

Distinguishing finite group characters and refined local-global phenomena

by

KIMBALL MARTIN (Norman, OK) and NAHID WALJI (Paris)

1. Introduction. In this paper, we consider two questions about seemingly different topics:

- (1) How often can two characters of a finite group agree?
- (2) How many local Euler factors determine an L -function?

The first question is just about characters of finite groups, and the second is a refined local-global principle in number theory. However, it has been observed, notably by Serre, that being able to say something about (1) allows one to say something about (2), which is our primary motivation, though both are natural questions. Our main results about the first question concern comparing primitive characters of degree ≤ 3 and characters of $\mathrm{PSL}(2, q)$ or $\mathrm{SL}(2, q)$. This will yield sharp bounds on how many Euler factors one needs to distinguish primitive 2- or 3-dimensional L -functions of Galois representations. We address the two questions in turn.

1.1. Distinguishing group characters. Let G be a finite group, and ρ, ρ' be two complex representations of G with characters χ, χ' . We will study the quantities

$$\delta(\rho, \rho') = \delta(\chi, \chi') = \frac{|\{g \in G : \chi(g) \neq \chi'(g)\}|}{|G|}.$$

Specifically, let $\delta_n(G)$ be the minimum of $\delta(\rho, \rho')$ as ρ, ρ' range over pairs of inequivalent irreducible n -dimensional representations of G , with the convention that $\delta_n(G) = 1$ if there are no such pairs ρ, ρ' . Note that

2010 *Mathematics Subject Classification*: Primary 11F80, 20C15; Secondary 20C33.

Key words and phrases: finite group representations, Galois representations, local-global principles.

Received 20 January 2017.

Published online 11 July 2017.

$\delta_n(G)$ tells us what fraction of elements of G we must check to distinguish irreducible degree n characters. Let $d_n = \inf_G \{\delta_n(G)\}$.

An elementary consequence of orthogonality relations is

PROPOSITION 1.1. *We have $d_n \geq 1/(2n^2)$.*

Buzzard, Edixhoven and Taylor constructed examples to show this bound is sharp when n is a power of 2, and Serre generalized this to arbitrary n (see [Ram94b]).

THEOREM 1.2 (Serre). *For any n , there exists G such that $\delta_n(G) = 1/(2n^2)$, so $d_n = 1/(2n^2)$.*

In particular, the infimum in d_n is a minimum. We will recall the proof of Proposition 1.1 and Serre’s construction in Section 2.2. For now, the main points to note are that Serre’s examples must be solvable and the representations are induced.

In this paper, we consider two kinds of refinements of determining d_n . The first refinement is by restricting to primitive representations, and the second is by restricting to certain families of groups.

Define $\delta_n^{\sharp}(G)$ to be the infimum of $\delta(\rho, \rho')$ where ρ, ρ' range over pairs of inequivalent irreducible primitive n -dimensional complex representations of G . Let $d_n^{\sharp} = \inf_G \{\delta_n^{\sharp}(G)\}$. From Serre’s theorem, we get the trivial bound $d_n^{\sharp} \geq d_n = 1/(2n^2)$.

Our first result is to determine d_n^{\sharp} for $n \leq 3$.

THEOREM 1.3. *We have $d_1^{\sharp} = 1/2$, $d_2^{\sharp} = 1/4$ and $d_3^{\sharp} = 2/7$. Furthermore, $\delta_2^{\sharp}(G) = 1/4$ if and only if G is an extension of $H \times_{C_2} C_{2m}$ where $m \in \mathbb{N}$ and $H = [48, 28]$ or $H = [48, 29]$. Also, $\delta_3^{\sharp}(G) = 2/7$ if and only if G is an extension of $\text{PSL}(2, 7)$.*

Here G being an extension of H by some $N \triangleleft G$ means $G/N \simeq H$. The groups $[48, 28]$ and $[48, 29]$ are the two groups of order 48 which are extensions of S_4 by the cyclic group C_2 and contain $\text{SL}(2, 3)$.

The $n = 1$ case is already contained in Proposition 1.1 as $d_1 = d_1^{\sharp}$. For $n = 2, 3$, these bounds are much better than the trivial bounds $d_2^{\sharp} \geq 1/8$ and $d_3^{\sharp} \geq 1/18$ from Proposition 1.1. For $n = 2$, related results were previously obtained by the second author in [Wal14] and will be discussed below.

Note that while d_n is a strictly decreasing sequence for $n \geq 1$, our result says this is not the case for d_n^{\sharp} .

In a slightly different direction, one can look for stronger lower bounds than $1/(2n^2)$ for certain families of groups. We do not begin a serious investigation of this here, but just treat two basic families of finite groups of Lie type which are related to the calculations for $\delta_2^{\sharp}(G)$ and $\delta_3^{\sharp}(G)$.

THEOREM 1.4. We compute $\delta_n(G)$ and $\delta_n^{\natural}(G)$ where $G = \text{PSL}(2, q)$ or $G = \text{SL}(2, q)$; for n not listed explicitly below, $\delta_n(G) = \delta_n^{\natural}(G) = 1$.

For $G = \text{SL}(2, q)$ with q arbitrary and for $G = \text{PSL}(2, q)$ with q even,

$$\delta_n(G) = \delta_n^{\natural}(G) \begin{cases} = 2/q & \text{if } n = (q \pm 1)/2 \text{ and } q \text{ is odd,} \\ \geq 1/6 & \text{if } n = q - 1, \end{cases}$$

and $\delta_{q+1}(G) \geq 1/6$ whereas $\delta_{q+1}^{\natural}(G) = 1$.

For $G = \text{PSL}(2, q)$ and q odd,

$$\delta_n(G) = \delta_n^{\natural}(G) \begin{cases} = 2/q & \text{if } n = (q - 1)/2 \text{ and } q \equiv 3 \pmod{4}, \\ = 2/q & \text{if } n = (q + 1)/2 \text{ and } q \equiv 1 \pmod{4}, \\ \geq 1/6 & \text{if } n = q - 1, \end{cases}$$

and $\delta_{q+1}(G) \geq 1/6$ whereas $\delta_{q+1}^{\natural}(G) = 1$.

We remark that we completely determine $\delta_{q\pm 1}(G)$ for $G = \text{SL}(2, q)$ and $\text{PSL}(2, q)$ in Section 6, but the exact formulas are a bit complicated and depend on divisibility conditions on $q \mp 1$. In particular, $\delta_{q\pm 1}(\text{SL}(2, q)) = 1/6$ if and only if $12 \mid (q \mp 1)$, and $\delta_{q\pm 1}(\text{PSL}(2, q)) = 1/6$ if and only if $24 \mid (q \mp 1)$.

The values for $\text{SL}(2, q)$ immediately give the following bounds.

COROLLARY 1.5. $d_{(q\pm 1)/2}^{\natural} \leq 2/q$ for q any odd prime power greater than 3.

Note the upper bound in the corollary for $q = 7$ is the exact value of d_3^{\natural} .

Even though Theorem 1.3 implies d_n^{\natural} is not a decreasing sequence for $n \geq 1$, this corollary at least suggests that $d_n^{\natural} \rightarrow 0$ as $n \rightarrow \infty$.

The proof of Theorem 1.3 relies on consideration of various cases according to the possible finite primitive subgroups of $\text{GL}_2(\mathbb{C})$ and $\text{GL}_3(\mathbb{C})$ which are “minimal lifts”, and about half of these are of the form $\text{PSL}(2, q)$ or $\text{SL}(2, q)$ for $q \in \{3, 5, 7, 9\}$. Thus Theorem 1.4 is a generalization of one of the ingredients for Theorem 1.3. However, most of the work involved in the proof of Theorem 1.3 is the determination of and reduction to these minimal lifts, as described in Section 3.

1.2. Distinguishing L -functions. Let F be a number field, and consider an L -function $L(s)$, which is a meromorphic function of a complex variable s satisfying certain properties, principally having an Euler product $L(s) = \prod L_v(s)$ where v runs over all primes of F for s in some right half-plane. For almost all (all but finitely many) v , we should have $L_v(s) = (p_v(q_v^{-s}))^{-1}$ where q_v is the size of the residue field of F_v and p_v a polynomial of a fixed degree n , which is the *degree* of the L -function.

Prototypical L -functions of degree n are the L -functions $L(s, \rho) = \prod L(s, \rho_v)$ of n -dimensional Galois representations $\rho : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_n(\mathbb{C})$

(or into $\mathrm{GL}_n(\overline{\mathbb{Q}_p})$) and L -functions $L(s, \pi) = \prod L(s, \pi_v)$ of automorphic representations π of $\mathrm{GL}_n(\mathbb{A}_F)$. In fact it is conjectured that all (nice) L -functions are automorphic. These L -functions are local-global objects, and one can ask how many local factors $L_v(s)$ determine $L(s)$.

First consider the automorphic case: suppose π, π' are irreducible cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_F)$, S is a set of places of F and we know that $L(s, \pi_v) = L(s, \pi'_v)$ for all $v \notin S$. Strong multiplicity one says that if S is finite, then $L(s, \pi) = L(s, \pi')$ (in fact, $\pi \simeq \pi'$). Ramakrishnan [Ram94b] conjectured that if S has density $< 1/(2n^2)$, then $L(s, \pi) = L(s, \pi')$, and this density bound would be sharp. This is true when $n = 1$, and Ramakrishnan also showed it when $n = 2$ [Ram94a].

Recently, in [Wal14] the second author showed that when $n = 2$, one can in fact obtain stronger bounds under various assumptions, e.g., the density bound $1/8$ from [Ram94a] may be replaced by $1/4$ if one restricts to nondihedral representations (i.e., not induced from quadratic extensions) or by $2/9$ if the representations are not twist-equivalent.

Our motivation for this project was to try to understand an analogue of [Wal14] for larger n . However, the analytic tools known for $\mathrm{GL}(2)$ that are used in [Wal14] are not known for larger n . Moreover, the classification of $\mathrm{GL}(2)$ cuspidal representations into dihedral, tetrahedral, octahedral and icosahedral types has no known nice generalization to $\mathrm{GL}(n)$. So, as a proxy, we consider the case of Galois (specifically Artin) representations. The strong Artin conjecture says that all Artin representations are automorphic, and Langlands' principle of functoriality says that whatever is true for Galois representations should be true (roughly) for automorphic representations as well.

Consider ρ, ρ' to be irreducible n -dimensional Artin representations for F , i.e., irreducible n -dimensional continuous complex representations of the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ of F . To almost all places v of F , we can associate a well-defined Frobenius conjugacy class Fr_v of $\mathrm{Gal}(\bar{F}/F)$, and $L(s, \rho_v)$ determines the eigenvalues of $\rho(\mathrm{Fr}_v)$, and thus $\mathrm{tr} \rho(\mathrm{Fr}_v)$. Let S be a set of places of F , and suppose $L(s, \rho_v) = L(s, \rho'_v)$, or even just $\mathrm{tr} \rho(\mathrm{Fr}_v) = \mathrm{tr} \rho'(\mathrm{Fr}_v)$, for all $v \notin S$.

Continuity means that ρ and ρ' factor through a common finite quotient $G = \mathrm{Gal}(K/F)$ of $\mathrm{Gal}(\bar{F}/F)$, for some finite normal extension K/F . View ρ, ρ' as irreducible n -dimensional representations of the finite group G . The Chebotarev density theorem tells us that if C is a conjugacy class in G , then the image of Fr_v in $\mathrm{Gal}(K/F)$ lies in C for a set of primes v of density $|C|/|G|$. This implies that if the density of S is $< \delta_n(G)$ (or $< \delta_n^{\natural}(G)$ if ρ, ρ' are primitive), then $\rho \simeq \rho'$, i.e., $L(s, \rho) = L(s, \rho')$. Moreover, this bound on the density of S is sharp.

Consequently, Proposition 1.1 tells us that if the density of S is $< 1/(2n^2)$, then $L(s, \rho) = L(s, \rho')$, and Serre's result implies this bound is sharp. (See Rajan [Raj98] for an analogous result on ℓ -adic Galois representations.) In fact, this application to Galois representations was Serre's motivation, and it also motivated the bound in Ramakrishnan's conjecture. For us, the Chebotarev density theorem together with Theorem 1.3 yields

COROLLARY 1.6. *Let ρ, ρ' be irreducible primitive n -dimensional Artin representations of F . Suppose $\text{tr } \rho(\text{Fr}_v) = \text{tr } \rho'(\text{Fr}_v)$ for a set of primes v of F of density c .*

- (1) *If $n = 2$ and $c > 3/4$, then $\rho \simeq \rho'$.*
- (2) *If $n = 3$ and $c > 5/7$, then $\rho \simeq \rho'$.*

When $n = 2$, if ρ and ρ' are automorphic, i.e., satisfy the strong Artin conjecture, then the above result already follows by [Wal14]. When $n = 2$, the strong Artin conjecture for ρ is known in many cases—for instance, if ρ has solvable image from Langlands [Lan80] and Tunnell [Tun81], or if $F = \mathbb{Q}$ and ρ is “odd” via Serre's conjecture from Khare–Wintenberger [KW09]. We remark that the methods of [Wal14] are quite different than ours here.

The above corollary suggests the following statement may be true: if π, π' are cuspidal automorphic representations of $\text{GL}_3(\mathbb{A}_F)$ which are not induced from characters and if $L(s, \pi_v) = L(s, \pi'_v)$ for a set of primes v of density $> 5/7$, then $\pi \simeq \pi'$. Since not all cuspidal π, π' come from Artin representations, the $5/7$ bound is not even conjecturally sufficient for general π, π' . However, it seems reasonable to think that coincidences of a large fraction of Euler factors only happen for essentially algebraic reasons, so the density bounds are likely to be the same in both the Artin and the automorphic cases.

2. Notation and background. Throughout, G, H and A will denote finite groups, and A will be abelian. Denote by $Z(G)$ the center of G .

If G and N are groups, by a (group) *extension* of G by N we mean a group H with a normal subgroup N such that $H/N \simeq G$. The extension is called *central* or *cyclic* if N is a central or cyclic subgroup of H .

If G, H , and Z are groups such that $Z \subset Z(G) \cap Z(H)$, then the central product $G \times_Z H$ of G and H with respect to Z is defined to be the direct product $G \times H$ modulo the central subgroup $\{(z, z) : z \in Z\}$.

If χ_1, χ_2 are characters of G , their inner product is

$$(\chi_1, \chi_2) = |G|^{-1} \sum_G \chi_1(g) \overline{\chi_2(g)}.$$

We denote a cyclic group of order m by C_m .

2.1. Finite subgroups of $GL_n(\mathbb{C})$. Next we recall some definitions and facts about finite subgroups of $GL_n(\mathbb{C})$.

Let G be a finite subgroup of $GL_n(\mathbb{C})$, so one has the standard representation of G on $V = \mathbb{C}^n$. We say G is *reducible* if there exists a nonzero proper subspace $W \subset V$ which is fixed by G .

Suppose G is irreducible. Schur’s lemma implies that $Z(G) \subset Z(GL_n(\mathbb{C}))$. In particular, $Z(G)$ is cyclic. If there exists a nontrivial decomposition $V = W_1 \oplus \cdots \oplus W_k$ such that G acts transitively on the W_j , then we say G is *imprimitive*. In this case, each W_j has the same dimension, and the standard representation is induced from a representation on W_1 . Otherwise, call G *primitive*.

Let $A \mapsto \bar{A}$ denote the quotient map from $GL_n(\mathbb{C})$ to $PGL_n(\mathbb{C})$. Similarly, if $G \subset GL_n(\mathbb{C})$, let \bar{G} be the image of G under this map. We call the projective image \bar{G} *irreducible* or *primitive* if G is. Finite subgroups of $PGL_n(\mathbb{C})$ have been classified for small n , and we can use this to describe the finite subgroups of $GL_n(\mathbb{C})$.

Namely, suppose $G \subset GL_n(\mathbb{C})$ is irreducible. Then $Z(G)$ is a cyclic subgroup of scalar matrices, and $\bar{G} = G/Z(G)$. Hence the irreducible finite subgroups of $GL_n(\mathbb{C})$, up to isomorphism, are a subset of the set of finite cyclic central extensions of the irreducible subgroups \bar{G} of $PGL_n(\mathbb{C})$.

Let H be an irreducible subgroup of $PGL_n(\mathbb{C})$. Given one cyclic central extension G of H which embeds (irreducibly) in $GL_n(\mathbb{C})$, note that the central product $G \times_{Z(G)} C_m$ also does for any cyclic group $C_m \supset Z(G)$, and has the same projective image as G . (Inside $GL_n(\mathbb{C})$, this central product just corresponds to adjoining more scalar matrices to G .) Conversely, if $G \times_{Z(G)} C_m$ is an irreducible subgroup of $GL_n(\mathbb{C})$, so is G . We say G is a *minimal lift* of H to $GL_n(\mathbb{C})$ if G is an irreducible subgroup of $GL_n(\mathbb{C})$ with $\bar{G} \simeq H$ such that G is not isomorphic to $G_0 \times_{Z(G_0)} C_m$ for any proper subgroup G_0 of G .

2.2. Serre’s construction. Here we explain the proof of Proposition 1.1 and describe Serre’s construction.

Suppose χ_1 and χ_2 are two distinct irreducible degree n characters of a finite group G . Let Y be the set of elements of G such that $\chi_1(g) \neq \chi_2(g)$. Then

$$|G|((\chi_1, \chi_1) - (\chi_1, \chi_2)) = \sum_Y \chi_1(g)(\overline{\chi_1(g)} - \overline{\chi_2(g)}).$$

Using the bound $|\chi_i(g)| \leq n$ for $i = 1, 2$ and orthogonality relations, we get

$$|G| = |G|((\chi_1, \chi_1) - (\chi_1, \chi_2)) \leq 2n^2|Y|.$$

This proves Proposition 1.1.

We now recall Serre's construction proving Theorem 1.2, which is briefly described in [Ram94b] using observations from [Ser81, Sec. 6.5].

Let H be an irreducible subgroup of $\mathrm{GL}_n(\mathbb{C})$, containing ζI for each n th root of unity ζ , such that \bar{H} has order n^2 . This means that H is of "central type" with cyclic center. Such H exist for all n . For instance, one can take $\bar{H} = A \times A$, where A is an abelian group of order n . Some nonabelian examples of such \bar{H} were given by Iwahori and Matsumoto [IM64, Sec. 5]. They conjectured that groups of central type are necessarily solvable, and this was proved using the classification of finite simple groups by Howlett and Isaacs [HI82].

Since $|H| = n^3$ and $|Z(H)| = n$, the identity $\sum |\mathrm{tr} h|^2 = |H|$ implies $\mathrm{tr} h = 0$ for each $h \in H \setminus Z(H)$, i.e., the set of $h \in H$ such that $\mathrm{tr} h = 0$ has cardinality $n^3 - n = (1 - 1/n^2)|H|$.

Let $G = H \times \{\pm 1\}$ and consider the representations of G given by $\rho = \tau \otimes 1$ and $\rho' = \tau \otimes \mathrm{sgn}$, where τ is the standard representation of H and sgn is the nontrivial character of $\{\pm 1\}$. Then $\mathrm{tr} \rho(g) = \mathrm{tr} \rho'(g) = 0$ for $2(n^3 - n) = (1 - 1/n^2)|G|$ elements of G . On the remaining $2n$ elements of $Z(G)$, $\mathrm{tr} \rho$ and $\mathrm{tr} \rho'$ must differ on precisely n elements, giving G with $\delta_n(G) = 1/(2n^2)$ as desired.

Finally, we show that ρ and ρ' so constructed are induced for $n > 1$. It suffices to show τ is induced. Since \bar{H} is solvable, there is a subgroup of prime index p , so there exists a subgroup K of H of index p which contains $Z = Z(H)$. Set $\chi = \mathrm{tr} \tau$. Now $\sum_K |\chi(k)|^2 = \sum_Z |\chi(k)|^2 = |H|$. On the other hand $\sum_K |\chi(k)|^2 \leq \sum_{i=1}^r \sum_K |\psi_i(k)|^2 = r|K|$, where $\chi|_K = \psi_1 + \cdots + \psi_r$ is the decomposition of $\chi|_K$ into irreducible characters of K . Thus $r \geq p$ and we must have equality, which means τ is induced from a ψ_i . We note that, more generally, Christina Durfee informed us of a proof that ρ, ρ' must be induced if $\delta(\rho, \rho') = 1/(2n^2)$.

3. General methods

3.1. Central extensions and minimal lifts. The first step in the proof of Theorem 1.3 is the determination of the minimal lifts of irreducible finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ and $\mathrm{PGL}_3(\mathbb{C})$. Here we explain our method for this.

Let G be a group and A an additive abelian group, which we view as a G -module with trivial action. Then a short exact sequence of groups

$$(3.1) \quad 0 \rightarrow A \xrightarrow{\iota} H \xrightarrow{\pi} G \rightarrow 1,$$

where ι and π are homomorphisms, such that $\iota(A) \subset Z(H)$ gives a central extension H of G by A . Let $M(G, A)$ be the set of such sequences. (Note these sequences are often called central extensions, but for our purpose it makes sense to call the middle term H the central extension.) We say two

sequences in $M(G, A)$ are *equivalent* if there is a map ϕ that makes this diagram commute:

$$(3.2) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & H & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \parallel & & \downarrow \phi & & \parallel & & \\ 0 & \longrightarrow & A & \xrightarrow{\iota'} & H' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

Let $\tilde{M}(G, A)$ be $M(G, A)$ modulo equivalence.

If two sequences in $M(G, A)$ as above are equivalent, then $H \simeq H'$. However, the converse is not true. For instance, if we take $G \simeq A \simeq C_p$, then $|\tilde{M}(G, A)| = p$ but there are only two isomorphism classes of central extensions of C_p by itself, namely the two abelian groups of order p^2 .

Let $\text{Cent}(G, A)$ be the set of isomorphism classes of central extensions of G by A . Then the above discussion shows we have a surjective but not necessarily injective map $\Phi : \tilde{M}(G, A) \rightarrow \text{Cent}(G, A)$ induced from sending a sequence as in (3.1) to the isomorphism class of H .

Viewing A as a trivial G -module, we have a bijection between $\tilde{M}(G, A)$ and $H^2(G, A)$, with the class $0 \in H^2(G, A)$ corresponding to all split sequences in $M(G, A)$. We can use this to help determine minimal lifts of irreducible subgroups of $\text{PGL}_n(\mathbb{C})$. We recall $H_1(G, \mathbb{Z})$ is the abelianization of G , and $H_2(G, \mathbb{Z})$ is the Schur multiplier of G .

PROPOSITION 3.1. *Let G be an irreducible subgroup of $\text{PGL}_n(\mathbb{C})$. Then any minimal lift of G to $\text{GL}_n(\mathbb{C})$ is a central extension of G by C_m for some divisor m of the exponent of $H_1(G, \mathbb{Z}) \times H_2(G, \mathbb{Z})$.*

Proof. Any lift of G to an irreducible subgroup $H \subset \text{GL}_n(\mathbb{C})$ corresponds to an element of $\text{Cent}(G, A)$ where $A = C_m$ for some m , and thus corresponds to at least one element of $H^2(G, A)$. The universal coefficients theorem gives us the exact sequence

$$(3.3) \quad 0 \rightarrow \text{Ext}(H_1(G, \mathbb{Z}), A) \rightarrow H^2(G, A) \rightarrow \text{Hom}(H_2(G, \mathbb{Z}), A) \rightarrow 0.$$

Let m' be the gcd of m with the exponent of $H_1(G, \mathbb{Z}) \times H_2(G, \mathbb{Z})$. Recall that $\text{Ext}(\bigoplus \mathbb{Z}/n_i\mathbb{Z}, A) = \bigoplus A/n_iA$, so $\text{Ext}(H_1(G, \mathbb{Z}), C_m) = \text{Ext}(H_1(G, \mathbb{Z}), C_{m'})$. An analogous statement is true for $\text{Hom}(H_2(G, \mathbb{Z}), -)$, so $|H^2(G, C_m)| = |H^2(G, C_{m'})|$.

Assume $m \neq m'$. Consider a sequence as in (3.1) with $A = C_{m'}$. This gives a sequence

$$0 \rightarrow C_m \rightarrow H \times_{C_{m'}} C_m \rightarrow G \rightarrow 1$$

in $M(G, C_m)$ by extending $\iota : C_{m'} \rightarrow H$ to be the identity on C_m . Note that if one has an equivalence ϕ of two sequences in $M(G, C_m)$ constructed in this way, then commutativity implies $\phi(H) = H$, so restricting the isomorphism ϕ on the middle groups to H yields an equivalence of the corresponding

sequences in $M(G, C_{m'})$. Hence all elements of $\tilde{M}(G, C_m)$ arise from “central products” of sequences in $M(G, C_{m'})$, and thus no elements of $\text{Cent}(G, C_m)$ can be minimal lifts. ■

When $H_1(G, \mathbb{Z}) \times H_2(G, \mathbb{Z}) \simeq 1$, then $H^2(G, A) = 0$ for any abelian group A , which means all central extensions are split, i.e., $\text{Cent}(G, A) = \{G \times A\}$ for any A . When $H_1(G, \mathbb{Z}) \times H_2(G, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$, then (3.3) tells us that $|H^2(G, C_m)|$ has size 1 or 2 according to whether m is odd or even, so there must be a unique nonsplit extension $\tilde{G} \in \text{Cent}(G, C_2)$. Then the argument in the proof tells us that any cyclic central extension of G is a central product of either G or \tilde{G} with a cyclic group.

However, in general, knowing $H_1(G, \mathbb{Z})$ and $H_2(G, \mathbb{Z})$ is not enough to determine the size of $\text{Cent}(G, C_m)$. When $|\text{Cent}(G, C_m)| < |H^2(G, C_m)|$, we will sometimes need a way to verify that the central extensions of G by C_m we exhibit exhaust all of $\text{Cent}(G, C_m)$. For this, we will use a lower bound on the size of the fibers of Φ , i.e., a lower bound on the number of classes in $\tilde{M}(G, A)$ a given central extension $H \in \text{Cent}(G, A)$ appears in.

The *central automorphisms* of a group H with center Z , denoted $\text{Aut}_Z(H)$, are the automorphisms σ of H which commute with the projection $H \rightarrow H/Z$, i.e., satisfy $\sigma(h)h^{-1} \in Z$ for all $h \in H$.

PROPOSITION 3.2. *Let A be abelian and $H \in \text{Cent}(G, A)$ be such that $A = Z := Z(H)$. Then $|\Phi^{-1}(H)| \geq |\text{Aut}(Z)|/|\text{Aut}_Z(H)|$. Moreover, if H is perfect, then $|\Phi^{-1}(H)| \geq |\text{Aut}(Z)|$.*

Recall H being *perfect* means H equals its derived group, i.e., $H_1(H, \mathbb{Z}) = 0$. In particular, nonabelian simple groups are perfect. By (3.3), central extensions of perfect groups are simpler to study. In fact, a perfect group H has a universal central extension by $H_2(H, \mathbb{Z})$.

Proof of Proposition 3.2. Consider a commuting diagram of sequences as in (3.2) with $H' = H$. Suppose $\pi = \pi'$, which forces $\phi \in \text{Aut}_Z(H)$ and $\iota'(A) = \ker \pi = \iota(A)$. If we fix π and ι , there are $|\text{Aut}(Z)|$ choices for ι' , which gives $|\text{Aut}(Z)|$ elements of $M(G, A)$. Each different ι' must induce a different central automorphism $\phi \in \text{Aut}_Z(H)$. Thus at most $|\text{Aut}_Z(H)|$ of these $|\text{Aut}(Z)|$ bottom sequences can lie in the same equivalence class, which proves the first statement.

Adney and Yen [AY65] showed $|\text{Aut}_Z(H)| = |\text{Hom}(H, Z)|$ when H has no abelian direct factor. Consequently, $\text{Aut}_Z(H) = 1$ when H is perfect. ■

3.2. Reduction to minimal lifts. Let G be a finite group and ρ_1, ρ_2 be two inequivalent irreducible representations of G into $\text{GL}_n(\mathbb{C})$. Let $N_i = \ker \rho_i$ and $G_i = \rho_i(G)$ for $i = 1, 2$. We want to reduce the problem of finding lower bounds for $\delta(\rho_1, \rho_2)$ to the case where G_1 and G_2 are minimal lifts of \tilde{G}_1 and \tilde{G}_2 . Note that $\delta(\rho_1, \rho_2)$ is unchanged if we factor through the

common kernel $N_1 \cap N_2$, so we may assume $N_1 \cap N_2 = 1$. Then $N_1 \times N_2$ is a normal subgroup of G , $N_1 \simeq \rho_2(N_1) \triangleleft G_2$ and $N_2 \simeq \rho_1(N_2) \triangleleft G_1$.

Write $G_i = H_i \times_{Z(H_i)} Z_i$ for $i = 1, 2$, where H_i is a minimal lift of \bar{G}_i to $\text{GL}_n(\mathbb{C})$ and Z_i is a cyclic group containing $Z(H_i)$.

For a subgroup H of $\text{GL}_n(\mathbb{C})$, define $\alpha_n(H)$ to be the minimum of $|\{h \in H : \text{tr } h \neq 0\}|/|H|$ as one ranges over all embeddings (i.e., faithful n -dimensional representations) of H in $\text{GL}_n(\mathbb{C})$.

LEMMA 3.3. *Let $m = |\rho_1(N_2) \cap Z(G_1)|$. Then*

$$\delta(\rho_1, \rho_2) \geq \frac{m-1}{m} \alpha_n(H_1).$$

Proof. Let $K = N_2 \cap \rho_1^{-1}(Z(G_1))$, so $\rho_1(K)$ is a cyclic subgroup of $Z(G_1)$ of order m and $\rho_2(K) = 1$. Fix any $g \in G$. Then as k ranges over K , $\text{tr } \rho_1(gk)$ ranges over the values $\zeta \text{tr } \rho(g)$, where ζ runs through all m th roots of 1 in \mathbb{C} , attaining each value equally often. On the other hand, $\text{tr } \rho_2(gk) = \text{tr } \rho_2(g)$ for all $k \in K$. So provided $\text{tr } \rho_1(g) \neq 0$, $\text{tr } \rho_1$ and $\text{tr } \rho_2$ can agree on at most $\frac{1}{m}|K|$ values on the coset gK . Then note that the fraction of elements $g \in G$ for which $\text{tr } \rho_1(g) \neq 0$ is the same as the fraction of elements in $h \in H_1$ for which $\text{tr } h \neq 0$. ■

We say a subgroup H_0 of a group H is $Z(H)$ -free if $H_0 \neq 1$ and $H_0 \cap Z(H) = 1$. The above lemma implies that if G_1 has no $Z(G_1)$ -free normal subgroups, then $\delta(\rho_1, \rho_2) \geq \alpha_n(H_1)/2$ or $N_2 = 1$ (as the K in the proof must be nontrivial). This will often allow us to reduce to the case where $N_2 = 1$, and similarly $N_1 = 1$, i.e., $G = G_1 = G_2$, when we can check this property for G_1 and G_2 . The following allows us to simply check it for H_1 and H_2 .

LEMMA 3.4. *If H_1 has no $Z(H_1)$ -free normal subgroups, then G_1 has no $Z(G_1)$ -free normal subgroups.*

Proof. Suppose H_1 has no $Z(H_1)$ -free normal subgroups, but that N is a $Z(G_1)$ -free normal subgroup of G_1 . Let $N' = \{n \in H_1 : (n, z) \in G_1 = H_1 \times_{Z(H_1)} Z_1 \text{ for some } z \in Z_1\}$. Then $N' \triangleleft H_1$. If $N' = 1$, then $N \subset Z_1 = Z(G_1)$, contradicting N being $Z(G_1)$ -free. Hence $N' \neq 1$ and must contain a nontrivial $a \in Z(H_1)$. But then $(a, z) \in N \cap Z(G_1)$ for some $z \in Z_1$, which also contradicts N being $Z(G_1)$ -free. ■

This will often allow us to reduce to the case where $G = H \times_{Z(H)} A$ for some cyclic group $A \supset Z(H)$, where we can use the following.

LEMMA 3.5. *Let H be a finite group, $A \supset Z(H)$ an abelian group and $G = H \times_{Z(H)} A$. Then $\delta_n^{\natural}(G) \geq \min\{\frac{1}{2}\alpha_n(H), \delta_n^{\natural}(H)\}$.*

Proof. We may assume $m = |A| > 1$. Let $\rho_1, \rho_2 : G \rightarrow \text{GL}_n(\mathbb{C})$ be distinct primitive representations of G . They pull back to $H \times A$, so for $i = 1, 2$ we can view ρ_i as $\tau_i \otimes \chi_i$ where $\tau_i : H \rightarrow \text{GL}_n(\mathbb{C})$ is primitive

and $\chi_i : A \rightarrow \mathbb{C}^\times$. By a similar argument to the proof of Lemma 3.3, we have $\delta(\rho_1, \rho_2) \geq \frac{m-1}{m} \alpha_n(H)$ if $\chi_1 \neq \chi_2$. If $\chi_1 = \chi_2$, it is easy to see that $\delta(\rho_1, \rho_2) = \delta(\tau_1, \tau_2)$. ■

In the simplest situation, this method gives the following.

COROLLARY 3.6. *Let \mathcal{H} be the set of minimal lifts of \bar{G}_1 and \bar{G}_2 to $\mathrm{GL}_n(\mathbb{C})$. Suppose that no $H \in \mathcal{H}$ has a $Z(H)$ -free normal subgroup. Then*

$$\delta(\rho_1, \rho_2) \geq \min\left\{\frac{1}{2}\alpha_n(H), \delta_n^{\natural}(H) : H \in \mathcal{H}\right\}.$$

This corollary will address most but not all cases of our proof of Theorem 1.3. Namely, when $n = 3$, it can happen that \bar{G}_1 has a lift $H \simeq \bar{G}_1$ which is simple, so H is a $Z(H)$ -free normal subgroup of itself. Therefore we will need to augment this approach when H_1 or H_2 is simple.

4. Primitive degree 2 characters. In this section we will prove the $n = 2$ case of Theorem 1.3.

We used the computer package GAP 4 [GG16] for explicit group and character calculations in this section and the next. We use the notation $[n, m]$ for the m th group of order n in the Small Groups Library, which is accessible by the command `SmallGroup(n,m)` in GAP. We can enumerate all (central or not) extensions of G by N in GAP if $|G||N| \leq 2000$ and $|G||N| \neq 1024$ as all groups of these orders are in the Small Groups Library. We can also compute homology groups $H_n(G, \mathbb{Z})$ using the HAP package in GAP.

4.1. Finite subgroups of $\mathrm{GL}_2(\mathbb{C})$. Recall the classification of finite subgroups of $\mathrm{PGL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$. Any finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ is of one of the following types:

- (A) cyclic,
- (B) dihedral,
- (C) tetrahedral ($A_4 \simeq \mathrm{PSL}(2, 3)$),
- (D) octahedral (S_4),
- (E) icosahedral ($A_5 \simeq \mathrm{PSL}(2, 5) \simeq \mathrm{PSL}(2, 4) \simeq \mathrm{SL}(2, 4)$).

Now suppose G is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ with projective image \bar{G} in $\mathrm{PGL}_2(\mathbb{C})$. If \bar{G} is cyclic, then G is reducible. If \bar{G} is dihedral, then G is not primitive.

Assume \bar{G} is primitive. Then we have the following possibilities.

(C) Suppose $\bar{G} = A_4 \simeq \mathrm{PSL}(2, 3)$. In this case $H_1(A_4, \mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$ and $H_2(A_4, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. There is one nonsplit element of $\mathrm{Cent}(A_4, C_2)$, namely $\mathrm{SL}(2, 3)$; one nonsplit element of $\mathrm{Cent}(A_4, C_3)$, namely $[36, 3]$; and one element of $\mathrm{Cent}(A_4, C_6)$ which is not a central product with a smaller extension, namely $[72, 3]$. Of these central extensions (and the trivial extension A_4),

only $SL(2, 3)$ and $[72, 3]$ have irreducible faithful 2-dimensional representations.

Thus $SL(2, 3)$ and $[72, 3]$ are the only minimal lifts of A_4 to $GL_2(\mathbb{C})$. We check that neither $H = SL(2, 3)$ nor $H = [72, 3]$ has $Z(H)$ -free normal subgroups. In both cases, we have $\alpha_2(H) = 3/4$ and $\delta_2^{\natural}(H) = 2/3$.

(D) Next suppose $\bar{G} = S_4$. Note $H_1(S_4, \mathbb{Z}) \simeq H_2(S_4, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. There are three nonsplit central extensions of S_4 by C_2 : $[48, 28]$, $[48, 29]$, $[48, 30]$. Neither S_4 nor $[48, 30]$ has faithful irreducible 2-dimensional representations, but both $[48, 28]$ and $[48, 29]$ do.

Thus $H = [48, 28]$ and $H = [48, 29]$ are the minimal lifts of S_4 to $GL_2(\mathbb{C})$. Neither of them has $Z(H)$ -free normal subgroups. In both cases we compute $\alpha_2(H) = 5/8$ and $\delta_2^{\natural}(H) = 1/4$.

(E) Last, suppose $\bar{G} = A_5 = PSL(2, 5)$. This group is perfect and we have $H_2(A_5, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$, with $SL(2, 5)$ being the nontrivial central extension by C_2 (the universal central extension). Note that A_5 has no irreducible 2-dimensional representations.

Hence there is only one minimal lift of A_5 to $GL_2(\mathbb{C})$, $H = SL(2, 5)$. We can check that $SL(2, 5)$ has no $Z(SL(2, 5))$ -free normal subgroups, $\alpha_2(SL(2, 5)) = 3/4$ and $\delta_2^{\natural}(SL(2, 5)) = 2/5$ (cf. Theorem 1.4).

4.2. Comparing characters. Let $\rho_1, \rho_2 : G \rightarrow GL_2(\mathbb{C})$ be inequivalent primitive representations. By Corollary 3.6,

$$\delta(\rho_1, \rho_2) \geq \min \left(\frac{1}{2} \left\{ \frac{3}{4}, \frac{5}{8}, \frac{3}{4} \right\} \cup \left\{ \frac{2}{3}, \frac{1}{4}, \frac{2}{5} \right\} \right) = \frac{1}{4}.$$

This shows $\delta_2^{\natural} \geq 1/4$. Furthermore, we can only have $\delta(\rho_1, \rho_2) = 1/4$ if \bar{G}_1 or \bar{G}_2 is S_4 , which implies G_1 or G_2 is of the form $H \times_{C_2} C_{2m}$ for some m with $H = [48, 28]$ or $H = [48, 29]$. Thus we can only have $\delta_2^{\natural}(G) = 1/4$ if G is an extension of $H \times_{C_2} C_{2m}$ where $m \in \mathbb{N}$ and $H = [48, 28]$ or $H = [48, 29]$. Moreover, if G is such an extension, then $\delta_2^{\natural}(G)$ equals $1/4$ because $\delta_2^{\natural}(H)$ does.

This completes the proof of Theorem 1.3 when $n = 2$.

5. Primitive degree 3 characters. Here we prove the $n = 3$ case of Theorem 1.3.

5.1. Finite subgroups of $GL_3(\mathbb{C})$. First we review the classification of finite subgroups of $GL_3(\mathbb{C})$. The classification can be found in Blichfeldt [Bli17] or Miller–Blichfeldt–Dickson [MBD61]. We follow the classification system therein. The description involves three not-well-known groups, $G_{36} = [36, 9]$, $G_{72} = [72, 41]$, and $G_{216} = [216, 153]$. Explicit matrix presentations for preimages in $GL_3(\mathbb{C})$ are given in [Mar04, Sec. 8.1].

Any finite subgroup G of $\mathrm{GL}_3(\mathbb{C})$ with projective image \bar{G} is of one of the following types, up to conjugacy:

- (A) abelian,
- (B) a nonabelian subgroup of $\mathrm{GL}_1(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$,
- (C) a group generated by a diagonal subgroup and $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$,
- (D) a group generated by a diagonal subgroup, $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ and a matrix of the form $\begin{pmatrix} a & \\ & c \ b \end{pmatrix}$,
- (E) $\bar{G} \simeq G_{36}$,
- (F) $\bar{G} \simeq G_{72}$,
- (G) $\bar{G} \simeq G_{216}$,
- (H) $\bar{G} \simeq A_5 \simeq \mathrm{PSL}(2, 5) \simeq \mathrm{PSL}(2, 4) \simeq \mathrm{SL}(2, 4)$,
- (I) $\bar{G} \simeq A_6 \simeq \mathrm{PSL}(2, 9)$,
- (J) $\bar{G} \simeq \mathrm{PSL}(2, 7)$.

Of these types, (A), (B) are reducible, (C), (D) are imprimitive, and the remaining types are primitive. The first three primitive groups, (E), (F) and (G), have nonsimple projective images, whereas the latter three, (H), (I) and (J), have simple projective images.

Now we describe the minimal lifts to $\mathrm{GL}_3(\mathbb{C})$ of \bar{G} for cases (E)–(J).

(E) We have $H_1(G_{36}, \mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z}$ and $H_2(G_{36}, \mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$. The nonsplit extension of G_{36} by C_2 is [72, 19]. There is one nonsplit extension of G_{36} by C_4 which is not a central product, [144, 51]. However, G_{36} , [72, 19] and [144, 51] all have no irreducible 3-dimensional representations.

There is one nonsplit central extension of G_{36} by C_3 , [108, 15]; there is one by C_6 which is not a central product, [216, 25]; there is one by C_{12} which is not a central product, [432, 57]. All of these groups have faithful irreducible 3-dimensional representations.

Hence any minimal lift of G_{36} to $\mathrm{GL}_3(\mathbb{C})$ is $H = [108, 15]$, $H = [216, 25]$ or $H = [432, 57]$. In all of these cases, H has no $Z(H)$ -free normal subgroups, $\alpha_3(H) = 7/9$ and $\delta_3^{\natural}(H) = 1/2$.

(F) We have $H_1(G_{72}, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $H_2(G_{72}, \mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$. There is a unique nonsplit central extension of G_{36} by C_2 , [144, 120]; a unique central extension of G by C_3 , [216, 88]; and a unique central extension of G by C_6 which is not a central product, [432, 239]. Of these extensions (including G_{72}), only the latter two groups have faithful irreducible 3-dimensional representations.

Thus there are two minimal lifts of G_{72} to $\mathrm{GL}_3(\mathbb{C})$, $H = [216, 88]$ and $H = [432, 239]$. In both cases, H has no $Z(H)$ -free normal subgroups, $\alpha_3(H) = 8/9$ and $\delta_3^{\natural}(H) = 1/2$.

(G) We have $H_1(G_{216}, \mathbb{Z}) \simeq H_2(G_{216}, \mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$. There are four nonsplit central extensions of G_{216} by C_3 : [648, 531], [648, 532], [648, 533], and [648, 534]. Neither G_{216} nor [648, 534] has irreducible faithful 3-dimensional representations.

Thus there are three minimal lifts of G_{216} to $\mathrm{GL}_3(\mathbb{C})$, $H = [648, 531]$, $H = [648, 532]$, and $H = [648, 533]$. In all cases H has no $Z(H)$ -free normal subgroups, $\alpha_3(H) = 20/27$ and $\delta_3^{\natural}(H) = 4/9$.

(H) As mentioned in the $n = 2$ case, $A_5 \simeq \mathrm{PSL}(2, 5)$ is perfect and we have $H_2(A_5, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. The nontrivial extension by C_2 (the universal central extension) is $\mathrm{SL}(2, 5)$, but $\mathrm{SL}(2, 5)$ has no faithful irreducible 3-dimensional representations.

Thus the only minimal lift of A_5 to $\mathrm{GL}_3(\mathbb{C})$ is A_5 itself. We have $\alpha_3(A_5) = 2/3$ and $\delta_3^{\natural}(A_5) = \delta_3^{\natural}(\mathrm{PSL}(2, 5)) = 2/5$ (cf. Theorem 1.4).

(I) The group A_6 is also perfect, but (along with A_7) exceptional among alternating groups in that $H_2(A_6, \mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}$. Neither $A_6 \simeq \mathrm{PSL}(2, 9)$ nor its double cover $\mathrm{SL}(2, 9)$ has irreducible 3-dimensional representations. There is a unique nonsplit central extension of A_6 by C_3 , sometimes called the Valentiner group, which we denote $V_{1080} = [1080, 260]$ and it is also a perfect group. It is known (from Valentiner) that V_{1080} has an irreducible faithful 3-dimensional representation.

To complete the determination of minimal lifts of A_6 to $\mathrm{GL}_3(\mathbb{C})$, we need to determine the central extensions of A_6 by C_6 . Here we cannot (easily) proceed naively as in the other cases by testing all groups of the appropriate order because we do not have a library of all groups of order 2160. We have $|\tilde{M}(A_6, C_6)| = 6$, with one class accounted for by the split extension and one by $\mathrm{SL}(2, 9) \times_{C_2} C_6$. Since V_{1080} must correspond to two classes in $\tilde{M}(A_6, C_3)$, $V_{1080} \times_{C_3} C_6$ corresponds to two classes in $\tilde{M}(A_6, C_6)$ by the proof of Proposition 3.1. Since A_6 is perfect, it has a universal central extension by C_6 , which we denote \tilde{A}_6 . By Proposition 3.2, \tilde{A}_6 accounts for the remaining two classes in $\tilde{M}(A_6, C_6)$, and thus we have described all elements of $\mathrm{Cent}(A_6, C_6)$. The group \tilde{A}_6 is the unique perfect group of order 2160 and can be accessed by the command `PerfectGroup(2160)` in GAP, and we can check that it has no faithful irreducible 3-dimensional representations.

Hence V_{1080} is the unique minimal lift of A_6 to $\mathrm{GL}_3(\mathbb{C})$. We note $H = V_{1080}$ has no $Z(H)$ -free normal subgroups, $\alpha_3(H) = 7/9$, and $\delta_3^{\natural}(H) = 2/5$.

(J) The group $\mathrm{PSL}(2, 7)$ is perfect and $H_2(\mathrm{PSL}(2, 7), \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. Since $\mathrm{SL}(2, 7)$ has no faithful irreducible 3-dimensional representations, any minimal lift of $\mathrm{PSL}(2, 7)$ to $\mathrm{GL}_3(\mathbb{C})$ is just $H = \mathrm{PSL}(2, 7)$. Here $\alpha_3(H) = 2/3$ and $\delta_3^{\natural}(H) = 2/7$ by Theorem 1.4.

5.2. Comparing characters. Let G be a finite group and $\rho_1, \rho_2 : G \rightarrow \text{GL}_3(\mathbb{C})$ be two inequivalent primitive representations. Let G_i, N_i, H_i, Z_i be as in Section 3.2. As before, we may assume $N_1 \cap N_2 = 1$, so G contains a normal subgroup isomorphic to $N_1 \times N_2$ whose image in G_1 is N_2 and image in G_2 is N_1 .

PROPOSITION 5.1. *Suppose at least one of \bar{G}_1 and \bar{G}_2 is simple. Then $\delta(\rho_1, \rho_2) \geq 2/7$, with equality only if $\bar{G}_1 \simeq \bar{G}_2 \simeq \text{PSL}(2, 7)$.*

Proof. Say \bar{G}_1 is simple. Then by the above, H_1 is isomorphic to one of A_5, V_{1080} and $\text{PSL}(2, 7)$.

CASE I: $\bar{G}_1 \not\simeq \bar{G}_2$. For $i = 1, 2$, the fraction of $g \in G$ for which $|\text{tr } \rho_i(g)| = x$ is the same as the fraction of $h \in H_i$ for which $|\text{tr } h| = x$. Calculations show that the proportion of such $g \in G$ (given x) depends neither on the minimal lift H_i nor on its embedding into $\text{GL}_3(\mathbb{C})$, but just on \bar{G}_i . These proportions are given in Table 1.

Table 1. Fraction of group elements with primitive degree 3 characters having given absolute value

\bar{G}	3	1	0	$(1 \pm \sqrt{5})/2$	$\sqrt{2}$	$\sqrt{3}$
G_{36}	1/36	3/4	2/9			
G_{72}	1/72	7/8	1/9			
G_{216}	1/216	5/8	7/27			1/9
A_5	1/60	1/4	1/3	2/5		
A_6	1/360	3/8	2/9	2/5		
$\text{PSL}(2, 7)$	1/168	3/8	1/3		2/7	

If $\bar{G}_1 \simeq \text{PSL}(2, 7)$, we see $\delta(\rho_1, \rho_2) \geq 2/7$ just from considering elements with absolute character value $\sqrt{2}$. Looking at other absolute character values shows this inequality is strict.

If $\bar{G}_1 \simeq A_5$ or A_6 and \bar{G}_2 is not isomorphic to A_5 or A_6 , then considering elements with absolute character value $(1 \pm \sqrt{5})/2$ shows $\delta(\rho_1, \rho_2) \geq 2/5$.

So assume $\bar{G}_1 \simeq A_5$ and $\bar{G}_2 \simeq A_6$. Then $G_1 = A_5 \times C_m$ and $G_2 \simeq V_{1080} \times_{C_3} C_{3r}$ for some $m, r \in \mathbb{N}$. Suppose $\delta(\rho_1, \rho_2) < 1/3$. By Lemma 3.3, $\rho_1(N_2)$ and $\rho_2(N_1)$ are either $Z(G_1)$ - and $Z(G_2)$ -free normal subgroups of G_1 and G_2 or trivial. This forces $N_1 = 1$, so $G \simeq G_1$, but a quotient of G_1 cannot be isomorphic to G_2 . Hence $\delta(\rho_1, \rho_2) \geq 1/3 > 2/7$ in this case.

CASE II: $\bar{G}_1 \simeq \bar{G}_2$. First suppose N_1 or N_2 is trivial, say N_1 . Then $G \simeq G_1$. By Lemma 3.5, we have $\delta_3^{\natural}(G) \geq \min\{1/3, \delta_3^{\natural}(H_1)\}$. Thus $\delta_3^{\natural}(G) = 2/7$ if and only if $H_1 = \text{PSL}(2, 7)$.

So assume N_1 and N_2 are nontrivial. By Lemma 3.3, we can assume $\rho_1(N_2)$ and $\rho(N_1)$ are $Z(G_1)$ - and $Z(G_2)$ -free normal subgroups of G_1 and G_2 . This is only possible if $N_1 \simeq N_2 \simeq H_1 \simeq H_2$ is isomorphic to A_5 or $\text{PSL}(2, 7)$.

Let $N = \rho_1^{-1}(N_2) \triangleleft G$ and identify $N = N_1 \times N_2$. Fix $g \in G$. Then for any $n_1 \in N_1$, $\text{tr } \rho_1(g(n_1, 1)) = \text{tr } \rho_1(g)$ but $\text{tr } \rho_2(g(n_1, 1)) = \text{tr } \rho_2(g(n_1, 1))$. Since $\rho_2(g(N_1 \times 1)) = H_2 \times \{z\}$ for some $z \in Z_2$, the fraction of elements of $g(N_1 \times 1)$ (and thus of G) on which $\text{tr } \rho_1$ and $\text{tr } \rho_2$ can agree is at most the maximal fraction of elements of H_1 with a given trace. By Table 1 this is less than $1/2$ for either $\bar{G}_1 \simeq A_5$ or $\bar{G}_1 \simeq \text{PSL}(2, 7)$. ■

To complete the proof of Theorem 1.3 for $n = 3$, it suffices to show $\delta(\rho_1, \rho_2) > 2/7$ when \bar{G}_1 and \bar{G}_2 are each one of G_{36} , G_{72} and G_{216} . Using Corollary 3.6, in this situation we see that

$$\delta(\rho_1, \rho_2) \geq \min\left(\frac{1}{2}\left\{\frac{7}{9}, \frac{8}{9}, \frac{20}{27}\right\} \cup \left\{\frac{1}{2}, \frac{1}{2}, \frac{4}{9}\right\}\right) = \frac{10}{27}.$$

This finishes Theorem 1.3.

6. Families $\text{SL}(2, q)$ and $\text{PSL}(2, q)$. We consider $\text{SL}(2, q)$ and $\text{PSL}(2, q)$ for even and odd prime powers q . We separate these into three subsections: $\text{SL}(2, q)$, q odd; $\text{SL}(2, q) \simeq \text{PSL}(2, q)$, q even; and $\text{PSL}(2, q)$, q odd. We refer to, and mostly follow the notation of, Fulton–Harris [FH91] for the representations of these groups.

Choose an element $\Delta \in \mathbb{F}_q^\times - (\mathbb{F}_q^\times)^2$. Denote by $\mathbb{E} := \mathbb{F}_q(\sqrt{\Delta})$ the unique quadratic extension of \mathbb{F}_q . We can write the elements of \mathbb{E} as $a + b\delta$, where $\delta := \sqrt{\Delta}$. The norm map $N : \mathbb{E}^\times \rightarrow \mathbb{F}_q^\times$ is then defined as $N(a + b\delta) = a^2 - b^2\Delta$. We also use \mathbb{E}^1 to mean the kernel of the norm map.

6.1. $\text{SL}(2, q)$ for odd q . The order of $\text{SL}(2, q)$ is $(q + 1)q(q - 1)$. We begin by describing the conjugacy classes for $\text{SL}(2, q)$:

- (A) I .
- (B) $-I$.
- (C) Conjugacy classes of the form $[c_2(\epsilon, \gamma)]$, where $c_2(\epsilon, \gamma) = \begin{pmatrix} \epsilon & \gamma \\ & \epsilon \end{pmatrix}$ with $\epsilon = \pm 1$ and $\gamma = 1$ or Δ . So there are four conjugacy classes, each of size $(q^2 - 1)/2$.
- (D) Conjugacy classes of the form $[c_3(x)]$, where $c_3(x) = \begin{pmatrix} x & & \\ & x^{-1} & \\ & & 1 \end{pmatrix}$ with $x \neq \pm 1$. Since the conjugacy classes $c_3(x)$ and $c_3(x^{-1})$ are the same, we have $(q - 3)/2$ different conjugacy classes, each of size $q(q + 1)$.
- (E) Conjugacy classes of the form $[c_4(z)]$, where $c_4(z) = \begin{pmatrix} x & \Delta y \\ & y & \\ & & x \end{pmatrix}$ with $z = x + \delta y \in \mathbb{E}^1$ and $z \neq \pm 1$. Since $c_4(z) = c_4(\bar{z})$, we have $(q - 1)/2$ conjugacy classes, each of size $q(q - 1)$.

We give a brief description of the representations that appear in the character table. The first set of representations, denoted W_α , are induced from

the subgroup B of upper triangular matrices. Given a character $\alpha \in \widehat{\mathbb{F}_q^\times}$, we can extend this to a character of B , which we then induce to a $(q + 1)$ -dimensional representation W_α of $\mathrm{SL}_2(\mathbb{F}_q)$. If $\alpha^2 \neq 1$, then the induced representation is irreducible. If $\alpha = 1$, then W_1 decomposes into its irreducible constituents: the trivial representation U and the Steinberg representation V . If $\alpha^2 = 1$ and $\alpha \neq 1$, then it decomposes into two irreducible constituents denoted W^+ and W^- .

For the remaining irreducible representations, we consider characters α and φ of the diagonal subgroup A and the subgroup $S := \{c_4(z) : z \in \mathbb{E}^1\}$, respectively, where the characters agree when restricted to $A \cap S$. Then we construct a virtual character $\pi_\varphi := \mathrm{Ind}_A^G(\alpha) - W_\alpha - \mathrm{Ind}_S^G(\varphi)$ (note that the virtual character will not depend on the specific choice of α).

When $\varphi = \overline{\varphi}$, π_φ decomposes into two distinct characters. In the case when φ is trivial, π_1 decomposes into the difference between the characters for the Steinberg representation and the trivial representation. If φ is the unique (nontrivial) order 2 character of S , then π_φ decomposes into two distinct irreducible characters of equal dimension; we will label the corresponding representations X^+ and X^- . If $\varphi \neq \overline{\varphi}$, then π_φ corresponds to an irreducible representation, which we denote as X_φ . Two irreducibles X_φ and $X_{\varphi'}$ are equivalent if and only if $\varphi = \varphi'$ or $\varphi = \overline{\varphi'}$. We note that out of all the irreducible representations, the imprimitive representations are exactly all the W_α (for $\alpha^2 \neq 1$).

We define some notation that will appear in the character table for $\mathrm{SL}(2, q)$. Let $\alpha \in \widehat{\mathbb{F}_q^\times}$ with $\alpha \neq \pm 1$, and φ a character of \mathbb{E}^1 with $\varphi^2 \neq 1$. Fix τ to be the nontrivial element of $\widehat{\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2}$, and let

$$s^\pm(\epsilon, \gamma) = \frac{1}{2}(\tau(\epsilon) \pm \tau(\epsilon\gamma)\sqrt{\tau(-1)q}),$$

$$u^\pm(\epsilon, \gamma) = \frac{1}{2}\epsilon(-\tau(\epsilon) \pm \tau(\epsilon\gamma)\sqrt{\tau(-1)q}).$$

Lastly, we define ψ to be the nontrivial element of $\widehat{\mathbb{E}^1 / (\mathbb{E}^1)^2}$. The character table is:

		$[I]$	$[-I]$	$[c_2(\epsilon, \gamma)]$	$[c_3(x)]$	$[c_4(z)]$
Size:		1	1	$(q^2 - 1)/2$	$q(q + 1)$	$q(q - 1)$
Rep	#					
U	1	1	1	1	1	1
X^\pm	2	$(q - 1)/2$	$\frac{1}{2}(q - 1)\psi(-1)$	$u^\pm(\epsilon, \gamma)$	0	$-\psi(z)$
W^\pm	2	$(q + 1)/2$	$\frac{1}{2}(q + 1)\tau(-1)$	$s^\pm(\epsilon, \gamma)$	$\tau(x)$	0
X_φ	$(q - 1)/2$	$q - 1$	$(q - 1)\varphi(-1)$	$-\varphi(\epsilon)$	0	$-\varphi(z) - \varphi(1/z)$
V	1	q	q	0	1	-1
W_α	$(q - 3)/2$	$q + 1$	$(q + 1)\alpha(-1)$	$\alpha(\epsilon)$	$\alpha(x) + \alpha(1/x)$	0

The pair of representations X^\pm . The two $(q - 1)/2$ -dimensional representations X^+ and X^- have the same trace character values for exactly all group elements outside of $[c_2(\epsilon, \gamma)]$, so we have $\delta(X^+, X^-) = 2/q$.

The pair of representations W^\pm . The two $(q + 1)/2$ -dimensional representations W^+ and W^- have the same trace character values exactly for all group elements outside of the $[c_2(\epsilon, \gamma)]$ conjugacy classes. So again we have $\delta(W^+, W^-) = 2/q$.

$(q - 1)$ -dimensional representations. There are $(q - 1)/2$ such representations, denoted X_φ , where $\varphi \in \mathbb{E}^1$, for $\varphi^2 \neq 1$. Note that $|\mathbb{E}^1| = q + 1$. In order to determine $\delta(X_\varphi, X_{\varphi'})$, we need to find the number of $z \in \mathbb{E}^1$ for which $\varphi(z) + \varphi(z^{-1}) = \varphi'(z) + \varphi'(z^{-1})$, and check whether $\varphi(-1) = \varphi'(-1)$.

We begin with the first equation. Note that $\text{Im}(\varphi), \text{Im}(\varphi') \subset \mu_{q+1}$, where μ_n denotes the n th roots of unity. Then $\varphi(z) + \varphi(z^{-1})$ is of the form $\zeta^a + \zeta^{-a}$, where ζ is the primitive $(q + 1)$ th root of unity $e^{2\pi i/(q+1)}$ and a is a nonnegative integer less than $q + 1$. Now $\zeta^a + \zeta^{-a} = \zeta^b + \zeta^{-b}$ for some $0 \leq a, b < q + 1$ implies that $a = b$ or $(q + 1) - b$. So $\varphi(z) + \varphi(z^{-1}) = \varphi'(z) + \varphi'(z^{-1})$ iff $\varphi(z) = \varphi'(z)$ or $\varphi(z) = \varphi'(z^{-1})$.

If $\varphi(z) = \varphi'(z)$, then this is equivalent to $(\varphi')^{-1}\varphi(z) = 1$, and the number of z for which this holds is $|\ker(\varphi')^{-1}\varphi|$. The number of z for which $\varphi(z) = \varphi'(z^{-1})$ is $|\ker \varphi' \varphi|$. Thus the number of $z \in \mathbb{E}^1$ for which $\varphi(z) + \varphi(z^{-1}) = \varphi'(z) + \varphi'(z^{-1})$ is

$$|\ker(\varphi')^{-1}\varphi| + |\ker \varphi' \varphi| - |\ker \varphi' \varphi \cap \ker(\varphi')^{-1}\varphi|.$$

Now \mathbb{E}^1 is a cyclic group, so we can fix a generator g . The elements of $\widehat{\mathbb{E}^1}$ can then be denoted as $\{\varphi_0, \varphi_1, \dots, \varphi_q\}$, where φ_m is defined via $\varphi_m(g) = \zeta^m$. Note that $|\ker \varphi_m| = (m, q + 1)$. Define

$$M_k(m, m') = \frac{(m + m', k) + (m - m', k) - (m + m', m - m', k) - 1 - t_{m, m'}}{2},$$

where $t_{m, m'} = 1$ if both k and $m + m'$ are even, and 0 otherwise. Then:

LEMMA 6.1. For distinct integers $0 \leq m, m' < q + 1$, we have

$$|\{[c_4(z)] : \varphi_m(z) + \varphi_m(z^{-1}) = \varphi_{m'}(z) + \varphi_{m'}(z^{-1})\}| = M_{q+1}(m, m').$$

If m and m' have the same parity, then $\varphi_m(-1) = \varphi_{m'}(-1)$, so

$$(6.1) \quad \delta(X_{\varphi_m}, X_{\varphi_{m'}}) = \frac{1}{q + 1} \left(\frac{q - 1}{2} - M_{q+1}(m, m') \right).$$

If m and m' have different parity, then

$$(6.2) \quad \delta(X_{\varphi_m}, X_{\varphi_{m'}}) = \frac{1}{q^2 - 1} \left(\frac{q^2 + 1}{2} - M_{q+1}(m, m')(q - 1) \right).$$

To determine the minimum possible value of δ above, we consider the maximum possible size of $M_k(m, m')$.

LEMMA 6.2. *Suppose $k = 2^j \geq 8$. Then*

$$\max M_k(m, m') = 2^{j-2} - 1 = k/4 - 1,$$

where m, m' run over distinct classes in $\mathbb{Z}/k\mathbb{Z} \setminus \{0, k/2\}$ with $m \not\equiv \pm m'$.

Suppose $k \in 2\mathbb{N}$ is not a power of 2 and let p be the smallest odd prime dividing k . Then

$$\max M_k(m, m') = \begin{cases} (k/4)(1 + 1/p) - 1, & k \equiv 0 \pmod{4}, \\ (k - 2)/4, & k \equiv 2 \pmod{4}, \end{cases}$$

where m, m' range as before.

In all the cases above, the maximum occurs with m, m' of the same parity if and only if $4 \mid k$.

Proof. Let $d = (m + m', k)$ and $d' = (m - m', k)$, so our restrictions on m, m' imply that d, d' are proper divisors of k of the same parity. Note that any pair of such d, d' arises from some m, m' if $d \neq d'$, and the case $d = d' = k/2$ does not occur. Then $M_k(m, m') = \frac{1}{2}(d + d' - (d, d') - 1 - t_{m, m'})$, and m, m' have the same parity if and only if d, d' are both even.

The case $k = 2^j$ has a maximum with $d = k/2$ and $d' = k/4$.

Suppose $k = 2pk'$ as in the second case. Then $d + d' - (d, d')$ is maximized when $d = k/2$ and $d' = k/p$, which is an admissible pair if k' is even. Otherwise, we get a maximum when $d = k/2$ and $d' = k/(2p)$. ■

In all cases we have

$$(6.3) \quad \max M_k(m, m') \leq k/3 - 1,$$

and equality is obtained if and only if $12 \mid k$ for suitable m, m' of the same parity. This leads to an exact formula for $\delta_{q-1}(\text{SL}(2, q))$ with $q > 3$ odd by combining with (6.1) and (6.2). We do not write down the final expression, but just note the consequence that $\delta_{q-1}(\text{SL}(2, q)) \geq 1/6$, with equality if and only if $12 \mid (q + 1)$.

(q + 1)-dimensional representations. Consider $W_\alpha, W_{\alpha'}$, where $\alpha, \alpha' \in \widehat{\mathbb{F}_q^\times} - \{\pm 1\}$ and $\alpha \neq \alpha'$. Since $|\mathbb{F}_q^\times| = q - 1$, we know that $\text{Im}(\alpha) < \mu_{q-1}$. So, given a generator g of the cyclic group \mathbb{F}_q^\times , we define the elements of $\widehat{\mathbb{F}_q^\times}$ as $\alpha_m(g) = \zeta^m$, where $\zeta := e^{2\pi i/(q-1)}$ and $0 \leq m \leq q - 2$.

Using similar arguments to the $(q - 1)$ -dimensional case above, we get:

LEMMA 6.3. *For distinct integers $0 \leq m, m' < q - 1$, we have*

$$|\{[c_3(x)] : \alpha_m(x) + \alpha_m(x^{-1}) = \alpha_{m'}(x) + \alpha_{m'}(x^{-1})\}| = M_{q-1}(m, m').$$

Given that the value of $\alpha_m(-1)$ is 1 if m is even and -1 if m is odd, we deduce that if m and m' have the same parity, then

$$\delta(W_{\alpha_m}, W_{\alpha_{m'}}) = \frac{1}{q - 1} \left(\frac{q - 3}{2} - M_{q-1}(m, m') \right),$$

whereas if m and m' have different parity, then

$$\delta(W_{\alpha_m}, W_{\alpha_{m'}}) = \frac{1}{q^2 - 1} \left(\frac{q^2 - 3}{2} - M_{q-1}(m, m')(q + 1) \right).$$

Combining these with Lemma 6.2 for $q > 5$ then leads to a formula for $\delta_{q+1}(\text{SL}(2, q))$. In particular, (6.3) gives $\delta_{q+1}(\text{SL}(2, q)) \geq 1/6$, with equality if and only if $12 \mid (q - 1)$.

6.2. $\text{SL}(2, q)$ for even q . We keep the notation from the previous section. The order of $\text{SL}(2, q)$ is again $q(q + 1)(q - 1)$. The conjugacy classes for $\text{SL}(2, q)$, q even, are as follows:

- (A) I .
- (B) $[N] = \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right]$. This conjugacy class is of size $q^2 - 1$.
- (C) $[c_3(x)]$, where $c_3(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$, with $x \neq 1$. We note that $[c_3(x)] = [c_3(x^{-1})]$, so there are $(q - 2)/2$ such conjugacy classes. Each one is of size $q(q + 1)$.
- (D) $[c_4(z)]$, where $c_4(z) = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix}$ for $z = x + \delta y \in \mathbb{E}^1$ with $z \neq 1$. Since $c_4(z) = c_4(\bar{z})$, there are $q/2$ such conjugacy classes, each of size $q(q - 1)$.

The representations for q even are constructed similarly to the case of q odd, with a couple of differences: Since, for q even, the subgroup S has odd order, it does not have characters of order 2, and so the irreducible representations X^\pm do not arise. Similarly, the character α cannot be of order 2, and so the irreducible representations W^\pm do not occur. The character table is:

		$[I]$	$[N]$	$[c_3(x)]$	$[c_4(z)]$
Size:		1	$q^2 - 1$	$q(q + 1)$	$q(q - 1)$
Rep	#				
U	1	1	1	1	1
X_φ	$q/2$	$q - 1$	-1	0	$-\varphi(z) - \varphi(z^{-1})$
V	1	q	0	1	-1
W_α	$(q - 2)/2$	$q + 1$	1	$\alpha(x) + \alpha(x^{-1})$	0

Representations of dimension $q - 1$. The analysis here is similar to that in Section 6.1, which gives

$$\delta(X_{\varphi_m}, X_{\varphi_{m'}}) = \frac{1}{q + 1} \left(\frac{q}{2} - M_{q+1}(m, m') \right).$$

Analogously to Lemma 6.2, for $k \geq 3$ odd,

$$(6.4) \quad \max M_k(m, m') = \begin{cases} \frac{1}{2}(k/p - 1), & k = p^j, \\ \frac{1}{2} \left(\frac{k}{p_1 p_2} (p_1 + p_2 - 1) - 1 \right), & k = p_1 p_2 k', \end{cases}$$

where m, m' run over all nonzero classes of $\mathbb{Z}/k\mathbb{Z}$ such that $m \not\equiv \pm m'$ and in the latter case are the two smallest distinct primes dividing k . The above

two equations give an exact expression for $\delta_{q-1}(\mathrm{SL}(2, q))$, $q \geq 4$. For k odd, note that

$$(6.5) \quad \max M_k(m, m') \leq \frac{7k - 15}{30},$$

with equality if and only if $15 \mid k$. Thus $\delta_{q-1}(\mathrm{SL}(2, q)) \geq 4/15$, with equality if and only if $15 \mid (q + 1)$.

Representations of dimension $q + 1$. A similar analysis to that in Section 6.1 gives

$$\delta(W_{\alpha_m}, W_{\alpha_{m'}}) = \frac{1}{q-1} \left(\frac{q-2}{2} - M_{q-1}(m, m') \right).$$

Combining this with (6.4) gives an exact formula for $\delta_{q+1}(\mathrm{SL}(2, q))$ for $q \geq 8$, and from (6.5) we again get $\delta_{q+1}(\mathrm{SL}(2, q)) \geq 4/15$, with equality if and only if $15 \mid (q - 1)$.

6.3. $\mathrm{PSL}(2, q)$ for odd q . The order of $\mathrm{PSL}(2, q)$ is $\frac{1}{2}q(q^2 - 1)$ if q is odd. The conjugacy classes are as follows:

- (A) I .
- (B) $[c_2(\gamma)]$, where $c_2(\gamma) = c_2(1, \gamma) = \begin{pmatrix} 1 & \gamma \\ & 1 \end{pmatrix}$ for $\gamma \in \{1, \Delta\}$.
- (C) $[c_3(x)]$ ($x \neq \pm 1$), where $c_3(x)$ is as in the previous two sections. Since $c_3(x) = c_3(-x) = c_3(1/x) = c_3(-1/x)$, the number of such conjugacy classes when $q \equiv 3 \pmod{4}$ is $(q - 3)/4$. In this case, all of the $c_3(x)$ conjugacy classes have size $q(q + 1)$. If $q \equiv 1 \pmod{4}$, then -1 is a square in \mathbb{F}_q and there is a conjugacy class denoted by $c_3(\sqrt{-1})$ which has size $q(q + 1)/2$; the remaining $c_3(x)$ conjugacy classes (there are $(q - 5)/4$ of them) have size $q(q + 1)$.
- (D) $[c_4(z)]$ for $z \in \mathbb{E}^1$, $z \neq \pm 1$, where $c_4(z)$ is defined as in the previous two sections. Since $c_4(z) = c_4(\bar{z}) = c_4(-z) = c_4(-\bar{z})$, when $q \equiv 1 \pmod{4}$, the number of such conjugacy classes is $(q - 1)/4$, and they are all of size $q(q - 1)$. When $q \equiv 3 \pmod{4}$, we can choose Δ to be -1 (since it is not a square), and so we see that $\delta \in \mathbb{E}^1$. The conjugacy class associated to $c_4(\delta)$ has size $q(q - 1)/2$, whereas the rest of the $c_4(z)$ conjugacy classes (of which there are $(q - 3)/4$ such classes) have size $q(q - 1)$.

The representations of $\mathrm{PSL}(2, q)$ are the representations of $\mathrm{SL}(2, q)$ which are trivial on $-I$; this depends on the congruence class of q modulo 4.

6.3.1. $q \equiv 1 \pmod{4}$. For the character table below, the notation is the same as in previous subsections.

		$[I]$	$[c_2(\gamma)]$	$[c_3(\sqrt{-1})]$	$[c_3(x)]$	$[c_4(z)]$
	Size:	1	$(q^2 - 1)/2$	$q(q + 1)/2$	$q(q + 1)$	$q(q - 1)$
Rep	#	1	2	1	$(q - 5)/4$	$(q - 1)/4$
U	1	1	1	1	1	1
W^\pm	2	$(q + 1)/2$	$s^\pm(1, \gamma)$	$\tau(\sqrt{-1})$	$\tau(x)$	0
X_φ	$(q - 1)/4$	$q - 1$	-1	0	0	$-\varphi(z) - \varphi(1/z)$
V	1	q	0	1	1	-1
W_α	$(q - 5)/4$	$q + 1$	1	$2\alpha(\sqrt{-1})$	$\alpha(x) + \alpha(1/x)$	0

Representations W^\pm . The trace characters of these $(q + 1)/2$ -dimensional representations agree everywhere but for the conjugacy classes $[c_2(\gamma)]$. This gives us $\delta(W^+, W^-) = 2/q$.

Representations of dimension $q - 1$. Assume $q \geq 9$. Any two representations $X_\varphi, X_{\varphi'}$ have trace characters that may differ only for the conjugacy classes $[c_4(z)]$. We may view φ as a map into $\mu_{(q+1)/2}$ and parametrize the φ by φ_m for nonzero $m \in \mathbb{Z}/\frac{q+1}{2}\mathbb{Z}$ as before. Analogously, we obtain

$$\delta(X_{\varphi_m}, X_{\varphi_{m'}}) = \frac{1}{q + 1} \left(\frac{q - 1}{2} - 2M_{(q+1)/2}(m, m') \right).$$

From (6.5), this gives $\delta_{q-1}(\text{PSL}(2, q)) \geq 4/15$, with equality if and only if $30 \mid (q + 1)$.

Representations of dimension $q + 1$. Assume $q \geq 13$. The analysis follows in a similar manner to previous sections. View $\alpha : \mathbb{F}_q^\times / \{\pm 1\} \rightarrow \mu_{(q-1)/2}$, and we can parametrize such α by $m \in \mathbb{Z}/\frac{q-1}{2}\mathbb{Z}$ as before. One difference is that we must consider the case when $x = \sqrt{-1}$. Note that this is the only conjugacy class of the form $[c_3(x)]$ that has size $q(q + 1)/2$. We find that $\alpha_m(\sqrt{-1}) = \alpha_{m'}(\sqrt{-1})$ if and only if m, m' have the same parity. Overall we get

$$\delta(W_{\alpha_m}, W_{\alpha_{m'}}) = \frac{1}{q - 1} \left(\frac{q - 5}{2} - 2M_{(q-1)/2}(m, m') + 1 - t_{m, m'} \right).$$

From (6.3) we get $\delta_{q+1}(\text{PSL}(2, q)) \geq 1/6$, with equality if and only if $24 \mid (q - 1)$.

6.3.2. $q \equiv 3 \pmod{4}$.

		$[I]$	$[c_2(\gamma)]$	$[c_3(x)]$	$[c_4(z)]$	$[c_4(\delta)]$
	Size:	1	$(q^2 - 1)/2$	$q(q + 1)$	$q(q - 1)$	$(q(q - 1))/2$
Rep	#	1	2	$(q - 3)/4$	$(q - 3)/4$	1
U	1	1	1	1	1	1
X^\pm	2	$(q - 1)/2$	$u^\pm(1, \gamma)$	0	$-\psi(z)$	$-\psi(\delta)$
X_φ	$(q - 3)/4$	$q - 1$	-1	0	$-\varphi(z) - \varphi(1/z)$	$-2\varphi(\delta)$
V	1	q	0	1	-1	1
W_α	$(q - 3)/4$	$q + 1$	1	$\alpha(x) + \alpha(1/x)$	0	0

where $u^\pm(1, \gamma)$ and ψ are defined as before.

Representations X^\pm . For W^\pm , the characters of the representations X^\pm agree everywhere but for the conjugacy classes $[c_2(\gamma)]$, so $\delta(X^+, X^-) = 2/q$.

Representations of dimension $q - 1$. Assume $q \geq 11$. Any two representations $X_\varphi, X_{\varphi'}$ have trace characters that may differ only for the conjugacy classes $[c_4(z)]$. In the case of the conjugacy class $[c_4(\delta)]$, we note that δ has order 2 in $\mathbb{E}^1/\{\pm 1\}$. Parametrize the nontrivial maps $\varphi : \mathbb{E}^1/\{\pm 1\} \rightarrow \mu_{(q+1)/2}$ by $1 \leq m \leq (q-3)/4$ as before. Then $\varphi_m(\delta) = \varphi_{m'}(\delta)$ if and only if m, m' have the same parity. We obtain

$$\delta(X_{\varphi_m}, X_{\varphi_{m'}}) = \frac{1}{q+1} \left(\frac{q-3}{2} - 2M_{(q+1)/2}(m, m') + 1 - t_{m, m'} \right).$$

By (6.3), we get $\delta_{q-1}(\mathrm{PSL}(2, q)) \geq 1/6$, with equality if and only if $24 \mid (q+1)$.

Representations of dimension $q + 1$. Assume $q \geq 11$. We obtain

$$\delta(W_{\alpha_m}, W_{\alpha_{m'}}) = \frac{1}{q-1} \left(\frac{q-3}{2} - 2M_{(q-1)/2}(m, m') \right).$$

By (6.5), we get $\delta_{q+1}(\mathrm{PSL}(2, q)) \geq 4/15$, with equality if and only if $30 \mid (q-1)$.

Acknowledgements. We thank a referee for pointing out an error in an earlier version. The first author was partially supported by a Simons Collaboration Grant. The second author was supported by Forschungskredit grant K-71116-01-01 of the University of Zürich and partially supported by grant SNF PP00P2-138906 of the Swiss National Foundation. This work began when the second author visited the first at the University of Oklahoma. The second author would like to thank the first author as well as the Mathematics Department of the University of Oklahoma for their hospitality.

References

- [AY65] J. E. Adney and T. Yen, *Automorphisms of a p -group*, Illinois J. Math. 9 (1965), 137–143.
- [Bli17] H. F. Blichfeldt, *Finite Collineation Groups*, Univ. of Chicago Press, Chicago, 1917.
- [FH91] W. Fulton and J. Harris, *Representation theory*, Grad. Texts in Math. 129, Springer, New York, 1991.
- [GG16] GAP Group, *GAP—Groups, Algorithms, Programming*, Version 4.8.3 (2016); <http://www.gap-system.org>.
- [HI82] R. B. Howlett and I. M. Isaacs, *On groups of central type*, Math. Z. 179 (1982), 555–569.
- [IM64] N. Iwahori and H. Matsumoto, *Several remarks on projective representations of finite groups*, J. Fac. Sci. Univ. Tokyo Sect. I 10 (1964), 129–146.
- [KW09] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture I*, Invent. Math. 178 (2009), 485–504.
- [Lan80] R. P. Langlands, *Base Change for $\mathrm{GL}(2)$* , Ann. of Math. Stud. 96, Princeton Univ. Press, Princeton, NJ, and Univ. of Tokyo Press, Tokyo, 1980.

- [Mar04] K. Martin, *Four-dimensional Galois representations of solvable type and automorphic forms*, Ph.D. thesis, California Inst. of Technology, Pasadena, CA, 2004.
- [MBD61] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and Applications of Finite Groups*, Dover Publ., New York, 1961.
- [Raj98] C. S. Rajan, *On strong multiplicity one for l -adic representations*, Int. Math. Res. Notices 1998, no. 3, 161–172.
- [Ram94a] D. Ramakrishnan, *Appendix: A refinement of the strong multiplicity one theorem for $GL(2)$* , Invent. Math. 116 (1994), 645–649.
- [Ram94b] D. Ramakrishnan, *Pure motives and automorphic forms*, in: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math. 55, Amer. Math. Soc., Providence, RI, 1994, 411–446.
- [Ser81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.
- [Tun81] J. Tunnell, *Artin’s conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) 5 (1981), 173–175.
- [Wal14] N. Walji, *Further refinement of strong multiplicity one for $GL(2)$* , Trans. Amer. Math. Soc. 366 (2014), 4987–5007.

Kimball Martin
Department of Mathematics
University of Oklahoma
Norman, OK 73019, U.S.A.
E-mail: kmartin@math.ou.edu

Nahid Walji
The American University of Paris
75007 Paris, France
E-mail: nwalji@aup.edu