Primitive monodromy groups of genus at most two

Frohardt, Daniel ; Guralnick, Robert ; Magaard, Kay

DOI:
10.1016/j.jalgebra.2014.06.020

License:
Other (please specify with Rights Statement)

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Frohardt, D, Guralnick, R & Magaard, K 2014, 'Primitive monodromy groups of genus at most two' Journal of Algebra, vol. 417, pp. 234-74. https://doi.org/10.1016/j.jalgebra.2014.06.020

Journal of Algebra 417 (2014) 234–274

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Primitive monodromy groups of genus at most two

Daniel Frohardt, Robert Guralnick[1], Kay Magaard[*]

ARTICLE INFO

Article history:
Received 23 June 2012
Available online 19 July 2014
Communicated by Martin Liebeck

Keywords:
Primitive groups
Riemann surfaces

ABSTRACT

We show that if the action of a classical group G on a set Ω of 1-spaces of its natural module is of genus at most two, then $|\Omega| \leq 10\,000$.

Introduction

Let X be a compact, connected Riemann surface of genus g, and let $\phi : X \to \mathbb{P}^1\mathbb{C}$ be meromorphic of degree n. Let $B := \{x \in \mathbb{P}^1\mathbb{C}\colon |\phi^{-1}(x)| < n\}$ be the set of branch points of ϕ. It is well known that B is a finite set and that if $b_0 \in \mathbb{P}^1\mathbb{C} \setminus B$, then the fundamental group $\pi_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$ acts transitively on $F := \phi^{-1}(b_0)$ via path lifting. The image of the action of $\pi_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$ on $\phi^{-1}(b_0)$ is called the *monodromy group* of (X, ϕ) and is denoted by $\mathrm{Mon}(X, \phi)$.

We are interested in the structure of the monodromy group when the genus of X is less than or equal to two and ϕ is indecomposable in the sense that there do not exist holomorphic functions $\phi_1 : X \to Y$ and $\phi_2 : Y \to \mathbb{P}^1\mathbb{C}$ of degree less than the degree of ϕ such that $\phi = \phi_2 \circ \phi_1$. The condition that X is connected implies that $\mathrm{Mon}(X, \phi)$ acts transitively on F whereas the condition that ϕ is indecomposable implies that the action of $\mathrm{Mon}(X, \phi)$ on F is primitive.

[*] Corresponding author.

[1] The second author was supported by NSF grant DMS 0653873.

http://dx.doi.org/10.1016/j.jalgebra.2014.06.020
0021-8693/© 2014 Elsevier Inc. All rights reserved.

Our question is closely related to a conjecture made by Guralnick and Thompson [12] in 1990. By $cf(G)$ we denote the set of isomorphism types of the composition factors of G. In their paper Guralnick and Thompson [12] defined the set

$$\mathcal{E}^*(g) = \Bigl(\bigcup_{(X,\phi)} cf\,\mathrm{Mon}(X,\phi)\Bigr) \setminus \{A_n, \mathbb{Z}/p\mathbb{Z}\colon\ n > 4,\ p \text{ a prime}\}$$

where X is a compact connected Riemann surface of genus g, and $\phi : X \to \mathbb{P}^1(\mathbb{C})$ is meromorphic, and conjectured that $\mathcal{E}^*(g)$ is finite for all $g \in \mathbf{N}$. Building on works of Guralnick and Thompson [12], Neubauer [24], Liebeck and Saxl [15], and Liebeck and Shalev [17], the conjecture was established in 2001 by Frohardt and Magaard [6].

The set $\mathcal{E}^*(0)$ is distinguished in that it is contained in $\mathcal{E}^*(g)$ for all g. Moreover the proof of the Guralnick–Thompson conjecture shows that it is possible to compute $\mathcal{E}^*(0)$ explicitly and indeed to describe the minimal covers $\phi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ (at least those whose monodromy group is not an alternating or symmetric of the same degree as the cover).

The idea of the proof of the Guralnick–Thompson conjecture is to employ Riemann's Existence Theorem to translate the geometric problem to a problem in group theory as follows. If $\phi : X \to \mathbb{P}^1\mathbb{C}$ is as above with branch points $B = \{b_1, \dots, b_r\}$, then the set of elements $\alpha_i \in \pi_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$ each represented by a simple loop around b_i forms a standardized set of generators of $\pi_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$. We denote by σ_i the image of α_i in $\mathrm{Mon}(X,\phi) \subset S_F \cong S_n$. Thus we see that

$$\mathrm{Mon}(X,\phi) = \langle \sigma_1, \dots, \sigma_r \rangle \subset S_n$$

and that

$$\prod_{i=1}^{r} \sigma_i = 1.$$

Moreover the conjugacy class of σ_i in $\mathrm{Mon}(X,\phi)$ is uniquely determined by ϕ. Recall that the index of a permutation $\sigma \in S_n$ is equal to the minimal number of transpositions needed to express σ as a product of such. The Riemann–Hurwitz formula asserts that

$$2(n+g-1) = \sum_{i=1}^{r} \mathrm{Ind}(\sigma_i),$$

where g is the genus of X.

Definition 1. If $\tau_1, \dots, \tau_r \in S_n$ generate a transitive subgroup G of S_n such that $\prod_{i=1}^{r} \tau_i = 1$ and $2(n+g-1) = \sum_{i=1}^{r} \mathrm{Ind}(\tau_i)$ for some $g \in \mathbf{N}_0$, then we call $(\tau_1, \dots, \tau_r)$ a *genus g-system* and G a genus g-group. We call a genus g-system $(\tau_1, \dots, \tau_r)$ primitive if the subgroup of S_n it generates is primitive.

If X, ϕ are as above, then we say that $(\sigma_1, \ldots, \sigma_r)$ is the genus g-system induced by ϕ.

Theorem 1 *(Riemann's Existence Theorem). For every genus g-system $(\tau_1, \ldots, \tau_r)$ of S_n there exist a Riemann surface Y and a cover $\phi' : Y \to \mathbb{P}^1\mathbb{C}$ with branch point set B such that the genus g-system induced by ϕ' is $(\tau_1, \ldots, \tau_r)$.*

Definition 2. Two covers Y_i, ϕ_i, $i = 1, 2$, are equivalent if there exist holomorphic maps $\xi_1 : Y_1 \to Y_2$ and $\xi_2 : Y_2 \to Y_1$ which are inverses of one to another such that $\phi_1 = \xi_1 \circ \phi_2$ and $\phi_2 = \xi_2 \circ \phi_1$.

The Artin braid group acts via automorphisms on $\prod_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$. We have that all sets of canonical generators of $\prod_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$ lie in the same braid orbit. Also the group G acts via diagonal conjugation on genus g-generating sets. The diagonal and braiding actions on g-generating sets commute and preserve equivalence of covers; that is if two genus g-generating sets lie in the same orbit under either the braid or the diagonal conjugation action, then the corresponding covers given by Riemann's Existence Theorem are equivalent. We call two genus g-generating systems *braid equivalent* if they are in the same orbit under the group generated by the braid action and diagonal conjugation. We have, see for example [27, Proposition 10.14].

Theorem 2. *Two covers are equivalent if and only if the corresponding genus g-systems are braid equivalent.*

Suppose now that $(\tau_1, \ldots, \tau_r)$ is a primitive genus g-system of S_n. Express each τ_i as a product of a minimal number of transpositions; i.e. $\tau_i := \prod_j \sigma_{i,j}$. The system $(\sigma_{1,1}, \ldots, \sigma_{r,s})$ is a primitive genus g-system generating S_n consisting of precisely $2(n + g - 1)$ transpositions. By a famous result of Clebsch, see Lemma 10.15 in [27], any two primitive genus g-systems of S_n are braid equivalent. Thus we see that every genus g-system can be obtained from one of S_n which consists entirely of transpositions.

So generically we expect primitive genus g-systems of S_n to generate either A_n or S_n.

We define $P\mathcal{E}^*(g)_{n,r}$ to be the braid equivalence classes of primitive genus g-systems $(\tau_1, \ldots, \tau_r)$ of S_n such that $G := \langle \tau_1, \ldots, \tau_r \rangle$ is a primitive subgroup of S_n with $A_n \nleq G$. We also define $G\mathcal{E}^*(g)_{n,r}$ to be the conjugacy classes of primitive subgroups of S_n which are generated by members of $P\mathcal{E}^*(g)_{n,r}$.

We also define

$$P\mathcal{E}^*(g) := \bigcup_{(n,r) \in \mathbf{N}^2} P\mathcal{E}^*(g)_{n,r},$$

and similarly

$$G\mathcal{E}^*(g) := \bigcup_{(n,r) \in \mathbf{N}^2} G\mathcal{E}^*(g)_{n,r}.$$

We note that the composition factors of elements of $G\mathcal{E}^*(g)$ are elements of $\mathcal{E}^*(g)$.

Our assumption that $G = \mathrm{Mon}(X, \phi)$ acts primitively on F is a strong one and allows us to organize our analysis along the lines of the Aschbacher–O'Nan–Scott theorem exactly as was done in the original paper of Guralnick and Thompson [12]. We recall the statement of the Aschbacher–O'Nan–Scott theorem from [12].

Theorem 3. *Suppose G is a finite group and H is a maximal subgroup of G such that*

$$\bigcap_{g \in G} H^g = 1.$$

Let Q be a minimal normal subgroup of G, let L be a minimal normal subgroup of Q, and let $\Delta = \{L = L_1, L_2, \ldots, L_t\}$ be the set of G-conjugates of L. Then $G = HQ$ and precisely one of the following holds:

(A) *L is of prime order p.*
(B) *$F^*(G) = Q \times R$ where $Q \cong R$ and $H \cap Q = 1$.*
(C1) *$F^*(G) = Q$ is nonabelian, $H \cap Q = 1$.*
(C2) *$F^*(G) = Q$ is nonabelian, $H \cap Q \neq 1 = L \cap H$.*
(C3) *$F^*(G) = Q$ is nonabelian, $H \cap Q = H_1 \times \cdots \times H_t$, where $H_i = H \cap L_i \neq 1$, $1 \leq i \leq t$.*

We summarize briefly what is known about $G\mathcal{E}^*(0)$ and $P\mathcal{E}^*(0)$. The members of $G\mathcal{E}^*(0)$ that arise in case (C2) were determined by Aschbacher [2]. In all such examples $Q = A_5 \times A_5$. Shih [26] showed that no elements of $G\mathcal{E}^*(0)$ arise in case (B) and Guralnick and Thompson [12] showed the same in case (C1). In his thesis Neubauer [23] showed that in case (A) either $G'' = 1$ and G/G' is an abelian subgroup of $GL_2(p)$, or that $n \leq 256$. Recently Magaard, Shpectorov and Wang [20], determined all elements of $P\mathcal{E}^*(0)_{n,r}$ with $n \leq 256$. The elements G of $G\mathcal{E}^*(0)$ arising in case (C3) have generalized Fitting subgroups with fewer than 5 components; i.e. $t \leq 5$. This was shown by Guralnick and Neubauer [10] and later strengthened by Guralnick [13] to $t \leq 4$. Moreover Guralnick showed that the action of L_i on the cosets of H_i is a member of $G\mathcal{E}^*(0)$. In case (C3) where L_i is of Lie type of rank one all elements of $G\mathcal{E}^*(0)$ and $G\mathcal{E}^*(1)$ were determined by Frohardt, Guralnick, and Magaard [3], moreover they show that $t \leq 2$. In [14] Kong shows that if G is an almost simple group of type $L_3(q)$, then $G \in G\mathcal{E}^*_{(q^2+q+1,r)}(g)$ with $g \leq 2$ only if $q \leq 13$, and $G \in G\mathcal{E}^*_{(q^2+q+1,r)}(0)$ if and only if $q \leq 7$. Combining the results of Frohardt and Magaard [7] with those of Liebeck and Seitz [16] we have that if $F^*(G)$ is exceptional of Lie type and $G \in G\mathcal{E}^*(0)_{n,r}$, then $n \leq 65$. In [11] Guralnick and Shareshian show that $G\mathcal{E}^*(0)_{n,r} = \varnothing$ if $r \geq 9$. Moreover they show that if $G \in G\mathcal{E}^*(0)_{n,r}$ with $F^*(G)$ alternating of degree $d < n$, then either $r \leq 4$ or $r = 5$ and $n = d(d-1)/2$. In [19] Magaard showed that if $F^*(G)$ is sporadic and $G \in G\mathcal{E}^*(0)_{n,r}$ then $n \leq 280$. We would like to take this opportunity to point out that $\mathrm{Aut}(HS) \in G\mathcal{E}^*(0)_{100,3}$ which was missed in Ref. [19]. Furthermore we thank the referee for pointing out that $\mathrm{Aut}(HS)$ possesses four genus zero systems in its action on 100 points with signatures $(2,4,10), (2,5,6), (2,4,5)$, and $(2,4,6)$. The referee has further pointed out that first two of these genus zero systems are rational and rigid. This is because in both of these cases the involution has an odd number of transpositions, and therefore the corresponding genus 0 field is rational. Thus there exists $\phi : \mathbb{P}^1\mathbb{Q} \to \mathbb{P}^1\mathbb{Q}$ of a degree 100 with monodromy group $\mathrm{Aut}(HS)$.

This leaves open the cases $F^*(G) = A_d^t$, $t, r \leq 4$, and the cases $F^*(G) = L^t$, $t \leq 4$, where L is a classical group of Lie type. In light of the results of [1] we suspect that if G is in the second case and $G \in G\mathcal{E}^*(0)$, then L_i/H_i is a point action, i.e. equivalent to an action of L_i acting on an orbit of one-spaces of its natural module. Hence they are the focus of this paper.

Another problem closely related to the Guralnick–Thompson conjecture is the description of the monodromy groups from the generic Riemann surface of genus g to $\mathbb{P}^1(\mathbb{C})$ of degree n. This is related to Zariski's thesis where he answered a conjecture of Enrique by showing that the generic Riemann surface of genus $g > 6$ does not admit a solvable map of fixed degree n to $\mathbb{P}^1(\mathbb{C})$ (i.e. where the monodromy group is solvable). The condition on n being fixed was removed in [10]. Note that any Riemann surface of genus at 6 admits a degree 4 map to $\mathbb{P}^1(\mathbb{C})$ (and so is solvable). Interestingly, Zariski's methods were mostly group theoretic.

Recall that the images of the canonical generators of $\pi_1(\mathbb{P}^1\mathbb{C} \setminus B, b_0)$ are determined uniquely up to conjugacy in G. We say that a G-cover of $\mathbb{P}^1\mathbb{C}$ has *ramification type* $C_1, \ldots, C_r$ if the ith canonical generator lies in conjugacy class C_i of G. The moduli space of G-covers of $\mathbb{P}^1\mathbb{C}$ with ramification type $C_1, \ldots, C_r$ is a *Hurwitz space* and is denoted by $\mathcal{H}(G, 0, C_1, \ldots, C_r)$. Via the Riemann–Hurwitz formula we see that every G-cover $X \in \mathcal{H}(G, 0, C_1, \ldots, C_r)$ has the same genus g. So the forgetful functor $\mathcal{F} : \mathcal{H}(G, 0, C_1, \ldots, C_r) \to \mathcal{M}_g$ is well defined and so the problem of determining maps of degree n from the generic Riemann surface of genus g can be rephrased as follows:

For which groups G and which ramification types $C_1, \ldots, C_r$ of G is the forgetful functor $\mathcal{F} : \mathcal{H}(G, 0, C_1, \ldots, C_r) \to \mathcal{M}_g$ dominant; i.e. is the image of $\mathcal{H}(G, 0, C_1, \ldots, C_r)$ dense in $\mathcal{M}_g$?

Now Theorem 2 of Guralnick–Magaard [9] shows that if the image of $\mathcal{H}(G, 0, C_1, \ldots, C_r)$ under the forgetful functor is dense in $\mathcal{M}_g$, then one of the following holds

1. $g \leq 2$,
2. $g = 3$ and G is affine of degree 8 or 16,
3. $g = 3$ and $G \cong L_3(2)$,
4. $g \geq 3$ and $G \cong S_n, n \geq (g+2)/2$ or $A_n, n > 2g$.

It is well known that S_n does cover $\mathbb{P}^1\mathbb{C}$ generically. However it was only in 2006 when Magaard and Völklein [21] proved that A_n and $L_3(2)$ also cover $\mathbb{P}^1\mathbb{C}$ generically. It was later shown by Magaard, Völklein and Wiesend [22] that $AGL_3(2)$ and $AGL_4(2)$ cover

$\mathbb{P}^1\mathbb{C}$ generically. This leaves only the first possibility, and is a reason why our ultimate goal is to determine $P\mathcal{E}^*(g)$ where $g \leq 2$.

Our two primary results here are Theorem 4, which shows that if $n > 10^4$ then the elements of $P\mathcal{E}^*_{n,r}(g)$ with $g \leq 2$ are not point actions of classical groups, and Theorem 5 which is more technical but can be applied to a wider class of actions. Combining Theorem 4 with the main theorem of [4] shows that if $n > 10^4$, then the elements of $P\mathcal{E}^*_{n,r}(g)$ with $g \leq 2$ are generally not subspace actions of classical groups. The potential exceptions to the statement are also explicitly given in [4]. These potentially exceptional actions are precisely those actions whose permutation modules do not contain the permutation module of the action on singular points as a submodule. The main result of [1] determines all classes of maximal subgroups of classical groups whose permutation module does not contain the permutation module of the action on singular points. For these classes of maximal subgroups we hope to establish the hypotheses of Theorem 4 which would then show that if $n > 10^4$, then the elements of $G\mathcal{E}^*_{n,r}(g)$ with $g \leq 2$ are either cyclic of prime order n or contain the alternating group A_n.

To establish Theorem 5 we show that for any pair (G, Ω), where G is a classical group acting primitively on a set Ω such that the hypotheses of Theorem 5 are satisfied, and any generating r-tuple $(\tau_1, \ldots, \tau_r)$ of G which satisfies the product 1 condition, then the expression $\sum_{i=1}^r \mathrm{Ind}(\tau_i)$ is greater than $(2 + \epsilon)n$ for some positive constant ϵ. We achieve this by proving effective lower bounds on $\mathrm{Ind}(\tau_i)$ using Scott's Theorem 14 and the technique of translating tuples, see Lemma 15.

1. Statement of results

Definition. $\underline{x} = (x_1, x_2, \ldots, x_r)$ is a *normalized generating r-tuple* for G provided

1. $G = \langle x_1, x_2, \ldots, x_r \rangle$.
2. $x_1 x_2 \ldots x_r = 1$.
3. $x_i \neq 1$, $i = 1, 2, \ldots, r$.

If, in addition, G is a transitive permutation group of degree N and

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

then $\underline{x}$ has genus g.

The formula above is the Riemann–Hurwitz Formula (RH). The Riemann Existence Theorem [12] guarantees that given a normalized generating tuple $\underline{x}$ for a permutation group G there is a surface X and a covering $\rho : X \mapsto \mathbb{P}^1(\mathbb{C})$ such that $G \cong \mathrm{Mon}(X, \rho)$ and the genus of X is the genus of the tuple $\underline{x}$, written $g(\underline{x})$.

The primary result of this paper is the following.

Theorem 4. *If (G, Ω) is a primitive classical point action of degree at least 10^4, then the action has genus larger than 2.*

The case of point actions will lead to almost all the examples (indeed using [4] and some ongoing work of AGM, one can eliminate most other situations).

The proof of Theorem 4 uses inequalities based on RH and estimates for the fixed point ratios of elements of G.

Definition. For x a permutation of the finite set Ω, let $F_\Omega(x)$ (or $F(x)$) denote the fixed points of x on Ω and let $f_\Omega(x)$ (or $f(x)$) denote the *fixed point ratio* of this permutation. That is, $f(x) = |F(x)|/|\Omega|$.

Definition. Let V be a vector space and let $x \in \Gamma L(V)$. If x acts as a permutation on the set Ω then the triple (x, V, Ω) satisfies Grassmann Condition ϵ provided

$$f_\Omega(x) < \frac{|W|}{|V|} + \epsilon$$

for some eigenspace W for the action of x on V.

A classical group G with natural module V acting as a permutation group on the set Ω satisfies Grassmann Condition ϵ provided (x, V, Ω) satisfies Grassmann Condition ϵ for every $x \in G$.

Note: For the purposes of the previous definition, an eigenspace for the action of x on V is a set $W \subset V$ which is a subspace of V over some (possibly proper) subfield of the field of definition on which x acts as a scalar. Note that $|W|$ does not depend on its field of scalars.

The role of Grassmann Conditions in the proof of Theorem 4 is apparent in the statement of the following technical results which together yield Theorem 4. The key feature of the point actions is that with known exceptions they satisfy Grassmann Condition 1/100. Theorem 5 also applies to other actions that satisfy this condition.

Theorem 5. *Let G be a linear group with module V where V contains at least 10^4 projective points and no constituent for the action of G on V has dimension 1. If $\underline{x}$ is a normalized generating r-tuple for G in some primitive permutation action, then one of the following is true.*

1. $g(\underline{x}) > 2$.
2. *G does not satisfy Grassmann Condition 1/100. More specifically, for some $i \in \{1, \ldots, r\}$, the group $\langle x_i \rangle$ contains an element y that violates Grassmann Condition 1/100.*
3. *The characteristic of V, the dimension of V over its prime field, and the signature of $\underline{x}$ are given in Table 1.*

Table 1
Characteristic, dimension and signature of exceptional cases in Theorem 5.

p	$\dim_{\mathbf{F}_p}(V)$	$\mathrm{sig}(\underline{x})$
11	$5, 6$	$(2, 3, 7)$
7	6	$(2, 3, 7)$
5	$7, 8, 9$	$(2, 3, 7)$
3	12	$(2, 3, 7)$
2	$14, 15, \dots, 21$	$(2, 3, 7)$
3	10	$(2, 3, 8)$
2	16	$(2, 4, 5)$

Note: The *signature* $\mathrm{sig}(\underline{x})$ of the r-tuple $\underline{x} = (x_1, x_2, \dots, x_r)$ is the r-tuple $(d_1, d_2, \dots, d_r)$, where $d_i = o(x_i)$.

Theorem 6. *Let G be a classical group with natural module V. Let Ω be a primitive point action for G with $|\Omega| \geq 10^4$ and assume that G does not satisfy Grassmann Condition* $1/100$. *Then $g(\underline{x}) > 2$ for every normalized generating tuple $\underline{x}$ such that $\langle x_i \rangle$ contains an element y violating Grassmann Condition* $1/100$.

Theorem 7. *Let G be a classical group with natural module V. Assume $\underline{x}$ is a normalized generating tuple for G and that Ω is a primitive point action for G with $|\Omega| \geq 10^4$. If the characteristic of V, the dimension of V over its prime field, and the signature of $\underline{x}$ are given in Table 1 then $g(\underline{x}) > 2$.*

Definition. The almost simple classical group G has a *point action* on Ω provided G has a natural module V of dimension n over $\mathbf{F}_q$ where (G, Ω, n, V) satisfy one of the following conditions.

L: $F^*(G) \cong L_n(q)$, and Ω is the set of all points in V. $n \geq 2$.

O^ϵ, **s**: $F^*(G) \cong O_n^\epsilon(q)$, V is a non-degenerate orthogonal space of type ϵ, and Ω is the set of singular points in V. n is even, $n \geq 6$, $\epsilon = +$ or $-$.

O^ϵ, **n**: $F^*(G) \cong O_n^\epsilon(q)$, V is a non-degenerate orthogonal space of type ϵ, and Ω is the set of $+$-type points in V. n is even, $n \geq 6$, $\epsilon = +$ or $-$.

O, **s**: $F^*(G) \cong O_n(q)$, V is a non-degenerate orthogonal space, and Ω is the set of singular points in V. n is odd, $n \geq 5$, and q is odd.

O, δ: $F^*(G) \cong O_n(q)$, V is a non-degenerate orthogonal space, and Ω is the set of δ-type points in V. n is odd, $n \geq 5$, $\delta = +$ or $-$, and q is odd.

Sp: $F^*(G) \cong Sp_n(q)$, V is a non-degenerate symplectic space and Ω is the set of points in V. n is even, $n \geq 4$.

Sp, δ: $F^*(G) \cong Sp_n(q)$, V is a symplectic space, and $\widetilde{V}$ is an orthogonal space of dimension $n+1$ such that $\operatorname{rad}\widetilde{V}$ is anisotropic of dimension 1 and $V \cong \widetilde{V}/\operatorname{rad}\widetilde{V}$, and Ω is the set of all complements to $\operatorname{rad}\widetilde{V}$ in $\widetilde{V}$ of type δ. n is even, $n \geq 4$, $\delta = +$ or $-$, and q is even.

$U, \mathbf{s}$: $F^*(G) \cong U_n(q^{1/2})$, V is a non-degenerate hermitian space, and Ω is the set of singular points in V. $n \geq 3$, q is a square.

$U, \mathbf{n}$: $F^*(G) \cong U_n(q^{1/2})$, V is a non-degenerate hermitian space, and Ω is the set of nonsingular points in V. $n \geq 3$, q is a square.

We prove Theorems 5, 6, and 7 in the subsequent sections. Since the action of a classical group G on its natural module V satisfies the hypotheses of Theorem 5, it is evident that Theorem 4 follows from these theorems.

2. Proof of Theorem 5

2.1. Notation and preliminary results

Let G be an almost simple classical group with natural module V of dimension n_q over $\mathbf{F}_q$ and let p be the characteristic of $\mathbf{F}_q$. Then $V_{\mathbf{F}_p}$ is an $\mathbf{F}_p$-vector space and all elements of G correspond to $\mathbf{F}_p$-linear maps. We have $G = \widehat{G}/Z$ where $\widehat{G} \subseteq GL(V_{\mathbf{F}_p})$ and Z acts as scalars on $V_{\mathbf{F}_p}$. Set $n_p = \dim_{\mathbf{F}_p} V_{\mathbf{F}_p}$, so that $n_p = n_q \log_p(q)$.

Definition. $v_q(y)$ [resp., $v_p(y)$] is the codimension of the largest eigenspace of the action of an associate of y on V [resp., $V_{\mathbf{F}_p}$].

Regarding V as an $\mathbf{F}_p$-space, $v_p(x) = \max(\operatorname{codim} C_V(\widehat{x})\colon \widehat{x} \mapsto x \text{ under } \widehat{G} \to G)$.

Let Ω be a primitive G-set of order N. Let $\underline{x} = (x_1, \ldots, x_r)$ be a normalized generating tuple for G.

Let $g = g(\underline{x})$, and let

$$\underline{d} = (d_1, \ldots, d_r)$$

be the signature of $\underline{x}$, so that $d_i = o(x_i)$, $i = 1, \ldots, r$.

When the context is clear, we will write n instead of n_q or n_p and v instead of v_q or v_p.

The Cauchy–Frobenius Formula says that if $x \in G$ has order d, then

$$\operatorname{Ind}(x) = N - \frac{1}{d} \sum_{y \in \langle x \rangle} F(y).$$

Combining this with (RH), we have

$$\sum_{i=1}^{r} \frac{1}{d_i}\left(1 + \sum_{y \in \langle x_i \rangle^\sharp} f(y)\right) = r - 2 - 2\left(\frac{g-1}{N}\right). \tag{3}$$

Definition.

$$\epsilon_0 = 2\left(\frac{g-1}{N}\right),$$

$$A(\underline{d}) = \sum \frac{d_i - 1}{d_i}.$$

Definition. For $x \in G$, with $o(x) = d$, set

$$\kappa(x) = \frac{1}{d}\left(1 + \sum_{y \in \langle x \rangle^\sharp} p^{-v(y)}\right).$$

Fact 8. *If G satisfies Grassmann Condition ϵ then*

$$\sum \kappa(x_i) > r - 2 - A(\underline{d})\epsilon - \epsilon_0.$$

Proof. Since $p^{-v(y)} = \frac{|W|}{|V|}$ where W is the largest eigenspace for V, we have $f(y) < p^{-v(y)} + \epsilon$ for all $y \in G$. Therefore,

$$r - 2 - \epsilon_0 < \sum_{i=1}^{r} \frac{1}{d_i}\left(1 + (d_i - 1)\epsilon - \sum_{y \in \langle x \rangle^\sharp} p^{-v(y)}\right) < A(\underline{d})\epsilon + \sum \kappa(x_i). \qquad \square$$

The relevance of this result can be seen from the main result of [5].

Theorem 9 *(Grassmann Theorem). There is a function $\hat{\epsilon} : \mathbf{N} \to \mathbf{R}^+$ such that*

1. *(G, Ω) satisfies Grassmann Condition $\hat{\epsilon}(m)$ whenever (G, Ω) is a classical subspace action of degree m, and*
2. *$\lim_{m\to\infty} \hat{\epsilon}(m) = 0$.*

In the balance of this subsection we obtain upper bounds for $\kappa(x)$ that will be used in the proof of Theorem 5.

Set

$$\zeta(d) = \zeta(d, p) = \frac{1}{d}\left(1 + \sum_{m \mid d, m>1} \phi(m)p^{-1}\right),$$

where ϕ is the Euler ϕ-function on integers. When a is not an integer we take $\phi(a) = 0$. Since

$$\begin{aligned}\kappa(x) &= \frac{1}{d}\left(1 + \sum_{m \mid d, m>1} \phi(m)p^{-v(x^{d/m})}\right) \\ &= \frac{1}{d}\left(1 + \sum_{m \mid d, m<d} \phi\left(\frac{d}{m}\right)p^{-v(x^m)}\right),\end{aligned}$$

it follows that if x has order d, then

$$\kappa(x) \le \zeta(d) = \frac{1}{d} + \frac{1}{p} - \frac{1}{dp}. \tag{4}$$

Note that ζ is a decreasing function of both d and p.

For each positive integer $s \ge 1$, set

$$\zeta_s(d) = \frac{1}{d}\left(1 + \phi(d) \cdot p^{-s} + \sum_{m|d,1<m<d} \phi(m)p^{-1}\right).$$

More generally, for a finite sequence $s_1, s_2, \dots, s_l$ of positive integers, let

$$\zeta_{s_1,s_2,\dots,s_l}(d) = \frac{1}{d}\left(1 + \sum_{i=1}^{l} \phi(d/i)p^{-s_i} + \sum_{m|d,1<m<d/l} \phi(m)p^{-1}\right).$$

The following statement is evident.

Fact 10. *If x has order d and $v(x^i) \ge s_i$, $i = 1, \dots, l$, then $\kappa(x) \le \zeta_{s_1,\dots,s_l}(d)$.*

The estimates for $\kappa(x)$ can be further refined by taking into consideration the possible actions of elements of a given order on a vector space over $\mathbf{F}_p$.

Definition. For each prime p and integer $d \ge 2$ let $\mu_*(d, p)$ be the smallest positive integer μ such that $\mu = \dim([V, x])$ for some linear operator x of order d acting on a vector space V over $\mathbf{F}_p$.

Note that each $x \in G$ is the image of some element $\widehat{x}$ in $\widehat{G}$ with $\dim C_{V_p}(\widehat{x}) = v(x)$.

If $y \in G$ has order m then $v(y) \ge \mu_*(m, p)$. This inequality holds in particular when $m|d$, $o(x) = d$, and $y = x^{d/m}$. Set

$$\zeta^*(d) = \zeta^*(d, p) = \frac{1}{d}\left(1 + \sum_{m|d,m>1} \phi(m)p^{-\mu_*(m,p)}\right).$$

Then

$$\kappa(x) \le \zeta^*(d). \tag{5}$$

Similarly, if

$$\zeta^*_{s_1,\dots,s_l}(d) = \frac{1}{d}\left(1 + \sum_{m|d,m>1} \phi(m)p^{-\alpha(d/m)}\right), \qquad \alpha(i) = \max\bigl(s_i, \mu_*(d/i, p)\bigr),$$

then

$$\kappa(x) \le \zeta^*_{s_1,\dots,s_l}(d) \tag{6}$$

whenever $v(x^i) \ge s_i$, $i = 1, \dots, l$.

Lemma 11.

1. *If* $p > 2$ *then* $\zeta^*(d) < \frac{3}{d} + .04$.
2. *If* $p = 2$ *then* $\zeta^*(d) < \frac{4}{d} + .032$.

Proof. Suppose $p > 3$. Then $\mu_*(d) = 1$ if and only if $d = p$ or $d|p-1$, and $\mu_*(d) > 1$ for all other d. Since at most $p-1$ nontrivial powers of an element have order p and at most $p-2$ nontrivial powers of an element have order dividing $p-1$ this implies that $\zeta^*(d,p) \le \frac{1}{d}(1 + (2p-3)p^{-1} + (d-1-(2p-3))p^{-2}) < \frac{1}{d}(1 + 2 + d/p^2) = 3/d + 1/p^2 \le 3/d + 1/5^2$. If $p = 3$, then $\mu_*(m,p) = 1$ if and only if $m = 2$ or 3, and $\mu_*(m,p) = 2$ if and only if $m = 4, 6$, or 8. This implies that $\sum_{m|d,\mu_*(m,p)=2} \phi(m) \le \phi(4) + \phi(6) + \phi(8) = 8$. Therefore $\zeta^*(d,3) \le \frac{1}{d}(1 + 3 \cdot 3^{-1} + 8 \cdot 3^{-2} + (d-12) \cdot 3^{-3}) < 3/d + 1/27$.

For $p = 2$, we note that $\mu_*(m,2) = 1$ if and only if $m = 2$; $\mu_*(m,2) = 2$ if and only if $m = 3$ or 4; $\mu_*(m,2) = 3$ if and only if $m = 6$ or 7; and $\mu_*(m,2) = 4$ if and only if $m = 5, 8, 12, 14$, or 15. It follows from this that $\zeta^*(d,2) \le 4/d + 1/32$. □

Corollary 12. *Let* $x \in G$ *have order* d*, and let* k *be a real number.*

1. *If* $p > 2$ *and* $\zeta(d) \ge k > .04$ *then* $d \le \frac{3}{k-.04}$.
2. *If* $p = 2$ *and* $\zeta(d) \ge k > .032$ *then* $d \le \frac{4}{k-.032}$.

The precise value of $\mu_*(d,p)$, the smallest possible commutator dimension for an element of order d over $\mathbf{F}_p$, can be computed using the following statement.

Fact 13.

1. *If* d_p *is the largest power of* p *dividing* d *and* $d_{p'} = d/d_p$*, then* $\mu_*(d,p) = \mu_*(d_p,p) + \mu_*(d_{p'},p)$.
2. *For* $a \ge 1$, $\mu_*(p^a,p) = p^{a-1}$.
3. *If* $(d,p) = 1$ *then either* $\mu_*(d,p)$ *is the exponent of* $p \pmod d$ *or* $\mu_*(d,p) = \mu_*(a,p) + \mu_*(b,p)$ *for some integers* a, b *with* $ab = d$, $a, b > 1$, *and* $(a,b) = 1$.

Proof. We may assume that $d > 1$. Suppose x is an operator of order d on V that achieves the minimum commutator dimension. Without loss, assume that $\dim V$ is minimal.

V is a direct sum of indecomposable $\mathbf{F}_p\langle x\rangle$-submodules V_i. Setting $x_i = x|_{V_i}$ we have $o(x) = \gcd(\{o(x_i)\})$ and $\dim([V,x]) = \sum \dim([V_i,x_i])$. Since $\dim([V_i,x_i^m]) \le \dim([V_i,x_i])$ for all $m \in \mathbf{N}$, by minimality of $\dim([V,x])$ we may assume that $o(x_i)$ is relatively prime to $o(x_j)$ when $i \ne j$.

To prove statement 2, suppose $d = p^a$. Then V consists of a single Jordan block with eigenvalue 1. The order of a Jordan block of size b with eigenvalue 1 is p^a where $p^{a-1} < b \leq p^a$. [Proof: $(y-1)^{b-1} \neq 0$ and $(y-1)^b = 0$ imply $y^{p^k} = 1$ exactly when $p^k \geq b$.] Therefore $p^a \geq \dim V > p^{a-1}$, whence $\dim V = p^{a-1} + 1$ by minimality, and $\mu_*(a,p) = \dim([V,x]) = \dim V - 1 = p^{a-1}$.

To prove 1, note that since $ab \geq a - 1 + b$ for positive integers a and b, for unipotent u and semisimple s the commutator dimension of $u \otimes s$ is always at least as large as the commutator dimension of $u \oplus s$.

The last statement follows easily from the fact that if x acts irreducibly and semisimply on V then $\dim V$ is the exponent of $p \pmod{d}$. This completes the proof of Fact 13. □

2.2. System bounds

The results of the previous subsection apply to individual elements. We shall require stronger bounds, which depend on the system, not merely the individual generating elements. As in [6], we use a result of L. Scott on linear groups together with a fact about group generation to control the contributions of elements with large fixed point ratios to the index sum.

Theorem 14 *(Scott). Suppose $\widehat{G}$ is a group of linear operators on V with $[V, \widehat{G}] = V$ and $C_V(\widehat{G}) = 1$. If $\widehat{G} = \langle g_1, \ldots, g_r \rangle$ where $\prod g_i = 1$, then $\sum \dim([V, g_i]) \geq 2 \dim V$.*

Proof. See [25]. □

Lemma 15. *Assume that $\underline{e}$ is an ordered r-tuple that is a permutation of one of the following.*

1. $(m, m, 1, \ldots, 1)$, $m \geq 1$.
2. $(2, 2, m, 1, \ldots, 1)$, $m \geq 2$.
3. $(2, 3, m, 1, \ldots, 1)$, $m = 3, 4$, *or* 5.

Set $C_i = C_i(\underline{e}) = \frac{2}{e_i(2 - A(\underline{e}))}$.

Let H be a group with generators $\{y_1, \ldots, y_r\}$ where $y_1 y_2 \cdots y_r = 1$. Then there is an ordered M-tuple $(z_1, \ldots, z_M)$, of elements of H, where $M = \sum_j C_j$ such that the following conditions hold.

1. $z_1 z_2 \cdots z_M = 1$.
2. $\{1, \ldots, M\} = \bigcup_{i=1}^{n} \mathcal{C}_i$ *(disjoint union) where $|\mathcal{C}_i| = C_i$ and z_j is conjugate to $y_i^{e_i}$ for all $j \in \mathcal{C}_i$.*
3. *The group K generated by $\{z_j\}$ is normal of index $2/(2 - A(\underline{e}))$ in H, and H/K is cyclic, dihedral, or isomorphic to Alt_4, Sym_4, or Alt_5.*

Proof. By the well-known properties of generators and relations (see [18], for example), if $\underline{e}$ is one of the specified tuples, then the group $\langle y_i,\ i = 1, \dots, r \mid y^{e_i} = \prod_i y_i = 1\rangle$ is, in the respective cases, cyclic of order m, dihedral of order $2m$, or isomorphic to Alt_4, Sym_4, or Alt_5. In each case, this group has order $2/(2 - A(\underline{e}))$. The statements follow from the proof of Lemma 3.2 in [5] or from [10]. □

Note that if $\underline{C}(\underline{e}) = (C_1(\underline{e}), \dots, C_r(\underline{e}))$ then

$$\begin{aligned} \underline{C}(m, m, 1, \dots, 1) &= (1, 1, m, \dots, m), \\ \underline{C}(2, 2, m, 1, \dots, 1) &= (m, m, 2, 2m, \dots, 2m), \\ \underline{C}(2, 3, 3, 1, \dots, 1) &= (6, 4, 4, 12, \dots, 12), \\ \underline{C}(2, 3, 4, 1, \dots, 1) &= (12, 8, 6, 24, \dots, 24), \\ \underline{C}(2, 3, 5, 1, \dots, 1) &= (30, 20, 12, 60, \dots, 60). \end{aligned}$$

Assume now that $\underline{x}$ is a normalized generating r-tuple for G, a classical group with natural module V with $\dim(V/C_{\widehat{G}}(V)) = n$.

Lemma 16. *If $\underline{e}$ and $\underline{C}$ are as above, then, for each i^* in $\{1, \dots, r\}$,*

$$(C_{i^*} - 1)v\bigl(x_{i^*}^{e_{i^*}}\bigr) + \sum_{i \neq i^*} C_i v\bigl(x_i^{e_i}\bigr) \geq n.$$

If $p = 2$, then

$$\sum C_i v\bigl(x_i^{e_i}\bigr) \geq 2n.$$

Proof. We apply Theorem 14 to the preimages $\hat{z}_j$ of the elements z_j under the homomorphism $\widehat{G} \to G$. In general, we can choose $M-1$ preimages $\hat{z}_j$ so that $\dim([V, \hat{z}_j]) = v(x_i^{e_i})$, when $j \in \mathcal{C}_i$. If j^* is the remaining subscript and $j^* \in \mathcal{C}_{i^*}$, then $\dim([V, \hat{z}_{i^*}]) \leq n$, and we have the first statement.

If $p = 2$, then $\dim([V, \hat{z}_j]) = v(x_i^{e_i})$ whenever $j \in \mathcal{C}_i$ because $|\mathbf{F}^\times| = 1$. □

Fact 17. *Suppose $r = 3$ and $d_1 \leq d_2 \leq d_3$.*

1. *If $n > d_1$, then $v(x_i) \geq 2$ for $i \geq 2$.*
2. *If $n > d_2$, then $v(x_1) \geq 2$ for all i.*
3. *If $n \geq 4$ and $d_1 \leq 3$, then $\kappa(x_i) < \zeta_2(d_i)$ for $i > 1$.*
4. *If $n \geq 4$ and $d_2 \leq 3$, then $\kappa(x_i) < \zeta_2(d_i)$ for all i.*

Proof. Setting $\underline{e} = (d_1, 1, d_1)$ and $i^* = 3$, Lemma 16 implies that $d_1 v(x_2) = v(x_1^{d_1}) + d_1 v(x_2) \geq n$. Therefore $v(x_2) \geq n/d_1 > 1$, so the first statement holds for $i = 2$. Using $\underline{e} = (d_1, d_1, 1)$ and $i^* = 2$ establishes the statement for $i = 3$. To establish the second statement, use $\underline{e} = (1, d_2, d_2), i^* = 3$. The remaining two statements follow from Fact 10. □

Set $\zeta^t(d) = \frac{1}{d}(1 + \sum_{m|d,m<d} \phi(d/m)p^{-\max(1,n-mt)})$.
Note that

$$\zeta^t(d) = \zeta_{n-t,n-2t,\ldots}(d).$$

Lemma 18. *If $j \neq k$ and $\sum_{i\neq j,k} v(x_i) \leq t$, then $\kappa(x_j) \leq \zeta^t(d_j)$ and $d_j \geq n/t$.*

Proof. Without loss, $j = 1$ and $k = 2$. From Lemma 16 with $\underline{e} = (m, m, 1, \ldots, 1)$ and $i^* = 2$ we have $v(x_1^m) \geq n - mt$. The total contribution of the $\phi(d_1/m)$ generators of $\langle x_1^m \rangle$ to $\kappa(x_1)$ is therefore at most $\phi(d_1/m) \cdot \frac{1}{d_1} \cdot p^{-\max(1,n-mt)}$. This implies the inequality for $\kappa(x_j)$. Since $v(x_1^{d_1}) = 0$, it also follows that $d_1 \geq n/t$. □

Lemma 19. *If j, k, l are distinct, $d_k = d_l = 2$, and $\sum_{i\neq j,k,l} v(x_i) \leq t$, then $\kappa(x_j) \leq \zeta^{2t}(d_j)$ and $d_j \geq n/2t$.*

Proof. Argue as in the proof of Lemma 18. Assume $j = 1$, $k = 2$, $l = 3$, and use Lemma 16 with $\underline{e} = (m, 2, 2, 1, \ldots, 1)$ and $i^* = 1$ to get $v(x_1^m) \geq n - 2mt$. □

Lemma 20. *Suppose $\underline{d} = (2, d_2, d_3)$ and $v(x_2^2) = v$.*

1. *$\kappa(x_3) \leq \zeta^v(d_3)$ and $d_3 \geq n/v + 1$.*
2. *If $p = 2$ then $\kappa(x_3) \leq \zeta^{v/2}(d_3)$ and $d_3 \geq 2n/v$.*

Proof. Using $\underline{e} = (2, 2, k)$, $i^* = 3$, in Lemma 16, we have $v(x_3^k) \geq n - kv$ in general, and $v(x_3^k) \geq n - kv/2$ when $p = 2$. Using $\underline{e} = (2, 2, d_3)$, $i^* = 2$, we have $(d_3 - 1)v \geq n$ in general and $d_3 v \geq 2n$ when $p = 2$. □

Lemma 21. *If $r = 3$ and $i \neq j$, then $d_i v(x_j) \geq n$. In particular, $\kappa(x_j) \leq \zeta_{\lceil n/d_i \rceil}(d_j)$, where $\lceil x \rceil$ is the smallest integer not less than x.*

Proof. Without loss, $i = 1$ and $j = 2$. The first statement follows from Lemma 16 with $\underline{e} - (d_1, 1, d_1)$ and $i^* = 3$. The second statement follows from the first. □

Lemma 22. *Assume that $\underline{d} = (2, 3, d)$. If p is odd, set $s_2 = \lceil n/2 \rceil$, $s_3 = \lceil n/3 \rceil$, $s_4 = \lceil n/5 \rceil$, and $s_5 = \lceil n/11 \rceil$. If $p = 2$, set $s_2 = \lceil 2n/3 \rceil$, $s_3 = \lceil n/2 \rceil$, $s_4 = \lceil n/3 \rceil$, and $s_5 = \lceil n/6 \rceil$. Then*

$$v(x_3^k) \geq s_k, \qquad d = 2, 3, 4, 5.$$

In particular $\kappa(x_3) \leq \zeta^*_{s_2,s_2,s_3,s_4,s_5}(d)$.

Proof. Lemma 16 with $\underline{e} = (2, 3, e)$ and $e = 2, 3, 4, 5$, with $i^* = 3$ shows that $(C_3(\underline{e}) - 1)v(x_3^{\underline{e}}) \geq n$ in general and $C_3(\underline{e})v(x_3^{\underline{e}}) \geq 2n$ when $p = 2$. We have $C_3(\underline{e}) = 3, 4, 6, 12$ in the respective situations, and the result follows immediately. □

Lemma 23. *Assume that* $\underline{d} = (2, 4, d)$. *If* p *is odd, set* $s_2 = \lceil n/3 \rceil$ *and* $s_3 = \lceil n/7 \rceil$. *If* $p = 2$, *set* $s_2 = \lceil n/2 \rceil$ *and* $s_3 = \lceil n/4 \rceil$. *Then*

$$v\big(x_3^k\big) \geq s_k, \qquad d = 2, 3.$$

In particular $\kappa(x_3) \leq \zeta^*_{s_2,s_2,s_3}(d)$.

Proof. Use Lemma 16 with $\underline{e} = (2, 4, e)$ and $e = 2, 3$, with $i^* = 3$ for the general case. We have $C_3(\underline{e}) = 4, 8$ in the respective situations. □

Lemma 24. *Suppose* $p = 2$, $n \geq 14$, $r = 3$, *and* $\{i, j, k\} = \{1, 2, 3\}$. *Then*

1. $v(x_i^2) + v(x_j^2) \geq 28/d_k$.
2. *If* $d_i = d_j = 3$, *then* $v(x_k^2) \geq 5$.
3. *If* $d_i = 3$ *and* $d_j = 4$, *then* $v(x_k^2) \geq 3$.

Proof. Without loss, $i = 1$, $j = 2$, and $k = 3$. Use Lemma 16 with $\underline{e} = (2, 2, d_3), (3, 3, 2)$, and $(3, 4, 2)$, respectively. □

2.3. Initial reductions

The proof of Theorem 5 uses routine, but extensive, calculations based on the results of the previous subsections. We have verified these calculations using GAP4 [8].

Assume that

1. G is a classical group with natural module V and $\mathbf{F}_p$ dimension n.
2. V contains at least 10^4 points.
3. $\underline{x}$ is a normalized generating r-tuple for G in a primitive action.
4. Every power of every element of $\underline{x}$ satisfies Grassmann Condition 1/100.
5. $g(\underline{x}) \leq 2$.

To prove Theorem 5 it suffices to show that the characteristic of V, the dimension of V over its prime field, and the signature of $\underline{x}$ are given in Table 1.

Unless stated otherwise, we assume that $d_1 \leq d_2 \leq \cdots \leq d_r$ and that $v(x_i) \leq v(x_{i+1})$ whenever $d_i = d_{i+1}$. Also recall that ϵ_0 and $A(d)$ were defined just before Fact 8.

We have $\epsilon_0 < 2 \cdot 10^{-4}$ and $\epsilon < 10^{-2}$. Combining Fact 8 with the inequality $\kappa(x_i) \leq \frac{1}{d_i} + \frac{1}{p} - \frac{1}{d_i p}$, we have the following inequalities.

Fact 25. $A(\underline{d}) > (.99A(\underline{d}) - 2.0002)p$. *Consequently*

1. $p < \frac{A(\underline{d})}{.99A(\underline{d})-2.0002}$
2. $A(\underline{d}) < \frac{2.0002p}{.99p-1}$

Lemma 26. $n \geq 3$.

1. *If* $p \leq 97$ *then* $n \geq 4$.
2. *If* $p \leq 19$ *then* $n \geq 5$.
3. *If* $p = 7$ *then* $n \geq 6$.
4. *If* $p = 5$ *then* $n \geq 7$.
5. *If* $p = 3$ *then* $n \geq 10$.
6. *If* $p = 2$ *then* $n \geq 14$.

Proof. The enumerated statements are immediate consequences of the inequality $(p^n - 1)/(p-1) \geq 10\,000$.

If $n = 2$, then $F^*(G) \cong L_2(p)$, and $F(x) \leq 2$ for all $x \in G^\sharp$. It follows that $f(x) \leq 1/5000$ for all $x \in G^\sharp$, so Eq. (3) cannot hold for $g \leq 2$. □

Set $S = S(\underline{d}) = r - 2 - .01A(\underline{d}) - .0002$, the right hand side of the inequality in Fact 8. For $i = 1, \ldots, r$, set $\kappa_i = \kappa(x_i)$. Set $\Sigma = \sum \kappa_i$. Then $\Sigma > S$ by Fact 8 and assumptions on $\underline{x}$.

Lemma 27.

1. *If* $p \geq 17$, *then* $r = 3$.
2. *If* $p \geq 7$, *then* $r \leq 4$.
3. *If* $p = 7$, *then* $r \leq 4$ *and* $S \geq (r-3) + .9761$.
4. *If* $p = 5$, *then* $r \leq 5$ *and* $S \geq (r-3) + .9744$.
5. *If* $p = 3$, *then* $r \leq 6$ *and* $S \geq (r-3) + .9693$.
6. *If* $p = 2$, *then* $r \leq 8$ *and* $S \geq (r-3) + .9589$.

Proof. Since ζ is a decreasing function, we have $\zeta(d) \leq \zeta(2) = (p+1)/2p$, so $\kappa(x_i) \leq (p+1)/2p$ for all i. Therefore $r \cdot \frac{p+1}{2p} > r - 2 - .01A(\underline{d}) - .0002 > .99r - 2.0002$, whence

$$r < \frac{4.0004p}{.98p - 1}.$$

All assertions about r, except the first, follow from this.

If $r = 4$, then $A(\underline{d}) \geq 13/6$, so $p < 17$ by Fact 25.1.

The statements concerning S follow from Fact 25.2. □

Lemma 28.

1. *If* $r = 3$*, then* $S \geq .9698$*.*
2. *If* $r = 3$ *and* $d_1 = 2$ *then* $S \geq .9748$*.*
3. *If* $r = 3$*,* $d_1 = 2$*, and* $d_2 = 3$ *then* $S \geq .9781$*.*
4. *If* $\underline{d} = (2, 3, 7)$*, then* $S \geq .9795$*.*

Proof. These statements follow from straightforward computations. □

2.4. Completion of the proof

Lemma 29. $n \geq 4$.

Proof. Suppose $n = 3$. Then Ω is the set of points in the natural module for $F^*(G) \cong L_3(p)$. We have $N = p^2 + p + 1$. By Lemma 26, $p > 100$, so $A(\underline{d}) < 2.02$ by Fact 25.2. It follows that $\underline{d} = (2, 3, 7)$.

Since x_1 is an involution in G, we have $\mathrm{Fix}(x_1) \leq p + 2$, and $\mathrm{Ind}(x_1) \geq \frac{1}{2}(p^2 - 1)$. By Lemma 21, $v(x_i) \geq 2$, for $i = 2, 3$. This implies that $\mathrm{Fix}(x_i) \leq 3$, $i = 2, 3$, whence $\mathrm{Ind}(x_i) \geq (d_i - 1)/d_i \cdot (p^2 + p - 2)$. It follows from the Riemann–Hurwitz equation that $g > 2$, a contradiction. □

Lemma 30. $p \leq 19$.

Proof. Suppose $p \geq 23$. Then $A(\underline{d}) \leq 2.0002p/(.99p - 1) < 2.114$ by Fact 25.2. This implies that $\underline{d}$ is one of the following: $(2, 3, d)$, $(2, 4, \leq 7)$, $(2, 5, 5)$, or $(3, 3, 4)$. Also, $S > .9787$ by Fact 8.

If $\underline{d} = (2, 3, d)$, $d \geq 8$, then Fact 17 implies that $\sum \kappa(x_i) \leq \zeta_2(2) + \zeta_2(3) + \zeta_2(d)$. Since $\phi(d) \geq 4$, it follows that $\zeta_2(d) \leq \frac{1}{d}(1 + (d - 5)/p + 4/p^2) = \frac{1}{p} + (1 + \frac{4}{p^2} + \frac{5}{p}) \cdot \frac{1}{d} \leq \zeta_2(8) < .1423$, whence $\sum \zeta_2(d_i) \leq .9778$, a contradiction.

In the remaining six cases, we have $\kappa_i \leq \zeta_2(d_i)$, $i = 2, 3$, and $\kappa_1 \leq \zeta(d_1)$ in all cases, and $\kappa_1 \leq \zeta_2(2)$ in the $(2, 3, 7)$ case. By inspection, either $\Sigma < S$ or $p = 23$ and $\underline{d} = (2, 4, 5)$ or $(2, 3, 7)$.

Suppose $\underline{d} = (2, 4, 5)$. Then $v(x_3) \geq \mu_*(5, 23) = 4$. If $v(x_1) \geq 2$, then $\sum \kappa_i < .9628$, so we must have $v(x_1) = 1$. Therefore $v(x_2) \geq n - v(x_1) \geq 3$. Furthermore, $n = 4$, by Lemma 21. This implies that $v(x_2^2) \geq 2$ since every involution t in $PGL(4, 23)$ with $v(t) = 1$ is not a square in that group. It follows that $\sum \kappa_i < .974$, a contradiction.

We must have $\underline{d} = (2, 3, 7)$, whence $v(x_3) \geq \mu_*(7, 23) = 3$, and $\kappa_3 \leq \zeta_3(7)$. This implies that $\sum \kappa_i < .9786$, which is not so. □

Proposition 31. *If* $p > 7$ *then* $p = 11$*,* $\underline{d} = (2, 3, 7)$*, and* $n = 5$ *or* 6*.*

Proof. By Lemmas 26 and 30, $n \geq 5$. Suppose $p > 7$. Then $p \geq 11$, and for purposes of estimation with $\zeta(d)$ and $\zeta_k(d)$ we may assume that $p = 11$.

Since $A(\underline{d}) \leq 2.2246$ by Fact 25, we have $S \geq (r-3) + .9775$.

If $r > 3$, then $\underline{d} = (2,2,2,3)$ by the condition on $A(\underline{d})$. Since $\sum_{i \neq j} v(x_i) \geq n \geq 5$ for $j = 3,4$, we have $v(x_3) > 1$ and either $v(x_2) > 1$ or $v(x_4) > 1$. Therefore $\sum \kappa_i \leq \max(2\zeta(2) + \zeta_2(2) + \zeta_2(3), \zeta(2) + 2\zeta_2(2) + \zeta(3)) < 1.95$, a contradiction.

Thus $r = 3$. Since $\zeta(d_1) \geq S/3 > \zeta(4)$, it follows that $d_1 = 2$ or 3.

Suppose $d_1 = 3$. Then $\zeta(d_2) > (S - \zeta(3))/2 > \zeta(5)$, so $d_2 \leq 4$, and $\kappa_1 \leq \zeta_2(3)$ by Fact 17. Since $\zeta_2(4) < \zeta_2(3)$, this implies that $\kappa_3 > S - 2\zeta_2(3) > \zeta_2(4) > \zeta(5)$, whence $d_3 = 3$, which is impossible because $\underline{d} \neq (3,3,3)$. This shows that $d_1 = 2$.

Since $\kappa_3 \leq \zeta(d_3) \leq \zeta(d_2)$ and $\kappa_2 \leq \zeta(d_2)$, we must have $\zeta(d_2) > (S - \zeta(2))/2 > \zeta(8)$ so $d_2 \leq 7$. If $d_2 = 5, 6$, or 7, then $\kappa_2 \leq \max_{5 \leq d \leq 7}(\zeta_2(d)) \leq \zeta_2(6)$. [Recall that $p = 11$ for the purpose of calculation.] Since $\zeta(8) < \zeta_2(6)$ and $\zeta(d) < \zeta(8)$ for $d > 8$, we have $\kappa_3 \leq \zeta_2(6)$ and $\sum \kappa_i \leq \zeta(2) + 2\zeta_2(6) < S$. Therefore $d_2 \leq 4$.

Suppose $d_2 = 4$. Then $\kappa_3 \geq S - \zeta_2(2) - \zeta_3(4) > .2002 > \zeta_3(d)$ for $d > 6$, so $d_3 \leq 6$. If $d_3 = 5$, then $A(\underline{d}) = 2.05$, so $S \geq .9793$ and $\Sigma \leq \zeta_2(2) + \zeta_3(4) + \zeta_3(5) < .9781$. It follows that $d_3 = 6$. From Lemma 16 with $\underline{e} = (2,2,2)$, either $v(x_2^2) > 1$ or $v(x_3^2) > 1$. If $v(x_2^2) > 1$, then $\kappa_2 \leq \zeta_{3,2}(4)$. If $v(x_3^2) > 1$, then $\kappa_3 \leq \zeta_{3,2}(6)$. In either case, $\Sigma < .97 < S$.

Suppose $d_2 = 3$. Then $S \geq .9781$ and $\kappa_1 + \kappa_2 \leq \zeta_2(2) + \zeta_3(3) < .8426$, so $\kappa_3 > .1355$. If $d \geq 21$, then $\zeta(d) < \zeta(21) < .135$. Therefore $d_3 \leq 20$. By inspection, if $d_3 = 9$ or $d_3 \geq 11$, then $\zeta_3(d_3) < .137$, and the inequality cannot hold. Therefore d_3 is one of $7, 8$, or 10. If $d_3 = 8$, or 10, then $\kappa_3 \leq \zeta_{3,3}(d_3)$ by Lemma 22 and $\sum \kappa_i < S$.

Therefore $d_3 = 7$, so $S \geq .9795$ and the condition $\zeta_2(2) + \zeta_3(3) + \zeta_3(7) \geq S$ implies that $p = 11$ or 13. If $p = 13$, then $v(x_3)$ is necessarily even, so $\kappa_3 \leq \zeta_4(7)$ and $\sum \kappa_i < S$. Therefore $p = 11$. It follows that κ_2 is even, so $\kappa_2 \leq \zeta_4(3)$. If $v(x_1) > 2$, then $\sum \kappa_i \leq \zeta_3(2) + \zeta_4(3) + \zeta_3(7) < S$. Therefore $v(x_1) = 2$ and $n = 5$ or 6. □

Proposition 32. *If $p = 7$, then $n = 6$ and $\underline{d} = (2,3,7)$.*

Proof. By Lemma 27 $n \geq 6$, $r \leq 4$, and $S \geq (r-3) + .9761$.

Suppose $r = 4$. If $v(x_1) + v(x_2) = 2$, then $d_j \geq 3$, $j > 2$, and $\sum \kappa_i \leq 2\zeta(2) + 2\zeta^2(3) < 1.9$ by Lemma 18. Therefore $v(x_1) + v(x_2) \geq 3$, and in fact $v(x_i) \geq 2$ for at least 3 choices of i. It follows from inspection of values of $\zeta(d)$ and $\zeta_2(d)$ that $\sum \kappa_i < S$, a contradiction.

Therefore $r = 3$. If $v(x_1) = 1$, then $\kappa_2, \kappa_3 \leq \zeta^1(d) < .168$ by Lemma 18. Since $\kappa_1 \leq \zeta(2) < .572$, we have $\sum \kappa_i < S$, a contradiction. Therefore $v(x_i) \geq 2$ and $\kappa_i \leq \zeta_2(d_i)$ for all i. Since $\zeta_2(d) < .3$ for $d > 3$, we have $d_1 \leq 3$.

Suppose $d_1 = 3$. Then, by inspection of $\zeta_2(d)$, $d \geq 3$, we have $\underline{d} = (3,3,4)$. Either $v(x_1) = 2$, in which case $\sum \kappa_i \leq \zeta_2(3) + \zeta_4(3) + \zeta_4(4)$, or $v(x_1) \geq 3$, in which case $\sum \kappa_i \leq 2\zeta_3(3) + \zeta_2(4)$. In either case, $\sum \kappa_i < .97$, a contradiction. We conclude that $d_1 = 2$.

We have $\kappa_2 + \kappa_3 \geq S - \zeta_2(2) \geq .465$. Also $\kappa_i \leq \zeta_3(d_i), i > 1$ by Lemma 21. By inspection, $\zeta_3(d) < .2$ for $d > 6$, so $d_2 \leq 6$.

Suppose $v(x_1) = 2$. Then $\kappa_j \leq \zeta^2(d_j), j \geq 2$, whence $d_2 \leq 4$ because $\zeta^2(d) < .21$ for $d > 4$. If $d_2 = 4$, then $d_3 \geq 5$ because $A(\underline{d}) > 2$, so $\sum \kappa_i \leq \zeta_2(2) + \zeta^2(4) + \zeta^2(5) < .97$, a contradiction. Therefore $d_2 = 3$ and $d_3 \geq 7$, so $S \geq .9781$, and $\kappa_2 + \kappa_3 \geq .4678$, whence $\kappa_3 \geq .4678 - \zeta^2(3) > .1341$. By inspection, $d_3 \in \{7, 8, 9, 12\}$. By Lemma 22, $\kappa_3 < \zeta_{4,3,2,2}(d_3)$, and we conclude that $\underline{d} = (2, 3, 7)$. Note that $n = 6$ by Lemma 21.

We may assume henceforth that $v(x_1) \geq 3$, so $\kappa_1 \leq .5015$ and $\kappa_2 + \kappa_3 > .4747$.

If $d_2 = 6$, then $d_3 = 6$ by inspection of the values of $\zeta_3(d)$, $d \geq 6$. From Lemma 16 with $\underline{e} = (2, 2, 2)$ we have $v(x_j^2) > 1$ for some $j > 1$, so $\kappa_2 + \kappa_3 \leq \zeta_3(6) + \zeta_{3,2}(6) < S - \kappa_1$. This implies that $d_2 < 6$.

By inspection, $d_2 \neq 5$. If $d_2 = 4$, then $\kappa_2 \leq \zeta_3(4) < .2872$, so $\kappa_3 > .1875$. This implies that $d_3 \leq 6$. From Lemma 16 with $\underline{e} = (2, 2, d_3)$ we have $v(x_2^2) > 1$, so $\kappa_2 \leq \zeta_{3,2}(4) < .257$. When $d_3 = 6$, the same argument shows that $\kappa_3 \leq \zeta_{3,2}(6) < .2$. In each case, $\sum \kappa_i < S$.

So $d_2 \neq 4$, and we have $d_2 = 3$. Also, $\kappa_1 + \kappa_2 \leq \zeta_3(2) + \zeta_3(3) < .8368$. So $\kappa_3 \geq S - \kappa_1 - \kappa_2 > .1413$. By inspection of $\zeta_3(d)$, we have $d_3 \leq 18$. By Lemma 22, $\kappa_3 \leq \zeta_{3,3,2,2}(d_3)$, so by inspection $d_3 = 7$. If $n > 6$, then $v(x_1) \geq 3$ and $v(x_j) \geq 4$, $j > 1$, so $\sum \kappa_i \leq \zeta_3(2) + \zeta_4(3) + \zeta_4(7) < .9781 < S$. Therefore $n = 6$. □

Proposition 33. *If $p = 5$, then $\underline{d} = (2, 3, 7)$, $n = 7$, 8, or 9, $v(x_1) = 3$, and $v(x_3) = 6$.*

Proof. By Lemma 27, $n \geq 7$, $r \leq 5$, and $S \geq (r - 3) + .9744$.

If $r = 5$, then $\sum \kappa_i \leq 3\zeta(2) + 2\zeta_2(2) < S$ because $v(x_i) > 1$ for at least two choices of i. Therefore $r \leq 4$.

Suppose $r = 4$. If $v(x_1) + v(x_2) \leq 3$, then Lemma 18 implies that $d_i \geq 7/3 > 2$ for $i = 3, 4$, and $\kappa_i \leq \zeta^3(d_i) \leq \zeta^3(3) = .3344$. Since $\kappa_1 + \kappa_2 \leq 2\zeta(2) = 1.2$, it follows that $\Sigma < S$. Therefore $v(x_1) + v(x_2) \geq 4$. Moreover, $v(x_i) + v(x_j) \geq 4$ whenever $i \neq j$. If $v(x_1) = 1$, then $\sum \kappa_i \leq \zeta(2) + 2\zeta_3(2) + \zeta_3(3) < 1.95$. If $v(x_1) = 2$, then $\sum \kappa_i \leq 3\zeta_2(2) + \zeta_2(3) = 1.92$. Therefore $v(x_1) \geq 3$. If $d_3 > 2$, then we have $\sum \kappa_i < 2\zeta_3(2) + 2\zeta(3) < 1.95$, noting that $\kappa_1, \kappa_2 \leq \zeta_3(2)$ since $\zeta(3) < \zeta_3(2)$. So $d_3 = 2$ and $\kappa_1 + \kappa_2 + \kappa_3 \leq 3\zeta_3(2) = 1.512$. From Lemma 16 with $\underline{e} = (2, 2, 2, 1)$ we have $v(x_4) \geq 3$, so $\kappa_4 \leq \zeta_3(d)$ and $\sum \kappa_i \leq 3\zeta_3(2) + \zeta_3(d) < 1.9$. We conclude that $r \neq 4$. Thus, $r = 3$.

If $v(x_1) = 1$, then Lemma 18 shows that $d_2 \geq 7$ and $\kappa_i \leq \zeta^1(d_i)$, $i = 2, 3$. So $\sum \kappa_i \leq \zeta(2) + 2\zeta^1(d) < .9$. Therefore $v(x_1) \geq 2$, and in fact $\kappa_i \leq \zeta_2(d_i)$ for all i. Since $\zeta^*(d) \leq .29$ for $d \geq 12$ by Lemma 11 and $\zeta_2(d) \leq .32$ for $4 \leq d \leq 11$ by inspection it follows that $d_1 \leq 3$, whence $\kappa_i \leq \zeta_3(d_i)$, $i = 2, 3$, by Lemma 21.

Suppose $d_1 = 3$. Then $\kappa_1 \leq \zeta_2(3) = .36$. If $d_2 \geq 4$, then $\kappa_i \leq \zeta_3(d) \leq .304$ for $i > 1$, and $\sum \kappa_i \leq .968$. Therefore $d_2 = 3$, so $v(x_1) \geq 3$ and $\kappa_1 + \kappa_2 \leq 2\zeta_3(3) < .6774$. If $d_3 > 4$, then $\kappa_3 \leq \zeta_3(d_3) \leq .27$, so $d_3 = 4$. From Lemma 16 with $\underline{e} = (3, 3, 2)$ we have $v(x_3^2) \geq 2$ so $\kappa_3 \leq \zeta_{3,2}(4) = .264 < S - \kappa_1 - \kappa_2$. We conclude that $d_1 = 2$.

We have shown that $v(x_1) > 1$. If $d_3 > 23$, then $\kappa_3 < \zeta^*(d_3) < .165$. Suppose $v(x_1) = 2$. Then $d_2 \geq 4$ and $\kappa_i \leq \zeta^2(d_i)$, $i = 2, 3$. Since $\kappa_1 \leq .52$ and $\zeta^2(d) \leq .203$ for $d > 4$, we must have $d_2 = 4$, whence $d_3 > 4$. If $d_3 \neq 6$, then $\sum \kappa_i \leq \zeta_2(2) + \zeta^2(4) + \zeta^2(5) < .973 < S$. Therefore $d_3 = 6$ and $A(\underline{d}) < 2.09$, so $S > .9789$. We have $\sum \kappa_i \leq \zeta_2(2) + \zeta^2(4) + \zeta^2(6) \leq .975$, a contradiction. This shows that $v(x_1) > 2$.

We have $\kappa_1 \le \zeta_3(2) = .504$ so $\kappa_2 + \kappa_3 > .47$. Also, $\kappa_i \le \zeta_4(d_i)$, $i = 1, 2$. Since $\zeta^*(d) < .2$ for $d \ge 20$ and $\zeta_4(d) < .21$ for $6 < d < 20$, we have $d_2 \le 6$. From Lemma 16 with $\underline{e} = (2, d_2, 2)$ and $i^* = 3$ it follows that $v(x_3^2) \ge 7/(d_2 - 1) > 1$. This implies that $\kappa_3 \le \zeta_{4,2}(d_3)$. If $d_2 = 6$, then $\kappa_2 \le .268$. We have $d_3 = 6$ as otherwise $\kappa_3 \le \min(\zeta^*(d_3), \zeta_{4,2}(d_3)) < .174$, so $\kappa_2, \kappa_3 \le \zeta_{4,2}(6) < .214$, and $\Sigma < S$. Therefore $d_2 < 6$. If $d_2 = 5$, then $\kappa_2 + \kappa_3 \le \zeta_4(5) + \zeta_{4,2}(6) \le .47$. If $d_2 = 4$, then $\kappa_2 \le \zeta_4(4) = .3008$. By Lemma 23, $\kappa_3 \le \zeta_{4,3}(d_3)$. If $d_3 > 23$, then $\kappa_3 < \zeta^*(d_3) < .165$. It follows from inspection that $\zeta_{4,3}(d) \le .214$ for $6 < d < 24$. Therefore $d_3 \le 6$, whence $v(x_2^2) \ge 2$ and $\kappa_2 \le \zeta_{4,2}(4) = .2608$. If $d_3 = 5$, then $\sum \kappa_i < S$. If $d_3 = 6$, then $\kappa_3 \le .2032$, and $\sum \kappa_i < S$. It follows from this paragraph that $d_2 \ne 4$. Therefore $d_2 = 3$.

We have $\kappa_1 + \kappa_2 \le \zeta_3(2) + \zeta_4(3) = .8384$. By Lemma 27, $S \ge .9781$, so $\kappa_3 \ge .1397$. Since $\kappa_3 < 3/d_3 + .04$ we may assume that $d_3 \le 30$. By Lemma 22, $\kappa_3 \le \zeta_{4,4,3,2}(d_3)$. By inspection, $d_3 = 7$.

If $v(x_1) \ge 4$, then $\sum \kappa_i \le \zeta_4(2) + \zeta_4(3) + \zeta_4(7) < S$. So $v(x_1) = 3$ and $n \le d_2 v(x_1) = 9$. □

Proposition 34. *If $p = 3$, then either*

1. $\underline{d} = (2, 3, 7)$, $n = 12$, $v(x_1) = 4$, $v(x_2) = 8$, *and* $v(x_3) = 12$ *or*
2. $\underline{d} = (2, 3, 8)$, $n = 10$, $v(x_1) = 4$, $v(x_2) = 6$, *and* $v(x_3^4) = 2$.

Proof. By Lemma 27, $n \ge 10$, $r \le 6$, and $S \ge (r - 3) + .9693$.

We note that $\zeta^*(d) < .11$ for $d > 42$ by Lemma 11 and $\zeta^*(d) < .11$ by direct computation for $24 < d \le 42$. Also, $\zeta^*(d) < .2$ for $d > 12$. Thus, statements bounding κ_i with weaker bounds need only be verified for a finite number of possible values of d_i. We shall use this implicitly in the following argument.

Since $n > r$, we have $\kappa_i \le \zeta_2(d_i)$ for at least two choices of i. If $r = 6$, then $\sum \kappa_i \le 4\zeta(2) + 2\zeta_2(2) < 3.8$, a contradiction, so $r \le 5$.

Suppose $r = 5$. If $v(x_1) + v(x_2) + v(x_3) = 3$, then $d_i \ge 4$ and $\kappa_i \le \zeta^3(d_i) < .3$ for $i = 4, 5$ by Lemma 18. If $v(x_1) + v(x_2) + v(x_3) = 4$, then $d_i \ge 3$ and $\kappa_i \le \zeta^4(d_i) < .35$ for $i = 4, 5$. Since $\kappa_1 + \kappa_2 + \kappa_3 \le 3\zeta(2) = 2$ we have $\Sigma < S$ in this case. Therefore $v(x_i) + v(x_j) + v(x_k) \ge 5$ for any choice of distinct i, j, k. If $v(x_i) = 1$ for two values of i, then $v(x_i) \ge 3$ for three values and $\sum \kappa_i \le 2\zeta(2) + 3\zeta_3(2) < 2.9$. Therefore $v(x_i) = 1$ for at most one value of i, and $\sum \kappa_i \le \zeta(2) + 4\zeta_2(2) < 2.9$. We conclude that $r \le 4$.

Suppose $r = 4$. If $v(x_1) + v(x_2) = 2, 3, 4$, respectively, then $\kappa_1 + \kappa_2$ is respectively at most 1.3334, 1.2223, 1.1852, while Lemma 18 implies that for $i = 3$ or 4, $\kappa_i \ge \zeta^2(d_i)$ and $d_i \ge 5$, $\kappa_i \ge \zeta^3(d_i)$ and $d_i \ge 4$, $\kappa_i \ge \zeta^4(d_i)$ and $d_i \ge 3$, in the respective cases. By inspection, $\kappa_3 + \kappa_4$ is respectively at most .401, .511, .67, whence $\sum \kappa_i < S$. It follows that $v(x_1) + v(x_2) \ge 5$. Since the same is true of $v(x_i) + v(x_j)$, $i \ne j$, it follows that $v(x_i) \ge 3$ for at least 3 choices of i. Since $\zeta(2) < .67$, $\zeta_3(2) < .52$, and $\zeta(d) < .56$, $\zeta_3(d) < .36$ when $d > 2$, we have $d_3 = 2$, else $\sum \kappa_i < 1.96 < S$. Set $v = v(x_1)$. If $v = 1$, then $\kappa_1 + \kappa_2 + \kappa_3 \le \zeta(2) + 2\zeta_4(2) < 1.68$ and, by Lemma 19, $\kappa_4 \le \zeta^2(d_4)$ where $d_4 \ge 5$, so $\kappa_4 < .21$. If $v = 2$, then $\kappa_1 + \kappa_2 + \kappa_3 \le \zeta_2(2) + 2\zeta_3(2) < 1.6$ and, by Lemma 20, and inspection of ζ^2 values, $\kappa_4 \le \zeta^4(d_4)$ where $d_4 \ge 4$, so $\kappa_4 < .28$. If $v > 2$, then $\kappa_1 + \kappa_2 + \kappa_3 \le 3\zeta_3(2) < 1.56$. From Lemma 16 with $\underline{e} = (2, 2, 2, 1)$ and $i^* = 4$ we have $v(x_4) \ge 4$ and $\kappa_4 \le \zeta_4(3) < .35$. In all cases, $\sum \kappa_i < S$. Therefore $r \ne 4$.

We have $r = 3$. By inspection, $d > 6$ implies $\zeta^*(d) \le .25$. Therefore $d_1 \le 6$ and $A(\underline{d}) \le 3 \cdot 5/6 < 2.84$, so $S > .9714$. By inspection, $\kappa_1 \le \zeta(2) < .67$.

If $v(x_1) = 1$, then, by Lemma 18, $d_i \ge 10$ and $\kappa_i \le \zeta^1(d_i) < .11$, $i = 2, 3$. If $v(x_1) = 2$, then $\kappa_1 \le \zeta_2(2) < .556$. Also, by Lemma 18, $d_i \ge 5$ and $\kappa_i \le \zeta^2(d_i) < .201$, $i = 2, 3$. It follows that $v(x_1) > 2$, so $\kappa_i \le \zeta_3(d_i)$ for all i.

Suppose $d_1 \ge 4$. Then $\kappa_i \le \zeta_3(d_i) \le \zeta_3(4) < .3519$ for all i, so $\sum_{j \ne i} \kappa_j \ge S - \zeta_3(4) > .619$, $i = 1, 2, 3$. If $v(x_i) = 3$ for some i, then Lemma 18 shows that $\kappa_j \le \zeta^3(d_j) \le .254$ for $j \ne i$. If $v(x_i) = 4$ for some i, then $\kappa_i \le \zeta_4(d_i) \le \zeta_4(4) < .34$ and $\kappa_j \le \zeta^4(d_j) < .28$, $j \ne i$. It follows that $v(x_i) \ge 5$ for all i, so $\kappa_i \le \zeta_5(4) < .336$. Since $\zeta^*(d_3) \le .25$ for all $d > 4$ with $d \ne 6$ we conclude that $d_i = 4$ or 6 for all i. From Lemma 16 with $\underline{e} = (2, 2, 2)$ we have $v(x_i^2) \ge 2$ for some i. Therefore $\kappa_i \le \zeta_{5,2}(d_i) < .28$ for some i. Since $\kappa_j \le \zeta_5(d_j) < .34$ for all j it follows that $\Sigma < .96 < S$.

Suppose $d_1 = 3$. Then $\kappa_1 \le \zeta_3(3) < .36$. If $v(x_1) = 3$, then $d_i \ge 4$ and $\kappa_i \le \zeta^3(d_i) < .26$, $i = 2, 3$, by Lemma 18, whence $\sum \kappa_i < S$. Therefore $v(x_1) \ge 4$ and $\kappa_1 \le \zeta_4(3) < .342$, so $\kappa_2 + \kappa_3 \ge S - \kappa_1 > .6295$. If $d > 3$ and d is odd, then $\zeta^*(d) < .21$. For all $d \ge 3$ we have $\zeta_4(d) \le \zeta_4(3) < .342$. It follows that d_i is even whenever $d_i > 3$. If $d_2 > 3$, then Lemma 16 with $\underline{e} = (3, 2, 2)$ implies that $v(x_i^2) > 1$ for some $i > 1$. Therefore $\kappa_2 + \kappa_3 \le \zeta_{4,2}(d_i) + \zeta_4(d_{5-i}) \le \zeta_{4,2}(4) + \zeta_4(4) < S - \kappa_1$. This implies that $d_2 = 3$, so $d_3 > 3$. From Lemma 16 with $\underline{e} = (3, 3, 2)$ and $i^* = 3$ we have $v(x_3^2) \ge 2$. Therefore $\sum \kappa_i \le 2\zeta_4(3) + \zeta_{4,2}(d_3) \le 2\zeta_4(3) + \zeta_{4,2}(4) < S$, a contradiction.

We have $d_1 = 2$ and $\kappa_1 \le \zeta_3(2) < .5186$. Since $\zeta^*(d) < .22$ for $d > 8$ it follows that $d_2 \le 8$. By Lemma 21, $v(x_i) \ge 5$ for $i = 2, 3$.

We claim that if $i = 2$ or 3 and $d_i > 4$, then $\kappa_i \le .236$ and furthermore, either $\kappa_i < .204$ or $d_i = 6$ and $v(x_i^2) \ge 3$. Since $\zeta^*(d) < .2$ for $d \ge 13$ and $\zeta_5^*(d) < .204$ for d odd with $4 \le d < 12$, it suffices to assume that d_i is even and $d_i \le 12$. We have $\kappa_i \le \zeta_5(d_i) < .236$. Suppose $v(x_i^2) = 1$. By Lemma 20, $\kappa_{5-i} \le \zeta^1(d_{5-i})$ and $d_{5-i} \ge 11$, so $\kappa_{5-i} < .11$. It follows that $\sum \kappa_i < .97 < S$. Therefore $v(x_i^2) > 1$. Suppose $v(x_i^2) = 1$. Then $\kappa_i \le \zeta_{5,2}(d_i) < .281$. By Lemma 20, $\kappa_{5-i} \le \zeta^2(d_{5-i})$ and $d_{5-i} \ge 6$, so $\kappa_{5-i} < .17$. This also implies that $\sum \kappa_i < .97 < S$. Therefore $v(x_i^2) \ge 3$ and $\kappa_i \le \zeta_{5,3}^*(d_i)$. The claim follows.

It follows from the claim that if $d_2 > 4$ then $\underline{d} = (2, 6, 6)$ and $v(x_i^2) \ge 3$ for $i = 2, 3$. By Lemma 16 with $\underline{e} = (2, 3, 3)$ we have $v(x_i^3) > 1$ for some $i > 1$, so $\kappa_2 + \kappa_3 \le \zeta_{5,3}(6) + \zeta_{5,3,2}(6) < .435 < S - \kappa_1$. This shows that $d_2 \le 4$.

Suppose $d_2 = 4$. Set $v = v(x_2^2)$. If $v = 1$, then $\kappa_2 \le \zeta_5(4) < .336$ and, as above, $\kappa_3 < .11$. If $v = 2$, then $\kappa_2 \le \zeta_{5,2}(4) \le .28$ and $\kappa_3 \le \zeta^2(d_3) \le \zeta^2(6) < .17$. In either case, $\kappa_2 + \kappa_3 < .45 < S - \kappa_1$. Therefore $v \ge 3$ and we have $\kappa_2 \le \zeta_{5,3}(4) < .2614$. If $d_3 \ne 5, 6, 8, 9, 12$, then $\kappa_3 < \zeta^*(d_3) < .15$, so we may assume that $d_3 \in \{5, 6, 8, 9, 12\}$. By Lemma 23 and the condition that $v(x_3) \ge 5$, $\kappa_3 \le \zeta_{5,4,2}(d_3)$. By inspection, this is at most .191 for $d_3 > 5$, so $\sum \kappa_i < .971 < S$ in this case. We must have $\underline{d} = (2, 4, 5)$. Thus, $A(\underline{d}) = 2.05$ and $S = .9793$. If $v(x_1) = 3$, then $\Sigma \leq \zeta_3(2) + \zeta^3(4) + \zeta^3(5) < .975 < S$. Therefore $v(x_1) \geq 4$ and $\kappa_1 \leq \zeta_4(2) < .507$. We have $\kappa_2 \leq \zeta_{5,3}(4) < .262$ and $\kappa_3 \leq \zeta_5(5) \leq .204$, so $\sum \kappa_i < .973 < S$, a contradiction. This shows that $d_2 \neq 4$, so $d_2 = 3$.

We have $S > .9781$ by Lemma 28. By Lemma 21, $v(x_1) \geq 4$ and $v(x_2) \geq 5$. Since $v(x_1) + v(x_2) \geq 10$, we have $\kappa_1 + \kappa_2 \leq \max(\zeta_4(2) + \zeta_6(3), \zeta_5(2) + \zeta_5(3)) < .8405$. By Lemma 22, $\kappa_3 \leq \zeta_{5,5,4,2}(d_3)$. If $d_3 > 8$, then $\kappa_3 < .137 < S - \kappa_1 - \kappa_2$. Therefore $d_3 = 7$ or 8.

If $d_3 = 7$, then $S > .9795$. If $n > 12$, then $v(x_1) \geq 5$, $v(x_2) \geq 7$, and $v(x_3) \geq 7$, so $\sum \kappa_i \leq \zeta_5(2) + \zeta_7(3) + \zeta_7(7) < S$. Therefore $n \leq 12$. Since $\zeta_6(2) + 1/3 + 1/7 > S([2, 3, 7])$ we must have $v(x_1) \leq 5$. We have $n \geq 10$. Therefore $v(x_1) \leq n - v(x_1)$. From the strong form of Scott's Theorem we have $\max(v(x_1), n - v(x_1)) + v(x_2) + v(x_3) \geq 2n$. Therefore $v(x_2) + v(x_3) \geq n + v(x_1) \geq 4n/3$. Since $p = 3$, we have $v(x_2) \leq 2n/3$, so $v(x_3) \geq 2n/3$. Since 3 has multiplicative order 6 modulo $d_3 = 7$, $v(x_3)$ is necessarily a multiple of 6. Since $10 \leq n \leq 12$ we must have $v(x_3) = n = 12$. If $v(x_1) \geq 5$, then $v(x_2) \geq 7$ and $\sum \kappa_i \geq \zeta_5(2) + \zeta_7(3) + \zeta_{12}(7) > S([2, 3, 7])$, a contradiction. Therefore $v(x_1) = 4$ and $v(x_2) = 8$.

Suppose $d_3 = 8$. If $n > 10$, then $v(x_1) \geq 4$, $v(x_2) \geq 6$, $v(x_2^2) \geq 6$, and $v(x_2^4) \geq 3$, so $\Sigma \leq \zeta_4(2) + \zeta_5(3) + \zeta_{6,6,1,3}(8) < S$. Therefore $n = 10$. If $d_1 > 4$, then $d_1 = 5$, $5 \leq d_2 \leq 6$, and $d_3 \geq 8$ by the strong form of Scott's Theorem, so $\Sigma \leq \zeta_5(2) + \zeta_5(3) + \zeta_{8,5,1,2}(8) < S$. Therefore $d_1 = 4$, whence $d_2 = 6$. Since $\Sigma \leq \zeta_4(2) + \zeta_6(3) + \zeta_{6,5,1,3}(8) < S$, we also have $v(x_3^4) = 2$. □

Proposition 35. *If $p = 2$, then $14 \leq n \leq 21$ and one of the following is true.*

1. $\underline{d} = (2, 3, 7)$
2. $n = 16$, $\underline{d} = (2, 4, 5)$, $v(x_1) = 4$, $v(x_2) = 12$, *and* $v(x_3) = 16$.

Proof. Assume that $p = 2$. By Lemma 27, $n \geq 14$, $r \leq 8$, and $S > (r - 3) + .9589$.

Step 1.

1. $\zeta^*(2) = .75$.
2. If $d > 2$, then $\zeta^*(d) \leq .5$.
3. If $d > 4$, then $\zeta^*(d) \leq .375$.
4. If $d > 6$, then $\zeta^*(d) < .282$.
5. If $d > 8$, then $\zeta^*(d) \leq .25$.
6. If $d > 12$, then $\zeta^*(d) < .19$.
7. If $d > 14$, then $\zeta^*(d) \leq .15$.
8. If $d > 30$, then $\zeta^*(d) < .094$.
9. If $d > 42$, then $\zeta^*(d) < .08$.

In view of Lemma 11, the assertions follow immediately from inspection of the values of $\zeta^*(d)$ for $d < 100$.

Step 2. $r < 5$.

If $r = 8$, then $v(x_i) \geq 2$ for at least 2 choices of x_i, so $\sum \kappa_i \leq 6\zeta(2) + 2\zeta_2(2) = 5.75$. If $r = 7$, then $v(x_i) \geq 3$ for at least 2 choices of x_i since $v(x_1) + \cdots + v(x_6) \geq 14 > 6 \cdot 2$. Therefore $\sum \kappa_i \leq 5\zeta(2) + 2\zeta_3(2) \leq 4.875 < S$. This shows that $r \leq 6$.

Suppose $r = 6$. Set $w = v(x_1) + v(x_2) + v(x_3) + v(x_4)$. If $w \leq 6$, then Lemma 18 implies that $d_5, d_6 > 2$ and $\kappa_i \leq \zeta^6(d_i) < .34$, $i = 5, 6$, so $\sum \kappa_i \leq 4\zeta(2) + 2 \cdot .34 < 3.7$. Therefore $v(x_1) + v(x_2) + v(x_3) + v(x_4) \geq 7$, and the same is true for any other choice of 4 distinct subscripts. If $v(x_i) = 1$ for 3 values of i, then $v(x_j) \geq 4$ for all other values and $\sum \kappa_i \leq 3\zeta(2) + 3\zeta_4(2) < 3.9$. If $v(x_i) = 1$ for exactly 2 values of i, then $v(x_j) \geq 3$ for at least 3 values of j and $\sum \kappa_i \leq 2\zeta(2) + \zeta_2(2) + 3\zeta_3(2) < 3.9$. It follows that $v(x_i) = 1$ for at most 1 choice of i, and $\sum \kappa_i \leq \zeta(2) + 5\zeta_2(2) < 3.9$. Therefore $r < 6$.

Suppose $r = 5$. We claim that if i, j, and k are distinct, then $v(x_i) + v(x_j) + v(x_k) \geq 7$. Assume that $v(x_i) + v(x_j) + v(x_k) \leq 6$. Then, by Lemma 18, $d_l > 2$ for $l \neq i, j, k$ and $\kappa_l \leq \zeta^6(d_l)$. If $d_l > 6$, then $\kappa_l < .3$ by Step 1. If $3 \leq d_l \leq 6$, then $\zeta^6(d_l) < .34$ by inspection. This implies that $\sum \kappa_i < 3\zeta(2) + 2 \cdot .34 = 2.93 < S$, and the claim follows.

We claim further that if $v(x_i) + v(x_j) \leq 4$ for distinct i, j, then $d_k = 2$ for all $k \neq i, j$. For the purpose of establishing this claim we remove the running assumption on the ordering of x_i for the balance of this paragraph and show that if $v(x_1) + v(x_2) \leq 4$ then $d_k = 2$ for $k > 2$. If $v(x_1) + v(x_2) = 2$, then $v(x_k) \geq 5$ for $k > 2$ by the previous paragraph, and $\sum \kappa_i \leq 2\zeta(2) + \sum_{k>2} \zeta_5(d_k)$. Since $\zeta_5(2) < .52$ and $\min(\zeta_5(d), \zeta^*(d)) < .4$ for $d > 2$, we have either $\sum \kappa_i \leq 2\zeta(2) + 2\zeta_5(2) + .4 < 2.94$ or $d_k = 2$ for all $k > 2$. If $v(x_1) + v(x_2) = 3$, then $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_2(2) = 1.4$ and $\sum \kappa_i \leq \kappa_1 + \kappa_2 + \sum_{k>2} \zeta_4(d_k)$. Since $\zeta_4(2) < .54$ and $\min(\zeta_4(d), \zeta^*(d)) < .41$ when $d > 2$, either $\sum \kappa_i < 2.9$ or $d_k = 2$ for all $k > 2$. Finally, if $v(x_1) + v(x_2) = 4$, then $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_3(2) < 1.32$. Considering that $\zeta_3(2) < .57$ and $\min(\zeta_3(d), \zeta^*(d)) < .44$ for $d > 2$, either $\sum \kappa_i < 2.9$ or $d_k = 2$ for all $k > 2$. Since $\sum \kappa_i \geq S$ we conclude in every case that $d_k = 2$ for all $k > 2$. This completes the argument that if $v(x_i) + v(x_j) \leq 4$ for some $i \neq j$, then $d_k = 2$ whenever $k \neq i, j$.

Reverting to the ordering of x_i, so that d_5 is the largest value of d_i, the previous paragraph implies that if $d_5 > 2$, then $v(x_i) + v(x_j) \geq 5$ for every pair of distinct $i, j < 5$. In that case, $\sum_{i<5} \kappa_i \leq \max(\zeta(2) + 3\zeta_4(2), \zeta_2(2) + 3\zeta_3(2)) < 2.4$, and $\kappa_5 \leq \zeta^*(d_5) \leq .5$, whence $\sum \kappa_i < S$. We conclude that $d_i = 2$ for all i. From Lemma 16 with $\underline{e} = (2, 2, 2, 1, 1)$ it follows that $v(x_i) + v(x_j) \geq 7$ whenever $i \neq j$, whence $\kappa_i \leq \max(\{\zeta_a(2) + 4\zeta_{7-a}(2) \colon a = 1, 2, 3\}) < 2.8 < S$. This completes the argument that $r \neq 5$.

Step 3. $r = 3$.

Suppose $r = 4$. Since $v(x) + v(x') + v(x'') \geq 14$ for every set of 3 generators $\{x, x', x''\}$ it follows that $v(x) \geq 5$ for at least two of the four generators, so $\kappa_i \leq \zeta_5(d_i)$ for at least two values of i.

We claim that $A(\underline{d}) \leq 3$. Suppose $A(\underline{d}) > 3$. Then $\sum 1/d_i < 1$. The ordering assumption on d_i implies that $d_2 > 2$ and $d_4 > 4$, so $\kappa_i \leq .5$ for $i > 1$ and $\kappa_4 \leq .375$. If $d_1 > 2$, then $\sum \kappa_i \leq 1.875$, which is not the case, so $d_1 = 2$. It follows that $d_3 > 4$, since otherwise $1/d_1 + 1/d_2 + 1/d_3 \geq 1$. This implies that $\kappa_1 + \kappa_2 + \kappa_3 \leq 1.625$. Therefore $\kappa_4 > .3$, so $d_4 \leq 6$ and $A(\underline{d}) \leq A(2,4,6,6) < 3$, a contradiction. This establishes the claim, and we conclude that $S \geq 1.9698$.

Set $w = v(x_1)+v(x_2)$. Then, by Lemma 18, $\kappa_3 \leq \zeta^w(d_3)$, $\kappa_4 \leq \zeta^w(d_4)$, and $d_3 \geq 14/w$. If $w \leq 3$, then $\kappa_1 + \kappa_2 \leq 1.5$, $d_i \geq 5$, and $\kappa_i < \zeta^3(d_i) < .201$ for $i > 2$. If $w = 4$, then $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_3(2) < 1.32$, $d_i \geq 4$, and $\kappa_i < \zeta^4(d_i) < .26$ for $i > 2$. If $w = 5$, then $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_4(2) < 1.282$, $d_i \geq 3$, and $\kappa_i < \zeta^5(d_i) < .335$ for $i > 2$. If $w = 6$, then $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_5(2) < 1.266$, $d_i \geq 3$, and $\kappa_i < \zeta^6(d_i) < .336$ for $i > 2$. In each case, $\sum \kappa_i \leq 1.96 < S$. This implies that $v(x_1) + v(x_2) \geq 7$. More generally, $v(x_i) + v(x_j) \geq 7$ whenever $i \neq j$.

Suppose $d_3 > 2$ and set $v = v(x_1)$. We claim that $v = 1$. If $v = 2$, then $\kappa_i \leq \zeta_5(d_i)$ for all $i > 1$. Since $\zeta^*(d) < \zeta_5(4) < .5$ when $d > 4$ and $\zeta_k^*(3) \leq \zeta_k^*(4)$ for all k it follows that $\Sigma \leq \zeta_2(2) + \zeta_5(2) + 2\zeta_5^*(4) < 1.93$. Similarly, if $v = 3$, then $\Sigma \leq \zeta_3(2) + \zeta_4(2) + 2\zeta_4^*(4) < 1.91$. If $v = 4$, then $\Sigma \leq 2\zeta_4(2) + \zeta_3^*(4) + \zeta_4^*(4) < 1.91$. If $v = 5$, then $\Sigma \leq 2\zeta_5(2) + \zeta_2^*(4) + \zeta_5^*(4) < 1.93$. If $v \geq 6$, then $\kappa_1 + \kappa_2 \leq 2\zeta_6(2) < 1.02$ and $\kappa_3 + \kappa_4 \leq \max_{t=1,2,3}(\zeta_t^*(4) + \zeta_{7-t}^*(4)) < .9$. In all cases, $\Sigma < S$.

Therefore $v(x_1) = 1$ and $v(x_i) \geq 6$ for $i > 1$. We have $\kappa_1 + \kappa_2 \leq \zeta(2) + \zeta_6(2) < 1.26$. Also, $\kappa_i \leq \zeta_6^*(d_i)$ when $i > 2$. If $d > 4$, then $\zeta_6^*(d) < .34$. Therefore $d_3 \leq 4$ and $\kappa_3 < .39$. From Lemma 16 with $\underline{e} = (1, 2, d_3, 2)$ we have $2d_3 + d_3 v(x_4^2) \geq 28$, whence $v(x_4^2) \geq 28/d_3 - 2 \geq 5$. Therefore $\kappa_4 \leq \zeta_{6,5}^*(d_4)$. If $d_4 \geq 4$, then $\kappa_4 < .3$ and $\Sigma < 1.95$. Therefore $d_4 = 3$, whence $d_3 = 3$, and $\kappa_i \leq \zeta_6(3) < .35$ for $i = 3$ or 4. Once again, $\Sigma < S$. This shows that $d_3 = 2$.

We have $A(\underline{d}) < 2.5$, so $S > 1.9748$. As before, set $v = v(x_1)$. From Lemma 19, $\kappa_4 \leq \zeta^{2v}(d_4)$ and $d_4 \geq 7/v$. If $v = 1$, then $\kappa_1 + \kappa_2 + \kappa_3 \leq \zeta(2) + 2\zeta_6(2) < 1.766$ and $\kappa_4 \leq \zeta^2(d_4) < .144$ because $d_4 \geq 7$. If $v = 2$, then $\kappa_1 + \kappa_2 + \kappa_3 \leq \zeta_2(2) + 2\zeta_5(2) < 1.657$ and $\kappa_4 \leq \zeta^4(d_4) < .255$ because $d_4 \geq 4$. If $v = 3$, then $\kappa_1+\kappa_2+\kappa_3 \leq \zeta_3(2)+2\zeta_4(2) = 1.625$ and $\kappa_4 \leq \zeta^6(d_4) < .336$ because $d_4 \geq 3$. This shows that $\Sigma < S$ when $v \leq 3$. Therefore $v \geq 4$ and $\kappa_1 + \kappa_2 + \kappa_3 \leq 3\zeta_4(2) < 1.594$. From Lemma 16 with $\underline{e} = (2, 2, 2, 1)$ we have $v(x_4) \geq 7$, so $\kappa_4 \leq \zeta_7(d_4) < .379$ because $d_4 > 2$. In this case as well, $\sum \kappa_i < S$. This shows that $r < 4$.

Step 4. $v(x_i) \geq 4$ for all i.

Since $A(\underline{d}) < r = 3$, $S > .9698$. Set $v = v(x_1)$. We apply Lemma 18 once again to bound v from below. If $v = 1, 2$, or 3, then $\kappa_1 \leq \zeta_v(2) \leq .75, .625, .563$, respectively. For $i > 1$, $\kappa_i \leq \zeta^v(d_i)$ where $d_i \geq 14, 7, 5$ in the respective cases. Using Step 1 and inspection, we have $\kappa_i < .08, .15, .201$ in the respective cases. It follows that $\sum \kappa_i < S$ whenever $v(x_1) < 4$. Therefore $v(x_1) \geq 4$. More generally, since the argument that established this does not use the ordering assumption on x_i, it follows that $v(x_i) \geq 4$ for all i.

Step 5. $d_1 = 2$.

Assume that $d_1 > 2$. It follows from Step 1 that $d_1 \leq 6$, so $A(\underline{d}) < 2.84$ and $S > .9714$. Since $v(x_1) \geq 4$, we have $\kappa_1 \leq \zeta_4^*(d_1)$. It follows from Step 1 and inspection that $\kappa_i < .41$ for all i.

If $v(x_1) = 4$, then $d_i \geq 4$, $i = 2, 3$ and $\kappa_i \leq \zeta^4(d_i) < .255$, which implies that $\sum \kappa_i < S$. Therefore $v(x_1) \geq 5$, and, similarly, $v(x_i) \geq 5$ for all i. Thus $\kappa_i \leq \zeta_5^*(d_i)$ for all i. In particular, $\kappa_i < .3907$ for all i.

Suppose $d_1 > 4$. Since $\zeta_5^*(d) < .27$ when $d > 4$, $d \neq 6$ and $\zeta_5^*(6) < .35$, it follows that $d_i = 6$ for all i. Lemma 24 implies that $v(x_i^2) \geq 3$ for at least two choices of i, so $\sum \kappa_i \leq \zeta_5^*(6) + 2\zeta_{5,3}^*(6) < .95$. Therefore $d_1 \leq 4$.

Suppose $d_1 = 4$. Then $d_2 \leq 6$ since otherwise $\kappa_i \leq \zeta_5^*(d_i) < .27$ for $i = 2, 3$ and $\Sigma < \zeta_5^*(4) + 2 \cdot .27 < S$. It follows from Step 1 that $d_3 \leq 12$ as otherwise $\Sigma < S$. This implies that $A(\underline{d}) \leq A(4, 6, 12) = 2.5$, so $S \geq .9748$. Also, Lemma 24 implies that $v(x_1^2) + v(x_2^2) \geq 3$. We claim that $d_3 \leq 8$. If $d_2 = 5$ or 6, then $\kappa_1 + \kappa_2 < \zeta_5^*(4) + \zeta_5^*(6) < .7345$, so $\zeta_5^*(d_3) \geq \kappa_3 > .24$. It follows from inspection that $d_3 \leq 8$ in this case. If $d_2 = 4$, then $\kappa_1 + \kappa_2 \leq \zeta_5^*(4) + \zeta_{5,2}^*(4) < .7188$, so $\zeta_5^*(d_3) > .25$ and $d_3 \leq 8$ in this case as well.

From Lemma 24.1 we have $v(x_1^2) + v(x_2^2) \geq 4$ and $v(x_1^2) + v(x_3^2) \geq 5$. If $v(x_1^2) = 1$, then $v(x_2^2) \geq 3$ and $v(x_3^2) \geq 4$. So $\kappa_2 \leq \zeta_{5,3}^*(d_2) < .3021$, $\kappa_3 \leq \zeta_{5,4}^*(d_3) < .2813$, and $\sum \kappa_i < .974 < S$. If $v(x_1^2) = 2$, then $\kappa_1 \leq \zeta_{5,2}^*(4) < .3282$, $\kappa_2 \leq \zeta_{5,2}^*(d_2) < .3438$, and $\kappa_3 \leq \zeta_{5,3}^*(d_3) < .3021$, whence $\sum \kappa_1 < .9741 < S$. We conclude that $v(x_1^2) \geq 3$, so that $\kappa_1 \leq \zeta_{5,3}(4) < .3$. Without loss, if $d_i = 4$, $i = 2, 3$, then $\kappa_i \leq \zeta_{5,3}^*(4) < .3$. If $d_i > 4$ for some i, then $\kappa_i \leq \zeta_5^*(d_i) < .35$. Since $v(x_2^2) + v(x_3^2) \geq 7$ by Lemma 24, we have either $v(x_2^2) \geq 4$ or $v(x_3^2) \geq 4$, whence $\kappa_i \leq \zeta_{5,4}^*(d_i) < .3$ for some $i > 1$. It follows that $\Sigma < .95 < S$, so we conclude that $d_1 \neq 4$.

We may therefore suppose $d_1 = 3$, so that $\kappa_1 \leq \zeta_5^*(3) \leq .3542$. By Lemma 21, $\kappa_i \leq \zeta_5^*(d_i)$ for $i = 2, 3$. As in the argument when $d_1 = 4$, it follows that $d_2 \leq 6$. By Lemma 16 with $\underline{e} = (1, 1, 1)$, we have $v(x_i) \geq 7$ for two choices of i. If $d_2 = 6$, then $\kappa_1 + \kappa_2 \leq \max(\zeta_5^*(3) + \zeta_7^*(6), \zeta_7^*(3) + \zeta_5^*(6)) < .6902$. It follows from inspection of ζ_5^* values that $d_3 = 6$. Since $v(x_2^2) + v(x_3^2) \geq 10$ by Lemma 24.1 we have $\sum \kappa_i \leq \zeta_5^*(3) + \zeta_5^*(6) + \zeta_{5,5}^*(6) < .3542 + .3438 + .2709 < .97 < S$.

If $d_2 = 5$, then $\kappa_2 \leq .225$ and $\kappa_3 \leq \zeta_5^*(d_3) < .344$, so $\Sigma < S$.

If $d_2 = 4$, then $\kappa_1 + \kappa_2 \leq \max(\zeta_5^*(3) + \zeta_7^*(4), \zeta_7(3) + \zeta_5(4)) < .7332$. By Lemma 24.3, $\kappa_3 \leq \zeta_{5,3}^*(d)$. It follows that $\zeta_{5,3}^*(d) > .24$, so $d_3 = 4$ or 6 by inspection. If $d_3 = 4$, then $\kappa_2 \leq \zeta_{5,3}^*(4) < .3$ by the same result, and $\sum \kappa_i < \zeta_5^*(3) + 2\zeta_{5,3}^*(4) < S$. Therefore $d_3 = 6$. If $v(x_2^2) \geq 3$, then $\sum \kappa_i \leq \zeta_5^*(3) + \zeta_{5,3}^*(4) + \zeta_{5,3}^*(6) < S$. If $v(x_2^2) = 2$, then $v(x_3^2) \geq 8$ by Lemma 24 and $\sum \kappa_i < \zeta_5^*(3) + \zeta_{5,2}^*(4) + \zeta_{5,5}^*(6) < S$, so we may assume that $v(x_2^2) = 1$. From Lemma 16 with $\underline{e} = (3, 2, 3)$ we have $4v(x_3^3) + 6 \geq 28$ whence $v(x_3^3) \geq 6$ and $\kappa_3 < \zeta_{5,5,6}^*(6) < .2 < S - \kappa_1 - \kappa_2$. This shows that $d_2 \neq 4$.

If $d_2 = 3$ then $\kappa_2 \leq \zeta_7^*(3) \leq .3386$ and, by Lemma 24.2, $\kappa_3 \leq \zeta_{5,5}^*(d_3) \leq .2735$, so $\Sigma \leq .97 < S$.

Step 6. $d_2 \leq 4$.

By Lemma 28 and the previous step, $S \geq .9748$. Assume that $d_2 > 4$. By Step 4, $v(x_1) \geq 4$. If $v(x_1) = 4$, then $\kappa_1 \leq \zeta_4(2) < .532$, and $\kappa_i \leq \zeta_{10,6,2}^*(d_i)$ by Lemma 18. By inspection, $\kappa_i < .22$ for $i \geq 2$. This implies that $\Sigma < S$. We conclude that $v(x_1) > 4$.

We have $\kappa_1 \leq \zeta_5(2) < .5157$. If $d_i > 8$ and $d_i \neq 12$, then $\kappa_i \leq \zeta^*(d_i) < .2$. If $d_i = 12$, then $\kappa_i \leq \zeta_7^*(12) < .232$. It follows that either $d_2 \leq 8$ or $d_2 = d_3 = 12$. In the latter case, Lemma 16 with $\underline{e} = (2, 3, 3)$ shows that $v(x_2^3) + v(x_3^3) \geq 7$, so $v(x_i^3) \geq 4$ for some $i > 1$, and $\kappa_i \leq \zeta_{7,1,4}^*(12) < .21$. This implies that $\Sigma < S$. We conclude that $d_2 \leq 8$. From Lemma 16 with $\underline{e} = (2, d_2, 2)$ we have $v(x_3^2) \geq 2 \cdot 14/d_2 > 3$. Consequently, $\kappa_3 \leq \zeta_{7,4}^*(d_3)$. Suppose $d_2 = 8$. Then $\kappa_2 \leq \zeta_7^*(8) < .254$. If $d_2 > 12$, then $\kappa_3 < .19$ by Step 1 and $\Sigma < S$, so $d_2 \leq 12$. By Lemma 16 with $\underline{e} = (2, 2, 12)$, $v(x_2^2) > 2$, so $\kappa_2 \leq \zeta_{7,3}^*(8) < .223$. Since $\zeta_{7,4}^*(12) < .222$, we conclude that $\kappa_2 + \kappa_3 < .446 < S - \kappa_1$, a contradiction. Therefore $d_2 < 8$. Since $\zeta_7^*(7) < .15$, it is evident that $d_2 \neq 7$.

Suppose $d_2 = 6$. Then $A(\underline{d}) < 2.34$ and $S > .9764$, so $\kappa_2 + \kappa_3 \geq S - \kappa_1 > .4607$. Set $w = v(x_2^2)$. Then w is necessarily even because x_2^2 has order 3. If $w = 2$, then $\kappa_2 \leq \zeta_7^*(6) < .336$. By Lemma 20, $d_3 \geq 14$ and $\kappa_3 \leq \zeta^1(d_3)$. By Step 1 and inspection of the values of $\zeta^1(d)$ for $14 \leq d \leq 30$ we have $\kappa_3 < .08$, so $\Sigma < S$ in this case. If $w = 4$, then $\kappa_2 \leq \zeta_{7,4}^*(6) < .2735$. By Lemma 20, $d_3 \geq 7$ and $\kappa_3 \leq \zeta^2(d_3)$. Observing that $\zeta^2(d) < .1431$ for $7 \leq d \leq 28$, we conclude from Step 1 that $\Sigma < S$ in this case as well. If $w = 6$, then $\kappa_2 \leq \zeta_{7,6}^*(6) < .2579$. We have $d_3 \geq d_2 = 6$, and, by Lemma 20, $\kappa_3 \leq \zeta^3(d_3)$. Since $\zeta^3(d) < .18$ for $6 \leq d \leq 12$ we conclude from Step 1 that $\kappa_3 < .18$, whence, once again, $\Sigma < S$. It follows that $w \geq 8$, so $\kappa_2 \leq \zeta_{8,8}^*(6) < .2527$. From Lemma 16 with $\underline{d} = (2, 6, 2)$ we have $v(x_3^2) \geq 5$, so $\kappa_3 \leq \zeta_{7,5}^*(d_3)$. If $d_3 > 6$ and $d_3 \neq 12$, then $\zeta_{7,5}^*(d_3) < .2$ and $\Sigma < S$. Therefore either $d_3 = 6$ or $d_3 = 12$. Recall that, by Lemma 16 with $\underline{e} = (2, 3, 3)$, $v(x_2^3) + v(x_3^3) \geq 7$. If $v(x_2^3) = 1$, then $\kappa_3 \leq \zeta_{7,5,6}^*(d_3) < .2$, and $\Sigma < S$. Therefore $v(x_2^3) \geq 2$, so $\kappa_2 < \zeta_{8,8,2}^*(6) < .211$. If $d_3 = 6 = d_2$, then we may assume that $\kappa_3 \leq \kappa_2$, whence $\kappa_2 + \kappa_3 < .43$. If $d_3 = 12$, then $\kappa_3 \leq \zeta_{7,5}^*(12) < .217$ and $\kappa_2 + \kappa_3 < .43$. In either case, $\Sigma < S$. Therefore $d_2 \neq 6$.

Suppose $d_2 = 5$. Then $\kappa_2 < .2063$, so $\kappa_3 \geq S - \kappa_1 - \kappa_2 > .25$. We have $\kappa_3 < \zeta_{7,6}^*(d_3)$ by Lemma 16 with $\underline{e} = (2, 5, 2)$. It follows from Step 1 and inspection that $d_3 = 6$. From Lemma 16 with $\underline{e} = (2, 5, 3)$ we have $v(x_3^3) \geq 2$, so $\kappa_3 < \zeta_{7,6,2}^*(d_3) < .22$, a contradiction.

Step 7. If $d_2 = 4$, then $n = 16$, $\underline{d} = (2, 4, 5)$, $v(x_1) = 4$, $v(x_2) = 12$, and $v(x_3) = 16$.

Suppose $d_2 = 4$. Then $A < 2.25$ and $S > .9773$. Also, $\kappa_2 \leq \zeta_7^*(4) < .379$.

Assume that $v(x_1) = 4$. Then $\kappa_1 \leq \zeta_4(2) < .532$. By Lemma 18, $d_3 > 3$ and $\kappa_2 \leq \zeta^4(d_3)$, so $\kappa_2 < .255$ by inspection and Step 1. From Lemma 16 with $\underline{e} = (1, 4, 4)$ we have $v(x_3^4) \geq 2n - 4 \cdot 4 \geq 12$, so $v(x_3) \geq 12$ and $v(x_3^2) \geq 12$ as well. By Lemma 23 we have $v(x_3^3) \geq 4$. Therefore $\kappa_3 \leq \zeta^*_{12,12,4,12}(d_3)$. If $d_3 > 5$ then $\kappa_3 < .178$ by Step 1 and inspection. Therefore $d_3 = 5$. We have $n \leq d_2 v(x_1) \leq 16$ and $v(x_i) \geq n-4 \geq 10$, $i = 2, 3$. Since 2 has multiplicative order 4 modulo 5, we also have $4|v(x_3)$, so $v(x_3) = 12$ or 16. If $v(x_3) = 12$, then $v(x_2) \geq 2n - v(x_1) - v(x_3) = 16$. However, $v(x_2) \leq 3n/4$ because x_2 is an element of order 4 acting in characteristic 2. These inequalities are not compatible with the condition $n \leq 16$. We conclude that $v(x_3) = 16$, $n = 16$, and $v(x_2) = 12$.

We may therefore assume that $v(x_1) > 4$. Then $\kappa_1 \leq \zeta_5(2) < .5157$. Set $w = v(x_2^2)$. Assume that $w \leq 2$. Then, by Lemma 20, $d_3 \geq 14$, and $\kappa_3 \leq \zeta^1(d_3)$. So $\kappa_3 < .08 < S - \kappa_1 - \kappa_2$. Therefore $w > 2$. If $w = 3$ or 4, then $\kappa_2 \leq \zeta^*_{7,3}(4) < .2852$, $d_3 \geq 7$, and $\kappa_3 \leq \zeta^2(d_3)$, so $\kappa_3 < .144$ by inspection and Step 1. Once again, $\Sigma < S$. If $w = 5$ or 6, then $\kappa_2 \leq \zeta^*_{7,5}(4) < .2618$, and $\kappa_3 \leq \zeta^3(d_3)$. If $d_3 \geq 6$, then $\kappa_3 < .19$ and $\Sigma < S$, so $d_3 = 5$. By Lemma 20, $w = 6$. Thus, $\kappa_2 \leq \zeta^*_{7,6}(4) < .2579$ and $\kappa_3 \leq \zeta^3(5) < .2004$, so $\Sigma < S$. We conclude that $w = v(x_2^2) \geq 7$, so $\kappa_2 \leq \zeta^*_{7,7}(4) < .2559$. By Lemma 23, $\kappa_3 \leq \zeta^*_{7,7,4}(d_3)$. If $d_3 > 5$, then $\kappa_3 < .2$ by Step 1 and inspection, so $\Sigma < S$. If $d_3 = 5$, then $S = .9793$, and $\kappa_3 \leq .2063$, so once again $\Sigma < S$. This completes the argument that $d_3 \neq 4$.

Step 8. If $d_2 = 3$ then $\underline{d} = (2, 3, 7)$.

It suffices to assume that $d_2 = 3$ and $d_3 > 7$. We have $A(\underline{d}) < 2.17$ and $S > .9781$. Also, $v(x_2)$ is even because x_2 is an element of order 3 acting over $\mathbf{F}_2$. In particular, $v(x_2) \geq 8$ and $\kappa_2 < .33595$. We have $\kappa_3 \leq \zeta^*_{10,10,7,5,3}(d_3)$ by Lemma 22. By inspection, $\kappa_3 \leq .132$. If $v(x_1) \geq 6$, then $\kappa_1 < .50782$ and $\Sigma < S$, so $v(x_1) = 5$ by Lemma 21. We have $\kappa_1 \leq \zeta_5(2) < .5157$.

It follows that $v(x_2) \geq n - 5 \geq 9$, whence $v(x_2) \geq 10$, and $\kappa_2 \leq \zeta_{10}(3) < .334$. We have $\kappa_1 + \kappa_2 < .8497$.

By inspection, if $d > 7$ and $d \neq 8$ or 12, then $\zeta^*_{10,10,7,5,3}(d) < .114$. It follows that $d_3 = 8$ or 12. If $d_3 = 8$, then $A(\underline{d}) < 2.05$, so $S > .9793$ and $\Sigma \leq \zeta_5(2) + \zeta_{10}(3) + \zeta^*_{10,10,7,5}(8) < .9793 < S$. We conclude that $d_3 = 12$, whence $A(\underline{d}) < 2.09$ and $S > .9789$. Since x_3^4 has order 3, $v(x_3^4)$ must be even, and $v(x_3^4) \geq 6$. If $v(x_2) = 10$, then $v(x_3) \geq 2n - v(x_1) - v(x_2) \geq 13$, so $\kappa_3 \leq \zeta^*_{13,10,7,6}(12)$, and $\sum \kappa_i \leq \zeta_5(2) + \zeta_{10}(3) + \zeta^*_{13,10,7,6}(12)$. If $v(x_2) > 10$, then $v(x_2) \geq 12$ and $\sum \kappa_i \leq \zeta_5(2) + \zeta_{10}(3) + \zeta^*_{10,10,7,6}(12)$. In either case, $\Sigma < S$, a contradiction.

Step 9. Conclusion.

By Steps 3, 5, 6, 7, and 8, it suffices to show that if $\underline{d} = (2, 3, 7)$ then $14 \leq n \leq 21$.

Assume that $\underline{d} = (2, 3, 7)$. By Lemma 26, $n \geq 14$. If $n > 21$, then $v(x_1) \geq 8$, $v(x_2) \geq 11$, and $v(x_3) \geq 11$, so $\sum \kappa_i \leq \zeta_8(2) + \zeta_{11}(3) + \zeta_{11}(7) < .9795 < S$. □

Theorem 5 now follows from Propositions 31–35.

Note that for $p = 2, 3$, or 5, further information about values of $v(y)$ for certain elements y is recorded in Propositions 33, 34, and 35.

3. Proof of Theorem 6

Retaining the notation of Section 2.1, assume that Ω is a primitive point action for G with $|\Omega| \geq 10^4$ and that $x \in G$.

3.1. Linear and symplectic groups

Proposition 36. *If Ω consists of all points in the L action or Sp action, then $f(x) - q^{-v(x)} < 1/100$.*

Proof. We have $N = (q^n - 1)/(q - 1)$, so $q^{n-1} < N < 2q^{n-1} \leq q^n$.

Suppose x is a linear transformation. Then the fixed points of x are contained in the union of its eigenspaces, the largest of which has dimension $n-v$. We claim $f(x)-q^{-v(x)} < q^{-n/2} < 1/100$. It suffices to establish the first inequality.

If $v \leq n/2$, then the fixed points of x lying outside the largest eigenspace are contained in a space of dimension v. This implies that $f(x) \leq \frac{q^{n-v}-1}{q-1} + \frac{q^v-1}{q-1}$, so

$$\frac{F(x)}{N} - q^{-v} \leq \frac{q^{n-v} - 1}{q^n - 1} + \frac{q^v - 1}{q^n - 1} - q^{-v} < q^{-(n-v)} \leq q^{-n/2}.$$

If $v = \frac{n+1}{2}$, then the fixed points of x lying outside the largest eigenspace are contained in the union of two nontrivial spaces having total dimension $n - v = (n + 1)/2$. For fixed m, the largest value of $q^a + q^{m-a}$ for a in $\{1, 2, \ldots, m - 1\}$ is $q^{m-1} + q$. Therefore $F(x) \leq \frac{q^{n-v}-1}{q^n-1} + \frac{q^{(n-1)/2}-1}{q-1} + 1$, so

$$\frac{F(x)}{N} - q^{-v} < \frac{q^{(n-1)/2} - 1}{q^n - 1} + \frac{q - 1}{q^n - 1} < q^{-n/2}.$$

If $v \geq n/2 + 1$, then x has at most $q - 1$ eigenspaces, each of which has dimension at most $n/2 - 1$, so $F(x) \leq (q - 1)\frac{q^{n/2-1}-1}{q-1}$ and

$$\frac{F(x)}{N} \leq (q - 1)\left(\frac{q^{n/2-1} - 1}{q^n - 1}\right) < q^{-n/2}.$$

This completes the analysis for x a linear transformation.

Now suppose x is not a linear transformation. Then x induces a field automorphism because graph automorphisms do not act on Ω. Let d be the order of x modulo InnDiag. Then $F(x) \leq \frac{q^{n/d}-1}{q^{1/d}-1}$, so $f(x) > .01$ implies that

$$q^{n(d-1)/d} < \frac{q^n - 1}{q^{n/d} - 1} < 100\frac{q - 1}{q^{1/d} - 1} = 100q^{(d-1)/d}\left(\frac{1 - q^{-1}}{1 - q^{-1/d}}\right).$$

Since $q^{-1/d} \leq 1/2$, we have $q^{n(d-1)/d} < 200q^{(d-1)/d}(1 - q^{-1}) < 200q^{(d-1)/d}$. It follows that $q^{(n-1)(d-1)/d} < 200$, so $200^{d/(d-1)} > q^{n-1}$.

By the first line of this argument, $2q^{n-1} > N > 10\,000$. Therefore $q^{n-1} > 5000 > 200^{3/2}$, whence $\frac{d}{d-1} > \frac{3}{2}$, and $d = 2$.

If x is not a standard field automorphism, then $F(x) \le \frac{q^{n/2-1}-1}{q^{1/2}-1} + 1$, so

$$\begin{aligned} .01 < f(x) &\le \left(q^{1/2}+1\right)\left(\frac{q^{n/2-1}-1}{q^n-1}\right) + \frac{1}{N} \\ &< \frac{3}{2}q^{1/2} \cdot q^{-(n/2+1)} + .0001. \end{aligned}$$

This implies that $q^{n+1} < (\frac{1}{.0066})^2 < 160^2$.

On the other hand, we have $F(x) > .01N > 100$, so $\frac{q^{n/2-1}-1}{q^{1/2}-1} + 1 > 100$. It follows from this that $q^{n-2} > 99^2$, whence $q^3 < (160/99)^2$, which is impossible. Therefore x must be a standard field automorphism.

We have $f(x) = \frac{q^{1/2}+1}{q^{n/2}+1}$ and $v_q(x) = n/2$. If $f(x) - q^{-v_q(x)} > .01$, then $q^{-(n-1)/2} > .01$, whence $q^{n-1} < 10\,000$. On the other hand, $q^{n-1} \cdot \frac{q}{q-1} > \frac{q^n-1}{q-1} = N > 10\,000$. That is,

$$q^{n-1} < 10\,000 < \frac{q^n}{q-1}.$$

Since $n > 2$, the first inequality implies that $q < 100$. Since q is both a perfect square and a prime power, it follows easily by inspection that these two inequalities cannot both hold. □

Proposition 37. *If Ω consists of hyperplanes of type δ in the Sp action, then $f(x) < q^{-v(x)} + 1/100$.*

Proof. We have $N = \frac{1}{2}(q^n + \delta q^{n/2})$. Since q^n is an even power of 2 and $2^{14} + 2^7 < 20\,000$, we have $q^n \ge 2^{16}$.

If x is a field automorphism, then $F(x) \le q^{n/2}$ in either action, so $f(x) \le 2(q^{n/2} - 1)^{-1} < .01$.

If x is in InnDiag, then $F(x) \le \frac{1}{2}(q^{n-v} + q^{n/2})$, so $F(x) - q^{-v(x)}N < q^{n/2}$, and $f(x) - q^{-v} < .01$, as before. □

3.2. Actions of unitary and orthogonal groups

We record here properties of orthogonal and unitary actions that will be used in the analysis.

Fact 38. *Let W be an orthogonal or hermitian space of dimension m over $\mathbf{F}_q$, and let $\pi(W)$ be the number of points of a given type in W. If $\operatorname{rad} W$, the totally singular radical of W, has dimension r, then*

$$P(m) - S(m+r) \le \pi(W) \le P(m) + S(m+r)$$

where $P(m)$ and $S(m)$ are as given below.

Type	$P(m)$	$S(m)$
$U, \mathbf{s}$	$\frac{q^{m-1/2}-1}{q-1}$	$\frac{q^{m/2-1/2}}{q^{1/2}+1}$
$U, \mathbf{n}$	$\frac{q^{m-1/2}}{q^{1/2}+1}$	$\frac{q^{m/2-1/2}}{q^{1/2}+1}$
$O, \mathbf{s}$	$\frac{q^{m-1}-1}{q-1}$	$q^{m/2-1}$
$O, \mathbf{n}$ $(q\ even)$	q^{m-1}	$q^{m/2-1}$
$O, \mathbf{n}$ $(q\ odd)$	$\frac{1}{2}q^{m-1}$	$\frac{1}{2}q^{m/2-1/2}$

In particular, $N > q^{n-2}$.

Proof. When $r = 0$, this follows immediately from Table 2 for all cases except odd-dimensional orthogonal spaces in even characteristic, in which case $\pi(W) = P(m)$. The general case follows since $\pi(W) = \frac{q^r-1}{q-1} + q^r\pi(W/R)$ for singular points and $\pi(W) = q^r\pi(W/R)$ for nonsingular points. □

Fact 39. *Assume that V is an even-dimensional unitary space or orthogonal space of type $+$. For $k \leq n/2 - 1$, set $F_k = P(n-k) + S(n)$. Set $F_{n/2} = 2(\frac{q^{n/2}-1}{q-1})$. If $q = q_0^2$, set $F^* = \frac{q_0^n-1}{q_0-1}$.*

1. *If x is linear and $v(x) = k$, $k \leq n/2$, then $F(x) \leq F_k$.*
2. *If x is linear and $v(x) \geq n/2$, then $F(x) \leq F_{n/2}$.*
3. *If x is semilinear then $F(x) \leq F^*$.*

Proof. This is a straightforward consequence of the previous statement. □

Fact 40. *Suppose x preserves a non-degenerate sesquilinear or bilinear form on V, $X_\lambda = \ker(X - \lambda I)^n$, and $X_\mu = \ker(X - \mu I)^n$. If $\lambda\bar{\mu} \neq 1$ then $X_\mu \subseteq X_\lambda^\perp$.*

Proof. Argue by induction on $k+l$ that if k and l are positive integers, $v \in \ker(X - \lambda I)^k$, and $w \in \ker(X - \mu I)^l$ then $\langle v, w\rangle = 0$. □

3.3. Unitary and orthogonal groups

To complete the proof of Theorem 6 we assume that V admits a nondegenerate orthogonal or unitary form, and that the action of G is on the points of type t in V.

To estimate $f(x) - q^{-v(x)}$ we bound $F(x)$ from above and N from below. For a subspace W of V, let $\pi(W) = \pi_t(W)$ be the number of points of type t in W. It is apparent that $F(x) = \sum \pi(E_\lambda)$ where $\{E_\lambda\}$ is the collection of eigenspaces for x.

Lemma 41. *If x acts linearly on V, then either*

1. $f(x) - q^{-v(x)} < 1/100$ *or*

2. *V has even dimension, the action is on singular points, and some eigenspace for the action of x on V is a totally singular subspace of dimension* $\dim V/2$.

Proof. We have $F(x) = \sum \pi(E_\mu)$ where the sum is over the eigenspaces E_μ for the action of (some pull-back of) x in the group of linear transformations of V.

Suppose $v = v(x) \leq n/2$, and let λ be the principal eigenvalue. Then $\dim E_\lambda = n - v$. Let X_λ be the corresponding generalized eigenspace, that is $X_\lambda = \ker(x - \lambda I)^n$, and set $w = \operatorname{codim}_V X_\lambda$. Then $w \leq v$.

If X_λ is totally singular, then $\dim X_\lambda \leq n/2$, and it follows that $X_\lambda = E_\lambda$, so the second alternative holds. We may therefore suppose that X_λ is not totally singular. It follows from Fact 40 that $\lambda\bar{\lambda} = 1$ and that $E_\mu \subseteq X_\lambda^\perp$ whenever $\mu \neq \lambda$.

This implies that

$$F(x) \leq \pi(E_\lambda) + \pi\big(X_\lambda^\perp\big).$$

Setting $r = \dim \operatorname{rad}(E_\lambda)$, we have $r \leq \operatorname{codim}_{X_\lambda}(E_\lambda) = v - w$. So $\dim X_\lambda^\perp = w \leq v - r$. By Fact 38, $F(x) \leq P(n-v) + S(n-v+r) + P(v-r) + S(v-r)$ because $X_\lambda^\perp$ is non-degenerate.

Since $N \geq P(n) - S(n)$ and $P(n-v) \leq q^{-v}P(n)$, it follows that

$$\begin{aligned} F(x) - q^{-v}N &\leq S(n-v+r) + P(v-r) + S(v-r) + q^{-v}S(n) \\ &= S(n-v+r) + P(v-r) + S(v-r) + S(n-2v), \end{aligned}$$

because $S(n) = Kq^{n/2}$ where K is independent of n.

Set $D(x) = F(x) - q^{-v}N$. We claim that $D(x) < (q+1)S(n-2) + 2$.

We have shown that $D(x) \leq \phi(v,r)$ where $\phi(v,r) = S(n-v+r) + P(v-r) + S(v-r) + S(n-2v)$. By elementary calculus, ϕ attains its maximum on the region $\{(v,r)\colon\ 1 \leq v \leq n/2,\ 0 \leq r \leq v\}$ at $(1,1)$. Therefore $D(x) \leq \phi(1,1) = S(n) + S(n-2) + P(0) + S(0) < (q+1)S(n-2) + 2$ since $P(0) < 1$ and $S(0) < 1$.

Set $D = (q+1)S(n-2)+2$. It suffices to show that if $N \geq 10\,000$ then $D/N < 1/100$.

In all cases, $N > q^{n-2}$ by Fact 38. When V is unitary, $S(n-2) = q^{(n-3)/2}/(q^{1/2}+1)$, and it is easy to see that $D < q^{(n-2)/2}$. So $D^2 < N$, which implies that $D/N < 1/100$.

We may therefore assume that V is orthogonal. If either the action is on singular points or q is even, then $S(n-2) = q^{n/2-2}$, and $D < a^{n/2-1}(1+q^{-1}+2/(q^{n/2-1})) < 8q^{(n-2)/2}/5$. Therefore, $D/N < \frac{8}{5}q^{-(n-2)/2}$, and $q^{(n-2)/2} < 160$. This implies that $n \leq 16$ and $q \leq 11$ since $n \geq 6$. Among the pairs (n,q) of such values, the only ones for which both $q^{(n-2)/2} < 160$ and $N > 10\,000$ are $(6,11), (7,7), (8,5), (11,3)$, and $(16,2)$.

In the nonsingular case when q is odd, $S(n-2) = \frac{1}{2}q^{(n-3)/2}$, so $D \leq q^{(n-1)/2}(q+1)/2q + 2 < q^{(n-1)/2}$. In this case, $N \geq \frac{1}{2}q^{n-1}(1 - q^{-(n-1)/2}) > \frac{4}{9}q^{(n-1)}$. Therefore, $D/N < \frac{9}{4}q^{-(n-1)/2}$, and $q^{(n-1)/2} < 225$. This implies that $n \leq 10$ and $q \leq 7$. By inspection, the only pairs (n,q) for which both $q^{(n-2)/2} < 160$ and $N > 10\,000$ are

$(6,8), (8,4), (16,2)$. A straightforward calculation shows that $f(x) - q^{-v} < 1/100$ in these cases.

A straightforward calculation shows that $f(x) - q^{-v} < 1/100$ in these cases. This shows that the result holds when $v \leq n/2$.

If $v \geq n/2 + 1$, then every eigenspace has dimension at most $n/2 - 1$, and there are at most $q - 1$ eigenspaces. Therefore $F(x) \leq (q-1)(\frac{q^{n/2-1}-1}{q-1}) < q^{n/2-1} < \sqrt{N}$. Since $N \geq 10\,000$ this implies that $F(x)/N < 1/100$.

This leaves the case $v = (n+1)/2$, where n is necessarily odd. Every eigenspace has dimension at most $(n-1)/2$, so $F(x) \leq 2(q^{(n-1)/2} - 1)/(q-1) + 1 \leq F$ where $F = q^{(n-1)/2}$. A short calculation, described below, shows that the conclusion holds in this case.

Suppose V is unitary and set $q_0 = q^{1/2}$. Then $N = \frac{q^{n-1/2}-1}{q-1} - \frac{q^{(n-1)/2}}{q_0+1}$ in the singular case, and $N = \frac{q^{n-1/2}+q^{(n-1)/2}}{q_0+1}$ in the nonsingular case. By computation, $F/N < 1/100$ when $(n, q_0) = (3,5), (5,3)$, or $(9,2)$. Since F/N is a decreasing function of both q and n, it follows that $n = 3, 5$, or 7. Furthermore, $q_0 \leq 4$ when $n = 3$ and $q_0 = 2$ when $n = 5$ or 7. By inspection, $N < 10\,000$ in these cases.

In the orthogonal case, q is necessarily odd because n is odd. We have $N = \frac{q^{n-1}-1}{2}$ in the singular case, and $N = \frac{q^{n-1} \pm q^{(n-1)/2}}{2}$ in the nonsingular case. By computation, $F/N < 1/100$ when $(n, q) = (7,7)$ or $(11,3)$. Since F/N is a decreasing function of both q and n, it follows that $n = 7$, or 9. Furthermore, $q \leq 5$ when $n = 7$ and $q = 3$ when $n = 9$. By inspection, $N < 10\,000$ in these cases.

This completes the proof of Lemma 41. □

Lemma 42. *If x acts semilinearly on V then either*

1. $f(x) - q^{-v(x)} < 1/100$ *or*
2. *the dimension n of V is even, and x has a totally singular eigenspace of dimension n over $F_{q^{1/2}}$.*

Proof. Assume that x acts semilinearly on V with $f(x) \geq 1/100$. Let d be the order of x mod $PGL(V)$. We claim that $d = 2$.

Suppose $d > 2$ and set $q_1 = q^{1/d}$. Then the points fixed by x must lie in an n-dimensional space over $GF(q_1)$, so $F(x) \leq \psi(d) = \frac{q^{n/d}-1}{q^{1/d}-1}$.

If V is orthogonal, and the action is on singular points, then $\psi(d) < 1/100$ when $(d, q_1, n) = (3,2,8), (4,2,6), (3,3,6)$, or $(3,3,7)$. If the action is on nonsingular points, then $\psi(d) < 1/100$ when $(d, q_1, n) = (3,2,6), (3,3,6)$, or $(3,3,7)$. For a given parity of n and a given parity of q the ratio $\psi(d)$ is a decreasing function of d, n, and q. We have $N < 10\,000$ when V is an orthogonal space of dimension 6 over F_8, so $d = 2$ in the orthogonal case.

In the unitary case, q is necessarily a square. We have $F(x)/N < 1/100$ when $(d, q_1, n) = (3, 2^2, 3), (3, 2^2, 4), (4, 2, 3)$, or $(4, 2, 4)$, and the claim holds for the unitary case as well.

We have $d = 2$. Let E be the primary eigenspace for x. Then E is an $\mathbf{F}_{q_0}$ space of dimension at most n where $q_0 = q^{1/2}$. If $\dim E \leq n-1$, then $F(x) < (q_0^{n-1}-1)/(q_0-1)+1$, and a short computation shows that $F(x)/N < 1/100$ whenever $N > 10\,000$. Therefore E has dimension n, and $F(x) \leq \psi(2)$.

We may assume that $\psi(2) - q_0^{-n}N \geq N/100$, and in particular, that $\psi(2) > N/100$.

Then $F(x) \leq \frac{q_0^n-1}{q_0-1}$, and the conditions $F(x)/N \geq 1/100$, $N \geq 10\,000$ imply that (n, q_0) is on one of the following lists.

Unitary groups, nonsingular action: $(8,2), (9,2), (4,5)$;

singular action: $(8,2), (9,2), (6,3), (5,4), (4,7), (4,8), (4,9)$.

Orthogonal groups, nonsingular action: $(8,2), (6,3)$;

singular action: $(10,2), (7,3), (6,4)$.

For $U_9(2^2)$, we have $\psi(2) \leq N/100 + q^{-n/2}N$.

For all other cases, the upper bounds in Fact 38 imply that $F(x) < N/100 - q^{-n/2}N$ whenever E is not totally singular. □

Lemma 43. *If $f(x) - q^{-v} \geq 1/100$ for some $x \in G^\sharp$ then the action is on singular points and one of the following is true.*

1. *V is unitary and $(n, q_0) \in \{(4,7), (4,8), (4,9), (6,3), (8,2)\}$.*
2. *V is orthogonal of $+$ type and $(n, q) \in \{(6,11), (6,13), (6,16), (8,5), (10,4)\}$.*

Proof. The two previous lemmas show that it suffices to assume that the action is on the singular points of an even-dimensional space V and V contains a totally singular subspace of dimension $\dim V/2$.

Suppose first that V is a unitary space of dimension $2m$ over $\mathbf{F}_q$ where $m \geq 2$ and $q = q_0^2$. Then $N = \frac{(q_0^{2m}-1)(q_0^{2m-1}+1)}{q_0^2-1}$.

If x has a totally singular eigenspace of dimension m, then the fixed points of x are contained in the union of two subspaces of V each of dimension m, so $F(x) \leq 2(\frac{q_0^{2m}-1}{q_0^2-1})$. Otherwise, x has an eigenspace of dimension $2m$ over $\mathbf{F}_{q_0}$, and $F(x) \leq \frac{q_0^{2m}-1}{q_0-1}$.

In either case, $f(x) \leq \frac{q_0+1}{q_0^{2m-1}+1}$. By assumption, $f(x) \geq 1/100$. Therefore $q_0^{2m-2} < 100(\frac{q_0+1}{q_0}) \leq 150$. Since $2^8 > 150$, it follows that $2m-2 < 8$. Therefore $m \leq 4$. By inspection, one of the following holds: $m = 2$, $q_0 \leq 9$; $m = 3$, $q_0 \leq 3$; or $m = 4$, $q_0 = 2$.

By further inspection, $N < 10^4$ when $m = 2$, $q_0 \leq 5$ and when $m = 3$, $q_0 = 2$. One of the conditions in 1 must therefore hold.

Now suppose V is an orthogonal $+$ space of dimension $2m$ over $\mathbf{F}_q$, $m \geq 3$. Then $N = \frac{(q^m-1)(q^{m-1}+1)}{q-1}$.

Suppose $q = 2$. Then x has a single eigenspace and $F(x) \leq q^m - 1$, so $f(x) \leq \frac{1}{q^{m-1}+1}$. Since $N > 10\,000$, we have $m \geq 8$. Therefore $f(x) < 1/100$. We may therefore assume that $q \geq 3$.

Suppose x fixes a totally singular subspace of dimension m. Then the fixed points of x are contained in the union of two subspaces of V each of dimension m, so $F(x) \leq 2(\frac{q^m-1}{q-1})$.

We have $f(x) \leq \frac{2}{q^{m-1}+1}$. The assumption that $f(x) > 1/100$ implies that $q^{m-1} < 200$. Since $q \geq 3$ and $3^5 > 200$, it follows that $m \leq 5$ and that one of the following holds: $m = 3$, $q \leq 13$; $m = 4$, $q \leq 5$; or $m = 5$, $q = 3$.

By inspection, $N < 10^4$ when $m = 3$, $q \leq 9$, when $m = 4$, $q \leq 4$, and when $m = 5$, $q = 3$, so one of the following must hold: $2m = 6$ and $q = 11$ or 13; $2m = 8$ and $q = 5$.

If x fixes a subspace of dimension $2m$ over $\mathbf{F}_{q^{1/2}}$, then $F(x) \leq \frac{q^m-1}{q^{1/2}-1}$. Therefore $f(x) \leq \frac{q^{1/2}+1}{q^{m-1}+1}$.

The condition $f(x) \geq 1/100$ implies that $q^{m-1}+1 \leq 100(q_0+1)$, so $q_0^{2m-2} \leq 100(q_0 + 1) \leq 150q_0$, and $q_0^{2m-3} \leq 150$.

We have $m \leq 5$ because $2^8 > 150$, and one of the following holds: $m = 3$, $q_0 \leq 5$; $m = 4$, $q_0 = 2$; or $m = 5$, $q_0 = 2$.

By inspection, $N < 10^4$ for $m = 3$, $q_0 \leq 3$ and for $m = 4$, $q_0 = 2$. Since $\frac{5+1}{25^2+1} < 1/100$, the case $m = 3$, $q_0 = 5$ does not satisfy the hypotheses. This leaves the cases $2m = 6$, $q = 4^2$ and $2m = 10$, $q = 2^2$. □

Lemma 44. *If one of the conclusions of Lemma 43 holds then $g(\underline{x}) > 2$ whenever $\underline{x}$ is a normalized generating tuple for G.*

Proof. We consider the cases in turn. We assume throughout that $N > 10^4$, that $\underline{x}$ is a normalized generating tuple for G, with signature $\underline{d}$, and that $g(\underline{x}) \leq 2$.

By Theorem 5, it suffices to assume that there is an element y involved in $\underline{x}$ which violates Grassmann Condition 1/100.

Step 1. For some i, $\langle x_i \rangle$ contains an element y such that one of the following is true.

1. y fixes two totally singular subspaces of dimension $n/2$.
2. y is a semilinear map on V, y has order 2, and y fixes a subspace of dimension n over $F_{q^{1/2}}$.

Step 2. $\underline{x}$ does not have signature $(2, 3, 7)$.

Proof. If $\underline{x}$ has signature $(2, 3, 7)$, then every element of G must act linearly on V. By Step 1, $\underline{x}$ must involve an element y which has two totally singular eigenspaces of dimension $n/2$. No such element can violate Grassmann Condition 1/100 when G is of type $U_4(q_0^2)$, $U_6(3^2)$, $O_6(16)$, or $O_{10}(4)$. When G is of type $U_8(2^2)$ no element can have two distinct totally singular eigenspaces. In all other cases, the element of order 7 can have at most one eigenvalue. When $q = 11$ or 5, the element of order 3 can have at most one eigenvalue as well. A short computation using fixed point estimates shows that $g(\underline{x}) > 2$ in all cases. □

Step 3. G is not of type $U_4(q^2)$.

Proof. $N = (q^2+1)(q^3+1)$, and, for all $x \in G^\sharp$, we have $F(x) \leq F$ where $F = (q+1)(q^2+1)$. The Riemann–Hurwitz Formula implies that $A(\underline{d}) \leq (2N+2)/(N-F)$. Since $\underline{d} \neq (2,3,7)$, we must have $q=7$, $\underline{d} = (2,3,8)$. In this case, $v(x_3^2) > 1$, and x_3^2 must act linearly on V, so $F(x_3) \leq F(x_3^2) \leq 2(q^2+1)$. By computation, $g(\underline{x}) > 2$. □

Step 4. G is not of type $O_6^+(q)$.

Proof. We have $N = (q^3-1)(q^2+1)/(q-1)$. Set $F_1 = (q^4-1)/(q-1) + q^2$, $F_2 = (q^3-1)/(q-1) + q^2$, and $F_3 = 2(q^3-1)/(q-1)$. When $q = 16$, set $q_0 = 4$ and $F^* = (q^3-1)/(q_0-1)$.

Then $F(x) \leq F_1$ for all $x \in G^\sharp$, and the Riemann–Hurwitz Formula implies that $A(\underline{d}) \leq (2N+2)/(N-F_1)$. It follows that $\underline{d}$ is one of the following: $(2,3,d)$; $(2,4,d)$, $d \leq 29$; $(2,5,d)$, $d \leq 11$; $(2,6,d)$, $d \leq 8$; $(2,7,7)$; $(3,3,d)$, $d \leq 8$; $(3,4,4)$; or $(2,2,2,3)$.

By inspection, if $\mathcal{B}$ is the set of all elements in $G^\sharp$ for which $F(x) > \max(F_2, F^*)$ then $\sum \frac{|\{\mathcal{B} \cap \langle x_i \rangle\}|}{d_i} < 1$. Set $F' = \max(F_2, F_3, F^*)$.

The Riemann–Hurwitz Formula now implies that $A(\underline{d}) \leq (2N+2+1(F_1-F'))/(N-F')$, whence $\underline{d}$ is one of the following: $(2,3,d)$, $d \leq 19$; $(2,4,d)$, $d \leq 7$; $(2,5,5)$; or $(3,4,4)$.

Inspecting this list it follows that $\sum \frac{|\{\mathcal{B} \cap \langle x_i \rangle\}|}{d_i} \leq 1/2$, so $A(\underline{d}) \leq (2N+2+\frac{1}{2}(F_1 - F'))/(N-F')$, which further reduces the possible signatures. Further iterations of this procedure show that $\underline{x}$ must have signature $(2,3,7)$, which was already ruled out by Step 2. □

Step 5. G is not of type $U_6(3^2)$.

Proof. In this case, using $N = (q_0^6-1)(q_0^5+1)/(q-1)$, $F_1 = (q_0^9-1)/(q-1) + q_0^5/(q_0+1)$, $F_2 = (q_0^7-1)/(q-1) + q_0^5/(q_0+1)$, $F_3 = 2(q^3-1)/(q-1)$, and $F^* = (q_0^6-1)/(q_0-1)$, a short modification of the analysis in the previous step again reduces to the case $\underline{d} = (2,3,7)$, which was treated earlier. □

Step 6. G is not of type $O_8^+(5)$.

Proof. The argument of the previous two steps shows that either $\underline{d} = (2,3,d)$ for some d or $\underline{d} \in \{(2,4,\leq 8), (2,5,\leq 6), (3,3,\leq 5)\}$.

In the former situation, the contribution of elements having $v(y) = 1$ is less than $2/3$, and it follows that $d < 200$, whence the contribution is less than $5/12$. Continuing in this way shows that no tuple $\underline{x}$ can have $g(\underline{x}) \leq 2$.

In the remaining cases, bounding the contributions from elements with $v(y) \leq 2$ leads to the same conclusion. □

Step 7. G is not of type $U_8(2^2)$.

Proof. The argument of the previous steps shows that either $\underline{d} = (2, 3, d)$ or $(2, 4, d)$ for some d or $\underline{d} \in \{(2, 5, \leq 17), (2, 6, \leq 10), (2, 7, \leq 8), (3, 3, \leq 10), (3, 4, \leq 5), (2, 2, 2, 3)\}$.

If β_1 is the contribution to $A(\underline{d})$ from elements having $v(y) = 1$ and β_2 is the contribution from elements with $v(y) \leq 2$, then the Riemann–Hurwitz Formula implies that $A(\underline{d}) \leq (2N + 2 - \beta_1(F - F') - \beta_2(F' - F''))/(N - F'')$, where $F(x) \leq F$ for all $x \in G^\sharp$, $F(x) \leq F'$ for all x with $v(x) > 1$, and $F(x) \leq F''$ for all x with $v(x) > 2$.

Using this criterion eliminates the individual cases other than $(2, 3, d)$, $(2, 4, d)$. Using estimates for indexes, this reduces to $(2, 3, \leq 19)$, or $(2, 4, \leq 9)$.

In the $(2, 3, d)$ case, we have $\mathrm{Ind}(x_2) \geq \frac{2}{3}(N - 2(q_0^4 - 1)(q_0^3 + 1)/(q - 1))$ because $v(x_2) \geq 4$ and the eigenspaces for x_2, an element of order 3, must be nondegenerate. Bounding $v(x_3^k)$, and hence $F(x_3^k)$, for $k = 1, 2, 3, 4$, shows that $g(\underline{x}) > 2$ for all choices of d.

In the $(2, 4, d)$ case, consideration of the subcases $v(x_2^2) = 1$, $v(x_2^2) > 1$ leads to the same conclusion. □

Step 8. G is not of type $O_{10}^+(4)$.

Proof. The argument in Step 4 shows that either $\underline{d} = (2, 3, d)$ or $(2, 4, d)$ for some d or $\underline{d} \in \{(2, 5, \leq 12), (2, 6, \leq 9), (2, 7, 7), (3, 3, \leq 9), (3, 4, \leq 5), (2, 2, 2, 3)\}$.

Its extension in Step 7 reduces to the earlier treated case $\underline{d} = (2, 3, 7)$. □

Combining Lemmas 43 and 44 we have the following result.

Proposition 45. *If G is unitary or orthogonal and G violates Grassmann Condition* 1/100 *then $g(\underline{x}) > 2$ for every normalized generating tuple for G.*

Propositions 36, 37, and 45 establish Theorem 6.

4. Proof of Theorem 7

We assume here that $\underline{x}$ and V satisfy one of the conditions listed in Table 1. Suppose Ω is a primitive G-set of [projective] points in V with $|\Omega| \geq 10\,000$.

That is, one of the following is true where $n_p = \dim_{\mathbf{F}_p}(V)$.

1. $\underline{x}$ has signature $(2, 3, 7)$ and one of the following holds.
   (a) $p = 11$ and $n_p = 5$ or 6.
   (b) $p = 7$ and $n_p = 6$.
   (c) $p = 5$ and $n_p = 7, 8$, or 9.
   (d) $p = 3$ and $n_p = 12$.
   (e) $p = 2$ and $14 \leq n_p \leq 21$.
2. $\underline{x}$ has signature $(2, 3, 8)$, $p = 3$, and $n_p = 10$.
3. $\underline{x}$ has signature $(2, 4, 5)$, $p = 2$, and $n_p = 16$. Furthermore $v_p(x_1) = 4$, $v_p(x_2) = 12$, and $v_p(x_3) = 16$.

Table 2
Number of t-points in classical n-space of type X over $\mathbf{F}_q$.

X	Condition	t	$CP(X,n,q,t)$
L			$\frac{q^n-1}{q-1}$
O^ϵ	$n=2m$	Singular	$\frac{(q^m-\epsilon 1)(q^{m-1}+\epsilon 1)}{q-1}$
O^ϵ	$n=2m$	δ	$\frac{(2,q)}{2}(q^m-\epsilon 1)q^{m-1}$
O^ϵ	$n=2m+1$	Singular	$\frac{q^{2m}-1}{q-1}$
O^ϵ	$n=2m+1$	δ	$\frac{q^m(q^m-\epsilon\delta)}{2}$
U	$q=q_0^2$	Singular	$\frac{(q_0^n-(-1)^n)(q_0^{n-1}+(-1)^n)}{q-1}$
U	$q=q_0^2$	Non-singular	$\frac{(q_0^n-(-1)^n)q_0^{n-1}}{q_0+1}$
S	$n=2m, q$ even	ϵ hyperplane	$\frac{q^m(q^m+\epsilon 1)}{2}$

Then V is an n_q-dimensional $\mathbf{F}_q$-module where $q^{n_q}=p^n$, and n_q and q satisfy the conditions listed for point actions.

Fact 46. *The number $CP(X,n,q,t)$ of t-points in a classical n-space of type X over $GF(q)$ is given in Table 2.*

Proof. See [5]. □

We calculate a lower bound for $g(\underline{x})$ in each of the cases using the following lemma.

Lemma 47.

1. *If $\underline{d}=(2,3,7)$, then $v(x_1)\geq n/3$, $v(x_2)\geq n/2$, and $v(x_3)\geq n/2$.*
2. *If $\underline{d}=(2,3,8)$ then $v(x_1)\geq n/3$, $v(x_3)\geq n/2$, $v(x_2)\geq n/2$, $v(x_2^2)\geq n/2$, and $v(x_2^4)\geq n/5$.*
3. *If $\underline{d}=(2,4,5)$, then $v(x_1)\geq n/4$, $v(x_2)\geq n/2$, $v(x_2^2)\geq n/4$, and $v(x_3)\geq n/2$.*
4. *The number of t-points in an n-space with radical of dimension r of type X over $\mathbf{F}_q$ is $(q^r-1)/(q-1)+q^rCP(X,n-r,q,t)$ for singular points and $q^rCP(X,n-r,q,t)$ for non-singular points.*
5. *Assume that q is even. Let $G=O(2m+1,q)\cong Sp(2m,q)$ act on the $2m+1$-dimensional orthogonal space V, where V has a 1-dimensional radical R. If x is a linear transformation in G then x fixes at most $q^m(q^{m-v(x)}+1)/2$ complements to R of each type.*
6. *If W is a space of codimension v in the non-degenerate space V then $\dim\operatorname{rad}W\leq v$.*
7. *Let $\mathrm{Fix}_2(x)$ be the number of fixed points of x lying outside its principal eigenspace. Set $v=v(x)$. Then*
   (a) *If $(o(x),q-1)=1$ then $\mathrm{Fix}_2(x)=0$.*
   (b) *$\mathrm{Fix}_2(x)=0$ in case of type S.*
   (c) *If $2v\leq n$ then $\mathrm{Fix}_2(x)$ is bounded by the number of type t points in some v-dimensional space.*

(d) *If* $(o(x), q-1) = d_0$ *and every* $n - v$*-dimensional space contains at most* M *points then* $\mathrm{Fix}_2(x) \le (d_0 - 1)M$.

8. *If* $\mathrm{Fix}(x^j) \le F_j$ *for all positive powers of* x*, then*

$$\mathrm{Ind}(x) \ge \frac{d-1}{d} N - \frac{1}{d}\left(\sum_{k|d,k<d} \phi\left(\frac{d}{k}\right) F_k\right).$$

9. *If* $\mathrm{Ind}\, x_i \ge H_i$ *for all* i *then* $g(\underline{x}) \ge \frac{1}{2}\sum H_i - N + 1$.

Proof. The first three statements follow from Lemma 16.

The fourth statement is a straightforward count of points in $R \oplus W$ where R is totally singular of dimension r and W is non-degenerate.

Statement 5 follows from a straightforward calculation, as in the proof of Proposition 8.1 of [5].

The next statement is clear because $\mathrm{rad}\, W \subseteq W^{\perp}$.

To prove 7, note that the principal eigenspace of x has dimension $n-v$, and every fixed point of x lying outside the principal eigenspace must lie in an eigenspace of dimension at most $n-v$.

All eigenvalues of x must have order dividing both $o(x)$ and $q-1$, so there are at most $d_0 = (o(x), q-1)$ eigenvalues in toto. Statements 7(a) and 7(d) now follow immediately.

In type S only the eigenvalue $\lambda = 1$ corresponds to fixed points, so statement 7(b) holds.

The total dimension of all secondary eigenspaces is at most v, and all secondary fixed points of x lie in the direct sum of such subspaces. Statement 7(c) follows.

Statements 8 and 9 follow easily from the Cauchy–Frobenius and Riemann–Hurwitz Formulas, respectively. □

In all cases except $L_{14}(2)$ acting on the points in its natural module and $U_8(2^2)$ acting on singular points the lower bound is larger than 2.

However, in those cases, we use the following additional facts:

1. If x has order 7 and acts as a linear transformation over $\mathbf{F}_2$ or $\mathbf{F}_4$ then x has a single eigenspace and $3|v(x)$.
2. If x has order 3 and acts as a linear transformation over $\mathbf{F}_2$ then x has a single eigenspace and $2|v(x)$.

Using these additional facts, it is easy to establish the following lemma and complete the proof of Theorem 7.

Lemma 48. *If* $\underline{d} = (2, 3, 7)$ *and the action is either* $L_{14}(2)$ *on points or* $U_8(2^2)$ *on singular points, then the genus is at least* 20.

Proof. Suppose $G = L_{14}(2)$. Then x_i has only one eigenspace for $i = 1, 2, 3$, $2|v(x_2)$, and $3|v(x_3)$. It follows that $v_1 \geq 5$, $v_2 \geq 8$, and $v_3 \geq 9$. Furthermore, $\mathrm{Ind}(x_1) \geq \frac{1}{2}(2^{14} - 2^9) = 7936$, $\mathrm{Ind}(x_2) \geq \frac{2}{3}(2^{14} - 2^6) = 10\,880$, and $\mathrm{Ind}(x_3) \geq \frac{6}{7}(2^{14} - 2^5) = 14\,016$. This implies that $g(\underline{x}) > 30$.

Suppose $G = U_8(2^2)$. Then x_1 and x_3 have at most one eigenspace, and $3|v(x_3)$. We have $v_1 \geq 3$, $v_2 \geq 4$, and $v_3 = 6$, and it follows that $g(\underline{x}) > 2$. □

References

[1] Michael Aschbacher, Robert Guralnick, Kay Magaard, Rank 3 permutation characters and primitive groups of low genus, in preparation.

[2] Michael Aschbacher, On conjectures of Guralnick and Thompson, J. Algebra 135 (1990) 277–343.

[3] Daniel Frohardt, Robert Guralnick, Kay Magaard, Genus 0 actions of group of Lie rank 1, in: Arithmetic Fundamental Groups and Noncommutative Algebra, Berkeley, CA, 1999, in: Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 449–483.

[4] Daniel Frohardt, Robert Guralnick, Kay Magaard, Incidence matrices, permutation characters, and the minimal genus of a permutation group, J. Combin. Theory Ser. A 98 (2002) 87–105.

[5] Daniel Frohardt, Kay Magaard, Grassmannian fixed point ratios, Geom. Dedicata 82 (2000) 21–104.

[6] Daniel Frohardt, Kay Magaard, Composition factors of monodromy groups, Ann. of Math. 154 (2001) 327–345.

[7] Daniel Frohardt, Kay Magaard, Fixed point ratios in exceptional groups of Lie type of rank at most two, Comm. Algebra 30 (2002) 571–602.

[8] The GAP Group, GAP – Groups Algorithms, and Programming, 2008, version 4.4.12.

[9] Robert Guralnick, Kay Magaard, On the minimal degree of a primitive permutation group, J. Algebra 207 (1998) 127–145.

[10] Robert M. Guralnick, Michael G. Neubauer, Monodromy groups of branched covering: the generic case, in: Recent Developments in the Inverse Galois Problem, Seattle, WA, 1993, in: Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 325–352.

[11] Robert Guralnick, John Shareshian, Symmetric and alternating groups as monodromy groups of Riemann surfaces. i. Generic covers and covers with many branch points, Mem. Amer. Math. Soc. 189 (886) (2007), with an appendix by R. Guralnick and R. Stafford.

[12] Robert Guralnick, John Thompson, Finite groups of genus zero, J. Algebra 131 (1990) 303–341.

[13] Robert Guralnick, Monodromy groups of coverings of curves, in: Galois Groups and Fundamental Groups, in: Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge, 2003, pp. 1–46.

[14] Xianfen Kong, Genus 0, 1, 2 actions of some almost simple groups of Lie rank 2, PhD thesis, Wayne State University, 2011.

[15] Martin Liebeck, Jan Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, Proc. Lond. Math. Soc. 63 (1991) 266–314.

[16] Martin Liebeck, Gary Seitz, Reductive subgroups of exceptional algebraic groups, Mem. Amer. Math. Soc. 121 (580) (1996).

[17] Martin Liebeck, Aner Shalev, Simple groups, permutation groups, and probability, J. Amer. Math. Soc. 12 (1999) 497–520.

[18] Wilhelm Magnus, Non-Euclidean Tesselations and Their Groups, Academic Press, New York–London, 1974.

[19] Kay Magaard, Monodromy and sporadic groups, Comm. Algebra 21 (1993) 4271–4297.

[20] Kay Magaard, Sergey Shpectorov, G. Wang, Generating sets of affine groups of low genus, in: Computational Algebraic and Analytic Geometry, in: Contemp. Math., vol. 572, 2012, pp. 173–192.

[21] Kay Magaard, Helmut Völklein, The monodromy group of a function on a general curve, Israel J. Math. 141 (2004) 355–368.

[22] Kay Magaard, Helmut Völklein, Götz Wiesend, The combinatorics of degenerate covers and an application to general curves of genus 3, Albanian J. Math. 2 (2008) 145–158.

[23] Michael Neubauer, On solvable monodromy groups of fixed genus, PhD thesis, University of Southern California, 1989.
[24] Michael Neubauer, On monodromy groups of fixed genus, J. Algebra 153 (1992).
[25] Leonard Scott, Matrices and cohomology, Ann. of Math. 105 (1977) 473–492.
[26] Tanchu Shih, A note on groups of genus zero, Comm. Algebra 19 (1991) 2813–2826.
[27] Helmut Völklein, Groups as Galois Groups: An Introduction, Cambridge University Press, 1996.