

BEAUVILLE SURFACES AND FINITE SIMPLE GROUPS

SHELLY GARION, MICHAEL LARSEN, AND ALEXANDER LUBOTZKY

In memory of Fritz Grunewald, an inspiring mathematician and a dear friend

ABSTRACT. A Beauville surface is a rigid complex surface of the form $(C_1 \times C_2)/G$, where C_1 and C_2 are non-singular, projective, higher genus curves, and G is a finite group acting freely on the product. Bauer, Catanese, and Grunewald conjectured that every finite simple group G , with the exception of A_5 , gives rise to such a surface. We prove that this is so for almost all finite simple groups (i.e., with at most finitely many exceptions). The proof makes use of the structure theory of finite simple groups, probability theory, and character estimates.

Catanese [Cat] defined a *Beauville surface* to be an infinitesimally rigid complex surface of the form $X := (C_1 \times C_2)/G$, where C_1 and C_2 are non-singular projective curves of genus ≥ 2 , and G is a finite group acting freely on the product. Every $g \in G$ respects the product decomposition $C_1 \times C_2$. Let G^0 denote the subgroup of G (of index ≤ 2) which preserves the ordered pair (C_1, C_2) . Any Beauville surface can be presented in such a way that G^0 acts effectively on each factor. Catanese called such a presentation *minimal* and proved that it is unique [Cat, Proposition 3.13]. A Beauville surface is *mixed* (resp. *unmixed*) if $[G : G^0] = 2$ (resp. $G = G^0$).

There has been an effort to classify finite groups G appearing in minimal presentations of unmixed Beauville surfaces. A finite group G appears in this way if and only if it admits an *unmixed Beauville structure*. This consists of an ordered quadruple $(x_1, y_1, x_2, y_2) \in G$

2000 *Mathematics Subject Classification*. Primary 20D06; Secondary 14H30 14J10 20H10.

SG was supported by a European Postdoctoral Fellowship (EPDI) during her stay at the Max-Planck-Institute for Mathematics.

ML was supported by grants from the National Science Foundation and the United States - Israel Binational Science Foundation.

AL was supported by grants from the European Research Council and the National Science Foundation.

such that each set $\{x_i, y_i\}$ generates G and

$$\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = \{e\},$$

where $\Sigma(x, y)$ is the union of conjugacy classes of all powers of x , all powers of y , and all powers of xy . Bauer, Catanese, and Grunewald proved [BCG, Theorem 7.16] that all sufficiently large alternating groups admit an unmixed Beauville structure and conjectured [BCG, Conjecture 7.17] that all (non-abelian) finite simple groups except A_5 do so. (The group A_5 is a genuine exception.)

Some progress has been made on this conjecture. In [FuGo] it was shown that it holds for alternating groups, i.e., that A_n admits an unmixed Beauville structure for all $n \geq 6$. Partial results for groups of the form $\mathrm{PSL}_2(q)$ and ${}^2B_2(2^{2f+1})$ were given in [BCG]; complete results for the same two families together with the Ree groups ${}^2G_2(3^{2f+1})$ were proved in [FuJo] and [GaPe]. Additionally, the groups of the form $G_2(q)$ and ${}^3D_4(q)$ (in characteristic $p > 3$) and $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ (all q) were treated in [GaPe].

The goal of the current paper is to prove the Bauer-Catanese-Grunewald conjecture for almost all finite simple groups.

Theorem 1. *For every sufficiently large non-abelian finite simple group G , there exists a Beauville surface with minimal presentation $C_1 \times C_2/G$.*

Before saying something about the proof, let us put our result in a more general group-theoretic context. The existence of an unmixed Beauville structure on G amounts to the realization of G as a quotient of (hyperbolic) triangle groups in two “independent” ways. The question of which finite simple groups are quotients of triangle groups has attracted a lot of attention in the group theory literature. There has been special interest in the $(2, 3, 7)$ -triangle group, also known as the Hurwitz group (see [Con] and the references therein), but considerable attention has been paid to other triangle groups as well (see [Mar] and the references therein). Usually the question has been asked from the angle of characterizing finite simple quotients of a fixed triangle group. Here the point of view is different: given a finite simple group, we will provide several (in fact, many) “triangle” generations of it. In this context, one should mention the old conjecture of Higman, proved by Everitt [Eve], asserting that for every hyperbolic triangle group Γ , all but finitely many alternating groups are quotients of Γ . Of course, this gives Theorem 1 for almost all the alternating groups. One should not be tempted to conjecture that given Γ , almost all finite simple groups

are quotients of Γ . In this connection, [Mar] has some intriguing and suggestive results.

Taking an even broader perspective, one can study finite quotients and representations of Fuchsian groups (see, e.g., [LiSh1] and [LaLu]), but usually triangle groups are the most difficult to deal with.

Let us now give a short description of the proof. As mentioned above, the result is known for alternating groups, and we can ignore the finitely many sporadic groups. By the classification of finite simple groups, we need only consider groups of Lie type. For each such group which is sufficiently large, we will present two maximal tori T_1 and T_2 . If C_i denotes the set of all conjugates of elements of T_i , we ensure that $C_1 \cap C_2 = \{e\}$, and that in each C_i we can find x_i and y_i such that

- (a) $G = \langle x_i, y_i \rangle$,
- (b) $x_i y_i \in C_i$.

To assure (a), we use some of the well developed theory bounding the indices and the number of maximal subgroups in G . On the other hand, (b) can be proved by means of character estimates. While it is quite likely that the estimates we need can be deduced from Lusztig's theory, a much softer and more elementary method is presented in §1. This method works for general finite groups and may have some independent interest and applications.

The paper is organized as follows. In §1, the new character estimate is presented. In §2, we state Proposition 7, which claims that two tori exist with some desired properties. We illustrate the proposition by proving it for groups of the form $\mathrm{PSL}_n(q)$ for all but finitely many pairs (n, q) . We then present Theorem 1 modulo Proposition 7, leaving the detailed case analysis required to prove Proposition 7 in general to §3. The only groups not covered by prior work are now the Ree groups ${}^2F_4(2^{2f+1})$, which are discussed in §4, using a different method which is applicable to groups whose maximal subgroup structure is well understood.

This paper is dedicated to the memory of Fritz Grunewald, who has been influential in the area of Beauville surfaces by connecting it to group theory [BCG]. It has been typical of Fritz to serve as a bridge between different areas of mathematics. His legacy as a mathematician and as an outstanding personality will be remembered for many years.

Acknowledgment. The first-named author would like to thank Ingrid Bauer, Fabrizio Catanese and Fritz Grunewald for introducing her to the fascinating world of Beauville structures and for many useful discussions. She is also grateful to Bob Guralnick and Eugene Plotkin for many helpful discussions.

1. ELEMENTARY CHARACTER BOUNDS FOR GENERAL FINITE GROUPS

Let G be any finite group. We say that $a \in G$ is *abstractly regular* if the centralizer $Z(a)$ of a in G is abelian. We give an upper bound for the absolute value of irreducible characters evaluated at abstractly regular elements.

Lemma 2. *Let A denote a maximal abelian subgroup of G and $N = N(A)$ its normalizer in G . If $a \in A$ is abstractly regular, then $g^{-1}ag \in A$ if and only if $g \in N$.*

Proof. As A is abelian and $a \in A$, $A \subset Z(a)$. As a is abstractly regular, $Z(a)$ is abelian. Since A is maximal abelian, $A = Z(a)$. Thus,

$$g^{-1}Ag = g^{-1}Z(a)g = Z(g^{-1}ag).$$

If $g^{-1}ag \in A$, then $Z(g^{-1}ag)$ contains A . Since

$$|Z(g^{-1}ag)| = |Z(a)| = |A|,$$

we have

$$g^{-1}Ag = g^{-1}Z(a)g = Z(g^{-1}ag) = A,$$

so $g \in N$. The converse is trivial. \square

Theorem 3. *Let A denote a maximal abelian subgroup of G . Suppose that there exist proper subgroups A_1, \dots, A_n of A such that every element in*

$$A^\circ := A \setminus (A_1 \cup A_2 \cup \dots \cup A_n)$$

is abstractly regular. Let $N = N(A)$ denote the normalizer of A . If χ is any irreducible character of G , then

$$|\chi(a)| \leq (4/\sqrt{3})^n [N : A]$$

for all $a \in A^\circ$.

Proof. Let $A^* = \text{Hom}(A, \mathbb{C}^\times)$. We identify $\mathbb{Z}A^*$ with the ring of characters of virtual complex representations on A . Let $\phi \in \mathbb{Z}A^*$ be the character associated to the restriction of χ to A . For each i from 1 to n , let $\phi_i \in A^*$ be a character which is trivial on A_i and non-trivial on a . For every non-trivial root of unity ω , there exists an integer k such that $|\omega^k - 1| \geq \sqrt{3}$, so replacing ϕ_i by a character of the form ϕ_i^k , we may assume that $|\phi_i(a) - 1| \geq \sqrt{3}$. Let

$$\psi = \phi \prod_{i=1}^n (\phi_i - 1).$$

Let g_1, \dots, g_k denote a set of coset representatives for G/N . By Lemma 2, distinct pairs (g_i, a) , with $a \in A^\circ$, give rise to distinct elements $g_i^{-1}ag_i$. Therefore,

$$\sum_{a \in A^\circ} |\chi(a)|^2 = \frac{1}{k} \sum_{a \in A^\circ} \sum_{i=1}^k |\chi(g_i^{-1}ag_i)|^2 \leq \frac{1}{k} \sum_{g \in G} |\chi(g)|^2 = \frac{|G|}{k} = |N|.$$

As $|\phi_i(a) - 1| \leq 2$ for all i ,

$$\sum_{a \in A} |\psi(a)|^2 = \sum_{a \in A^\circ} |\psi(a)|^2 \leq 4^n \sum_{a \in A^\circ} |\phi(a)|^2 = 4^n \sum_{a \in A^\circ} |\chi(a)|^2 \leq 4^n |N|.$$

Writing ψ as a linear combination $\sum c_i \psi_i$ of $\psi_i \in A^*$, we have

$$\sum_{a \in A} |\psi(a)|^2 = |A| \sum_i c_i^2.$$

Thus,

$$\sum_i c_i^2 \leq 4^n [N : A].$$

As the c_i are integers,

$$\begin{aligned} |\chi(a)| = |\phi(a)| &\leq 3^{-n/2} |\psi(a)| = 3^{-n/2} \left| \sum_i c_i \psi_i(a) \right| \leq 3^{-n/2} \sum_i |c_i| \\ &\leq 3^{-n/2} \sum_i c_i^2 \leq (4/\sqrt{3})^n [N : A]. \end{aligned}$$

□

Corollary 4. *Let χ be an irreducible character of $G = \mathrm{SL}_{r+1}(\mathbb{F}_q)$. If $t_1 \in G$ has an irreducible characteristic polynomial, then*

$$(1) \quad |\chi(t_1)| \leq \frac{2(r+1)^2}{\sqrt{3}}.$$

If $r \geq 2$ and the characteristic polynomial of $t_2 \in G$ has an irreducible factor of degree r , then

$$(2) \quad |\chi(t_2)| \leq \frac{2r^2}{\sqrt{3}}.$$

Proof. Let $P(x)$ denote the characteristic polynomial of t_1 . Every non-zero vector $v \in \mathbb{F}_q^{r+1}$ determines an isomorphism

$$[Q(x)] \mapsto Q(t_1)(v)$$

of \mathbb{F}_q -vector spaces from $\mathbb{F}_q[x]/(P(x)) \cong \mathbb{F}_{q^{r+1}}$ to \mathbb{F}_q^{r+1} . Thus we can identify t_1 with multiplication by a generating element α of the extension $\mathbb{F}_{q^{r+1}}$ of \mathbb{F}_q . The centralizer A of t_1 consists of determinant 1 \mathbb{F}_q -linear automorphisms of $\mathbb{F}_{q^{r+1}}$ which commute with multiplication by α and therefore multiplication by all scalars in $\mathbb{F}_{q^{r+1}}$. Thus $A =$

$\ker \mathbb{F}_{q^{r+1}}^\times \rightarrow \mathbb{F}_q^\times$. Any element of the normalizer N corresponds to an \mathbb{F}_q -linear operator T on $\mathbb{F}_{q^{r+1}}$ such that for some $\beta \in \mathbb{F}_{q^{r+1}}$, $T(\alpha x) = \beta T(x)$ for all $x \in \mathbb{F}_{q^{r+1}}$. If $Q(x)$ is a polynomial in $\mathbb{F}_q[x]$, $Q(\alpha) = 0$ implies $Q(\beta) = 0$, so $\alpha \mapsto \beta$ defines an element of $\text{Gal}(\mathbb{F}_{q^{r+1}}/\mathbb{F}_q) \cong \mathbb{Z}/(r+1)\mathbb{Z}$. If the automorphism is trivial, then T corresponds to an element in $Z(A) = A$. Thus $[N : A] \leq r + 1$.

On the other hand, any element in A which corresponds to a generator of the field $\mathbb{F}_{q^{r+1}}$ over \mathbb{F}_q has centralizer A , so we may define F_i to be the i th maximal proper subfield of $\mathbb{F}_{q^{r+1}}$ over \mathbb{F}_q and A_i to denote the elements of A which can be regarded as elements of F_i . The number n of such maximal subfields is the number of distinct prime factors of $r + 1$. Writing

$$r + 1 = p_1^{a_1} \cdots p_n^{a_n},$$

with $2 \leq p_1 < p_2 < \cdots < p_n$, we have

$$(4/\sqrt{3})^n \leq \frac{2}{\sqrt{3}} \cdot (r + 1).$$

Theorem 3 now implies (1).

If $r \geq 2$ and the characteristic polynomial factors as $P(x)(x - a)$, we can identify \mathbb{F}_q^{r+1} with $\mathbb{F}_{q^r} \times \mathbb{F}_q$ and the centralizer of t_2 with multiplication operators $(\beta, N(\beta)^{-1})$ on this algebra, where $\beta \in \mathbb{F}_{q^r}^\times$ and N denotes the norm map to \mathbb{F}_q . The proof now proceeds as before. \square

At this point, the reader who is primarily interested in the case $\text{SL}_n(\mathbb{F}_q)$ can proceed directly to §2. Here we generalize these examples, replacing SL_n by any simply connected simple algebraic group \underline{G} . Our reference for the theory of such groups is [Car].

Let \mathbb{F}_q be a finite field and \underline{G} a simply connected simple algebraic group over \mathbb{F}_q . Let $G = \underline{G}(\mathbb{F}_q)$. It is often useful to think of $\underline{G}(\mathbb{F}_q)$ as $\underline{G}(\overline{\mathbb{F}}_q)^F$. By the classification of (non-abelian) finite simple groups, with finitely many exceptions, each such group is an alternating group, a Suzuki or Ree group, or a quotient of $\underline{G}(\mathbb{F}_q)$ by its center, for some \underline{G} . With finitely many exceptions, G determines \underline{G} and \mathbb{F}_q . Let \underline{B} be a Borel subgroup of \underline{G} and \underline{T}_0 a maximal torus of \underline{B} defined over \mathbb{F}_q . Let \underline{N} denote the normalizer of \underline{T}_0 and let $W := \underline{N}/\underline{T}_0$ denote the Weyl group of \underline{G} with respect to \underline{T}_0 . Thus F acts on W compatibly with its action on the character and cocharacter groups X and Y of \underline{T}_0 . Note that W^F is never trivial, since \underline{B} defines an F -stable longest root α , and the reflection s_α is therefore F -invariant. The group \underline{G} is determined up to isomorphism by its Dynkin diagram, the prime power q , and the order m of F viewed as an automorphism of the Dynkin diagram of \underline{G} .

Let $W' := W \rtimes \langle \mathbb{Z}/m\mathbb{Z} \rangle$, where 1 acts on W by F . There is a bijective correspondence between G -conjugacy classes of \mathbb{F}_q -rational maximal tori in \underline{G} and F -conjugacy classes in W , i.e., W -orbits under the W -action $z.w := z^{-1}wF(z)$. There is also a bijection between F -conjugacy classes in W and W -orbits in the coset $W \rtimes 1 \subset W'$. For each \mathbb{F}_q -rational torus \underline{T} of \underline{G} , we write $T = \underline{T}(\mathbb{F}_q)$ and denote by T^{reg} the set of G -conjugacy classes of regular semisimple elements of T .

Proposition 5. *Let $[w']$ denote a W -orbit in $W \rtimes 1$ and \underline{T}' an \mathbb{F}_q -rational maximal torus of \underline{G} in the class of tori associated with $[w']$. Let $T' := \underline{T}'(\mathbb{F}_q)$. Suppose that $t' \in T'$ is regular semisimple and χ is an irreducible character of G . Then*

$$|\chi(t')| \leq (4/\sqrt{3})^n |\text{Stab}_W(w')|,$$

where n denotes the number of subgroups of prime order in $\text{Stab}_W(w')$.

Proof. As T' contains a regular semisimple element, \underline{T}' is a non-degenerate torus in the sense of [Car]. Let \underline{N}' denote the normalizer of \underline{T}' . By [Car, 3.6.5], there exists an isomorphism $\underline{N}'/\underline{T}' \cong W$ mapping $N_G(T')/T'$ to $\text{Stab}_W(w')$. In particular, the index of T' in its normalizer equals $|\text{Stab}_W(w')|$. Let $\langle x_1 \rangle, \dots, \langle x_n \rangle$ denote the elements of prime order in $N_G(T')/T'$. Let y_i denote an element of $N_G(T')$ representing the class x_i , and let $A_i \subset T'$ denote the intersection $T' \cap Z_G(y_i)$. As \underline{G} is simply connected, Steinberg's theorem [Car, 3.5.6] implies $T' = Z_G(a)$ for every regular semisimple element of T' . We claim that every element a of

$$T' \setminus (A_1 \cup \dots \cup A_n)$$

is regular semisimple and therefore regular. By [Car, 3.5.4], if a is not regular, the centralizer \underline{H} of a in \underline{G} is a connected reductive group with maximal torus \underline{T}' such that the Weyl group of \underline{H} with respect to \underline{T}' is a non-trivial subgroup of the Weyl group of \underline{G} with respect to \underline{T}' . Therefore, there is some non-trivial F -stable element of $\underline{N}'/\underline{T}'$ which commutes with a . Some power of this element is of prime order, and therefore some power is of the form x_i for some $i \leq n$, and it follows that a belongs to A_i .

The proposition now follows immediately from Theorem 3. \square

Corollary 6. *For all $A, B > 0$ there exists C such that if \underline{G} is of rank r , $\text{Stab}_W(w')$ is abelian of order less than Ar^2 and has a cyclic subgroup of index less than B , then for every regular semisimple $t' \in T'$ and every irreducible character χ ,*

$$|\chi(t')| \leq Cr^3.$$

Proof. Let $H := \text{Stab}_W(w')$. The number of subgroups of H of any given prime order p is bounded in terms of B , and the number of subgroups of order $p > B$ is at most 1. On the other hand, the number n of distinct primes p_i dividing $|H|$ is $o(\log |H|)$ since the sum of the $\log p_i$ is at most $\log |H|$, and if the p_i are arranged in ascending order, $\log p_i > \log i$. Thus $(4/\sqrt{3})^n = |H|^{o(1)} = r^{o(1)}$. It follows that for all $\epsilon > 0$,

$$|\chi(t')| = O(r^{2+\epsilon}),$$

which implies the corollary. □

2. PROOF OF THE MAIN THEOREM

Let $\delta(G)$ denote the minimum degree of a non-trivial irreducible representation of G . By estimates of Landazuri-Seitz [LaSe], there exists an absolute constant $c_1 > 0$ such that

$$(3) \quad \delta(G) \geq c_1 q^r,$$

where \underline{G} is of rank r .

We need one more result before beginning the proof of the main theorem.

Proposition 7. *There exist absolute constants c_2 and c_3 such that for every sufficiently large group of Lie type G (of rank r), there exist maximal tori \underline{T}_1 and \underline{T}_2 such that for all $g \in G$,*

$$(4) \quad T_1 \cap g^{-1}T_2g = Z(G);$$

for every regular $t \in T_1 \cup T_2$ and every irreducible character χ of G ,

$$(5) \quad |\chi(t)| \leq c_2 r^3;$$

and

$$(6) \quad |T_i^{\text{rcc}}| \geq \frac{c_3 |T_i|}{r^2},$$

where T_i^{rcc} denotes the set of G -conjugacy classes of regular semisimple elements of T_i .

At this point, we prove the proposition only for the case $G = \text{SL}_{r+1}(\mathbb{F}_q)$. In section 3, we prove it in the remaining cases for which the Frobenius map is standard. The proposition holds also for the non-standard cases but we omit the proof, since it is not needed for Theorem 1. Thanks to [FuJo] and [GaPe] and the results of section 4, the conjecture of Bauer, Catanese, and Grunewald holds for *all* finite simple groups of Suzuki and Ree type.

Proof. Let T_1 and T_2 denote the centralizers of t_1 and t_2 as defined in Corollary 4. We can identify any element $t \in T_1$ with an element α of $\mathbb{F}_{q^{r+1}}$ of norm 1 in \mathbb{F}_q . If $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$, then the eigenvalues of t are the conjugates of α over \mathbb{F}_q , and each appears with the same multiplicity, $\frac{r+1}{k}$. We can identify any element $t \in g^{-1}T_2g$ with some $\beta \in \mathbb{F}_{q^r}^\times$. If β generates \mathbb{F}_{q^l} , the spectrum of t is the multiset union of the single eigenvalue $N(\beta)^{-1} \in \mathbb{F}_q$ and all \mathbb{F}_q -conjugates of β , each with multiplicity $\frac{r}{l}$. Therefore, every element in $T_1 \cap g^{-1}T_2g$ has a single eigenvalue, which must belong to \mathbb{F}_q . It follows that $T_1 \cap g^{-1}T_2g$ is the group of scalar matrices, i.e., $Z(G)$.

If $r \geq 2$, $t \in T_1 \cup T_2$ is regular semisimple, and χ is an irreducible character of G , then

$$|\chi(t)| \leq \frac{2(r+1)^3}{\sqrt{3}} \leq \frac{16r^3}{\sqrt{3}},$$

by Corollary 4. For rank 1, i.e., in the case $G = \mathrm{SL}_2$, we have $|\chi(t)| \leq 2$ for all regular elements and all irreducible characters.

The element in T_1 corresponding to α is regular if and only if $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{r+1}}$. The set of elements in $\mathbb{F}_{q^{r+1}}$ not generating the whole field has cardinality less than

$$\sum_{1 < d | r+1} |\mathbb{F}_{q^{\frac{r+1}{d}}}| \leq \sum_{i=1}^{(r+1)/2} q^i \leq \frac{q^{(r+1)/2+1} - 1}{q - 1} < 2q^{(r+1)/2}.$$

Except in rank 1, this quantity is less than $q^r/2 < |T_1|/2$ except when $q^{(r-1)/2} < 4$. This gives a finite list of exceptions together with the case $r = 1$. For SL_2 , a more careful estimate reveals that the number of elements in T_1 which are not regular is at most 2, so again more than half of the elements in T_1 are regular when $|G|$ is sufficiently large. Now $[N(T_1) : T_1] \leq r + 1$ implies

$$|T_1^{\mathrm{reg}}| \geq \frac{|T_1|}{2(r+1)} \geq \frac{|T_1|}{4r^2}.$$

Likewise, the element of T_2 corresponding to $\beta \in \mathbb{F}_{q^r}$ is regular as long as $r \geq 2$ and $\mathbb{F}_q(\beta) = \mathbb{F}_{q^r}$. There are less than

$$\sum_{i=0}^{r/2} q^i < 2q^{r/2}$$

non-regular elements. For $r = 1$, there are at most $2 < q^{r/2}$ non-regular elements in T_2 . Either way, if $|G|$ is sufficiently large, at least half of the elements of T_2 are regular, and the estimate for $|T_2^{\mathrm{reg}}|$ follows from $[N(T_2) : T_2] \leq r$.

□

We now prove the main theorem, assuming Proposition 7, for all finite simple groups of the form $G/Z(G)$, where $G = \underline{G}(\mathbb{F}_q)$.

Proof. By [GaPe], we may assume that G is not of the form $\mathrm{SL}_2(\mathbb{F}_q)$, $\mathrm{SL}_3(\mathbb{F}_q)$, or $\mathrm{SU}_3(\mathbb{F}_q)$.

Let X_i denote the union of all conjugacy classes $C_{i,j}$ of regular semisimple elements of T_i . We claim that for $i \in \{1, 2\}$, there exist $(x_i, y_i, z_i) \in X_i^3$ such that $x_i y_i = z_i$, and $\langle x_i, y_i \rangle = G$. Let $\bar{x}_i, \bar{y}_i, \bar{z}_i$ denote the images of x_i, y_i, z_i respectively in $\bar{G} := G/Z(G)$. By (4), we have

$$\Sigma(\bar{x}_1, \bar{y}_1) \cap \Sigma(\bar{x}_2, \bar{y}_2) = \{e\}.$$

To prove that triples (x_i, y_i, z_i) as above actually exist, we estimate the cardinality

$$N_i := \{(x_i, y_i, z_i) \in X_i^3 \mid x_i y_i = z_i\}$$

and compare this to the sum

$$(7) \quad \sum_{M \in \max G} |\{(x_i, y_i, z_i) \in (X_i \cap M)^3 \mid x_i y_i = z_i\}|,$$

where $\max G$ denotes the set of maximal proper subgroups of G . This quantity is bounded above by

$$\sum_{M \in \max G} |M|^2 = |G|^2 \sum_{M \in \max G} \frac{1}{[G : M]^2} \leq \frac{|G|^2}{m(G)^{1/2}} \sum_{M \in \max G} [G : M]^{-3/2},$$

where $m(G)$ is the minimal index of a proper subgroup of G or, equivalently, the minimal degree of a non-trivial permutation representation of G . By (3), $m(G) \geq c_1 q^r$. The main theorem of [LMS] asserts that for all $s > 1$,

$$\lim_{|G| \rightarrow \infty} \sum_{M \in \max G} [G : M]^{-s} \rightarrow 0,$$

where the limit is taken over any sequence of finite simple groups with order tending to ∞ . We could equally well take the limit over quasi-simple groups, since there is an index-preserving bijective correspondence between the maximal proper subgroups of a quasi-simple group and those of its simple quotient. This implies that (7) is bounded above by $q^{-r/2} |G|^2$ for all $|G|$ sufficiently large.

Decomposing X_i into conjugacy classes $C_{i,j}$, indexed by $j \in T_i^{\mathrm{rcc}}$, we can write

$$N_i = \sum_{j,k,l \in T_i^{\mathrm{rcc}}} |\{(x, y, z) \in C_{i,j} \times C_{i,k} \times C_{i,l} \mid xy = z\}|$$

Using the well-known formula [Ser, (7.3)] for the summand, this is

$$(8) \quad \sum_{j,k,l \in T_i^{\text{rcc}}} \frac{|G|^2}{|T_i|^3} \sum_{\chi \in G^*} \frac{\chi(C_{i,j})\chi(C_{i,k})\bar{\chi}(C_{i,l})}{\chi(1)}.$$

By (6), the contribution of the trivial character to (8) is

$$\frac{|G|^2 |T_i^{\text{rcc}}|^3}{|T_i|^3} \geq c_4 |G|^2 r^{-6},$$

for some constant c_4 independent of G . By (5), the absolute value of the sum of the contribution of all non-trivial characters to (8) is bounded above by

$$(9) \quad c_5 r^9 |G|^2 \sum_{\chi \neq 1} \chi(1)^{-1} \leq c_5 r^9 \delta(G)^{-1/4} |G|^2 \sum_{\chi \neq 1} \chi(1)^{-3/4}.$$

Now, [LiSh2, Corollary 1.3] asserts that for every $t > 1/2$,

$$\lim_{|G| \rightarrow \infty} \sum_{\chi} \chi(1)^{-t} = 1,$$

where G ranges over groups of Lie type not of the form $\text{SL}_2(\mathbb{F}_q)$, $\text{SL}_3(\mathbb{F}_q)$, or $\text{SU}_3(\mathbb{F}_q)$. (Actually, this corollary is stated in a form where G is assumed to be simple, but the proof, an immediate application of Theorems 1.1 and 1.2 of the same paper, holds equally when G ranges over quasi-simple groups, as in this case.) Having already excluded $\text{SL}_2(\mathbb{F}_q)$, $\text{SL}_3(\mathbb{F}_q)$, and $\text{SU}_3(\mathbb{F}_q)$, we may set $t = 3/4$, and conclude that

$$\lim_{|G| \rightarrow \infty} \sum_{\chi \neq 1} \chi(1)^{-3/4} = 0.$$

From this and (3), we deduce that for G sufficiently large, the right hand side of (9) is bounded above by

$$r^9 q^{-r/4} |G|^2,$$

and it follows that (8) is bounded below by

$$c_6 r^{-6} |G|^2$$

for G sufficiently large. Comparing this to our upper bound for (7), we conclude that for all G sufficiently large, there exist triples (x_i, y_i, z_i) with the properties claimed. \square

3. PAIRS OF MAXIMAL TORI

In this section, we prove Proposition 7 in the case that F is a standard Frobenius map.

Proof. For each choice of Dynkin diagram Δ and each positive integer m dividing the order of $\text{Aut}(\Delta)$, we specify two elements $w_1, w_2 \in W \times 1$. We then prove that if \underline{T}_1 and \underline{T}_2 are \mathbb{F}_q -rational maximal tori of \underline{G} corresponding to w_1 and w_2 respectively, then $T_i := \underline{T}_i(\mathbb{F}_q)$ satisfy (4), (5), and (6). Instead of proving (5) directly, we deduce it from Proposition 5 and the inequalities

$$(10) \quad [N_i : T_i] \leq c_7 r^2,$$

and

$$(11) \quad n_i \leq \log_4 r + c_8,$$

where N_i is the group of \mathbb{F}_q -points of the normalizer \underline{N}_i of \underline{T}_i , and n_i denotes the number of subgroups of prime order in $\text{Stab}_W(w_i)$.

We note that T_i will always contain at least one regular semisimple element and will therefore be non-degenerate, so if c_7 and c_8 exceed $|W|$, (10) and (11) hold trivially. We will only check these conditions, therefore, in the classical cases, i.e., A_r , 2A_r , B_r , C_r , D_r , and 2D_r .

By [Car, 3.2.2], $|T| = |Y/(F-1)Y|$, where Y denote the cocharacter group of \underline{T} . If \underline{T} is associated to the orbit of $(w, 1)$ in $W \times 1$, this equals the determinant of qw acting on the coweight space (or equivalently on the weight space). The eigenvalues of $(w, 1)$ are roots of unity, and decomposing the spectrum into Galois orbits, we obtain a formula for $|T|$ of the form $\prod_{j=1}^s \Phi_{k_j}(q)$, where Φ_k denotes the k th cyclotomic polynomial, and the total degree of the product is r . The subset of elements of T fixed by any particular non-trivial element of W is a polynomial in q of lower degree. As every semisimple element in T which is not regular is fixed by some non-trivial element of W , it follows that in fixed rank, (6) holds for all sufficiently large G .

To check (4) it is useful to note that for monic polynomials $R(x)$ and $S(x)$, the greatest common denominator of $R(q)$ and $S(q)$ divides the resultant of R and S . Also, for cyclotomic polynomials

$$\text{res}(\Phi_a(x), \Phi_b(x)) = \begin{cases} \ell & \text{if } b/a = \ell^k, \ell \text{ prime, } k \in \mathbb{Z} \setminus \{0\}. \\ 1 & \text{otherwise.} \end{cases}$$

To compute the resultant of two products of cyclotomic polynomials, we use bimultiplicativity. In general, the greatest common divisor $(R(q), S(q))$ divides $(\text{res}(R(x), S(x)), R(q))$. Since $T_1 \cap g^{-1}T_2g$ contains

$Z(G)$ for all g , it suffices to prove that $(R(q), S(q))$ divides $|Z(G)|$ to prove that $T_1 \cap g^{-1}T_2g = Z(G)$ for all $g \in G$.

We now specify choices for w_i in each case, except split A_r , which has already been treated, checking (6), (10), and (11) in the classical cases and (4) in all cases. Note that (6) follows from (10) as long as at least one quarter of the elements of T_i are regular semisimple, which we will see is in fact the case whenever G is sufficiently large. By Corollary 6, (11) follows from (10) as long as $\text{Stab}_W(w_i)$ is abelian with a cyclic subgroup of bounded order.

Case 1: $G = {}^2A_r^{\text{sc}}(q) = \text{SU}_{r+1}(\mathbb{F}_q)$.

In this case, $W = S_{r+1}$, and $m = 2$. The action of F is inner (it is in fact conjugation by a product of $\lfloor (r+1)/2 \rfloor$ disjoint 2-cycles), so $W' = S_{r+1} \times \mathbb{Z}/2\mathbb{Z}$, and S_{r+1} -orbits of elements of $S_{r+1} \times 1$ can be identified with S_{r+1} -conjugacy classes. We set

$$w_1 = ((1\ 2\ 3 \dots r+1), 1), \quad w_2 = ((1\ 2\ 3 \dots r), 1).$$

The stabilizers of w_1 and w_2 are cyclic groups of order $r+1$ and r respectively, just as in the split case. This gives (10) and (11).

We have

$$\begin{aligned} (|T_1|, |T_2|) &= (R(q), S(q)(q+1)) \\ &= (R(q), S(q))(R(q), q+1) | \text{res}(R(x), S(x))(\text{res}(R(x), x+1), q+1) \\ &= (r+1, q+1), \end{aligned}$$

where

$$R(x) = \frac{x^{r+1} - 1}{x - 1}, \quad S(x) = \frac{x^r - 1}{x - 1}.$$

Thus, $(|T_1|, |T_2|)$ divides the order of $Z(G)$, so $T_1 \cap g^{-1}T_2g = Z(G)$. This gives (4).

The analysis of non-regular elements of T_1 or T_2 works as in the split case, giving an $O(q^{(r+1)/2})$ upper bound, so again more than half of the elements are regular when G is large. This implies (6)

Case 2: $G = B_r^{\text{sc}}(q) = \text{Spin}_{2r+1}(\mathbb{F}_q)$.

Here the Weyl group is $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$, i.e., the group of permutations of the set $\{1, 2, \dots, r, 1', 2', \dots, r'\}$ which respects the partition $\{\{1, 1'\}, \dots, \{r, r'\}\}$. We set

$$w_1 = (1\ 2 \dots r\ 1'\ 2' \dots r'), \quad w_2 = (1\ 2 \dots r)(1'\ 2' \dots r').$$

The centralizers of w_1 and w_2 are $\mathbb{Z}/2r\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ respectively, so again we have (10) and (11). The torus orders are

$$|T_1| = q^r + 1, \quad |T_2| = q^r - 1,$$

so $(|T_1|, |T_2|)$ divides $(2, q^r - 1) = (2, q - 1) = |Z(G)|$.

We can identify T_i with $\{\lambda \in \overline{\mathbb{F}}_q \mid \lambda^{|T_i|} = 1\}$, and if $t \in T_i$ fails to be regular, the corresponding element λ satisfies $\lambda^{q^k \pm 1} = 1$ where $p^k \pm 1 \mid |T_i|$. Thus, we may assume $k \leq r/2$, and the number of non-regular elements of T_1 or T_2 is $O(q^{r/2})$.

Case 3: $G = C_r^{\text{sc}}(q) = \text{Sp}_{2r}(\mathbb{F}_q)$.

This case is in all respects parallel to that of $B_r^{\text{sc}}(q)$.

Case 4: $G = D_r^{\text{sc}}(q) = \text{Spin}_{2r}^+(\mathbb{F}_q)$.

We regard W as an index 2 subgroup of $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$. If r is divisible by 4, we set $s = r/2$ and let

$$\begin{aligned} w_1 &= (1\ 2 \dots s-1)(s \dots r)(1' 2' \dots (s-1)')(s' \dots r') \\ w_2 &= (1\ 2 \dots (s-1)\ 1' 2' \dots (s-1)')(s \dots r\ s' \dots r'). \end{aligned}$$

The centralizers of w_1 and w_2 are both contained in

$$\mathbb{Z}/(2s-2)\mathbb{Z} \times \mathbb{Z}/(2s+2)\mathbb{Z} \cong \mathbb{Z}/(s^2-1)\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2,$$

which has order $O(r^2)$ and a cyclic subgroup of index 4. We have

$$|T_1| = (q^{s-1} - 1)(q^{s+1} - 1), \quad |T_2| = (q^{s-1} + 1)(q^{s+1} + 1),$$

so $(|T_1|, |T_2|)$ divides

$$\begin{aligned} &\text{res}(x^{s-1} - 1, x^{s-1} + 1) \text{res}(x^{s-1} - 1, x^{s+1} + 1) \\ &\cdot \text{res}(x^{s+1} - 1, x^{s-1} + 1) \text{res}(x^{s+1} - 1, x^{s+1} + 1) = 16, \end{aligned}$$

but also the highest power of 2 dividing $(|T_1|, |T_2|)$ is 4 if q is odd and 1 if q is even. Thus, $(|T_1|, |T_2|) = |Z(G)|$.

If $r \equiv 2 \pmod{4}$, we set

$$\begin{aligned} w_1 &= (1\ 2 \dots r)(1' 2' \dots r'), \\ w_2 &= (1\ 2\ 1'\ 2')(3\ 4 \dots r\ 3'\ 4' \dots r'). \end{aligned}$$

The centralizers of w_1 and w_2 are $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/(2r-2)\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ respectively. Each has order $O(r)$ and a cyclic subgroup of index ≤ 4 . We have

$$|T_1| = q^r - 1, \quad |T_2| = (q^{r-2} + 1)(q^2 + 1),$$

so $(|T_1|, |T_2|)$ divides

$$(q^r - 1, q^{r-2} + 1)(q^r - 1, q^2 + 1) = |Z(G)|.$$

If r is odd, we set

$$\begin{aligned} w_1 &= (1\ 2 \dots r)(1' 2' \dots r'), \\ w_2 &= (1\ 1')(2\ 3 \dots r\ 2'\ 3' \dots r'). \end{aligned}$$

The centralizer of w_1 is $\mathbb{Z}/r\mathbb{Z}$, while the centralizer of w_2 is $\mathbb{Z}/(2r-2)\mathbb{Z}$. We have

$$|T_1| = q^r - 1, \quad |T_2| = (q^{r-1} + 1)(q + 1),$$

so $(|T_1|, |T_2|)$ divides

$$(q + 1, q^r - 1)(q^{r-1} + 1, q^r - 1) = (2, q + 1)^2 = |Z(G)|.$$

With one exception, we can bound the number of non-regular elements of T_i by $O(q^{(s-1)/2})$. This exception is T_2 in the case that r is $2 \pmod{4}$. Here elements of T_2 can be regarded as pairs $(\alpha, \beta) \in \overline{\mathbb{F}}_q^2$ such that $\alpha^{q^2+1} = \beta^{q^{r-2}+1} = 1$. A necessary condition that such a pair correspond to a non-regular element is that $\alpha^{q^a \pm 1} = 1$ for some positive $q^a \pm 1 < q^2 + 1$ or $\beta^{q^b \pm 1} = 1$ for some positive $q^b \pm 1 < q^{r-2} + 1$. The former condition can hold for as many as $\frac{2}{q^2+1}|T_2| \leq (2/5)|T_2|$ pairs, while the latter condition holds for $O(q^{(r+2)/2})$ pairs. We conclude that if G is sufficiently large, it is still true that more than half of the elements of T_2 are regular.

Case 5: $G = {}^2D_r^{\text{sc}}(q) = \text{Spin}_{2r}^-(\mathbb{F}_q)$.

We identify $W \rtimes \mathbb{Z}/2\mathbb{Z}$ with $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$. If r is even, we set

$$\begin{aligned} w_1 &= (1\ 2 \dots r\ 1'\ 2' \dots r'), \\ w_2 &= (1\ 1')(2\ 3 \dots r)(2'\ 3' \dots r'). \end{aligned}$$

The W -stabilizers of w_1 and w_2 are contained in their centralizers in $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$, which are respectively $\mathbb{Z}/2r\mathbb{Z}$ and $\mathbb{Z}/(r-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Each has order $O(r)$ and a cyclic subgroup of index ≤ 2 . We have

$$|T_1| = q^r + 1, \quad |T_2| = (q^{r-1} - 1)(q + 1),$$

so $(|T_1|, |T_2|)$ divides

$$(q + 1, q^r + 1)(q^{r-1} - 1, q^r + 1) = (2, q + 1)^2 = |Z(G)|.$$

There are $O(q^{r/2})$ non-regular elements in T_1 and at most $\frac{2}{q+1}|T_2| + O(q^{(r+1)/2})$ non-regular elements in T_2 . If G is sufficiently large, more than one quarter of the elements of T_i are regular.

If r is odd, we set

$$\begin{aligned} w_1 &= (1\ 2 \dots r\ 1'\ 2' \dots r'), \\ w_2 &= (1\ 2\ 1'\ 2')(3 \dots r)(3' \dots r'). \end{aligned}$$

The centralizers of w_1 and w_2 in $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$ are respectively $\mathbb{Z}/2r\mathbb{Z}$ and $\mathbb{Z}/(r-2)\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, each of order $O(r)$ with a cyclic subgroup of index ≤ 4 . We have

$$|T_1| = q^r + 1, \quad |T_2| = (q^{r-2} - 1)(q^2 + 1),$$

so $(|T_1|, |T_2|)$ divides

$$(q^2 + 1, q^r + 1)(q^{r-1} - 1, q^r + 1) = (2, q^2 + 1)^2 = (2, q + 1)^2 = |Z(G)|.$$

There are $O(q^{r/2})$ non-regular elements in T_1 and at most $\frac{2}{q^2+1}|T_2| + O(q^{(r+2)/2})$ non-regular elements in T_2 . If G is sufficiently large, more than half of the elements of T_i are regular.

Case 6: $G = {}^3D_4^{\text{sc}}(q)$.

By [Spr, Table 9], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_1(q)^2 \Phi_2(q)^2, \quad |T_2| = \Phi_{12}(q).$$

so $(|T_1|, |T_2|)$ divides

$$\text{res}(\Phi_1(x)^2 \Phi_2(x)^2, \Phi_{12}(x)) = 1.$$

Case 7: $G = E_6^{\text{sc}}(q)$.

By [Spr, Table 1], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_1(q) \Phi_2(q) \Phi_8(q), \quad |T_2| = \Phi_9(q),$$

so $(|T_1|, |T_2|)$ divides

$$\begin{aligned} (\text{res}(\Phi_1(x) \Phi_2(x) \Phi_8(x), \Phi_9(x)), \Phi_9(q)) &= (3, \Phi_9(q)) \\ &= (3, q - 1) = |Z(G)|. \end{aligned}$$

Case 8: $G = {}^2E_6^{\text{sc}}(q)$.

By [Spr, Table 1], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_1(q) \Phi_2(q) \Phi_8(q), \quad |T_2| = \Phi_{18}(q),$$

so $(|T_1|, |T_2|)$ divides

$$\begin{aligned} (\text{res}(\Phi_1(x) \Phi_2(x) \Phi_8(x), \Phi_{18}(x)), \Phi_{18}(q)) &= (3, \Phi_{18}(q)) \\ &= (3, q + 1) = |Z(G)|. \end{aligned}$$

Case 9: $G = E_7^{\text{sc}}(q)$.

By [Spr, Table 2], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_1(q) \Phi_9(q), \quad |T_2| = \Phi_2(q) \Phi_{14}(q),$$

so $(|T_1|, |T_2|)$ divides

$$\begin{aligned} (\text{res}(\Phi_1(x) \Phi_9(x), \Phi_2(x) \Phi_{14}(x))) &= (2, \Phi_1(q) \Phi_9(q)) \\ &= (2, q - 1) = |Z(G)|. \end{aligned}$$

Case 10: $G = E_8(q)$.

By [Spr, Table 3], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_{24}(q), \quad |T_2| = \Phi_{30}(q),$$

so $(|T_1|, |T_2|)$ divides

$$\text{res}(\Phi_{24}(x), \Phi_{30}(x)) = 1.$$

Case 11: $G = F_4(q)$.

By [Spr, Table 4], there exists elements w_1 and w_2 such that

$$|T_1| = \Phi_8(q), \quad |T_2| = \Phi_{12}(q),$$

so $(|T_1|, |T_2|)$ divides

$$\text{res}(\Phi_8(x), \Phi_{12}(x)) = 1.$$

Case 12: $G = G_2(q)$.

Let w_1 and w_2 denote rotations of π and $2\pi/3$ respectively. Then

$$|T_1| = \Phi_2(q)^2, \quad |T_2| = \Phi_3(q),$$

so $(|T_1|, |T_2|)$ divides

$$\text{res}(\Phi_2^2(x), \Phi_3(x)) = 1.$$

□

4. REE GROUPS

In this section we finish the proof of Theorem 1 by treating the family of Ree groups ${}^2F_4(2^{2f+1})$. The other family of Ree groups ${}^2G_2(3^{2f+1})$ and the Suzuki groups ${}^2B_2(2^{2f+1})$ can be treated similarly. However, alternative proofs for these groups have already been provided in [FuJo] and [GaPe].

The proof for the Ree groups $G = {}^2F_4(2^{2f+1})$ relies on the following two theorems.

Theorem 8. [Mal]. *The group $G = {}^2F_4(q)$, where $q = 2^{2f+1}$ ($f \geq 1$), contains two (cyclic) maximal tori T_1 and T_2 whose orders τ_1 and τ_2 are given by*

$$\tau_1 = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1 = 2^{4f+2} + 2^{3f+2} + 2^{2f+1} + 2^{f+1} + 1,$$

$$\tau_2 = q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1 = 2^{4f+2} - 2^{3f+2} + 2^{2f+1} - 2^{f+1} + 1.$$

Moreover,

$$N_G(T_1) \cong Z_{\tau_1} \rtimes Z_{12} \quad \text{and} \quad N_G(T_2) \cong Z_{\tau_2} \rtimes Z_{12}$$

are maximal subgroups in G , and they are the only maximal subgroups containing T_1 and T_2 respectively.

Recall that Z_n denotes a cyclic group of order n .

Theorem 9. [Gow]. *Let G be a finite simple group of Lie type, and let $z \neq 1$ be a semisimple element in G . Let C_1 and C_2 be any conjugacy classes of G consisting of regular semisimple elements. Then z is expressible as $z = xy$, where $x \in C_1$ and $y \in C_2$.*

We recollect a few observations on the orders τ_1 and τ_2 .

Lemma 10. *The orders τ_1 and τ_2 appearing in Theorem 8 satisfy:*

- (i) $\tau_1 \equiv 1 \pmod{12}$ and $\tau_2 \equiv 1 \pmod{12}$.
- (ii) If $f \geq 2$, then $\phi(\tau_1), \phi(\tau_2) \geq 12 \cdot 13 = 156$, where ϕ denotes the Euler function.
- (iii) τ_1 and τ_2 are relatively prime.

Proof. (i) Observe that when $f \geq 1$,

$$\begin{aligned}\tau_1 - 1 &= 2^{4f+2} + 2^{3f+2} + 2^{2f+1} + 2^{f+1}, \text{ and} \\ \tau_2 - 1 &= 2^{4f+2} - 2^{3f+2} + 2^{2f+1} - 2^{f+1},\end{aligned}$$

are both divisible by 3 and by 4, hence $\tau_1 - 1 \equiv 0 \pmod{12}$ and $\tau_2 - 1 \equiv 0 \pmod{12}$.

- (ii) It is well-known that $\phi(n) \geq \sqrt{n}$ for any $n > 6$ (see [SMC], pp. 9). If $f \geq 4$ then $\tau_1 \geq \tau_2 \geq 246241 > 400^2$ and the result immediately follows. For $f = 2$, $\tau_1 = 1321$ and $\tau_2 = 793$, and so $\phi(\tau_1) = 1320$ and $\phi(\tau_2) = 720$. For $f = 3$, $\tau_1 = 18577$ and $\tau_2 = 14449$, and so $\phi(\tau_1) = 17136$ and $\phi(\tau_2) = 14448$.
- (iii) Both τ_1 and τ_2 are odd, and if some odd prime divides both of them, then it also divides $\tau_1 - \tau_2 = 2\sqrt{2q}(q+1) = 2^{f+2}(q+1)$, and so it must divide $(q+1)$. Now, since

$$\tau_1 = q^2 + (q+1)(1 + \sqrt{2q}),$$

such a prime also divides $q^2 = 2^{4f+2}$, yielding a contradiction. \square

Let T be one of T_1, T_2 and set $\tau = |T|$.

Since T is cyclic, there exists some $z \in T$ of exact order τ . Note that z is regular and semisimple, and denote by C_z the conjugacy class of z in G . By Theorem 8,

$$\begin{aligned}|C_z \cap T| &= |\{t \in T : t = gzg^{-1} \text{ for some } g \in G\}| \\ &= |\{gzg^{-1} : g \in N_G(T)\}| \leq [N_G(T) : T] = 12.\end{aligned}$$

Moreover, $|z| = \tau$, $|N_G(T)| = 12 \cdot \tau$ and $\gcd(\tau, 12) = 1$, therefore $C_z \cap N_G(T) \subseteq (C_z \cap T)$ and so $|C_z \cap N_G(T)| \leq 12$.

By Lemma 10(ii), if $f \geq 2$ then T contains at least 156 elements of exact order τ , and each of them has at most 12 G -conjugates in T , thus one can find 13 elements $w_1, \dots, w_{13} \in T$ of exact order τ , each of them belonging to a different conjugacy class in G . These elements are regular and semisimple, and we denote their corresponding conjugacy classes by $C_{w_1}, \dots, C_{w_{13}}$.

By Theorem 9, one can write $z = x_j y_j$, where $x_j \in C_z$ and $y_j \in C_{w_j}$, for $1 \leq j \leq 13$. Observe that all the elements y_1, \dots, y_{13} are necessarily distinct, as they belong to distinct conjugacy classes. Therefore, all the elements x_1, \dots, x_{13} are also distinct.

Now, since $|C_z \cap N_G(T)| \leq 12$, there exists some $1 \leq j \leq 13$ such that $x_j \notin N_G(T)$. Since $T = \langle z \rangle$ and $N_G(T)$ is the only maximal subgroup of G containing T (by Theorem 8) it follows that $\langle x_j, z \rangle = \langle x_j, y_j \rangle = G$.

Applying the above argument for $T = T_1$ and $T = T_2$, we deduce that whenever $f \geq 2$, there exist x_1, y_1, z_1 of exact order τ_1 and x_2, y_2, z_2 of exact order τ_2 such that

$$x_1 y_1 z_1 = 1 = x_2 y_2 z_2, \text{ and} \\ \langle x_1, y_1 \rangle = G = \langle x_2, y_2 \rangle.$$

One can verify that this statement also holds for $f = 1$ using the MAGMA computer program [Mag].

Moreover, by Lemma 10(iii), τ_1 and τ_2 are relatively prime, therefore

$$\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = \{e\},$$

implying that (x_1, y_1, x_2, y_2) is an unmixed Beauville structure for the group $G = {}^2F_4(2^{2f+1})$.

REFERENCES

- [BCG] Bauer, Ingrid; Catanese, Fabrizio; Grunewald, Fritz: Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory. *Mediterr. J. Math.* **3** (2006), no. 2, 121–146.
- [Mag] Bosma, Wieb; Cannon, John; Playoust, Catherine: The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997) no. 3–4, 235–265
- [Car] Carter, Roger W.: Finite groups of Lie type. Conjugacy classes and complex characters. Pure and Applied Mathematics (New York). A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1985.
- [Cat] Catanese, Fabrizio: Fibred surfaces, varieties isogenous to a product and related moduli spaces. *Amer. J. Math.* **122** (2000), no. 1, 1–44.
- [Con] Conder, Marston: An update on Hurwitz groups. *Groups, Complexity and Cryptology*, to appear.
- [Eve] Everitt, Brent: Alternating quotients of Fuchsian groups. *J. Algebra* **223** (2000), no. 2, 457–476.

- [FuGo] Fuertes, Yolanda; González-Diez, Gabino: On Beauville structures on the groups S_n and A_n , *Math. Z.*, to appear.
- [FuJo] Fuertes, Yolanda; Jones, Gareth: Beauville surfaces and finite groups, arXiv:0910.5489.
- [GaPe] Garion, Shelly; Penegini, Matteo: New Beauville surfaces, moduli spaces, and finite groups, arXiv: 0910.5402v2
- [Gow] Gow, Rod: Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), no. 3, 311–315.
- [LaSe] V. Landazuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
- [LaLu] Larsen, Michael; Lubotzky, Alexander: Representation varieties of Fuchsian groups, in preparation.
- [LMS] Liebeck, Martin W.; Martin, Benjamin M. S.; Shalev, Aner: On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function. *Duke Math. J.* **128** (2005), no. 3, 541–557.
- [LiSh1] Liebeck, Martin W.; Shalev, Aner: Fuchsian groups, finite simple groups and representation varieties. *Invent. Math.* **159** (2005), no. 2, 317–367.
- [LiSh2] Liebeck, Martin W.; Shalev, Aner: Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc. (3)* **90** (2005), no. 1, 61–86.
- [Lus] Lusztig, George: Characters of reductive groups over a finite field. *Annals of Mathematics Studies*, 107. Princeton University Press, Princeton, NJ, 1984.
- [Mal] Malle, Gunter: The maximal subgroups of ${}^2F_4(q^2)$, *J. Algebra* **139** (1991), no. 1, 52–69.
- [Mar] Marion, Claude: On the (p_1, p_2, p_3) -generation of finite groups of Lie type, preprint.
- [SMC] Sándor, József; Mitrinović, Dragoslav S.; Crstici, Borislav: *Handbook of Number Theory I*, Second printing of the 1996 original, Springer, Dordrecht, 2006.
- [Ser] Serre, Jean-Pierre: Topics in Galois theory. Lecture notes prepared by Henri Darmon. *Research Notes in Mathematics*, 1. Jones and Bartlett Publishers, Boston, MA, 1992.
- [Spr] Springer, T. A.: Regular elements of finite reflection groups. *Invent. Math.* **25** (1974), 159–198.

MAX-PLANCK-INSTITUT FÜR MATHEMATIK, 53111 BONN, GERMANY

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, IN 47405 U.S.A.

EINSTEIN INSTITUTE OF MATHEMATICS, EDMOND J. SAFRA CAMPUS, GIVAT RAM, THE HEBREW UNIVERSITY OF JERUSALEM, JERUSALEM, 91904 ISRAEL