{\theta} > 1/7$, then one of the following is true.*
   (a) $d \leq 6$ *and* $\tilde{\theta} = 1/d$.
   (b) $d = 8$ *and* $4 \notin J$.
   (c) $d = 10$ *and* $5 \notin J$.
   (d) $d = 12$ *and* $4 \notin J$.

Proof. If $d \leq 3$ then these statements follow easily from Lemma 8.1. It therefore suffices to assume that $d > 3$. Using Lemma 8.1 again, the first statement now follows when $p > 3$. If $d > 8$, then the first statement follows from Lemma 8.3. This reduces the first statement to a small number of cases that are easily checked.

The remaining statements are proved similarly, though with more residual cases. For example, to prove (4), after applying Lemma 8.1 it suffices to assume that $d > 12$. Under this assumption Lemma 8.2 shows that it suffices to assume that $p < 18$. Also by Lemma 8.2, it suffices to assume that $d < 30$. □

The actual bounds stated in Lemma 14 are achieved for $p = 2$, with the exception of the bound in statement (1) for $d = 3$ which is achieved for $p = 3$. This observation leads to the following corollary.

**Corollary 15** *If $d > 2$ then $\zeta_0(d, p) + \zeta_0(d', p) \leq 5/4$ for every integer $d' \geq 2$.*

Proof. This follows immediately from Lemma 14.1 if $\zeta_0(d, p) \leq 1/2$. If $\zeta_0(d, p) > 1/2$, then $p = 3$ in which case $\zeta_0(d', p) \leq 2/3$ by Lemma 8.1 and $\zeta_0(d, p) + \zeta_0(d', p) \leq 4/9 + 2/3 < 5/4$. □

We record values of $\tilde{\theta}(d, 2, J)$ for small values of $d$ and relevant sets $J$ in the appendix.

# 4 Proof of Main Theorem

Let $\underline{x}$ be a generating system for $G$, and let $d_i = o(x_i)$, $i = 1, \ldots, r$. Without loss, we may assume that $d_i \leq d_{i+1}$ for $i = 1, \ldots, r-1$. Set $J_i = J_i(\underline{d})$.

**Lemma 16** *1. If $r = 3$ and $d_2$ is bounded, then $1 \in J_i$ for all $i$.*

2. *If $d_i = 2$ for all $i$, then $1 \in J_i$ for $i \in \{r-3, r-2, r-1, r\}$.*

3. *If $d_{r-1} = 2$, then $1 \in J_i$ for $i \in \{r-2, r-1\}$.*

4. *If the tuple $\underline{d}_j$ obtained by deleting $d_j$ from $\underline{d}$ is spherical with $A(\underline{d}_j)$ bounded away from 2, then $1 \in J_j$.*

5. *If the tuple $(d_j, j \in \mathcal{K})$ is homogeneous and the tuple $\underline{d}_{\mathcal{K}}$ obtained by deleting $d_j$ from $\underline{d}$, $j \in \mathcal{K}$ is spherical with $A(\underline{d}_{\mathcal{K}})$ bounded away from 2, then $1 \in J_k$ for $k$ the largest member of $\mathcal{K}$.*

6. *If $r = 3$, $d_1 = 2$, and $d_2 = 3$, then $\{1, 2, 3, 4, 5\} \subseteq J_3$.*

7. *If $r = 3$, $d_1 = 2$, and $d_2 = 4$ or $5$, then $\{1, 2, 3\} \subseteq J_3$.*

8. *If $r = 3$, $d_1 = 2$, and $d_j$ is bounded ($j = 2$ or $3$), then $\{1, 2\} \subseteq J_{5-j}$.*

9. *If $r = 3$, $d_1 = 2$, and $d_2 = d_3$ then $\{1, 2, 3\} \subseteq J_3$.*

10. *If $r = 3$, $d_1 = 3$, and $d_2 \leq 5$ then $\{1, 2\} \subseteq J_3$.*

11. *If $r = 3$, $d_{j-1} = d_j$, $j = 2$ or $3$, and $d_3$ is bounded, then $\{1, 2\} \subseteq J_j$.*

12. *If $r = 4$, $d_1 = d_2 = 2$, and $d_3$ and $d_4$ are bounded, then $1 \in J_i$, $i = 2, 3, 4$.*

13. *If $r = 4$, $d_1 = d_2$, and $d_3$ is bounded, then $1 \in J_2$.*

Proof. Each of these statements follows from consideration of a tuple constructed from $\underline{x}$ by applying an appropriate spherical exponent. We list the spherical exponents for each case: 1: $(1, d_2, d_2)$, $(d_1, 1, d_1)$, and $(d_2, d_2, 1)$ 2: $(1, \ldots, 1, 2, 2, 2)$ 3: $(1, \ldots, 1, 2, 2)$, $(1, \ldots, 1, 2, 1, 2)$ 4: $(d_1, \ldots, \hat{d}_i, \ldots, d_r)$ 5: $e_j = 1, (j \in \mathcal{K}); d_j, (j \notin \mathcal{K})$. 6: $(2, 3, d)$, $d = 2, 3, 4$, or 5. 7: $(2, c, d)$, $c = 4$ or 5, $d = 2$ or 3. 8: $(2, d_2, 2)$ or $(2, 2, d_3)$. 9: $(2, 2, 2)$ or $(2, 3, 3)$. 10: $(3, d_2, 2)$. 11: $(2, 2, d_3)$ or $(d_1, 2, 2)$. 12: $(1, 1, d_3 d_4, d_3 d_4)$, $(2, 2, 1, d_4)$, $(2, 2, d_3, 1)$. 13: $(1, 1, d_3, d_3)$. □

Set $\tilde{\theta}_i = \tilde{\theta}(d_i, p, J_i)$, and $\Sigma = \sum \tilde{\theta}_i$.

**Lemma 17** *If $r = 3$, then $\sum \tilde{\theta}_i \leq 41/42$.*

Proof. Assume that $r = 3$. and $\Sigma > 41/42$. Since $\tilde{\theta}_1 \leq 3/4$, it follows from Lemma 8.3 that $d_2 \leq 50$, whence $1 \in J_i$ for all $i$ by Lemma 16.1.

Lemma 14.2 implies that $d_1 \leq 6$, and further that if $d_1 = 6$, then $d_2 = d_3 = 6$. If $d_1 = d_2 = d_3 = 6$, then $2 \in J_3$ by Lemma 16.11, and $\theta_3 \leq 1/4$ by Lemma 14.3, so $\Sigma \leq 11/12$, a contradiction. Therefore $d_1 \leq 4$.

Suppose $d_1 = 4$. By Lemma 14.2, either $d_2 = 4$ or $d_2 = d_3 = 6$ because $\Sigma > 23/24$. In either case, $d_3 < 50$. If $d_2 = 4$, then Lemma 16.11 and Lemma 14.3 imply that $\tilde{\theta}_2 = 1/4$, so $\tilde{\theta}_1 + \tilde{\theta}_2 \leq 5/8$. It follows from Lemma 14.2 that $d_3 = 4$. Another application of Lemma 16.11 shows that $\tilde{\theta}_3 = 1/4$ and $\Sigma \leq 7/8$. On the other hand, if $d_2 = d_3 = 6$, then Lemma 16.11 and Lemma 14.3 imply that $\tilde{\theta}_3 \leq 1/4$, whence $\Sigma \leq 23/24$. It follows that $d_1 \leq 3$.

Assume that $d_1 = 3$. Then $\tilde{\theta}_1 = 1/3$, so $d_2 \leq 6$ by Lemma 14.2. If $d_3 > 6$, then $\tilde{\theta}_3 \leq 1/4$ and $\Sigma \leq 23/24$, so $d_3 \leq 6$. If $d_2 = d_3$ then $2 \in J_3$ by Lemma 16.11, and $\tilde{\theta}_2 + \tilde{\theta}_3 \leq 5/8$ by Lemma 14.2 and 3. We therefore have $d_2 < d_3 \leq 6$. Lemma 16.10 implies that $2 \in J_3$, so $\Sigma \leq 1/3 + 3/8 + 1/4$, a contradiction.

We have shown that $d_1 = 2$. Since $\tilde{\theta}_1 = 1/2$ and $\tilde{\theta}_2 \leq 3/8$, we have $d_3 < 50$ by Lemma 8.3. By Lemma 16.8, $\{1, 2\} \subseteq J_2, J_3$. If $d_2 = 3$, then $\{1, 2, 3, 4, 5\} \subseteq J_3$ by Lemma 16.6, and $\Sigma \leq 1/2 + 1/3 + 1/7 = 41/42$ by Lemma 14.4. If $d_2 > 3$, then Lemma 14.3 implies that $d_j = 4$ or $6$, $j = 2, 3$ since otherwise $\Sigma \leq 23/24$. Also, $\tilde{\theta}_2 \leq 1/4$. Since $(2, 4, 4)$ is not hyperbolic we must have $d_3 = 6$. From Lemma 16.7 or 9 we have $3 \in J_3$ and $\tilde{\theta}_3 = 1/6$. This implies that $\Sigma \leq 1/2 + 1/4 + 5/24$, a contradiction. □

**Lemma 18** *If $r > 3$ then one of the following is true.*

1. $\sum \tilde{\theta}_i \leq r - 2 - 1/42$.

2. $r = 4$, $d_3 > 2$, *and* $d_4 < 50$.

Proof. Set $\widetilde{\Sigma} = \sum_i (1 - \tilde{\theta}_i)$. Assume that $r > 3$ and $\widetilde{\Sigma} > r - 2 - 1/42$.

Suppose $d_r = 2$. Then $r > 4$ because $\underline{d}$ is hyperbolic. $\tilde{\theta}_i = 1/2$ for $i \geq r-3$ by Lemma 16.2, and $\tilde{\theta}_i \leq 3/4$ for all $i$ by Lemma 8.3. We have $\widetilde{\Sigma} \geq 4/2 + (r-4)/4 > 9/4$, a contradiction. It follows that $d_r > 2$.

Suppose $d_{r-1} = 2$. Then $\tilde{\theta}_i = 1/2$ for $i = r-2, r-1$ by Lemma 16.3, so $\sum_{i<r} (1 - \tilde{\theta}_i) \geq 1/4 + 2/2 = 5/4$. It follows from Lemma 8.3 that $d_r < 50$, whence $\tilde{\theta}_{r-3} = 1/2$ by Lemma 16.5 with $\mathcal{K} = \{1, \ldots, r-3\}$. We have $\sum_{i \geq r-3} (1 - \tilde{\theta}_i) \geq 3/2 + 4/9$ by Lemma 14.1, so $r = 4$ because $1 - \tilde{\theta}_1 \geq 1/4$. Lemma 16.4 implies that $1 \in J_4$, whence $\tilde{\theta}_4 \leq 3/8$, and $\sum (1 - \tilde{\theta}_i) \geq 17/8$, a contradiction. It follows that $d_{r-1} > 2$.

Now assume that $r > 4$. Then $d_1 = 2$ by Lemma 14.1. Also, $\sum_{i<r} (1 - \tilde{\theta}_i) \geq 3/4 + 4/9$, which implies that $d_r < 50$.

If $d_{r-2} > 2$, then $\sum_{i<r} (1 - \tilde{\theta}_i) \geq 2(3/4)$ by the previous paragraph, so $d_r \leq 4$ by Lemma 14.1. If $d_{r-2} = 2$, then $1 \in J_{r-2}$ by Lemma 16.5, and $\sum_{i<r} (1 - \tilde{\theta}_i) \geq 1 + 4/9$. Once again, we conclude that $d_r \leq 4$. This shows that $d_r \leq 4$ in all cases.

Suppose $d_{r-1} = 3$. If $d_{r-2} = 3$ then $r = 5$ by Lemma 14.1 and $r - 1 \in J_1$ by Lemma 16.5 with $\mathcal{K} = \{r-2, r-1\}$. This implies that $\sum (1 - \tilde{\theta}_i) \geq 2/4 + 4/9 + 2/3 + 4/9$, a contradiction. We must have $d_{r-2} = 2$, so $(d_{r-2}, d_{r-1}, d_r)$ and $(d_{r-3}, d_{r-1}, d_r)$ are spherical and, by Lemma 16.5, $\widetilde{\Sigma} \geq 1/4 + 2 \cdot 1/2 + 2 \cdot 4/9$, a contradiction.

We must have $d_{r-1} > 3$, and, in fact, $d_{r-1} = 4$. Thus $\tilde{\Sigma} \geq (r-3) \cdot 1/4 + 1/2 + 2 \cdot 1/2$, which implies that $r = 5$. Applying Lemma 16.5 with $\mathcal{K} = \{4, 5\}$, we have $1 \in J_5$ and $\tilde{\Sigma}\tilde{\theta}_i \geq 2 + 1/8$, a contradiction.

It remains to show that $d_4 < 50$. By Lemma 8.3, it suffices to show that $\tilde{\theta}_1 + \tilde{\theta}_2 + \tilde{\theta}_3 < 15/8$.

If $d_1 > 2$, then $\tilde{\theta}_1 + \tilde{\theta}_2 + \tilde{\theta}_3 < 3 \cdot 5/9 = 15/9$ by Lemma 14. If $d_1 = 2$ and $d_2 > 2$, then $\tilde{\theta}_1 + \tilde{\theta}_2 + \tilde{\theta}_3 < 5/4 + 5/9$ by Corollary 15. If $d_1 = d_2 = 2$, then $\tilde{\theta}_1 + \tilde{\theta}_2 \leq 3/2$, so $d_3$ is bounded. Therefore $1 \in J_2$ by Lemma 16.13. This implies that $\tilde{\theta}_2 \leq 1/2$. Since $\tilde{\theta}_1 + \tilde{\theta}_3 \leq 5/4$ (by Corollary 15), we have $\tilde{\theta}_1 + \tilde{\theta}_2 + \tilde{\theta}_3 \leq 7/4$. □

**Lemma 19** *If $r = 4$, $d_3 > 2$, and $d_4 < 50$, then $\sum \theta(x_i) \preceq 2 - 1/42$.*

Proof. We claim that

$$\sum \theta(x_i) \preceq \max_{j \in \{1,2,3,4\}} \left( \zeta_0(d_j, p) + \sum_{i \neq j} \tilde{\theta}(d_i, p, \{1\}) \right).$$

To prove the claim it suffices to show that, given $\epsilon_6 > 0$, if $n$ is sufficiently large then

$$\sum \theta(x_i) < \theta(x_j) + \sum_{i \neq j} \tilde{\theta}(d_i, p, \{1\}) + \epsilon_6$$

for some $j$. This is indeed the case for all choices of $j$ if $v(x_i)$ is sufficiently large for all $i$. If $v(x_j)$ is bounded for some $j$, then $v(x_i)$ must be large for $i \in \{1, \ldots, 4\}, i \neq j$ by the argument of Lemma 16.12, and the inequality holds for that choice of $j$.

Suppose $d_2 > 2$. Then $\theta(x_1) + \sum_{i \neq 1} \tilde{\theta}(d_i, p, \{1\}) \leq 3/4 + 3 \cdot 3/8$ and $\theta(x_j) + \sum_{i \neq j} \tilde{\theta}(d_i, p, \{1\}) \leq 5/9 + 1/2 + 2 \cdot 3/8$, $j > 1$, and the statement follows from the claim.

Without loss, then, $d_2 = 2$. If $\underline{d} \neq (2, 2, 4, 4)$, then $\theta(x_j) + \sum_{i \neq j} \tilde{\theta}(d_i, p, \{1\}) \leq 3/4 + 1/2 + 3/8 + 1/3$ for $j = 1, 2$ and $\theta(x_j) + \sum_{i \neq j} \tilde{\theta}(d_i, p, \{1\}) \leq 1/2 + 2 \cdot 1/2 + 3/8$ for $j = 3, 4$. Once again the statement follows from the claim.

If $\underline{d} = (2, 2, 4, 4)$, then consideration of the tuple generated from $x$ with the spherical exponent $(1, 2, 2, 2)$ shows that one of the quantities $v(x_1)$, $v(x_3^2)$, $v(x_4^2)$ must be large when $n$ is. The statement now follows easily. □

In view of Lemma 5 and Lemma 13, the Main Theorem follows from the previous three results.

# 5 Conclusion

Every permutation group of degree $n$ with a generating system of type $(2, 3, 7)$ must have genus at most $n/84$. Since there are groups of arbitrarily large finite order that have such generating systems (the groups $L_2(p)$ with $p \equiv 1 \bmod 84$, for instance), the asymptotic bound in the Theorem above cannot be improved.

This shows that the asymptotic lower bound cannot be improved.

CLEAN UP NEEDED HERE

The following family of examples shows that for arbitrarily large $m$ and $s$ there exist imprimitive systems of degree $ms$ and of genus approximately $2m$ for *NACF* groups. Thus, the assumption of primitivity in the Main Theorem cannot be removed.

Let $S$ be a nonabelian simple group of order $s$. Then $S$ is a homomorphic image of the free group $H$ on two letters which is the fundamental group of a genus 2 surface $Y$. Let $f : Y \to P^1(C)$ have monodromy group $S_m$. Then $Y$ has a Galois extension $X$ with monodromy group $S$, and the genus of $X$ is approximately $2s$. The degree of the composite $X \to P^1(C)$ is $ms$.

# 6 Appendix: Selected values of $\tilde{\theta}(d, 2, J)$

| $d$ | $\zeta_0(d,2)$ | $\tilde{\theta}(d,2,\{1\})$ | $\tilde{\theta}(d,2,\{1,2\})$ | $\tilde{\theta}(d,2,\{1,2,3\})$ |
|---|---|---|---|---|
| 2 | 3/4 | 1/2 | 1/2 | 1/2 |
| 3 | 1/2 | 1/3 | 1/3 | 1/3 |
| 4 | 1/2 | 3/8 | 1/4 | 1/4 |
| 5 | 1/4 | 1/5 | 1/5 | 1/5 |
| 6 | 3/8 | 1/3 | 1/4 | 1/6 |
| 7 | 1/4 | 1/7 | 1/7 | 1/7 |
| 8 | 9/32 | 1/4 | 3/16 | 3/16 |
| 9 | 17/96 | 1/6 | 1/6 | 1/9 |
| 10 | 3/16 | 7/40 | 3/20 | 3/20 |
| 11 | 47/512 | 1/11 | 1/11 | 1/11 |
| 12 | 1/4 | 11/48 | 5/24 | 1/6 |

# References


[FM.grass] D. Frohardt and K. Magaard, Grassmannian Fixed Point Ratios *Geom. Ded.* **82** (2000), 21–104

[FM.comp] D. Frohardt and K. Magaard, Composition Factors of Monodromy Groups, *Ann. of Math.* **154** (2001), 327–345

[Gur] R. Guralnick The genus of a permutation group, in *Groups, Combinatorics, and Geometry*, M. W. Liebeck and J. Saxl, eds. *London Mathematical Society Lecture Notes Series* **165** (1992), 351–363

[GurTho] R. Guralnick and J. Thompson Finite Groups of Genus Zero, *J. Algebra*, **131** (1990), 303–341.

[KurSte] H. Kurzweil and B. Stellmacher *The Theory of Finite Groups, An Introduction*, Springer-Verlag, New York, 2004

[LieSax] M. Liebeck and J. Saxl Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.*, **63** (1991), 266-314.

[LieSha] M. Liebeck and A. Shalev Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.*, **12** (1999), 497–520.

[Mag] W. Magnus *Noneuclidean Tesselations and Their Groups*, *Pure and Applied Mathematics* **61** Academic Press, New York, 1974

[Scott] L. Scott Matrices and cohomology *Ann. of Math.* **105** (1977), 473–492

[CFSG]