

TRANSITIVE PROJECTIVE PLANES AND INSOLUBLE GROUPS

NICK GILL

ABSTRACT. Suppose that a group G acts transitively on the points of \mathcal{P} , a finite non-Desarguesian projective plane. We prove that if G is insoluble then $G/O(G)$ is isomorphic to $\mathrm{SL}_2(5)$ or $\mathrm{SL}_2(5).2$.

MSC(2000): 20B25, 51A35.

1. INTRODUCTION

In 1959, Ostrom and Wagner proved that if a finite projective plane, \mathcal{P} , admits an automorphism group which acts 2-transitively on the set of points of \mathcal{P} , then \mathcal{P} is Desarguesian [OW59]. Ever since this result appeared it has been conjectured that the same conclusion holds if the phrase *2-transitively* is replaced by *transitively*.

A number of results have appeared which partially prove this conjecture under certain extra conditions. Most notably, in 1987 Kantor made use of the Classification of Finite Simple Groups to prove that if \mathcal{P} has order x and \mathcal{P} admits a group G which acts *primitively* on the set of points of \mathcal{P} , then either \mathcal{P} is Desarguesian and $G \geq \mathrm{PSL}(3, x)$, or else $x^2 + x + 1$ is a prime and G is a regular or Frobenius group of order dividing $(x^2 + x + 1)(x + 1)$ or $(x^2 + x + 1)x$ [Kan87].

In the 25 years since Kantor's result appeared, a number of authors have studied what remains, with particular attention being given to the special case where G acts *flag-transitively* and so has order $(x^2 + x + 1)(x + 1)$. Even in this special case, though, the number theory involved is very delicate and the question of whether a flag-transitive non-Desarguesian finite projective plane exists is still wide open (see, for instance, [Tha03, TZ08]).

In this paper we present two main results which depend only on the supposition that a group acts transitively on the set of points of a non-Desarguesian plane. These results build on those given in [Gil07] and constitute the closest approach to a proof of the conjecture so far. Indeed, in a sense that will be made clear below, the results presented here do for point-transitive finite projective planes what Kantor's result did for point-primitive finite projective planes. In light of the difficulties encountered in trying to strengthen Kantor's original result, it is fair to say that the results presented here are the best one could hope for without significant developments in the associated number theory.

In order to state the two results we make some definitions pertaining to a group G . We define $O(G)$ to be the largest odd-order normal subgroup in G and $F(G)$ to be the Fitting subgroup of G .

Theorem A. *Suppose that a group G acts transitively on the set of points of \mathcal{P} , a finite non-Desarguesian projective plane. Then the Sylow 2-subgroups of G are cyclic or generalized quaternion.*

The statement of the next theorem is quite long and technical. The corollaries that come after it will make clear the power of the statement.

Theorem B. *Suppose that a group G acts transitively on the set of points of a finite non-Desarguesian projective plane of order x . Then $x = u^2$ for some integer u and one of the following holds:*

- (1) G has a normal 2-complement (and so G is soluble).
- (2) $G/O(G)$ is isomorphic to $SL_2(3)$ or to a non-split degree 2 extension of $SL_2(3)$ (and so G is soluble).
- (3) G has a subgroup of index at most 2 equal to $O(G) \rtimes K$ where K is a group isomorphic to $SL_2(5)$. Furthermore if N_t is a Sylow t -subgroup of $F(G)$, for some prime t , then one of the following holds:
 - (i) t divides $u^2 + u + 1$;
 - (ii) t divides $u^2 - u + 1$, $N_G(N_t)$ contains a subgroup H such that $H \cong SL_2(5)$, H fixes a point of \mathcal{P} , $N_t \rtimes H$ is a Frobenius group, and N_t is abelian.

Furthermore there exists a prime t dividing both $|F(G)|$ and $u^2 - u + 1$.

The first corollary is one of the results mentioned in the abstract. It requires no proof.

Corollary 1.1. *Suppose that a group G acts transitively on the set of points of \mathcal{P} , a finite non-Desarguesian projective plane. If G is insoluble then $G/O(G)$ contains a subgroup H of index at most 2 such that H is isomorphic to $SL(2, 5)$.*

Appealing to the Odd Order Theorem, we observe that Corollary 1.1 implies the following: If G acts transitively on the points of a finite non-Desarguesian projective plane, then a composition factor of G is either of prime order or is isomorphic to A_5 . In other words we are very close to demonstrating that any counterexample to the conjecture mentioned above must be soluble. Such a conclusion is clearly the best one could hope for by making direct use of the Classification of Finite Simple Groups. Thus Corollary 1.1 brings the study of point-transitive finite projective planes to the same stage that Kantor's 1987 result brought the study of point-primitive finite projective planes [Kan87]. What is left is likely best attacked using number theory, and is undoubtedly very difficult indeed.

The next corollary is also reminiscent of Kantor's result, but in a different way. It is well-known that a finite Desarguesian projective plane of order q admits an odd order group of automorphisms acting transitively on the set

of points (take a *Singer cycle* in $\mathrm{PGL}_3(q)$). The next result asserts that the same is true for general finite projective planes.

Corollary 1.2. *Suppose \mathcal{P} is a finite projective plane admitting an automorphism group acting transitively on the set of points of \mathcal{P} . Then there is a group of odd order that acts transitively on the set of points of \mathcal{P} .*

1.1. Methods and structure. Our proof of Theorem A is group-theoretic. Our main tool for the proof is the following result which is of interest in its own right.

Lemma A. *Suppose that n is a positive integer and that $q = p^a$ for some integer a and prime $p \geq 7$. Let H be an even order subgroup of $\mathrm{GL}_n(q)$. Then there exists an involution $g \in H$ such that*

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

(For integers k, ℓ , we write k_{ℓ} for the largest integer dividing k that is coprime to ℓ .) Note that it is quite possible that the bound given in Lemma A also holds when $p = 3$ and/or 5 , however we have not attempted to prove this.

The connection between Lemma A and Theorem A is probably not immediately obvious. This connection is explored in §2, the culmination of which is Proposition 2.12 and the subsequent corollary which asserts that Lemma A implies Theorem A.

In §3 we give a proof of Lemma A. This proof involves a detailed examination of subgroups of $\mathrm{GL}_n(q)$, and the involutions that they contain. In particular there is no reference to groups acting on projective planes in §3.

In addition to Lemma A, there are several results in §3 that may be of independent interest. In particular one of the results that we prove (see Lemmas 3.16 and 3.17) bears reproduction here:

Proposition 1.3. *Suppose H is an odd order subgroup of $\mathrm{GL}_n(q)$ where $q = p^f$ and $p \geq 7$. Then*

$$|H|_{p'} < \frac{1}{2} 3^{n/3} q^n.$$

This result should be compared with, for instance, [Col08, Theorem A]. The bound given in Proposition 1.3 is not too far away from being sharp: suppose, for convenience, that $q \equiv 3 \pmod{4}$ and $n \equiv 3 \pmod{6}$, then one can easily find an odd-order subgroup in $\mathrm{GL}_n(q)$ of order $n \left(\left(\frac{3}{2}(q^3 - 1)\right)^{n/3}\right)$, which is roughly a factor of $\frac{n}{2^{n-1}}$ away from the stated bound.

The methods used to prove Proposition 1.3 could, in principle, be applied to give much sharper bounds. Indeed the methods could also be applied to give bounds for $|H|_{p'}$ under the weaker assumption that H is soluble (rather than odd-order).

Finally in §4 we analyse the situation where G is insoluble, and we prove Theorem B and Corollary 1.2.

Note that the methods used in different sections vary considerably and hence so does our notation. We explain our notation at the start of each section or subsection.

1.2. Acknowledgments. Thanks are due first to Professor Jan Saxl, who suggested to me some years ago that I should be able to prove a result similar to Theorem B by building on methods from my paper [Gil07]. It has taken me a long time to prove him right.

I would also like to thank Professor Cheryl Praeger and an anonymous referee for help with the exposition of this manuscript, and Professors Marty Isaacs, László Pyber and Trevor Wooley who gave technical advice at crucial junctures.

2. A FRAMEWORK TO PROVE THEOREM A

Our aim in this section is to set up a framework to prove Theorem A. In order to do this we will split into two subsections. The first subsection outlines some basic group theory results that will be needed in the remainder of the paper. In the second subsection we will apply these results to the projective plane situation; in particular we will state Lemma A, and will demonstrate that Lemma A implies Theorem A.

2.1. Some background group theory. Throughout this subsection we use standard group theory notation. For an element $g \in G$, we write g^G for the set of G -conjugates of g in G . A cyclic group of order n will sometimes just be written n . We write $G = N.H$ for an extension of N by H ; in other words G contains a normal subgroup N such that $G/N \cong H$. An element g is an *involution* if $g^2 = 1$ and $g \neq 1$.

Lemma 2.1. *Let G, H, N be groups with $N \triangleleft H \leq G$, and let $g \in N_G(H)$. If $|N|$ is odd then*

$$|H : C_H(g)| = |N : C_N(g)| \times |H/N : C_{H/N}(gN)|.$$

Proof. Take $C \leq H$ such that $C/N = C_{H/N}(gN)$. Then $C \geq C_H(g)$. Let $N^* = \langle g, N \rangle \cong N.2$ and take $c \in C$. Then $g^c \in N^*$.

Since $|N|$ is odd this implies that $g^{cn} = g$ for some $n \in N$ by Sylow's theorem. Thus $C = N.C_H(g)$. Then

$$|H : C| = |H : N.C_H(g)| = \frac{|H : C_H(g)|}{|N : N \cap C_H(g)|} = \frac{|H : C_H(g)|}{|N : C_N(g)|}.$$

Since $|H : C| = |H/N : C_{H/N}(gN)|$ we are done. \square

Note that the lemma also applies with $g \in H = G$, and we will usually use it in this context.

Lemma 2.2. *Let H be a group and let $N \triangleleft H$. Let t be a prime, let P be a Sylow t -subgroup of N , and let $g \in P$. Then*

$$\frac{|g^H|}{|g^N|} = \frac{|g^H \cap P|}{|g^N \cap P|}.$$

Proof. Observe that, by the Frattini argument, the set of N -conjugates of P is the same as the set of H -conjugates of P ; say there are c of these. Let d be the number of such N -conjugates of P which contain the element g . Now count the size of the following set in two different ways:

$$|\{(x, Q) : x \in g^H, Q \in P^H, x \in Q\}| = |g^H|d = c|g^H \cap P|.$$

Similarly we count the size of the following set in two different ways:

$$|\{(x, Q) : x \in g^N, Q \in P^N, x \in Q\}| = |g^N|d = c|g^N \cap P|.$$

Our result follows. \square

We now use the previous two results to study the centralizer of an involution in a subgroup of a direct product of groups.

Lemma 2.3. *Let H_1, \dots, H_r be groups, let H be a subgroup of $H_1 \times \dots \times H_r$, and let g be an involution in H . For $i = 1, \dots, r$, define*

- L_i to be the projection of H to $H_i \times H_{i+1} \times \dots \times H_r$,
- g_i to be the projection of g to $H_i \times H_{i+1} \times \dots \times H_r$.

For $i = 1, \dots, r-1$, define

- $\psi : L_i \rightarrow L_{i+1}$ to be the natural projection, and
- T_i to equal $\ker(\psi_i)$.

Let k be the smallest integer such that $|T_i|$ is even, and let P be a Sylow 2-subgroup of T_k .

(1) If $k = r$, then

$$|H : C_H(g)| = \left(\prod_{i=1}^{r-1} |T_i : C_{T_i}(g_i)| \right) |L_r : C_{L_r}(g_r)|.$$

(2) If $k < r$, then, provided $g_{k+1} = \dots = g_r = 1$,

$$|H : C_H(g)| = \left(\prod_{i=1}^k |T_i : C_{T_i}(g_i)| \right) \frac{|(g_k)^{L_k} \cap P|}{|(g_k)^{T_k} \cap P|}.$$

Proof. If T_1 has odd order then Lemma 2.1 implies that

$$\begin{aligned} |H : C_H(g)| &= |T_1 : C_{T_1}(g)| \times |H/T_1 : C_{H/T_1}(T_1g)| \\ &= |T_1 : C_{T_1}(g)| \times |\psi_1(H) : C_{\psi_1(H)}(\psi_1(g))| \\ &= |T_1 : C_{T_1}(g_1)| \times |L_2 : C_{L_2}(g_2)|. \end{aligned}$$

Now L_2 is a subgroup of $H_2 \times \dots \times H_r$ and so we can iterate the procedure. This implies that

$$|H : C_H(g)| = \left(\prod_{i=1}^{k-1} |T_i : C_{T_i}(g_i)| \right) |L_k : C_{L_k}(g_k)|.$$

If $k = r$ then we are done. If $k < r$ then we must calculate the centralizer of g_k in $L_k \leq H_k \times \cdots \times H_r$. Then we apply Lemma 2.2 using T_k for our normal subgroup N . Then

$$|L_k : C_{L_k}(g_k)| = |T_k : C_{T_k}(g_k)| \times \frac{|(g_k)^{L_k} \cap P|}{|(g_k)^{T_k} \cap P|}.$$

□

We conclude this subsection with some results concerning Sylow subgroups.

Lemma 2.4. *Let G be a group and let $H \triangleleft G$ with $|H|$ odd. Suppose that g is an involution in P , a 2-subgroup of G . Define $\phi : G \rightarrow G/H$ to be the natural projection map. Then*

$$|g^G \cap P| = |(gH)^{G/H} \cap \phi(P)|$$

Proof. Clearly ϕ maps $g^G \cap P$ onto $(gH)^{G/H} \cap \phi(P)$. Suppose that $\phi(g_1) = \phi(g_2)$ for $g_1, g_2 \in g^G \cap P$. Then $g_1H = g_2H$ and so $g_1^{-1}g_2 \in H$, which has odd order. Since $g_1^{-1}g_2$ also lies in P , which has even order, we conclude that $g_1 = g_2$. Thus $\phi|_{g^G \cap P}$ is 1-1 and the result follows. □

The next result is [Mar05, Theorem 1.5].

Lemma 2.5. *Let H be a nilpotent subgroup of the symmetric group S_n . Then H contains at most 1.52^n conjugacy classes.*

Lemma 2.6. *Let q be an odd prime power. The number of conjugacy classes of involutions in a subgroup of $\text{GL}_n(q)$ is strictly less than 3.04^n .*

Proof. Let H be a subgroup of $\text{GL}_n(q)$ and take P , a Sylow 2-subgroup of H . Observe that P contains a representative of every conjugacy class of involutions in H . Thus, to prove the result, we can assume that $H = P$, i.e. H is a 2-group. Let P_n be a Sylow 2-subgroup of $\text{GL}_n(q)$ and assume that $H \leq P_n$.

Observe first that $P_{2k+1} = 2 \times P_{2k}$ hence we obtain immediately that $C_{2k+1} \leq 2C_{2k}$ and it is sufficient to prove the result for n even; assume this from here on.

Suppose next that $q \equiv 3 \pmod{4}$. Then a Sylow 2-subgroup of $\text{GL}_n(q)$ is a subgroup of $\text{GL}_n(q^2)$ and $q^2 \equiv 1 \pmod{4}$. Hence it is sufficient to assume that $q \equiv 1 \pmod{4}$. In this case H is a subgroup of $(q-1)^n : S_n$; we take H to be a subgroup of $\langle D, M \rangle$ where D is the group of invertible diagonal matrices, and M is the set of permutation matrices.

Write D_0 for $D \cap H$ and observe first that there are at most $2^n - 1$ involutions in D_0 . Now consider a coset of D_0 in H , gD_0 , where g is an involution in $H \setminus D_0$. Choose a basis so that g corresponds to permutation

(12)(34) \cdots $(k-1, k)$ as follows:

$$g = \begin{pmatrix} & g_1 & & \\ g_1^{-1} & & & \\ & & g_3 & \\ & g_3^{-1} & & \\ & & & \ddots \end{pmatrix}.$$

Choose d to be a diagonal matrix:

$$d = \begin{pmatrix} d_1 & & \\ & d_2 & \\ & & \ddots \end{pmatrix}.$$

Now D_0 acts by conjugation on the coset gD_0 and observe that

- $gdg^{-1} = g$ if and only if $d_i = d_{i+1}$ for $i = 1, 3, \dots, k-1$;
- $(dg)^2 = 1$ if and only if $d_i d_{i+1} = 1$ for $i = 1, 3, \dots, k-1$ and $d_{k+1}, \dots, d_n = \pm 1$.

Let $D_1 = \{d \in D_0 : (dg)^2 = 1\}$, a subgroup of D_0 . Observe that $|C_{D_1}(g)| \leq 2^{n-\frac{k}{2}}$. What is more, since D_0 is abelian, $C_{D_1}(g) = C_{D_1}(gd)$ for any $d \in D_0$, thus every orbit of D_1 on the coset gD_0 must have size at least $\frac{|D_1|}{2^{n-\frac{k}{2}}}$. In other words the number of D_1 -conjugacy classes of involutions represented in the coset gD_0 is at most $2^{n-\frac{k}{2}} < 2^n$.

It is therefore clear that the number of conjugacy classes of involutions in H is strictly less than $2^n \times (C'_n + 1)$ where C'_n is the maximum number of conjugacy classes of involutions in a subgroup of S_n . Lemma 2.5 implies that $C'_n + 1 \leq 1.52^n$ and the result follows. \square

Lemmas 2.2 and 2.6 imply that if $g \in N \triangleleft H < \text{GL}_n(q)$ with $g^2 = 1$, then

$$\frac{|g^H \cap P|}{|g^N \cap P|} < 3.04^n$$

for P a Sylow 2-subgroup of N .

2.2. The projective plane situation. This subsection is the last, until Section 4, in which we will directly consider projective planes. Hence all the notation in this subsection is self-contained and we will develop this notation as we go along.

We begin by stating a hypothesis which will hold throughout this subsection. The conditions included represent, by [Wag59] and [Dem97, 4.1.7], the conditions under which a group may act transitively on the points of a non-Desarguesian projective plane.

Hypothesis 1. *Suppose that a group G acts transitively upon the points of a non-Desarguesian projective plane \mathcal{P} of order $x > 4$. If G contains any involutions then each fixes a Baer subplane; in particular they fix $u^2 + u + 1$ points where $x = u^2, u > 2$. Furthermore in this case any non-trivial element*

of G fixing at least u^2 points fixes either $u^2 + u + 1$, $u^2 + 1$ or $u^2 + 2$ points of \mathcal{P} .

We collect some significant facts that follow from Hypothesis 1:

Lemma 2.7. *The Fitting group and the generalized Fitting group of G coincide, i.e. $F^*(G) = F(G)$. What is more, $F(G)$ acts semi-regularly on the points of \mathcal{P} . Further, if p is a prime dividing $u^2 + u + 1$, then $p \equiv 1 \pmod{3}$ or $p = 3$ and 9 does not divide $u^2 + u + 1$.*

Proof. The results about the Fitting group of G can be found in [Gil07, Theorem A] and [Gil06, Theorem A]. The result about prime divisors can be found in [Kan87, p.33]. \square

Note that $u^2 - u + 1 = (u - 1)^2 + (u - 1) + 1$ hence Lemma 2.7 implies that if p is a prime dividing $u^2 - u + 1$, then $p \equiv 1 \pmod{3}$ or $p = 3$ and 9 does not divide $u^2 - u + 1$.

Write α for a point of \mathcal{P} . For integers k and w , write k_w (resp. $k_{w'}$) for the largest divisor of k which is a power of w (resp. coprime to w). We write $\text{Fix}(g)$ for the set of fixed points of g ; similarly $\text{Fix}(H)$ is the set of fixed points of a subgroup $H < G$. We begin with the following observation:

Lemma 2.8. *Suppose that G contains an involution. Then one of the following holds:*

- (1) *the Sylow 2-subgroups of G are cyclic or generalized quaternion;*
- (2) *All primes which divide $|F(G)|$ must also divide $u^2 + u + 1$.*

Proof. Suppose that the Sylow 2-subgroups of G are not cyclic or generalized quaternion. This is equivalent to supposing that the Sylow 2-subgroups of G contain a Klein 4-group. Let N be a Sylow r -subgroup of $F(G)$, for some prime r , and observe that any subgroup of G acts by conjugation on N . Then [Asc00, (40.6)] implies that a Sylow 2-subgroup of G does not act semi-regularly on N . Hence G contains an involution g for which $C_N(g)$ is non-trivial. Now $C_N(g)$ acts on $\text{Fix}(g)$, a set of size $u^2 + u + 1$. Because $F(G)$ acts semi-regularly on the points of \mathcal{P} we conclude that r divides $u^2 + u + 1$. \square

We will be interested in the second of these possibilities. So for the rest of this subsection we add the following to our hypothesis:

Hypothesis 2. *Suppose that G contains an involution and that all primes dividing $|F(G)|$ also divide $u^2 + u + 1$.*

Clearly if we can show that Hypotheses 1 and 2 lead to a contradiction then Lemma 2.8 will imply Theorem A. Over the rest of this subsection we will work towards showing that, provided Lemma A is true, such a contradiction does indeed follow from these hypotheses. (We will state Lemma A shortly.)

Write $u^2 + u + 1 = p_1^{a_1} \cdots p_r^{a_r}$ (a product of prime powers) and observe that, by Lemma 2.7, $p_i \equiv 1 \pmod{3}$ or else $p_i^{a_i} = 3$. Let $F(G) = N_1 \times N_2 \times \cdots \times N_r$

where $N_i \in \text{Syl}_{p_i} F(G)$ and set $Z = Z(F(G))$. Since $F^*(G) = F(G)$, we conclude that G/Z is a subgroup of

$$\text{Aut}N_1 \times \cdots \times \text{Aut}N_r$$

(see, for instance, [Asc00, (31.13)]). Write $V_i = N_i/\Phi(N_i)$. Here $\Phi(N_i)$ is the Frattini subgroup of N_i , hence V_i is a vector space over the field of size p_i . Observe that $|V_i| \leq p_i^{a_i}$.

A classical result of Burnside (see, for instance, [Gor68, Theorem 1.4]) tells us that $\text{Aut}N_i$ acts on V_i with kernel, K_i , a p_i -group. Thus G/Z is a subgroup of

$$K_1.\text{GL}(V_1) \times \cdots \times K_r.\text{GL}(V_r).$$

Let $K^\dagger = (K_1 \times \cdots \times K_r) \cap G/Z$ and take K to be the pre-image of K^\dagger in G . Thus G/K is a subgroup of

$$\text{GL}(V_1) \times \cdots \times \text{GL}(V_r).$$

Lemma 2.9. [Gil07, Lemma 13] *Let $x = u^2$ and let g be an involution in G . Then*

$$\frac{|g^G|}{|g^G \cap G_\alpha|} = u^2 - u + 1.$$

Lemma 2.10. *Let g be an involution in G . Then $u^2 - u + 1$ divides*

$$|G/K : C_{G/K}(gK)|.$$

Proof. By Lemma 2.9, $u^2 - u + 1$ divides $|G : C_G(g)|$. Then, by Lemma 2.1,

$$|G : C_G(g)| = |K : C_K(g)| \times |G/K : C_{G/K}(gK)|.$$

Now all primes dividing $|K|$ also divide $u^2 + u + 1$. But $u^2 + u + 1$ is coprime to $u^2 - u + 1$ so we have our result. \square

We wish to apply Lemma 2.3 to the group G/K which is a subgroup of $\text{GL}(V_1) \times \cdots \times \text{GL}(V_r)$. In applying Lemma 2.3 we take $H = G/K$. For $i = 1, \dots, r$,

- $H_i = \text{GL}(V_i)$,
- L_i is the projection of H to $\text{GL}(V_i) \times \text{GL}(V_{i+1}) \times \cdots \times \text{GL}(V_r)$.

For $i = 1, \dots, r - 1$,

- $\psi : L_i \rightarrow L_{i+1}$ is the natural projection, and
- T_i equals $\ker(\psi_i)$.

We can order the V_i so that $|T_i|$ is odd for $i < k$ and $|T_i|$ is even for $i \geq k$ where k is some integer. We adopt such an ordering; furthermore we choose such an ordering for which k is as large as possible. If $k < r$ then we also wish to guarantee that

$$p_k^{a_k-1} + \cdots + p_k + 1 < p_{k+1}^{a_{k+1}-1} + \cdots + p_{k+1} + 1.$$

If this is not the case then we simply swap V_k and V_{k+1} in our ordering. Thus we assume that the inequality holds.

Now we are dealing with an involution g in G but we will apply Lemma 2.3 not to g but gK in G/K . Then g_i will be the projection of gK onto $\mathrm{GL}(V_i) \times \cdots \times \mathrm{GL}(V_r)$. Recall that $u^2 + u + 1 = p_1^{a_1} \cdots p_r^{a_r}$ where the p_i are prime numbers; furthermore $|V_i| = p_i^{b_i}$ for some $b_i \leq a_i$. Finally, in order to state the next lemma concisely, we define T_r to equal L_r .

Lemma 2.11. *There exists $j \leq k$ such that*

$$(|T_j : C_{T_j}(g_j)|, u^2 - u + 1) > p_j^{a_j-1} + \cdots + p_j + 1.$$

Proof. We suppose that the proposition does not hold and seek a contradiction. In other words we suppose that, for all $i \leq k$,

$$(|T_i : C_{T_i}(g_i)|, u^2 - u + 1) \leq p_i^{a_i-1} + \cdots + p_i + 1$$

If $k = r$, then $T_r = L_r$ and Lemmas 2.3 and 2.10 imply that $u^2 - u + 1$ divides

$$\prod_{i=1}^r |T_i : C_{T_i}(g_i)|.$$

By our supposition this implies that

$$u^2 - u + 1 \leq \prod_{i=1}^r (p_i^{a_i-1} + \cdots + p_i + 1) < \frac{u^2 + u + 1}{2^r}.$$

This is clearly a contradiction.

Now suppose that $k < r$. Since P is a Sylow 2-subgroup of T_k which is isomorphic to a subgroup of $\mathrm{GL}(V_k)$, Lemma 2.6 implies that

$$\left(u^2 - u + 1, \frac{|(g_k)^{L_k} \cap P|}{|(g_k)^{T_k} \cap P|} \right) < 3.04^{a_k}.$$

Now $3.04^k < p_k^{a_k-1} + \cdots + p_k + 1$ except when

$$(P_k, a_k) \in \{(3, 1), (7, 1), (7, 2)\}$$

Thus, ignoring these exceptions, our supposition implies that

$$u^2 - u + 1 \leq \left(\prod_{i=1}^k (p_i^{a_i-1} + \cdots + p_i + 1) \right) (p_k^{a_k-1} + \cdots + p_k + 1).$$

Now recall that we have chosen an ordering such that $p_k^{a_k-1} + \cdots + p_k + 1 < p_{k+1}^{a_{k+1}-1} + \cdots + p_{k+1} + 1$. This implies that

$$u^2 - u + 1 \leq \prod_{i=1}^{k+1} (p_i^{a_i-1} + \cdots + p_i + 1) < \frac{u^2 + u + 1}{2^{k+1}}$$

and, once again, we have a contradiction.

We must deal with the exceptions. When $a_k = 1$, $\mathrm{GL}(V_k)$ is cyclic and so $|(g_k)^{L_k} \cap P| = 1$ and the result follows immediately. When $(p_k, a_k) = (7, 2)$, one simply uses the fact that

$$(u^2 - u + 1, |\mathrm{GL}(V_k)|) \leq 3 < p_k + 1$$

and we are done. \square

Proposition 2.12. *Hypothesis 1 and Lemma A imply that Hypothesis 2 is false.*

Proof. Suppose Hypotheses 1 and 2 are true. We show that Lemma A leads to a contradiction. Define K, V_i, L_i, T_i as in the lead up to Lemma 2.11. In particular G/K is a subgroup of $\mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_r)$, where we order the V_i as in Lemma 2.11 and recall that $|V_i| = p_i^{b_i}$ where $b_i \leq a_i$.

We first apply Lemma A to T_k which can be thought of as a subgroup of $\mathrm{GL}(V_k)$. Thus let g_k be an involution in T_k such that $|T_k : C_{T_k}(g_k)|_{p'_k}$ is minimised. If $p_k = 3$, then $a_k = 1$ and $|T_k : C_{T_k}(g_k)|_{p'_k} = 1$. If $p_k > 3$, then Lemma A implies that

$$|T_k : C_{T_k}(g_k)|_{p'_k} \leq p_k^{b_k-1} + \cdots + p_k + 1 \leq p_k^{a_k-1} + \cdots + p_k + 1.$$

Now, by Lemma 2.7 (and the comment immediately after), this implies that

$$(|T_k : C_{T_k}(g_k)|, u^2 - u + 1) \leq |T_k : C_{T_k}(g_k)|_{p'_k} \leq p_k^{a_k-1} + \cdots + p_k + 1.$$

Let gK be an involutory pre-image of g_k in G/K (such a pre-image must exist since $|T_i|$ is odd for $i < k$); as before take g_i to be the projection of gK onto $\mathrm{GL}(V_i) \times \cdots \times \mathrm{GL}(V_r)$. Observe that, in all cases $\langle T_j, g_j \rangle$ is isomorphic to a subgroup of $\mathrm{GL}(V_j)$.

Now, when $j < k$, T_j has odd order. Then $H_j = \langle T_j, g_j \rangle$ has a unique H_j -conjugacy class of involutions. Thus Lemma A implies that, for all $j < k$ where $p_j \neq 3$,

$$(|T_j : C_{T_j}(g_j)|, u^2 - u + 1) \leq p_j^{a_j-1} + \cdots + p_j + 1.$$

Indeed the same bound holds when $p_j = 3$ since in this case $a_j = 1$. This yields a contradiction to Lemma 2.11.

Thus we have demonstrated that, provided Lemma A is true, our Hypotheses 1 and 2 lead to a contradiction. \square

Corollary 2.13. *Lemma A implies Theorem A.*

Proof. This is immediate from Lemma 2.8 and Proposition 2.12. \square

3. PROVING LEMMA A

Throughout this section we occupy ourselves with a proof of Lemma A. Lemma A is a purely group theoretic result; we will not refer to projective planes in this section. We use standard group theory notation, as described at the start of Subsection 2.1. Note that Lemma A was stated on p.3.

Throughout this section $q = p^a$ with $p \geq 7$ and H is a subgroup of $\mathrm{GL}_n(q)$. Suppose that H lies in a maximal subgroup M of $\mathrm{GL}_n(q)$. In order to prove Lemma A we will go through the possibilities for M and H and demonstrate that, in all cases, Lemma A holds.

3.1. The maximal subgroups of $\mathrm{GL}_n(q)$. Before we embark on a proof of Lemma A we need to outline a classification of the maximal subgroups of $G = \mathrm{GL}_n(q)$. Such a classification was outlined in [Asc84]; we follow the treatment of this result given in [KL90]. We take V to be an n -dimensional vector space over \mathbb{F}_q . Let κ be a sesquilinear (resp. quadratic) form defined over V . We will assume that κ is either non-degenerate, or else is equal to the zero form. Define

$$\begin{aligned}\Gamma &= \{g \in \Gamma L(V) \mid \kappa(vg) = \lambda(g)\kappa(v)^{\alpha(g)} \text{ for all } v \in V\}; \\ \Delta &= \{g \in \mathrm{GL}(V) \mid \kappa(vg) = \lambda(g)\kappa(v) \text{ for all } v \in V\}; \\ S &= \{g \in \mathrm{SL}(V) \mid \kappa(vg) = \kappa(v) \text{ for all } v \in V\};\end{aligned}$$

where $\lambda(g) \in \mathbb{F}_q^*$ and $\alpha(g) \in \mathrm{Aut}(\mathbb{F}_q)$. In other words Γ (resp. Δ , S) is the set of *semisimilarities* (resp. *similarities*, *special isometries*) of κ . We record the groups we get for various choices of κ [KL90, Tables 2.1.B and 2.1.D]:

κ	Γ	Δ	S
Zero	$\Gamma L_n(q)$	$\mathrm{GL}_n(q)$	$\mathrm{SL}_n(q)$
Hermitian	$\Gamma U_n(q)$	$GU_n(q) \cdot (q-1)$	$SU_n(q)$
Alternating	$\Gamma Sp_n(q)$	$GO_n^-(q)$	$Sp_n(q)$
Orthogonal	$\Gamma O_n^\epsilon(q)$	$GO_n^\epsilon(q)$	$SO_n^\epsilon(q)$

Here ϵ gives the type of the orthogonal space; it takes the value \pm when n is even, and is blank when n is odd. The group Γ contains the scalars as a normal subgroup, which we denote Z . For $H \leq \Gamma$ we write \overline{H} for reduction modulo scalars: $\overline{H} = H/(H \cap Z)$.

Lemma 3.1. [KL90, Prop. 2.9.2] \overline{S} is simple except in the following cases:

- (1) $n = 1$ or $(n, q) \in \{(2, 2), (2, 3)\}$, or $S = SU(3, 2)$, $Sp(4, 2)$, $SO_2^\pm(q)$, $SO_3(3)$, or $SO_4^+(q)$.
- (2) κ is quadratic, and (1) does not hold. In this case \overline{S} contains a simple subgroup of index at most 2.

We will call situation (1) the *small rank setting*. Thus the small rank setting is described by particular values of (n, q) , and particular types of κ (strictly speaking, since $p \geq 7$, most of the listed cases do not occur). When we are not in the small rank setting, we write Ω (or Ω_κ) for the subgroup of S of index at most 2 such that $\overline{\Omega}$ is simple. Now [KL90, Prop. 2.9.2] implies that Ω is quasisimple.

For particular choices of κ, n and q we are interested in the maximal subgroups of X , a group satisfying $\Omega \leq X \leq \Gamma$; most of the time we will apply the following results with κ the zero form and $X = \Delta_\kappa \cong \mathrm{GL}_n(q)$.

Lemma 3.2. *Suppose we are not in the small rank setting for (κ, n, q) . Let X be a group satisfying $\Omega \leq X \leq \Gamma$. If M is a maximal subgroup of X then either M contains Ω or \overline{M} is a maximal subgroup of \overline{X} . Conversely, if M_1 is a maximal subgroup of \overline{X} then $M_1 = \overline{M}$ for some maximal subgroup M in X .*

Proof. The converse statement is immediate: take M to be the full pre-image of M_1 in X . Then M must be a proper subgroup of X and is clearly maximal.

Now suppose that M is maximal in X . Then \overline{M} must be a maximal subgroup of \overline{X} or else $\overline{M} \cong \overline{X}$. Suppose the latter case holds. Then M contains a perfect subgroup M_0 , which has index at most $|X : \Omega|$ in X . Since M_0 is perfect and Ω is quasisimple we conclude that M_0 contains Ω or else $M_0 \cap \Omega \leq Z(\Omega)$. But $|M_0| \geq \overline{\Omega} > |\Gamma : \Omega| \cdot |Z(\Omega)|$ (see [KL90, Tables 2.1.C and 2.1.D]) and so we conclude that M_0 contains Ω . \square

The maximal subgroups of \overline{X} are described in [KL90, Theorem 1.2.1]. In order to describe them we start with a family $\mathcal{C}(\Gamma)$ of subgroups of Γ (we will describe these in due course). We define

$$\begin{aligned}\mathcal{C}(X) &= \{X \cap H \mid H \in \mathcal{C}(\Gamma)\}; \\ \mathcal{C}(\overline{X}) &= \{\overline{H} \mid H \in \mathcal{C}(X)\}.\end{aligned}$$

Now we have the following result, originally due to Aschbacher [Asc84]:

Theorem 3.3. [KL90, Theorem 1.2.1] *Suppose we are not in the small rank setting for (κ, n, q) . Let X be a group satisfying $\Omega \leq X \leq \Gamma$. If H is a subgroup of \overline{X} then either H is contained in a member of $\mathcal{C}(\overline{X})$, or else H is almost simple with socle S such that if L is the full covering group of S , and if $\rho : L \rightarrow \text{GL}(V)$ is a representation of L such that $\rho(L) = S$, then ρ is absolutely irreducible.*

Corollary 3.4. *Suppose we are not in the small rank setting for (κ, n, q) . Let X be a group satisfying $\Omega \leq X \leq \Gamma$. If H is a subgroup of X then one of the following holds:*

- (1) H contains Ω ;
- (2) H is contained in $M_1 Z$ where $M_1 \in \mathcal{C}(X)$;
- (3) $H_1 \leq H \leq H_1 Z$ where H_1 is an almost quasisimple group such that $F^*(H_1)$ is absolutely irreducible on V .

Proof. Suppose that H does not contain Ω . Then Lemma 3.2 implies that \overline{H} is a proper subgroup of \overline{X} and we apply Theorem 3.3. If \overline{H} does not lie in a member of $\mathcal{C}(\overline{X})$ then \overline{H} is almost simple, and the third possibility holds. Otherwise \overline{H} lies inside a member \overline{M} of $\mathcal{C}(\overline{X})$. Choose \overline{M} to be maximal; Lemma 3.2 implies that H lies inside a maximal subgroup of X equal to the full pre-image of \overline{M} . Now $\overline{M} = \overline{M_1}$ for some $M_1 \in \mathcal{C}(X)$. Thus the full pre-image of \overline{M} is equal to $M_1 Z$ as required. \square

Our job now is to describe $\mathcal{C}(\Gamma)$, and hence $\mathcal{C}(X)$. Each of these splits into eight subfamilies: $\mathcal{C}_i(\Gamma)$ (resp. $\mathcal{C}_i(X)$), for $i = 1, \dots, 8$. We now sketch a description of these; full descriptions (with the same terminology) can be found in [KL90]. We are particularly interested in the case where $X = \Delta$ hence we introduce the following notation: take $H_\Gamma \in \mathcal{C}_i(\Gamma)$ and write $H = H_\Delta = H_\Gamma \cap \Delta$, for the corresponding member of $\mathcal{C}_i(\Delta)$.

- \mathcal{C}_1 : $H_\Gamma = N_\Gamma(W)$ where W is a subspace of V of dimension $m \leq \frac{n}{2}$ that is either non-degenerate or totally singular.
- \mathcal{C}_2 : Write $n = mt$, for $t \geq 2$. H_Γ is the stabilizer in Γ of an m -space decomposition. If $\kappa = 0$, then this is a decomposition $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$ where V_i is an m -dimensional subspace of V ; if κ is non-degenerate, then one must impose extra conditions on the subspaces V_i . In any case H is the stabilizer in Δ of this m -space decomposition.
- \mathcal{C}_3 : Write $n = mr$ for r prime. $H_\Gamma = \Gamma_{\#, \mu}$, a large subgroup of the group Γ_μ corresponding to a form μ on V where V is viewed as a vector space over \mathbb{F}_{q^r} (the precise description of this subgroup is given on [KL90, p. 111]). The form μ depends on κ , as described in [KL90, Table 4.3.A]; for instance if $\kappa = 0$ then $\mu = 0$. Then $H = \Gamma_{\#, \mu} \cap \Delta$.
- \mathcal{C}_4 : Write $n = n_1 n_2$ with $n_1 \geq 2$, and consider $V_1 \otimes V_2$, where V_1 (resp. V_2) is a vector space of dimension n_1 (resp. n_2). This induces an imbedding

$$\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \cong \mathrm{GL}_{n_1}(q) \circ \mathrm{GL}_{n_2}(q) \leq \mathrm{GL}(V) \cong \mathrm{GL}_n(q).$$

We can define forms on V_1 and V_2 , κ_1 and κ_2 , that combine to give a form on $V_1 \times V_2$; if chosen carefully this combination of forms may be identified with the form κ . Thus we induce an imbedding $\Delta_{\kappa_1} \otimes \Delta_{\kappa_2} \leq \Delta_\kappa$. We define $H_\Gamma = (\Delta_{\kappa_1} \otimes \Delta_{\kappa_2})\langle\phi\rangle$, where ϕ is a field automorphism; then $H = \Delta_{\kappa_1} \otimes \Delta_{\kappa_2}$ [KL90, (4.4.13)].

- \mathcal{C}_5 : Let V_0 be an n -dimensional vector space over \mathbb{F}_0 , a subfield of \mathbb{F}_q . Then V can be identified with $V_0 \otimes \mathbb{F}_q$, and a form, κ_0 , on V_0 can be extended to a form κ on V . We then define $H_\Gamma = N_\Gamma(V_0)Z$; in particular $H = \Delta_0 Z$ [KL90, (4.5.5)].
- \mathcal{C}_6 : Write $n = r^m$, for r prime and not equal to p . Then $H_\Gamma = N_\Gamma(R)$ where R is a particular symplectic-type r -subgroup of Δ .
- \mathcal{C}_7 : Write $n = m^t$. The groups here are similar to those in \mathcal{C}_4 ; this time we identify V with a tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_t$ where $V_i, i = 1, \dots, t$ is a vector space of dimension m . Then $H_\Gamma = (\Delta_{\kappa_1} \circ \cdots \circ \Delta_{\kappa_t})\langle(\phi) \times J\rangle$, where ϕ is a field automorphism, and $J \cong S_t$ permutes the V_i . We conclude that $H = (\Delta_{\kappa_1} \circ \cdots \circ \Delta_{\kappa_t})J$ [KL90, p.157].
- \mathcal{C}_8 : Here $H_\Gamma = \Gamma_\mu$ where μ is a non-degenerate form defined on V . Then $H = \Delta_\mu$. The form μ depends on κ , as described in [KL90, Table 4.8.A].

We record two significant corollaries.

Corollary 3.5. *Fix $n > 2$ and $q = p^a$ with $p \geq 7$, and set κ to be the zero form. Let X be a group satisfying $\Delta \leq X \leq \Gamma$. If H is a subgroup of X then one of the following holds:*

- (1) H contains Ω .
- (2) H is contained in $M_1 Z$ where $M_1 \in \mathcal{C}_i(X)$, for $i = 1, \dots, 7$.

- (3) H is contained in M_1Z where $M_1 \in \mathcal{C}_6(X_\xi)$ for some non-degenerate form ξ acting on V .
- (4) $H_1 \leq H \leq H_1Z$ where H_1 is almost quasisimple and $F^*(H_1)$ is absolutely irreducible on V .
- (5) H lies in X_ξ , for some non-degenerate form ξ acting on V and (ξ, n, q) lies in the small rank setting.

Note that, by X_ξ , we mean a group satisfying $\Delta_\xi \leq X_\xi \leq \Gamma_\xi$, for some non-degenerate form ξ acting on V . Note too that the requirement that κ be the zero form is somewhat superfluous; we retain this condition as it makes the corollary easier to state.

Proof. The result differs from Corollary 3.4 by specifying what happens when H is contained in M_1Z for $M_1 \in \mathcal{C}_8(X)$. So let us examine this case; here $M_1 = X_\xi$ for some non-degenerate form ξ acting on V ; in fact Δ_ξ contains Z so we conclude that $H \leq X_\xi$. We can now apply Corollary 3.4 again. If we lie in the small rank setting for (ξ, n, q) then (5) holds. Assume that we do not lie in the small rank setting. If H contains Ω_ξ then [KL90, Proposition 2.10.6] implies that (4) holds. If H contains an almost-simple group H_1 with $F^*(H_1) = S_1$ absolutely irreducible on V then, again, (4) holds.

Finally we have the possibility that H lies in $M \in \mathcal{C}(X_\xi)$. If $M \in \mathcal{C}_6(X_\xi)$, then (3) holds. If $M \in \mathcal{C}_i(X_\xi)$, for $i = 1, \dots, 5, 7$, then the descriptions that we have given above show that H must lie in $\mathcal{C}_i(X_\kappa)$ and (2) holds. (Observe that, if $M \in \mathcal{C}_i(X_\xi)$, for some $i = 1, \dots, 5, 7$, then M stabilizes some geometric configuration in V , as well as preserving ξ . Consider the group M_1 , the full stabilizer of this geometric configuration in X_κ . Then $M_1 \in \mathcal{C}_i(X_\kappa)$ as required.)

Finally, if ξ is alternating and q is even then it is possible that $M = X_\psi \in \mathcal{C}_8(X_\xi)$, where ψ is a non-degenerate quadratic form. In this case we repeat the above argument, and the result follows. \square

Corollary 3.6. *Suppose that M is a maximal subgroup of $\Delta = \mathrm{GL}_n(q)$ lying in one of the families $\mathcal{C}_i(\Delta)$, $i = 1, \dots, 8$. Then M is isomorphic to one of the following groups (t, m, r are all integers; r is prime).*

- \mathcal{C}_1 : $[q^{m(m-n)}].(\mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q))$, for $1 \leq m < n$.
- \mathcal{C}_2 : $\mathrm{GL}_m(q) \wr S_t$, for $n = mt$ with $t \geq 2$.
- \mathcal{C}_3 : $\mathrm{GL}_m(q^r).r$, for $n = mr$, and the extension is given by a field automorphism.
- \mathcal{C}_4 : $\mathrm{GL}_{n_1}(q) \circ \mathrm{GL}_{n_2}(q)$, for $n = n_1n_2$ with $2 \leq n_1 < \sqrt{n}$.
- \mathcal{C}_5 : $\mathrm{GL}_m(q_0)Z$ for $q = q_0^r$ and $Z = Z(\mathrm{GL}_m(q))$.
- \mathcal{C}_6 : The normalizer of an absolutely irreducible symplectic-type r -group, for $n = r^m$ with $r \neq p$.
- \mathcal{C}_7 : $\underbrace{(\mathrm{GL}_m(q) \circ \dots \circ \mathrm{GL}_m(q))}_t .S_t$ for $n = m^t$, $m \geq 3$.
- \mathcal{C}_8 : Δ_ξ for ξ a non-degenerate form on the associated vector space V .

Proof. This is immediate from the descriptions of $\mathcal{C}_i(\Delta)$ given above. (For the most part descriptions are given in [KL90].) \square

3.2. Preliminaries for a proof of Lemma A. We now have enough information about subgroups of $\mathrm{GL}_n(q)$ to begin a proof of Lemma A. Let us remind ourselves of the statement:

Lemma A. *Suppose that n is a positive integer and that $q = p^a$ for some integer a and prime $p \geq 7$. Let H be an even order subgroup of $\mathrm{GL}_n(q)$. Then there exists an involution $g \in H$ such that*

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Let us begin with a proof of Lemma A for $n = 2$ (when $n = 1$, the statement is a trivial consequence of the fact that $\mathrm{GL}_1(q)$ is abelian).

Lemma 3.7. *A maximal subgroup of $\mathrm{PSL}_2(q)$, for q odd, is isomorphic to one of the following groups:*

- (1) $D_{q \pm 1}$ (normalizers of tori);
- (2) $[q] : (\frac{q-1}{2})$ (a Borel);
- (3) S_4, A_4 , or A_5 ;
- (4) $\mathrm{PSL}_2(q_0)$, for $q = q_0^a$ where a is an odd prime;
- (5) $\mathrm{PGL}_2(q_0)$, for $q = q_0^2$.

Proof. This is well-known; see, for example, [Dic58]. \square

Lemma 3.8. *Let $H < \mathrm{GL}_2(q)$ and suppose that H has even order. Suppose that $q = p^a$ with $p \geq 7$. Then there exists an involution $g \in H$ such that*

$$|H : C_H(g)|_{p'} \leq q + 1.$$

Proof. Observe that $|H : C_H(g)|_{p'}$ divides $|H/(H \cap Z(\mathrm{GL}_2(q)) \cap \mathrm{PSL}_2(q))|_{p'}$ and that $H/(H \cap Z(\mathrm{GL}_2(q)) \cap \mathrm{PSL}_2(q))$ is a subgroup of $\mathrm{PSL}_2(q)$. If $H/(H \cap Z(\mathrm{GL}_2(q)) \cap \mathrm{PSL}_2(q)) = \mathrm{PSL}_2(q)$, then $H \geq \mathrm{SL}_2(q)$, H contains a central involution, and the result follows. If $H/(H \cap Z(\mathrm{GL}_2(q)) \cap \mathrm{PSL}_2(q)) < \mathrm{PSL}_2(q)$ it is sufficient to prove that $|H_1|_{p'} \leq q + 1$ for all maximal subgroups H_1 of $\mathrm{PSL}_2(q)$. This follows from Lemma 3.7. \square

The following result will be useful when we come to consider subgroups of $\mathrm{GL}_n(q)$ with a large normal odd-order subgroup.

Lemma 3.9. *Suppose that H is a subgroup of $\mathrm{GL}_n(q)$ where $n > 2$, $q = p^a$ and $p \geq 7$ is prime. If*

$$|H|_{(2p)'} \geq q^{n-1} + \cdots + q + 1,$$

then one of the following holds:

- (1) H contains $\mathrm{SL}_n(q)$.
- (2) H is contained in $M_1 Z$ where $M_1 \in \mathcal{C}_i(\mathrm{GL}_n(q))$, for $i = 1, \dots, 5$.
- (3) $H_1 \leq H \leq H_1 Z$ where H_1 is almost quasisimple and $F^*(H_1)$ is absolutely irreducible on V .
- (4) $n = 4$ and $H \leq \mathrm{GO}_4^+(q)$.

- (5) $H \leq (\mathrm{GL}_m(q) \circ \mathrm{GL}_m(q)) \cdot 2$ with $n = m^2$ for $m \geq 3$.
(6) $(n, q) = (3, 7)$ and $|H/(H \cap Z)|_{(2p)'} \text{ divides } 27$.

Proof. Since H is a subgroup of $\mathrm{GL}_n(q)$ we apply Corollary 3.5. If conclusion 5 of that corollary applies, then, since $p \geq 7$ and $n > 2$, we must have conclusion 4 here.

Thus we are left with the question of what happens when $H \leq M \in \mathcal{C}_6(\Delta_\zeta)$ for some form ζ that is non-degenerate or zero, or when $H \leq M \in \mathcal{C}_7(\Delta_\kappa)$ when κ is the zero form.

Consider the latter situation first. Then M is equal to

$$\underbrace{(\mathrm{GL}_m(q) \circ \cdots \circ \mathrm{GL}_m(q))}_t \cdot S_t$$

for $n = m^t$, $m \geq 3$. Observe that $t! < 7^{t^2}$ and so $|M|_{p'} < q^{m^2 t!} \leq q^{m^2 t + t^2} < q^{m^t - 1}$ unless $t = 2$ or $(m, t) = (3, 3)$. When $(m, t) = (3, 3)$, observe that $|M|_{(2p)'} < 3q^{18}$; when $t = 2$ we obtain conclusion 5.

We are left with the problem of showing that if $M \in \mathcal{C}_6(\Delta_\zeta)$ for some form ζ that is non-degenerate or zero, then either conclusion 6 holds or

$$|M|_{(2p)'} \leq q^{n-1} + \cdots + q + 1;$$

in fact we prefer to show that either conclusion 6 holds or $M_1 = (M/(M \cap Z)) \cap \mathrm{PSL}_n(q)$ satisfies the inequality

$$|M_1|_{(2p)'} |n, q-1|_{(2p)'} < q^{n-2}.$$

Observe that M_1 is a subgroup of $\mathrm{PSL}_n(q)$ and so its structure is given in [KL90, §4.6].

Suppose first that $n = 2^m$. Then

$$\begin{aligned} |M_1|_{(2p)'} |n, q-1|_{(2p)'} &\leq \max\{45, |Sp_{2m}(2)|_{(2p)'}, |\Omega_{2m}^+(2)|_{(2p)'}, |\Omega_{2m}^-(2)|_{(2p)'}\} \\ &\leq \max\{45, \prod_{i=1}^m (2^{2i-1} - 1)\} \\ &\leq \max\{45, 2^{m^2+m}\}. \end{aligned}$$

Now $\max\{45, 2^{m^2+m}\} < q^{2^m-2}$ for $m \geq 3$. When $m = 2$, we find that $|M_1|_{(2p)'} \leq 45$ and we are done.

Suppose that $n = r^m$ for r odd. Then $|M_1|_{(2p)'} \leq \max\{9, |Sp_{2m}(r)|_{(2p)'}\}$ and

$$|M_1|_{(2p)'} |n, q-1|_{(2p)'} < r^{2m^2+4m}.$$

This yields the required bound unless

$$(m, r) \in \{(2, 3), (1, 3), (1, 5), (1, 7)\}.$$

All of these can be ruled out individually, except $(m, r) = (1, 3)$. In this case we obtain conclusion 6. \square

In what follows we will prove Lemma A by referring to the five types of subgroup given in Corollary 3.5.

3.3. Easy cases. We begin by proving Lemma A for some easy situations; recall that $p \geq 7$. Apply Corollary 3.5 with $X = \mathrm{GL}_n(q)$. Set $Z := Z(\mathrm{GL}_n(q))$.

Case 1. Here $H \geq \Omega = \mathrm{SL}_n(q)$. If n is even then H contains a central involution and we are done. If n is odd then H contains an involution g such that $|H : C_H(g)|_{p'} = q^{n-1} + \cdots + q + 1$.

Case 5. In this case $n = 4$ and $H \leq \mathrm{GO}_4^+(q)$; now $\mathrm{GO}_4^+(q)$ has a normal subgroup N of index 2 isomorphic to

$$\mathrm{GL}_2(q) \circ \mathrm{GL}_2(q) = \mathrm{GL}_2(q) \times \mathrm{GL}_2(q) / \{(g, g^{-1}) \mid g \in Z(\mathrm{GL}_2(q))\}.$$

Now we apply Lemma 3.8 to the group N and the result follows.

Case 2 with $M_1 \in \mathcal{C}_7(\mathrm{GL}_n(q))$. In this case M is equal to

$$\underbrace{(\mathrm{GL}_m(q) \circ \cdots \circ \mathrm{GL}_m(q))}_t . S_t$$

for $n = m^t, m \geq 3$. Observe that $t! < 7^{t^2}$ and so $|M|_{p'} < q^{m^2 t t!} \leq q^{m^2 t + t^2} < q^{m^t - 1}$ unless $t = 2$ or $(m, t) = (3, 3)$. When $(m, t) = (3, 3)$, observe that $|M|_{(p)'} < 6q^{18}$ and we are done.

Finally suppose that $t = 2$ and so $H \leq M = (\mathrm{GL}_m(q) \circ \mathrm{GL}_m(q)) : 2$ with $m \geq 3$. Define $N = \mathrm{GL}_m(q) \circ \mathrm{GL}_m(q)$, a normal subgroup in M of index 2. More precisely N is equal to

$$\mathrm{GL}_m(q) \times \mathrm{GL}_m(q) / \{(g, h) \in Z(\mathrm{GL}_m(q)) \times Z(\mathrm{GL}_m(q)) \mid h = g^{-1}\}.$$

Let g be an involution in $M \setminus N$; then one can check that g is the projective image of $((a_1, \pm a_1^{-1}), b) \in (\mathrm{GL}_m(q) \times \mathrm{GL}_m(q)) \rtimes C_2$, with b non-trivial. Easy matrix calculations confirm that $|\mathrm{GL}_m(q)|$ divides $|M : C_M(g)|$, hence if H contains an involution g outside $N \cap H$ then $|H : C_H(g)|_{p'} < q^{\frac{m(m+1)}{2}}$ which satisfies our bound since $m \geq 3$.

If, on the other hand, H contains no such involution then we take $g \in N$. The largest conjugacy class C of involutions in N has $|C|_{p'}$ divisible by

$$\left(\frac{\prod_{i=1}^m (q^i - 1)}{\prod_{i=1}^{\lfloor \frac{m}{2} \rfloor} (q^i - 1) \prod_{i=1}^{\lceil \frac{m}{2} \rceil} (q^i - 1)} \right)^2.$$

Then $|H : C_H(g)|_{p'} \leq 2|N : C_N(g)|_{p'} < 2q^{\frac{1}{2}m^2}$ which satisfies our bound since $m \geq 3$.

Case 3 and Case 2 with $M_1 \in \mathcal{C}_6(\mathrm{GL}_n(q))$. In these cases $H \leq M \in \mathcal{C}_6(\Delta_\eta)$ for η non-degenerate or zero.

Suppose first that $n = r^m$ where r is an odd prime. Then

$$\begin{aligned} |M_1 / (M_1 \cap Z)| &\leq (n, q - 1) \cdot \max\{72, r^{2m} |\mathrm{Sp}_{2m}(r)|\} \\ &\leq (n, q - 1) \cdot \max\{72, r^{3m+2m^2}\}. \end{aligned}$$

One can check that $|M_1 / (M_1 \cap Z)| < q^{n-1}$ unless $n = 3, 5$ or 9 . If $n = 5$ or 9 , then one must have $q = 7$ and the result can be confirmed by inspection. If $n = 3$, then $|M_1 / (M_1 \cap Z)|_{2'}$ divides 81 and so any involution g in the center

of a Sylow 2-subgroup of $H \leq M_1$ will satisfy the required bound unless $q = 7$. If $n = 3$ and $q = 7$, then the result can be confirmed by inspection.

Suppose next that $n = 2^m$ for some $m \geq 2$. Then one can check that $|M_1/(M_1 \cap Z)|_{2'} < 7^{n-2}$ and so any involution g in the center of a Sylow 2-subgroup of $H \leq M_1$ will satisfy the required bound.

3.4. Case 4 (almost quasisimple). We need to prove Lemma A for H where $H_1 \leq H \leq H_1Z$ and H_1 is almost quasisimple such that $F^*(H_1)$ is absolutely irreducible. Clearly we can assume that $H = H_1$.

In what follows $g \in H$ is an involution. Suppose first that $Z = Z(F^*(H_1))$ has even order. Checking Schur multipliers [KL90, Theorem 5.1.4], we see that Z contains at most 3 involutions. Taking g to be one of these we obtain that $|H : C_H(g)|$ divides 3 and the result follows. Suppose from here on that $|Z|$ is odd.

Now Lemma 2.1 implies that

$$|H : C_H(g)| = |Z : C_Z(g)| \times |H/Z : C_{H/Z}(gZ)|.$$

Clearly if $g \in F^*(H_1)$, then

$$|H : C_H(g)| = |H/Z : C_{H/Z}(gZ)|.$$

Thus to prove Lemma A in this case it is sufficient to show that the simple group $S = F^*(H_1)/Z$ contains an involution g such that

$$(1) \quad |\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Our first step in proving this bound is to establish, given a simple group S , what the minimum possible value for n is. We observe first that an embedding of H in $\text{GL}(V)$ induces an imbedding of H/Z_1 in $\text{PGL}(V)$ where Z_1 is some central subgroup of $F^*(H_1)$. Define

$$R_p(G) = \min\{n \mid G \leq \text{PGL}_n(\mathbb{F}) \text{ for } \mathbb{F} \text{ a field of characteristic } p\}.$$

Lemma 3.10. [KL90, Corollary 5.3.3] *If L is quasisimple, then $R_r(L) \geq R_r(L/Z(L))$ for all primes r .*

The lemma implies that, given a simple group S , it is sufficient to prove that S contains an involution g satisfying (1), where $n = R_p(S)$. The next lemma establishes this fact for a large class of simple groups.

Lemma 3.11. *Let $p \geq 7$ be a prime, and let S be a non-abelian simple group. Assume that S is not isomorphic to A_5 and that S is not a group of Lie type in characteristic p . Then S contains an involution g such that*

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq p^{n-1} + \cdots + p + 1,$$

where $n = R_p(S)$.

Proof. The lemma is proved using information in [KL90]. In particular we use Propositions 5.3.7 and 5.3.8 as well as Theorem 5.3.9, all of which list values of $R_p(S)$ for different non-abelian simple groups S .

Suppose that $S = A_m$ is the alternating group on m letters with $m \geq 8$. Then $\text{Aut}(S) \cong S_m$ and S contains an involution g (a double transposition) such that

$$|S_m : C_{S_m}(g)| = \frac{m(m-1)(m-2)(m-3)}{8}.$$

In particular $|S_m : C_{S_m}(g)| < 7^{m-3}$ for $m \geq 8$. Now [KL90, Proposition 5.3.7] implies that $n \geq m-2$ and so $|S_m : C_{S_m}(g)| < 7^{m-3} \leq q^{n-1}$ as required. For $m = 6, 7$ one can check the result directly.

If S is a sporadic group then one can use [KL90, Table 5.1.C and Proposition 5.3.8] along with [CCN+85] to confirm the result in each case.

Next suppose that S is a group of Lie type of characteristic coprime to p . Values for $R_p(S)$ are given in [KL90, Theorem 5.3.9], and a series of (easy and tedious) calculations confirms the inequality that we require. We present two sample calculations: If $H = E_6(r)$ then $R_p(S) = r^9(r^2-1)$. Now observe that $|S| < r^{78}$; it is then sufficient to observe that $r^{78} < 7^{r^9(r^2-1)-1}$. If, on the other hand, $S = \Omega_{2m+1}(r)$ with r odd and $m > 3$ then $R_p(S) \geq r^{2(m-1)} - r^{m-1}$. Now $|S| < r^{2m^2+m}$ and it is sufficient to observe that $r^{2m^2+m} < 7^{r^{2(m-1)} - r^{m-1} - 1}$. \square

Let us deal with the case A_5 .

Lemma 3.12. *Suppose that $H_1 \leq H \leq H_1Z \leq \text{GL}_n(q)$ where H_1 is almost quasisimple and $q = p^a$ for some integer a and prime $p \geq 7$. If $F^*(H_1)/Z(F^*(H_1)) \cong A_5$, then H contains an involution g such that*

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Proof. Suppose, first, that $F^*(H_1)$ is not simple. Since the Schur multiplier of A_5 has order 2, this implies that $F^*(H_1)$ contains a unique central involution and the result follows.

Suppose, then, that $F^*(H_1) = A_5$. Since $p \geq 7$ does not divide $|A_5|$, the representation $A_5 \rightarrow \text{GL}_n(q)$ decomposes into a direct sum of irreducibles. Consulting [CCN+85] we see that the minimal degree of a non-trivial irreducible is 3 and so $n \geq 3$. Now the result follows from the fact that A_5 contains a unique conjugacy class of involutions, and this class has order 15. \square

The next lemma completes the proof of Lemma A for subgroups from case 4.

Lemma 3.13. *Let $p \geq 7, q = p^f$ and S be a quasisimple group of Lie type defined over a field of size p^e lying inside $\text{GL}(n, q)$, such that the associated vector space V is an absolutely irreducible $\mathbb{F}_q S$ -module. Then*

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Proof. We go through the possible quasisimple groups, as listed in the Classification of Finite Simple Groups. Since $p \geq 7$, S is not isomorphic to

${}^2B_2(q)$, ${}^2G_q(q)$ or ${}^2F_4(q)$. Note that the lemma is trivial if S contains a central involution; hence we assume that this is not the case.

We assume that the representation $S \rightarrow \mathrm{GL}_n(q)$ induced by the given embedding cannot be realised over a proper subfield of \mathbb{F}_q , otherwise we redefine q to take a smaller value. Since $p \geq 7$ we observe that the universal quasisimple cover of S is a simply connected group of Lie type, hence we can apply [KL90, Proposition 5.4.6].

Suppose S is a quasisimple cover of $\mathrm{PSL}_m(p^e)$. If m is odd, then S contains an involution such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} = ((p^e)^{m-1} + \cdots + (p^e) + 1).$$

Then [KL90, Propositions 5.4.6 and 5.4.11] imply that $f|e$ and $n \geq \frac{em}{f}$, and the result follows.

If m is even, then the absence of a central involution implies that V is not the natural module for S . Then [KL90, Propositions 5.4.6 and 5.4.11] imply that $n \geq \frac{e}{2f}m(m-1)$. We know that S contains an involution such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} = ((p^e)^{m-2} + \cdots + (p^e) + 1)((p^e)^{m-2} + \cdots + (p^e)^2 + 1).$$

Since $f|e$, the result follows immediately for $m \geq 4$. When $m = 2$, $S = \mathrm{PSL}_2(q)$ and contains an involution g such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} \leq p^e + 1.$$

Since $n \geq 2e/f$ we are done.

Suppose S is a quasisimple cover of $\mathrm{PSU}_m(p^e)$ (so S is defined over $\mathbb{F}_{p^{2e}}$). Assume that $m > 2$, since $\mathrm{PSU}_2(p^e) \cong \mathrm{PSL}_2(p^e)$ and this case is done. If m is odd, then S contains an involution such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} = (p^e)^{m-1} - \cdots - (p^e) + 1.$$

Then [KL90, Propositions 5.4.6 and 5.4.11] imply that $n \geq \frac{em}{f}$, and the result follows.

If m is even, then, once again, the absence of a central involution implies that V is not the natural module for S . Then [KL90, Propositions 5.4.6 and 5.4.11] imply that $n \geq \frac{e}{2f}m(m-1)$. We know that S contains an involution such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} = ((p^e)^{m-2} - \cdots - (p^e) + 1)((p^e)^{m-2} + \cdots + (p^e)^2 + 1).$$

The result follows immediately for $m \geq 4$.

For the remaining classical groups, since S has no central involution, we have S simple. We take g to be an involution that is central in the Levi subgroup L of a parabolic subgroup of S .

Suppose that $S = \mathrm{PSP}_{2m}(p^e)$ and assume that $m \geq 2$, since $\mathrm{PSP}_2(p^e) \cong \mathrm{PSL}_2(p^e)$. Choose L to be isomorphic to $(q-1) \cdot (\mathrm{PGL}_2(q) \times \mathrm{PSP}_{n-2}(q))$ [KL90, Proposition 4.1.19]. Then L contains a central involution g such that

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} \leq (p^e)^{2m-2} + \cdots + (p^e)^2 + 1.$$

Since $n \geq \frac{2me}{f}$, we are done.

Suppose that $S = \text{P}\Omega_m^\epsilon(p^e)$. Assume that $m \geq 7$ as, otherwise, $\text{P}\Omega^\epsilon(p^e)$ is either not simple, or else is isomorphic to a simple group that we have already covered. Choose L to be isomorphic to a Levi complement stabilizing a 2-dimensional totally singular subspace of the associated natural vector space, as described in [KL90, Proposition 4.1.20]. If m is odd, then L contains a central involution g such that

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq (p^e)^{m-1} - 1.$$

Since $n \geq \frac{me}{f}$, we are done. If m is even, then L contains a central involution g such that

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq ((p^e)^{m/2-1} - 1)((p^e)^{(m-2)/2} + 1).$$

Since $n \geq \frac{me}{f}$, we are done.

Now for the exceptional groups. In what follows we use the name of the exceptional group to refer to the adjoint version (which is simple, since $p \geq 7$).

Suppose first that $S = G_2(p^e)$; then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq \text{SL}_2(p^e) \circ \text{SL}_2(p^e)$. Thus

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq e((p^e)^4 + (p^e)^2 + 1).$$

Now $f|e$ and $n \geq \frac{7e}{f}$ [KL90, Propositions 5.4.6 and 5.4.12] and we are done.

Suppose that $S = F_4(p^e)$; then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq \text{Spin}_9(p^e)$. Thus

$$|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'} \leq e((p^e)^8 + (p^e)^4 + 1).$$

Now $f|e$ and $n \geq \frac{26e}{f}$ [KL90, Propositions 5.4.6 and 5.4.12] and we are done.

Suppose that S is a quasisimple cover of $E_6(p^e)$ (resp. ${}^2E_6(p^e)$); then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq \text{Spin}_{10}^+(p^e)$ (resp. $\text{Spin}_{10}^-(p^e)$). Thus $|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'}$ is at most

$$6e((p^e)^8 + (p^e)^4 + 1)((p^e)^6 + \epsilon(p^e)^3 + 1)((p^e)^2 + \epsilon(p^e) + 1).$$

Now $f|2e$ and $n \geq \frac{27e}{f}$ [KL90, Propositions 5.4.6 and 5.4.12] and we are done.

Suppose that $S = E_7(p^e)$; then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq \text{SL}_8(p^e)/(4, q-1)$ or $\text{SU}_8(q)/(4, q+1)$. Thus $|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'}$ is at most

$$2e((p^e)^8 + (p^e)^4 + 1)((p^e)^{12} + (p^e)^6 + 1)((p^e)^7 + 1)((p^e)^5 + 1)((p^e)^3 + 1).$$

Now $f|e$ and $n \geq \frac{56e}{f}$ [KL90, Propositions 5.4.6 and 5.4.12] and we are done.

Suppose that $S = E_8(p^e)$; then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq 2.(\text{PSL}_2(p^e) \times E_7(p^e))$. Thus $|\text{Aut}(S) : C_{\text{Aut}(S)}(g)|_{p'}$ is at most

$$e((p^e)^{10} + 1)((p^e)^{12} + 1)((p^e)^6 + 1)((p^e)^{30} - 1).$$

Now $f|e$ and $n \geq \frac{248e}{f}$ [KL90, Propositions 5.4.6 and 5.4.12] and we are done.

Finally suppose that $S = {}^3D_4(p^e)$; then [GLS94, Table 4.5.1] implies that S contains an involution g such that $C_S(g) \geq (\mathrm{SL}_2(p^{3e}) \circ \mathrm{SL}_2(p^e)).2$. Thus

$$|\mathrm{Aut}(S) : C_{\mathrm{Aut}(S)}(g)|_{p'} \leq 3e((p^e)^8 + (p^e)^4 + 1).$$

Now either $f|e$ and $n \geq \frac{24e}{f}$ [KL90, Comments after Proposition 5.4.6; Proposition 5.4.12], or else $f|3e$ and $n \geq \frac{24e}{f}$ [KL90, Comments after Proposition 5.4.6; Proposition 5.4.13] and we are done. \square

3.5. Odd-order subgroups of $\mathrm{GL}_n(q)$. We are left with Case 2 of Corollary 3.5. In order to deal with this we must prove some facts about odd order subgroups of $\mathrm{GL}_n(q)$, where $q = p^f$ and $p \geq 7$.

We begin by quoting a result of Pálffy [Pal82].

Lemma 3.14. *Let H be a primitive subgroup of S_n the symmetric group on n letters. If $n > 1$ and H is solvable, then $|H| \leq 24^{-1/2}n^c$ where $c = 3.24399\dots$.*

It is convenient to record a (basically weaker) variation of Pálffy's result as follows.

Lemma 3.15. *Let H be a primitive subgroup of S_n , the symmetric group on n letters. If H has odd order, then $|H| \leq 2^{n-1}$.*

Proof. Since $|H|$ is odd, H is soluble, and the bound in Lemma 3.14 applies. This yields the result for $n \geq 10$. For $n \leq 9$ we refer to [CCN+85] to confirm the result in all cases. \square

The next couple of results are aimed at giving an upper bound for $|H|_{p'}$ where H is an odd-order subgroup of $\mathrm{GL}_n(q)$. The background idea here is that a prototypical 'large' odd-order subgroup $H < \mathrm{GL}_n(q)$ contains a torus as a large normal subgroup. More precisely, we think of H as equalling a direct product $H_1 \times H_2 \times \dots \times H_k$ (for some $k \leq n$) where, for each i , the group H_i acts semi-linearly on some n_i -dimensional vector space over the field $\mathbb{F}_{q^{a_i}}$ (and $n = \sum_{i=1}^k a_i n_i$). What is more H_i normalizes a maximal split torus T_i of the group $\mathrm{GL}_{n_i}(q^{a_i})$. (i.e. H_i preserves a decomposition of the associated n_i -dimensional vector space over $\mathbb{F}_{q^{a_i}}$ into 1-dimensional subspaces).

We know that $|T_i| < q^{a_i n_i}$; we must study the size of $|H_i : H_i \cap T_i|$. In the action of H_i on the aforementioned decomposition, H_i can induce field automorphisms of order at most a_i on each 1-dimensional subspace - this allows for a possible index of $a_i^{n_i}$. In addition, H_i can permute the 1-dimensional subspaces. We can reduce to the case where the action on the set of subspaces is primitive, in which case Lemma 3.15 allows for a possible index of 2^{n_i-1} . This is more than cancelled out by the fact that $|T_i : H_i \cap T_i| \geq 2^{n_i}$. This reasoning motivates the following definition.

For a fixed positive integer n , we define a *partition of n* to be a positive list of integers, λ , that sum to n ; i.e.

$$(2) \quad \lambda = [\underbrace{1, \dots, 1}_{n_1}, \underbrace{2, \dots, 2}_{n_2}, \underbrace{3, \dots, 3}_{n_3}, \dots]$$

where $n = \sum_i in_i$. For a partition λ of this form define

$$\ell_\lambda = |\{i \mid n_i > 0\}|, \text{ and } c_\lambda = \frac{|1^{n_1} 2^{n_2} 3^{n_3} \dots|_{2'}}{2^{\ell_\lambda}}.$$

When we write $1^{n_1} 2^{n_2} 3^{n_3} \dots$ here, we omit all terms i^{n_i} for which $n_i = 0$; this leaves a finite number of terms in our definition. Now define

$$c_n = \max\{c_\lambda \mid \lambda \text{ is a partition of } n\}.$$

Lemma 3.16.

- (1) If $n = mk$, for $1 < m, k \in \mathbb{Z}^+$, then $c_n \geq (c_m)^k 2^{k-1}$;
- (2) If $n = r + s$, for $0 < r, s \in \mathbb{Z}^+$, then $c_n \geq c_r c_s$;
- (3) Suppose that λ is a partition of n for which $c_n = c_\lambda$.
 - If $n \equiv 0 \pmod{3}$, then $\lambda = [3, \dots, 3]$ and $c_n = \frac{1}{2} 3^{\frac{n}{3}}$.
 - If $n \equiv 1 \pmod{3}$, then $\lambda = [1, 3, \dots, 3]$ and $c_n = \frac{1}{4} 3^{\frac{n-1}{3}}$.
 - If $2 < n \equiv 2 \pmod{3}$, then $\lambda = [3, \dots, 3, 5]$ and $c_n = \frac{5}{4} 3^{\frac{n-2}{3}}$.
 - If $n = 2$, then $\lambda = [1, 1]$ or $[2]$ and $c_n = \frac{1}{2}$.

In particular

$$\frac{1}{4} 3^{\frac{n-1}{3}} \leq c_n \leq \frac{1}{2} 3^{n/3} < 7^{\min\{n/5, n/2-1\}}.$$

Proof. Let $n = mk$ and let

$$\lambda_m = [\underbrace{1, \dots, 1}_{m_1}, \underbrace{2, \dots, 2}_{m_2}, \underbrace{3, \dots, 3}_{m_3}, \dots]$$

be a partition of m for which $c_m = c_{\lambda_m}$ and set $\ell := \ell_{\lambda_m}$. Now let λ be the partition of n achieved by joining k copies of λ_m together. We have

$$c_{\lambda_m} = \frac{|1^{m_1} 2^{m_2} 3^{m_3} \dots|_{2'}}{2^\ell}, \text{ and}$$

$$c_\lambda = \frac{|1^{km_1} 2^{km_2} 3^{km_3} \dots|_{2'}}{2^\ell} = (c_{\lambda_m})^k \cdot 2^{\ell k - \ell}$$

and (1) follows.

For (2) suppose that $n = r + s$, and let λ_r (resp. λ_s) be a partition of r (resp. s) for which $c_r = c_{\lambda_r}$ (resp. $c_s = c_{\lambda_s}$). Now let λ be the partition of n achieved by joining λ_r to λ_s ; then $c_\lambda \geq c_{\lambda_r} c_{\lambda_s}$.

We are left with (3). Suppose that λ is the partition of n which is defined by (2) and for which $c_\lambda = c_n$.

Suppose that $1n_1 + 2n_2 + 3n_3 \geq 3$. Consider the partition, λ_0 , obtained by removing all occurrences of 1, 2 and 4 and instead inserting as many 3's as possible, along with either zero, one or two 1's. Now compare c_λ and c_{λ_0} : it is clear that the numerator of c_{λ_0} is at least three times as large as the

numerator of c_λ . On the other hand $\ell_{\lambda_0} \leq \ell_\lambda + 1$. We conclude that $c_{\lambda_0} \geq c_\lambda$. This is a contradiction, hence we may assume that $1n_1 + 2n_2 + 4n_4 < 3$,

Now suppose that $n_k > 0$ for some $k > 4$ and set $m := kn_k$. Consider the partition λ_1 , obtained by removing all occurrences of k and instead inserting as many 3's as possible, along with either zero, one or two 1's. We compare c_λ and c_{λ_1} as before. As before $\ell_{\lambda_1} \leq \ell_\lambda + 1$. Thus $c_{\lambda_1} > c_\lambda$ unless

$$\begin{aligned} \frac{1}{2}3^{\frac{m-2}{3}} &\leq k^{m/k} \\ \iff \frac{1}{2}e^{\frac{(\log 3)(m-2)}{3}} &\leq e^{m(\frac{\log k}{k})} \\ \iff \frac{(\log 3)(m-2)}{3 \log 2} &< m\left(\frac{\log k}{k}\right) \\ \implies m < k \text{ or } m &\leq 5. \end{aligned}$$

Since $m \geq k$ by definition, we conclude that, unless $m = k = 5$, $c_{\lambda_1} > c_\lambda$ which is a contradiction. Thus by repeating this step (and the previous if necessary) we conclude that $\lambda = 1^{n_1}2^{n_2}3^{n_3}5^{n_5}$ where $n_1 + 2n_2 \leq 2$ and $n_5 \leq 1$.

Suppose, next, that $n_5 = 1$ and $n_1 + n_2 > 0$. Consider the partition λ_2 , obtained by removing the 5 and one of the numbers less than 3, and instead inserting two 3's, along with either zero or one 1. We compare c_{λ_2} and c_λ : it is clear that the numerator of c_{λ_2} is strictly larger than that of c_λ , while the denominator is unchanged. This is a contradiction, and we conclude that if $n_5 = 1$, then $n_1 + n_2 = 0$.

Suppose, finally, that $n_3 > 0$ and $n_1 + 2n_2 = 2$. Consider the partition λ_3 , obtained by removing a 3 and the numbers less than 3, and instead inserting a 5. We compare c_{λ_3} and c_λ : it is clear that the numerator of c_{λ_3} is strictly larger than that of c_λ , while the denominator is either smaller or the same. This is a contradiction, and so we conclude that if $n_3 > 0$ then $n_1 + 2n_2 \leq 1$.

The result follows. \square

Lemma 3.17. *Suppose $H < GL_n(q)$ where $q = p^f$ and $p \geq 7$. If H has odd order then $|H|_{p'} < q^n c_n$.*

Proof. The result is immediate for $n = 1$. Lemma 3.7 implies that, for $n = 2$, $|H|_{p'} < q + 1$ and the result follows. For $n > 2$, we refer to Lemma 3.9. Note that H cannot lie in Case 3 by the Feit-Thompson theorem; Case 1 is also impossible and the result is immediate in Case 5. If H lies in Case 4 then $n = 4$ and $H \leq GO_4^+(q)$; then $|H|_{p'} \leq \frac{1}{2}(q-1)|H \cap \Omega_4^+(q)|_{p'}$. Now $\Omega_4^+(q) \cong SL_2(q) \circ SL_2(q)$ and, again, Lemma 3.7 implies that $|H \cap \Omega_4^+(q)|_{p'} < (q+1)^2$. Thus $|H|_{p'} < \frac{1}{2}(q-1)(q+1)^2$ and we are done.

We are left with the possibility that H lies in Case 2. We proceed by induction; the base case, $n = 1$, is already done. Now assume inductively that the statement is true for $H < GL_m(q)$ where $m < n$.

If H lies in Case 5 then $H \leq GL_m(q) \circ GL_m(q)$. Induction implies that

$$|H|_{p'} < (q^m c_m)^2 \leq q^{2m} (c_m)^2 < q^{m^2} (c_m)^2.$$

Now Lemma 3.16 (2) yields the result.

Now consider Case 2. First observe that if $H \leq M \in \mathcal{C}_5(GL_n(q))$ then $M = GL(n, q_0) \circ Z(GL(n, q))$ where $q = q_0^a$. Then it is sufficient to prove the result for $H \cap GL_n(q_0)$ considered as a subgroup of $GL_n(q_0)$. Thus we assume that H does not lie in a maximal subgroup of type 5.

If H lies in a parabolic subgroup of $GL_n(q)$ then $H/O_p(H) < GL_m(q) \times GL_{n-m}(q)$. Induction implies that

$$|H|_{p'} < q^m c_m \times c^{n-m} c_{n-m}.$$

Now Lemma 3.16 (2) yields the result.

If $H \leq M \in \mathcal{C}_4(GL_n(q))$ then $M = (GL_r(q) \circ GL_s(q))$ for $n = rs$ with $2 \leq r < s$. Induction implies that

$$|H|_{p'} < q^r c_r q^s c_s = q^{r+s} c_r c_s.$$

Lemma 3.16 (2) yields the result.

If $H \leq M \in \mathcal{C}_2(GL_n(q))$ then $M = GL_m(q) \wr S_t$ where $n = mt, t \geq 2$. We assume that H acts transitively on the m -space decomposition otherwise H lies in a parabolic subgroup. In fact we assume that H acts primitively on the m -space decomposition since otherwise H lies in a maximal subgroup $M_1 = GL_{m_1}(q) \wr S_{t_1}$, $M_1 \in \mathcal{C}_2(GL_n(q))$ with $t_1 < t$ and H acts primitively on this decomposition.

Induction and Lemma 3.15 imply that

$$|H|_{p'} < (q^m c_m)^t 2^{t-1}.$$

Lemma 3.16 (1) yields the result.

If $H \leq M \in \mathcal{C}_3(GL_n(q))$ then $M = GL_m(q^r).r$ where $n = mr$ and r is a prime. Induction implies that

$$|H|_{p'} < ((q^r)^m) c_m.r = q^n c_m |r|_{2'}.$$

If $r = 2$, then it is enough to check that $c_m \leq c_{2m}$ which is easy using the formulae given in Lemma 3.16 (3). If $r \geq 3$, then one can check the result directly using Lemma 3.16 (3). \square

It is worth combining results of the two previous lemmas to give the following immediate corollary that will be used repeatedly. (The corollary is a weak version of Proposition 1.3 which was stated in the introduction.)

Corollary 3.18. *Suppose H is an odd order subgroup of $GL_n(q)$ where $q = p^f, p \geq 7$ and $n \geq 2$. Then $|H|_{p'} < q^{\frac{3}{2}n-1}$.*

Lemma 3.19. *Let H be an odd order subgroup of $GL_n(q)$ and let σ be an involutory field automorphism of $GL_n(q)$. Suppose that H is normalized by g , an involution in $\langle GL_n(q), \sigma \rangle \backslash GL_n(q)$. Then*

$$|H : C_H(g)|_{p'} \leq q^{n-\frac{1}{2}} + q^{n-1} + \cdots + q + q^{\frac{1}{2}} + 1.$$

Proof. Note that, by [GLS94, Proposition 4.9.1], we know that g is $GL_n(q)$ -conjugate to σ or $(-I, \sigma)$, hence we take H to be normalized by σ . Observe that $C_{Z(G)}(g) = (\sqrt{q}-1)$ (which yields the result for $n = 1$) and that $q \geq 49$.

For $n = 2$, it is clear that $|H : C_H(g)|_{p'} < (\sqrt{q} + 1)k$ where $k = \max\{|H_1|_{p'} : H_1 \in \text{PSL}_2(q)\}$; we refer to Lemma 3.7, and the statement follows immediately.

For $n > 2$ we refer to Corollary 3.5, and observe that Cases 1 and 4 are impossible. If we are in Case 5 then $n = 4$ and $H \leq GO_4^+(q)$. Now $\Omega_4^+(q) \cong SL_2(q) \circ SL_2(q)$; thus Lemma 3.7 implies that $|H \cap \Omega_4^+(q)|_{p'} < (q+1)^2$ which yields the result immediately.

Suppose next that we are in Case 2 or 3. In particular suppose first that, either Case 3 holds, or $H \leq M \in \mathcal{C}_i(\langle GL_n(q), \sigma \rangle)$ for $i = 6, 7$. Then Lemma 3.9 implies that $M = (GL_n(q) \circ GL_n(q)).(\langle \sigma \rangle \times 2)$ and $H < N = GL_{\sqrt{n}}(q) \circ GL_{\sqrt{n}}(q)$. N is normalized in $GL_n(q)$ by τ , an involution which swaps the two copies of $GL_{\sqrt{n}}(q)$. Thus g may take two forms.

Firstly suppose that $g = (A, B)\sigma$ where $A, B \in GL_{\sqrt{n}}(q)$. Now N contains two normal subgroups isomorphic to $GL_{\sqrt{n}}(q)$ that are normalized by g and, by [BGL77, Proposition 1.1], there is only one class of involutions in each copy of $\langle GL_{\sqrt{n}}(q), g \rangle$. Then, by induction,

$$|H : C_H(\sigma)|_{p'} \leq (q^{\sqrt{n}-\frac{1}{2}} + \cdots + q + q^{\frac{1}{2}} + 1)^2 < q^{n-\frac{1}{2}} + q^{n-1} + \cdots + q + q^{\frac{1}{2}} + 1.$$

Secondly suppose that $g = (A, B)\tau\sigma$. Since g is an involution, $B = \pm A^{-\sigma}$. Then, for $(X, Y) \in N$,

$$(X, Y)^g = (AY^\sigma A^{-1}, A^{-\sigma} X^\sigma A^\sigma).$$

Thus (X, Y) will be centralized by g if and only if $X = AY^\sigma A^{-1}$. Thus $|N : C_N(g)| = |GL_{\sqrt{n}}(q)|$ and so

$$|H : C_H(g)|_{p'} \leq |GL_{\sqrt{n}}(q)|_{p'} < q^{\frac{\sqrt{n}(\sqrt{n}+1)}{2}}$$

and the result follows.

We are left with the possibility that $H \leq M \in \mathcal{C}_i(\langle GL_n(q), \sigma \rangle)$ for $i = 1, \dots, 5$. In this case we proceed by induction; the base case has already been attended to.

If $M \in \mathcal{C}_5(\langle GL_n(q), \sigma \rangle)$, then $|H|_{p'} < q|H_0|_{p'}$, where H_0 is an odd order subgroup of $GL_n(q_0)$ where $q = q_0^a$ for some integer $a > 1$. Then Corollary 3.18 implies that

$$|H|_{p'} \leq q|H_0|_{p'} < q^{\frac{n+\sqrt{n}}{2}+1}$$

and the result follows.

If $M \in \mathcal{C}_1(\langle GL_n(q), \sigma \rangle)$, then let $O_p(M)$ be the largest normal p -group of M and let $L = H/(H \cap O_p(M))$. Then

$$|H : C_H(g)|_{p'} = |L : C_L(g_L)|_{p'}$$

for some involution $g_L \in L$. Now $L \leq \mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q)$ and we apply induction:

$$\begin{aligned} |H : C_H(g)|_{p'} &< (q^{m-\frac{1}{2}} + \cdots + q^{\frac{1}{2}} + 1)(q^{n-m-\frac{1}{2}} + \cdots + q^{\frac{1}{2}} + 1) \\ &< q^{n-\frac{1}{2}} + q^{n-1} + \cdots + q + q^{\frac{1}{2}} + 1. \end{aligned}$$

A similar approach can be taken if $M \in \mathcal{C}_4(\langle \mathrm{GL}_n(q), \sigma \rangle)$. Then $M \cong (\mathrm{GL}_m(q) \circ \mathrm{GL}_t(q)) \langle \sigma \rangle$ for $n = mt$ and, once more, induction gives the result.

Now suppose that $M \in \mathcal{C}_3(\langle \mathrm{GL}_n(q), \sigma \rangle)$, so $M \cong (\mathrm{GL}_{\frac{n}{r}}(q^r).r) \langle \sigma \rangle$ with r prime. If $r = 2$, then any element from $\langle \mathrm{GL}_n(q), \sigma \rangle \setminus \mathrm{GL}_n(q)$ which normalizes M will act as a field automorphism of order 4 on $\mathrm{GL}_{\frac{n}{r}}(q^r)$. In particular such an element cannot be an involution. On the other hand if r is odd then $\langle M, \sigma \rangle \cong \mathrm{GL}_{\frac{n}{r}}(q^r).2r$ and g acts as an involutory field automorphism on $\mathrm{GL}_{\frac{n}{r}}(q^r)$. Then Lemma 2.1 implies that

$$|H : C_H(g)|_{p'} = |H \cap \mathrm{GL}_{\frac{n}{r}}(q^r) : C_{H \cap \mathrm{GL}_{\frac{n}{r}}(q^r)}(g)|_{p'}$$

and induction gives the result.

Finally consider the possibility that $M \in \mathcal{C}_2(\langle \mathrm{GL}_n(q), \sigma \rangle)$. Thus $H < \langle (\mathrm{GL}_m(q) \wr S_t), \sigma \rangle$ with $t \geq 2$. Just as for Lemma 3.17, we assume that $\langle H, \sigma \rangle$ acts primitively on the m -space decomposition. Take $g = s\sigma$ and note that s acts as a (possibly trivial) involution on the m -space decomposition.

We need to consider two situations which closely mirror the two cases discussed for \mathcal{C}_7 . First consider $C_S(g)$ where S is the projection of H onto a particular $\mathrm{GL}_m(q)$ that is fixed by s . By induction $|S : C_S(g)|_{p'} < q^{m-\frac{1}{2}} + \cdots + q^{\frac{1}{2}} + 1$. Alternatively if $\mathrm{GL}_m(q) \times \mathrm{GL}_m(q)$ are swapped by s , and S is the projection of H onto $\mathrm{GL}_m(q) \times \mathrm{GL}_m(q)$ then it is clear that $|S : C_S(g)|_{p'}$ is at most the size of an odd-order subgroup in $\mathrm{GL}_m(q)$. Thus, by Corollary 3.18, this is bounded above by $q^{\frac{3m-2}{2}}$.

Now write $N = \underbrace{\mathrm{GL}_m(q) \times \cdots \times \mathrm{GL}_m(q)}_t$. Then Lemma 2.1 implies that

$$|H : C_H(g)| = |H \cap N : C_{H \cap N}(g)| |H/N : C_{H/N}(gN)|.$$

Thus, writing s as the product of k transpositions in its action on the m -space decomposition, we have

$$\begin{aligned} |H \cap N : C_{H \cap N}(g)|_{p'} &< (q^{m-\frac{1}{2}} + \cdots + q + 1)^{t-2k} \times (q^{\frac{3m-2}{2}})^k \\ &< \frac{(q^m - 1)^t}{\sqrt{q} - 1} \times \frac{1}{(\sqrt{q} - 1)^{t-1}}. \end{aligned}$$

If $t \geq 2$ then, referring to Lemma 3.14, it is sufficient to prove that $3.25^t < (\sqrt{q} - 1)^{t-1}$ which is true, since $\sqrt{q} \geq 7$. If $t = 2$ the result follows from the fact that

$$|H : C_H(g)|_{p'} = |H \cap N : C_{H \cap N}(g)|_{p'}.$$

□

Lemma 3.20. *Let $H < GL_n(q)$ with $|H|$ odd. Suppose that g is an involution in $GL_n(q)$ which normalizes H . Then,*

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Proof. We proceed by induction on n . When $n = 1$ the result is trivial and, when $n = 2$, Lemma 3.8 gives the result.

Now suppose that $n > 2$ and refer to Lemma 3.9 for the group $\langle H, g \rangle$. Clearly Cases 1 and 3 are not relevant here. If Case 4 or Case 5 holds then our result is implied by the strong version of Lemma A which we have already proved in these cases. In Case 6 the result is immediate. Thus we are left with Case 2: $\langle H, g \rangle \leq M \in \mathcal{C}_i(GL_n(q))$ for $i = 1, \dots, 5$.

If $M \in \mathcal{C}_5(GL_n(q))$ then we can assume that $\langle H, g \rangle \leq GL_n(q_0)$ where $q = q_0^a$. Then it is sufficient to prove the result over the base case. Thus we assume that $M \notin \mathcal{C}_5(GL_n(q))$.

If $\langle H, g \rangle \leq M \in \mathcal{C}_1(GL_n(q))$ then $\langle H, g \rangle \leq Q : (GL_m(q) \times GL_{n-m}(q))$ where $Q = O_p(M)$ and $m > 1$. Set $L = M/Q$ and observe that

$$|H : C_H(g)|_{p'} = |H_L : C_{H_L}(g_L)|_{p'}$$

where $H_L = HQ/Q \leq L$ and $g_L = gQ \in H_L$. Now suppose, without loss of generality, that $m \leq n - m$, and set $N = H_L \cap GL_m(q)$.

Lemma 2.1 implies that

$$|H_L : C_{H_L}(g_L)| = |N : C_N(g)| \times |H/N : C_{H/N}(g_L N)|.$$

Now H/N is isomorphic to a subgroup of $GL_{n-m}(q)$ and induction implies that

$$|H/N : C_{H/N}(g_L N)|_{p'} \leq q^{n-m-1} + \cdots + q + 1.$$

Then g_L normalizes N and g_L either centralizes N or else $\langle g_L, N \rangle$ is isomorphic to a subgroup of $GL_m(q)$. Either way induction implies that

$$|H_L : C_{H_L}(g_L)|_{p'} \leq q^{m-1} + \cdots + q + 1,$$

as required.

If $\langle H, g \rangle \leq M \in \mathcal{C}_3(GL_n(q))$ then $\langle H, g \rangle \leq M = GL_m(q^r).r$ where $n = mr$ and r is prime. Let $N = GL_m(q^r)$ be normal in M and split into two cases. Suppose first that $|\langle H, g \rangle \cap N|$ is even. Then induction implies that

$$|H : C_H(g)|_{p'} \leq ((q^r)^{m-1} + \cdots + q + 1)r < q^{mr-1} + \cdots + q + 1$$

as required. Suppose on the other hand that $|H \cap N|$ is odd. Then $r = 2$ and Lemma 3.19 gives the result.

If $\langle H, g \rangle \leq M \in \mathcal{C}_4(GL_n(q))$ then $M \cong GL_{n_1}(q) \circ GL_{n_2}(q)$ where $n = n_1 n_2$ and $1 < n_1 < n_2$. Proceed similarly to the case \mathcal{C}_1 , observing that M has normal subgroups isomorphic to both $GL_{n_1}(q)$ and $GL_{n_2}(q)$; thus we define $N = H \cap GL_{n_1}(q)$. Suppose first that N has even order and take g to be an involution in N . Then Lemma 2.2 implies that, if P is a Sylow 2-subgroup

of N_i then

$$|H : C_H(g)| = |N : C_N(g)| \frac{|g^H \cap P|}{|g^N \cap P|} = |N : C_N(g)|.$$

By induction

$$|N : C_N(g)|_{p'} \leq q^{n_1-1} + \cdots + q + 1$$

and we are done. Suppose, on the other hand, that N has odd order. In particular this means that $H \cap Z(M)$ has order z , an odd number. Now Lemma 2.1 implies that, for g an involution in H ,

$$|H : C_H(g)| = |N : C_N(g)| \times |H/N : C_{H/N}(gN)|.$$

Observe that H/N is a subgroup of $\text{PGL}_{n_2}(q)$. Let H_X be the subgroup of $\text{GL}_{n_1}(q) \times \text{GL}_{n_2}(q)$ such that $H_X \cap Z(\text{GL}_{n_1}(q) \times \text{GL}_{n_2}(q)) \cong z \times z$, and such that $\pi(H_X) = H$ where π is the natural map,

$$\pi : \text{GL}_{n_1}(q) \times \text{GL}_{n_2}(q) \rightarrow \text{GL}_{n_1}(q) \circ \text{GL}_{n_2}(q).$$

Let $g_X \in H_X$ be the unique involution for which $\pi(g_X) = g$. Let g_2 (resp. H_2) be the image of g_X (resp. H_X) under the natural projection $\text{GL}_{n_1}(q) \times \text{GL}_{n_2}(q) \rightarrow \text{GL}_{n_2}(q)$. Observe that $H_2/(H_2 \cap Z(\text{GL}_{n_2}(q))) \cong H/N$. By induction

$$|H_2 : C_{H_2}(g_2)|_{p'} \leq q^{n_2-1} + \cdots + q + 1,$$

$$|N : C_N(g)|_{p'} \leq q^{n_1-1} + \cdots + q + 1$$

and the result follows.

Finally if $M \in \mathcal{C}_2(\text{GL}_n(q))$ then $\langle H, g \rangle < \text{GL}_m(q) \wr S_t$ where $n = mt$. Set $N = \underbrace{\text{GL}_m(q) \times \cdots \times \text{GL}_m(q)}_t$. We assume that N/H acts primitively on

the t copies of $\text{GL}_m(q)$ as otherwise H lies in a maximal subgroup $M_1 = \text{GL}_{m_1}(q) \wr S_{t_1}$, $M_1 \in \mathcal{C}_2(\text{GL}_n(q))$ with $t_1 < t$ such that H acts primitively on this decomposition.

If $g \in N$ then induction implies that $|H \cap N : C_{H \cap N}(g)|_{p'} < \frac{(q^m-1)^t}{q-1}$. Lemma 3.14 implies that $|H/N| < \frac{1}{\sqrt{24}} t^{3.25}$ which is sufficient unless $t = 2$, when the result is immediate.

If $g \in H \setminus N$, then we proceed very similarly to the proof of Lemma 3.19. First consider $C_S(g)$ where S is the projection of H onto a particular $\text{GL}_m(q)$ that is fixed by g . By induction $|S : C_S(g)|_{p'} < q^{m-1} + \cdots + q + 1$. Alternatively if $\text{GL}_m(q) \times \text{GL}_m(q)$ are swapped by g , and S is the projection of H onto $\text{GL}_m(q) \times \text{GL}_m(q)$ then it is clear that $|S : C_S(g)|_{p'}$ is at most the size of an odd-order subgroup in $\text{GL}_m(q)$.

If $m > 1$, then, by Corollary 3.18, this is bounded above by $q^{\frac{3m-2}{2}}$. Thus, for $m > 1$, $|H \cap N : C_{H \cap N}(g)|_{p'} < (q^{m-1} + \cdots + q + 1)^t$. As before, Lemma 3.14 yields the result.

If $g \in H \setminus N$ and $m = 1$ then it is clear that $|C_{H \cap N}(g)| > (q-1)^{\lceil \frac{n}{2} \rceil}$ and so $|H \cap N : C_{H \cap N}(g)|_{p'} \leq \left(\frac{q-1}{2}\right)^{\frac{n}{2}}$. It is therefore sufficient to prove that $|H/N|_{p'} < (2(q-1))^{\frac{n}{2}-1}$. Again Lemma 3.14 implies that $|H/N| \leq \frac{1}{\sqrt{24}} n^{3.25}$

and the result follows for $n \geq 6$. If $n = 5$ (resp. $n \leq 4$), then $|H/N|_{p'} \leq 5$ (resp. $|H/N|_{p'} \leq 3$) and the result follows immediately. \square

Lemma 3.21. *Let $H < GL_n(q)$ with $|H|$ odd. Let σ be a field automorphism of $GL_n(q)$ satisfying $\sigma^2 = 1$. Suppose that K is a 2-group in $\langle GL_n(q), \sigma \rangle$ which normalizes H . Then*

$$|H : C_H(g)|_{p'} \cdot |H : C_H(h)|_{p'} < q^{\frac{3n}{2}} c_n$$

for distinct involutions $g, h \in K$.

Note that if q is not square then $\langle GL_n(q), \sigma \rangle = GL_n(q)$. Note too that c_n was defined on p. 24 immediately before Lemma 3.16.

Proof. If $n = 1$, the result is immediate. If $n = 2$, then we must show that

$$|H : C_H(g)|_{p'} \cdot |H : C_H(h)|_{p'} < \frac{1}{2} q^3.$$

Lemma 3.8 implies that there exists g such that

$$|H : C_H(g)|_{p'} < q + 1.$$

Now Lemma 3.7 implies that $|H|_{p'} < \frac{1}{4}(q-1)^2$ and the result follows.

Now take $n \geq 3$ and consider $\langle H, K \rangle$ as a subgroup of $\langle GL_n(q), \sigma \rangle$ and refer to Corollary 3.5. We consider the five cases listed there; observe first that Case 4 is impossible. Consider Case 1 next: $\langle H, K \rangle$ contains Ω . Then, since $\langle H, K \rangle$ is soluble this implies that $n = 1$ which has been covered.

Now consider Case 5: we lie in the small rank setting. We have dealt with $n = 2$ hence we are left with $n = 4$ and $H < GO_4^+(q) \cong Z(SL_2(q) \circ SL_2(q)).4$; then $|H|_{p'} \leq \frac{1}{16}(q-1)(q+1)^2$ and we are done.

We move on to Case 3 which we expand to cover $H \leq M \in \mathcal{C}_6(\Delta_\eta)$ for η non-degenerate or zero. Now it is just a matter of checking that $(|M|_{p'})^2 < c_n q^n$ and the result follows immediately.

We are left with Case 2 or, more precisely, with the possibility that $\langle H, K \rangle \leq M_1 \in \mathcal{C}_i(\langle GL_n(q), \sigma \rangle)$ for some $i = 1, \dots, 5, 7$. Then $H \leq M \in \mathcal{C}_i(GL_n(q))$ for some $i = 1, \dots, 5, 7$. Clearly if $M \in \mathcal{C}_5(GL_n(q))$ then it is sufficient to prove the result for $H \cap M$ taking the place of H .

If $M \in \mathcal{C}_7(GL_n(q))$ then $M \cong (GL_m(q) \circ \dots \circ GL_m(q)).S_t$ with $n = m^t$ and $m \geq 3$. We can assume, as usual, that the action of S_t in the wreath product is primitive and now Lemma 3.15 and Corollary 3.18 imply that

$$|H|_{p'} < (q^{\frac{3m-2}{2}})^t 2^{t-1}.$$

This yields the result immediately.

We are left with the possibility that $H \leq M \in \mathcal{C}_i(GL_n(q))$ for some $i = 1, \dots, 4$ and we proceed by induction. If $M \in \mathcal{C}_1(GL_n(q))$ or $M \in \mathcal{C}_4(GL_n(q))$, then the result is immediate using induction and Lemma 2.1, since in this case $M/O_p(M)$ is isomorphic to $GL_m(q) \times GL_{n-m}(q)$ or $GL_m(q) \circ GL_{\frac{n}{m}}(q)$.

If $M \in \mathcal{C}_3(GL_n(q))$, then we have $M \cong GL_{\frac{n}{r}}(q^r).r$ where r is prime. If $r = 2$ then no involutory field automorphism of $GL_n(q)$ normalizes M hence

we $\langle H, K \rangle$ is isomorphic to a subgroup of $GL_{\frac{n}{r}}(q^r)$ and the result follows by induction.

Suppose, then, that r is odd and set $m := \frac{n}{r}$ and $H_1 := H \cap GL_m(q^r)$. Observe that $K \leq H_1$. Consider the case when $m = 1$. Then M does not contain a Klein 4-group, so we have a contradiction. If $m = 2$, then $M \cong GL_2(q^r)$. Note that any Klein 4-subgroup of $GL_2(q^r)$ intersects $Z(GL_2(q^r))$ non-trivially. Thus Lemma 3.20 implies that

$$|H : C_H(g)|_{p'} \cdot |H : C_H(h)|_{p'} \leq r^2(q^{n-1} + \dots + q + 1)$$

and the result follows.

If $m \geq 2$, then we apply induction to conclude that

$$|H_1 : C_{H_1}(g)|_{p'} \cdot |H_1 : C_{H_1}(h)|_{p'} < q^{\frac{3n}{2}} c_m$$

and so

$$|H : C_H(g)|_{p'} \cdot |H : C_H(h)|_{p'} < q^{\frac{3n}{2}} c_m r^2.$$

Now one can check, using the formulae given at Lemma 3.16 (3), that $c_n > c_m r^2$ and the result follows.

Finally assume that $H \leq M \in \mathcal{C}_2(GL_n(q))$. Then $M \cong GL_m(q) \wr S_t$. Write N for the normal subgroup of M isomorphic to $\underbrace{GL_m(q) \times \dots \times GL_m(q)}_t$

and let $H_1 = \langle H, K \rangle \cap N$; we may assume as usual that $\langle H, K \rangle / H_1$ acts primitively in the natural action on t copies of $GL_m(q)$.

Consider the action of $K = \langle g, h \rangle$ on the t copies of $GL_m(q)$; suppose that K has an orbit of length $t_1 > 1$ (note that t_1 is even). Then K normalizes $H_2 = H \cap \underbrace{(GL_m(q) \times \dots \times GL_m(q))}_{t_1}$ and we consider the induced action of

K_1 on a set of size t_1 ; we can assume that g is a product of $\frac{t_1}{2}$ transpositions, while h is a product of either $\frac{t_1}{2} - 1$ or $\frac{t_1}{2}$ transpositions. Lemma 3.17 implies that

$$|H_2 : C_{H_2}(g)|_{p'} \leq (q^m c_m)^{\frac{t_1}{2}};$$

similarly Lemmas 3.17, 3.19 and 3.20 imply that

$$|H_2 : C_{H_2}(h)|_{p'} \leq (q^m c_m)^{\frac{t_1}{2}-1} q^{2m}$$

which implies, in particular, that

$$|H_2 : C_{H_2}(g)|_{p'} \cdot |H_2 : C_{H_2}(h)|_{p'} \leq (q^{\frac{3m}{2}})^{t_1} c_m^{t_1}.$$

If K_1 has an orbit of length 1 then K_1 normalizes $H_3 = H \cap GL_m(q)$, for a particular copy of $GL_m(q)$. We apply induction to conclude that

$$|H_3 : C_{H_3}(g)|_{p'} \cdot |H_3 : C_{H_3}(g)|_{p'} \leq q^{\frac{3m}{2}} c_m.$$

Putting these results together we conclude that

$$|H_1 : C_{H_1}(g)|_{p'} \cdot |H_1 : C_{H_1}(g)|_{p'} \leq q^{\frac{3tm}{2}} (c_m)^t.$$

Now $|H/(H \cap N)| < 2^{t-1}$ and so, by Lemma 3.16,

$$|H : C_H(g)|_{p'} \cdot |H : C_H(g)|_{p'} \leq q^{\frac{3tm}{2}} (c_m)^t 2^{t-1} < q^{\frac{3n}{2}} c_n$$

as required. \square

3.6. Case 2. We are now ready to prove Lemma A for H satisfying Case 2 of Lemma 3.9, i.e. for $H \leq M \in \mathcal{C}_i(\mathrm{GL}_n(q))$, for $i = 1, \dots, 5$. (See p.3 for the statement of Lemma A.) If $M \in \mathcal{C}_5(\mathrm{GL}_n(q))$ then $M = \mathrm{GL}_n(q_0)Z(\mathrm{GL}_n(q))$ and it is enough to prove the result for $H \cap \mathrm{GL}_n(q_0) \leq \mathrm{GL}_n(q_0)$. We exclude this case and, for the rest, suppose that Lemma A holds for $m < n$, i.e. we proceed under the following hypothesis:

Inductive Hypothesis. *Let H_1 be an even order subgroup of $\mathrm{GL}_m(q)$ with $m < n$. Then H_1 contains an involution g such that $|H_1 : C_{H_1}(g)|_{p'} \leq q^{m-1} + \dots + q + 1$.*

Lemma 3.22. *If H has even order and $H \leq M \in \mathcal{C}_i(\mathrm{GL}_n(q))$ with $i = 1, 3$, or 4, then H contains an involution g such that*

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \dots + q + 1.$$

Proof. If $H \leq M \in \mathcal{C}_1(\mathrm{GL}_n(q))$ then $H \leq Q : (\mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q))$ where $Q = O_p(M)$ and $m > 1$. Set $L = M/Q$ and observe that, for any $g \in H$,

$$|H : C_H(g)|_{p'} = |H_L : C_{H_L}(g_L)|_{p'}$$

where H_L is a subgroup of L and g_L is an involution in H_L . Now suppose, without loss of generality, that $m \leq n - m$, and set $N = H_L \cap \mathrm{GL}_m(q)$.

Suppose that N has odd order. Lemma 2.1 implies that

$$|H_L : C_{H_L}(g_L)| = |N : C_N(g)| \times |H_L/N : C_{H_L/N}(g_L N)|.$$

Now H/N is isomorphic to a subgroup of $\mathrm{GL}_{n-m}(q)$ and induction implies that we can choose g_L such that

$$|H/N : C_{H/N}(g_L N)|_{p'} \leq q^{n-m-1} + \dots + q + 1.$$

Then g_L normalizes N and g_L either centralizes N or else $\langle g_L, N \rangle$ is isomorphic to a subgroup of $\mathrm{GL}_m(q)$. Either way, since N has odd order, $\langle g_L, N \rangle$ has at most one conjugacy class of involutions, and induction implies that

$$|H_L : C_{H_L}(g_L)|_{p'} \leq q^{m-1} + \dots + q + 1,$$

as required. If, on the other hand, N has even order then Lemma 2.2 implies that, for $g_L \in N$,

$$|H_L : C_{H_L}(g_L)| \leq |N : C_N(g_L)| \times \frac{|g_L^{H_L} \cap P|}{|g_L^N \cap P|}$$

where P is a Sylow 2-subgroup of N . By induction we can choose g_L so that

$$|N : C_N(g_L)|_{p'} \leq q^{m-1} + \dots + q + 1.$$

Furthermore Lemma 2.6 implies that

$$\frac{|g_L^{H_L} \cap P|}{|g_L^N \cap P|} < 3.04^m < q^{m-1} + \cdots + q + 1.$$

Since $m \leq n - m$ the result follows.

If $H \leq M \in \mathcal{C}_3(\mathrm{GL}_n(q))$ then $H \leq M = \mathrm{GL}_m(q^r).r$ where $n = mr$ and r is prime. Let $N = \mathrm{GL}_m(q^r)$ be normal in M and split into two cases. Suppose first that $|H \cap N|$ is even. Then induction implies that $H \cap N$ contains an involution g such that

$$|H : C_H(g)|_{p'} \leq ((q^r)^{m-1} + \cdots + q + 1)r < q^{mr-1} + \cdots + q + 1$$

as required. Suppose on the other hand that $|H \cap N|$ is odd. Then $r = 2$ and Lemma 3.19 gives the result.

If $H \leq M \in \mathcal{C}_4(\mathrm{GL}_n(q))$ then $M \cong \mathrm{GL}_{n_1}(q) \circ \mathrm{GL}_{n_2}(q)$ where $n = n_1 n_2$ and $1 < n_1 < n_2$. Proceed similarly to the case \mathcal{C}_1 , observing that M has normal subgroups isomorphic to both $\mathrm{GL}_{n_1}(q)$ and $\mathrm{GL}_{n_2}(q)$; thus we define $N = H \cap \mathrm{GL}_{n_1}(q)$. Suppose first that N has even order and take g to be an involution in N . Then Lemma 2.2 implies that

$$|H : C_H(g)| = |N : C_N(g)| \frac{|g^H \cap P|}{|g^N \cap P|}$$

where P is a Sylow 2-subgroup of N . By induction we can choose g so that

$$|N : C_N(g)|_{p'} \leq q^{n_1-1} + \cdots + q + 1.$$

Furthermore Lemma 2.6 implies that

$$\frac{|g^H \cap P|}{|g^N \cap P|} < 3.04^{n_1} < q^{n_1-1} + \cdots + q + 1,$$

and the result follows.

Suppose, on the other hand, that N has odd order. In particular this means that $H \cap Z(M)$ has order z , an odd number. Now Lemma 2.1 implies that, for g an involution in H ,

$$|H : C_H(g)| = |N : C_N(g)| \times |H/N : C_{H/N}(gN)|.$$

Observe that H/N is a subgroup of $\mathrm{PGL}_{n_2}(q)$. Let H_X be the subgroup of $\mathrm{GL}_{n_1}(q) \times \mathrm{GL}_{n_2}(q)$ such that $H_X \cap Z(\mathrm{GL}_{n_1}(q) \times \mathrm{GL}_{n_2}(q)) \cong z \times z$, and such that $\pi(H_X) = H$ where π is the natural map,

$$\pi : \mathrm{GL}_{n_1}(q) \times \mathrm{GL}_{n_2}(q) \rightarrow \mathrm{GL}_{n_1}(q) \circ \mathrm{GL}_{n_2}(q).$$

Let H_2 be the image of H_X under the natural projection $\mathrm{GL}_{n_1}(q) \times \mathrm{GL}_{n_2}(q) \rightarrow \mathrm{GL}_{n_2}(q)$. Observe that $H_2/(H_2 \cap Z(\mathrm{GL}_{n_2}(q))) \cong H/N$. By induction there exists an involution $g_2 \in H_2$ such that

$$|H_2 : C_{H_2}(g_2)|_{p'} \leq q^{n_2-1} + \cdots + q + 1.$$

Let g_X be an involution and preimage of g_2 in H_X ; define $g = \pi(g_X)$, an involution in H . Observe that

$$|H/N : C_{H/N}(gN)| = |H_2 : C_{H_2}(g_2)|_{p'} \leq q^{n_2-1} + \cdots + q + 1.$$

Furthermore either g centralizes N or else $\langle g, N \rangle$ is isomorphic to a subgroup of $\mathrm{GL}_{n_1}(q)$. Either way, induction implies that

$$|N : C_N(g)|_{p'} \leq q^{n_1-1} + \cdots + q + 1,$$

and the result follows. \square

3.6.1. $\mathcal{C}_2(\mathrm{GL}_n(q))$. The final case to consider is when $H \leq M \in \mathcal{C}_2(\mathrm{GL}_n(q))$. Then $M = \mathrm{GL}_m(q) \wr S_t, n = mt, t \geq 2$. Write

$$N = \underbrace{\mathrm{GL}_m(q) \times \cdots \times \mathrm{GL}_m(q)}_t.$$

We assume that M acts primitively on the associated decomposition of the associated vector space V into t subspaces of dimension m , since otherwise H lies in a maximal subgroup $M_1 = \mathrm{GL}_{m_1}(q) \wr S_{t_1}, M_1 \in \mathcal{C}_2(\mathrm{GL}_n(q))$ with $t_1 < t$ such that H acts primitively on this decomposition.

We need a result of Praeger and Saxl [PS80].

Lemma 3.23. *Let G be a primitive subgroup of the symmetric group S_n . Then G contains A_n or $|G| \leq 4^n$.*

An immediate corollary is the following:

Corollary 3.24. *Let G be a primitive subgroup of the symmetric group S_n . If $n \geq 5$, then G contains an involution g such that $|G : C_G(g)| \leq 5^{n-1}$.*

Proof. Lemma 3.23 implies that either $|H/H \cap N| \leq 4^n$ (which yields the result for $n \geq 8$) or $|H/H \cap N|$ contains the alternating group A_n .

If $H/H \cap N$ contains the alternating group A_n , then $H/H \cap N$ contains an involution g such that

$$|H/(H \cap N) : C_{H/(H \cap N)}(g(H \cap N))| < n^4.$$

Again this yields the result for $n \geq 8$. If $n < 8$, then $|S_n| = n! < 5^{n-1}$ and we are done. \square

Lemma 3.25. *Suppose that $H \cap N$ has odd order, H has even order, and $t < n$. Then H contains an involution g such that $|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1$.*

Proof. By Corollary 3.18,

$$|H \cap N|_{p'} < (q^{\frac{3m-2}{2}})^t.$$

Write $N = N_1 \times \cdots \times N_t$ where $N_i \cong \mathrm{GL}_m(q), i = 1, \dots, t$. Then, for g an involution in H , we can choose an ordering of the N_i so that g either normalizes N_i or swaps N_i with $N_{i\pm 1}$. Let H_i be the projection of H into N_i ; if g normalizes N_i then write g_i for the element of N_i induced by the

action of g . Since N is odd, $\langle g_i, H_i \rangle$ contains at most one conjugacy class of involutions and induction implies that

$$|H_i : C_{H_i}(g_i)|_{p'} \leq q^{m-1} + \cdots + q + 1.$$

If g swaps N_i and N_{i+1} then write $H_{i,i+1}$ for the projection of H into $N_i \times N_{i+1}$ (observe that the projection of H onto N_i is isomorphic to the projection of H onto N_{i+1}); write $g_{i,i+1}$ for the element of $N_i \times N_{i+1}$ induced by the action of g . Then Corollary 3.18 implies that

$$|H_{i,i+1} : C_{H_{i,i+1}}(g_{i,i+1})| \leq \sqrt{|H_{i,i+1}|} \leq q^{\frac{3m-2}{4}}.$$

Now write g as a product of k disjoint transpositions in its action upon the set $\{N_1, \dots, N_t\}$. Then

$$|H \cap N : C_{H \cap N}(g)|_{p'} \leq (q^{\frac{3m-2}{2}})^k (q^{m-1} + \cdots + q + 1)^{t-2k} \leq \frac{q^n - 1}{(q-1)^t}.$$

Now Lemma 2.1 implies that

$$|H : C_H(g)| = |H \cap N : C_{H \cap N}(g)| \times |H/(H \cap N) : C_{H/(H \cap N)}(g(H \cap N))|,$$

hence it is enough to prove that $H/(H \cap N)$ contains an involution h such that

$$|H/(H \cap N) : C_{H/(H \cap N)}(h)|_{p'} \leq (q-1)^{t-1}.$$

Corollary 3.24 yields the result. \square

We next consider the possibility that $H \cap N$ has odd order and $t = n$.

Lemma 3.26. *Suppose that $H \cap N$ has odd order and $t = n$. Then H contains an involution g such that $|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1$.*

Proof. Observe that $N = (q-1)^n$. First consider $C_S(g)$ where S is the projection of H onto a particular $q-1$ which is fixed by g . Clearly $|S : C_S(g)|_{p'} = 1$. Alternatively if $(q-1) \times (q-1)$ are swapped by g , and S is the projection of H onto $(q-1) \times (q-1)$ then it is clear that $|S : C_S(g)|_{p'} < \frac{q-1}{2}$. Thus, in all cases,

$$|N : C_N(g)|_{p'} < \left(\frac{q-1}{2}\right)^{\frac{n}{2}}.$$

Lemma 2.1 implies that it is sufficient to prove that H/N contains an involution h such that

$$|H/N : C_{H/N}(h)| \leq 2^{n/2}(q-1)^{n/2-1}.$$

Corollary 3.24 implies that H/N contains an involutions h such that

$$|H/N : C_{H/N}(h)| \leq 5^{n-1}$$

and this yields the result provided $q \geq 43$ and $n \geq 6$.

If $3 \leq n \leq 5$, then $|H/N| = 3$ and the result follows. If $n = 2$, then $|H/N| = 1$ and the result follows.

If $q < 43$ then $q = 7, 13, 19, 31$ or 37 . In all cases $|q - 1|_{p'} = 3$ and hence $|N : C_N(g)|_{p'} \leq 3$. Thus, by Lemma 2.1,

$$|H : C_H(g)|_{p'} \leq 3 \times 5^{n-1} \leq q^{n-1} + \cdots + q + 1.$$

This yields the result for $n \geq 6$ and we are done. \square

The final subcase is when $H \cap N$ has even order. We need a couple of classical theorems, the first is Glauberman's Z^* -theorem [Gla66].

Theorem 3.27. *Let x be an element of S , a Sylow 2-subgroup of a finite group K . Let $O(K)$ be the largest normal odd-order subgroup of K and let $Z^*(K)$ be the preimage of $Z(K/O(K))$ in K . Then $x \notin Z^*(G)$ if and only if there exists $y \in C_s(x) \setminus \{x\}$ such that y is conjugate to x in G .*

The second is (an easy consequence of) Alperin's fusion theorem (see [Gor68, p.244]).

Theorem 3.28. *Let g and h be elements of S , a Sylow t -subgroup of a finite group K . Suppose that $g^x = h$ for some $x \in K$. Then there exist elements x_i and Sylow t -subgroups Q_i of G , $1 \leq i \leq n$, and an element $y \in N_G(S)$ such that $x = x_1 \cdots x_n y$, $g \in P \cap Q_1$ and, for $i = 1, \dots, n$, $x_i \in N_G(P \cap Q_i)$ and $g^{x_1 x_2 \cdots x_i} \in P \cap Q_{i+1}$.*

Lemma 3.29. *Suppose that E is an elementary abelian 2-subgroup of $\mathrm{GL}_n(q)$ with q odd. Then $|E| \leq 2^n$.*

Proof. A commuting set of semisimple elements is the subset of a torus of $\mathrm{GL}_n(q)$. Since a torus is a direct product of at most n cyclic groups, the result follows. \square

We are ready to deal with the final subcase.

Lemma 3.30. *Suppose that $H \leq \mathrm{GL}_m(q) \wr S_t$ where $n = mt$. Write*

$$N = \underbrace{\mathrm{GL}_m(q) \times \cdots \times \mathrm{GL}_m(q)}_t.$$

Suppose that $H \cap N$ has even order. Then H contains an involution g such that

$$|H : C_H(g)|_{p'} \leq q^{n-1} + \cdots + q + 1.$$

Proof. Suppose first that $m = 1$. Then N contains at most 2^n involutions and so

$$|H : C_H(g)|_{p'} < 2^n \leq q^{n-1} + \cdots + q + 1,$$

as required. Assume now that $m > 1$.

Let V be the associated vector space for $\mathrm{GL}_n(q)$. Write $N = N_1 \times \cdots \times N_t$ with $N_i \cong \mathrm{GL}_m(q)$ for $i = 1, \dots, t$. Our analysis (and our notation) mirrors the set up in Lemma 2.3. Write L_i for the projection of $H \cap N$ onto $N_i \times \cdots \times N_t$ and write $\psi_i : L_i \rightarrow L_{i+1}$ for the natural projection. Let T_i be the kernel of ψ_i for $1 \leq i < t$; define $T_t := L_t$. Suppose that $|T_i|$ is odd for $i < k \leq t$ and $|T_i|$ is even for $i = k$.

Observe that $T_k \leq \text{GL}_m(q)$. Then, by induction, take an involution $g_k \in T_k$ such that

$$|T_k : C_{T_k}(g_k)|_{p'} \leq q^{m-1} + \cdots + q + 1.$$

Let $g \in G$ be an involution and pre-image of g_k in $H \cap N$ (such a pre-image must exist since $|T_i|$ is odd for $i < k$). Write g_i for the image of g under the projection of $H \cap N$ onto L_i . We proceed in stages:

- (1) **An upper bound for $|H \cap N : C_{H \cap N}(g)|_{p'}$.** Since $|T_i|$ is odd for $i < k$, $\langle T_i, g_i \rangle$ contains at most one conjugacy class of involutions, and induction implies that

$$|T_i : C_{T_i}(g_i)|_{p'} \leq q^{m-1} + \cdots + q + 1,$$

and Lemma 2.6 implies that $|(g_k)^{L_k} \cap P_k| < 2^{m+\frac{m}{2}-1}$ where P_k is a Sylow 2-subgroup of T_k . Furthermore Lemma 2.3 implies that

$$|H \cap N : C_{H \cap N}(g)|_{p'} = \prod_{i=1}^k |T_i : C_{T_i}(g_i)|_{p'} \frac{|(g_k)^{L_k} \cap P_k|_{p'}}{|(g_k)^{T_k} \cap P_k|_{p'}}.$$

(Note that if $k = t$ the final fraction is equal to 1.) Now combining these observations we obtain that

$$\begin{aligned} |H \cap N : C_{H \cap N}(g)|_{p'} &= \prod_{i=1}^k |T_i : C_{T_i}(g_i)|_{p'} \frac{|(g_k)^{L_k} \cap P_k|_{p'}}{|(g_k)^{T_k} \cap P_k|_{p'}} \\ &\leq (q^{m-1} + \cdots + q + 1)^k \frac{|(g_k)^{L_k} \cap P_k|_{p'}}{|(g_k)^{T_k} \cap P_k|_{p'}} \\ &\leq \begin{cases} (q^{m-1} + \cdots + q + 1)^k 2^{m+\frac{m}{2}-1}, & k < t \\ (q^{m-1} + \cdots + q + 1)^t, & k = t \end{cases} \\ &\leq \frac{(q^m - 1)^t}{(q - 1)^t} \\ &< \frac{q^{n-1} + \cdots + q + 1}{(q - 1)^{t-1}}. \end{aligned}$$

Notice that if $|H : C_H(g)| = |H \cap N : C_{H \cap N}(g)|$ then the result follows immediately; thus we assume that this is not the case, i.e. that H fuses the conjugacy class containing g to another.

- (2) **A lower bound for t .** It is clear that

$$\begin{aligned} |H : C_H(g)|_{p'} &\leq |H \cap N : C_{H \cap N}(g)|_{p'} |H / (H \cap N)|_{p'} \\ &< \frac{q^{n-1} + \cdots + q + 1}{(q - 1)^{t-1}} |t!|_{p'} \end{aligned}$$

Thus the result holds provided $|t!|_{p'} \leq 6^{t-1}$. So assume that $|t!|_{p'} > 6^{t-1}$; in particular assume that $t > 20$.

- (3) **A lower bound for k .** Let P be a Sylow 2-subgroup of $H \cap N$. Lemma 2.2 implies that, for $g \in P$,

$$(3) \quad |H : C_H(g)|_{p'} = |H \cap N : C_{H \cap N}(g)|_{p'} \frac{|g^H \cap P|_{p'}}{|g^{H \cap N} \cap P|_{p'}}.$$

Now let $\phi : N \rightarrow L_k$ be the natural projection map; then $\phi(P) \cong P$ is a Sylow 2-subgroup of L_k . Let $P_k = \phi(P) \cap T_k$ and choose g such that $\phi(g) \in P_k$. Then Lemma 2.3 implies that

$$(4) \quad |H \cap N : C_{H \cap N}(g)|_{p'} = \prod_{i=1}^k |T_i : C_{T_i}(g_i)|_{p'} \frac{|(g_k)^{L_k} \cap P_k|_{p'}}{|(g_k)^{T_k} \cap P_k|_{p'}}.$$

Let $P' \leq P$ be such that $\phi(P') = P_k$; let T be the full pre-image of T_k in $H \cap N$. Then Lemma 2.4 implies that

$$(5) \quad \begin{aligned} |g^{H \cap N} \cap P| &= |(g_k)^{L_k} \cap P_k| \\ |g^T \cap P| &= |(g_k)^{T_k} \cap P_k| \end{aligned}$$

Combining (3), (4) and (5), we obtain that

$$|H : C_H(g)|_{p'} = \prod_{i=1}^k |T_i : C_{T_i}(g_i)|_{p'} \frac{|g^H \cap P|_{p'}}{|g^T \cap P|_{p'}}.$$

Since T_k has odd order, $\langle T_k, g_k \rangle$ has at most one conjugacy class of involutions. Then Lemma 2.6 and induction imply that

$$|H : C_H(g)|_{p'} < (q^{m-1} + \dots + q + 1)^k (3.04^m + 1)^{t-k+1}$$

This yields the result unless $k = t$ or $(q, k) = (7, t - 1)$. We assume that one of these holds from here on and we note that if $k = t$, then $T = H \cap N$. We assume, moreover, that when $q = 7$ we have chosen an ordering for N_1, \dots, N_k so that k is minimal.

- (4) **A lower bound for m .** From the previous paragraph observe that

$$\begin{aligned} |H : C_H(g)|_{p'} &< (q^{m-1} + \dots + q + 1)^k (3.04^m + 1)^{t-k+1} \\ &\leq (q^{m-1} + \dots + q + 1)^t (3.04^m + 1) \\ &= (q^m - 1)^t \frac{3.04^m + 1}{(q - 1)^t} \\ &< (q^{n-1} + \dots + q + 1) \frac{3.04^m + 1}{(q - 1)^{t-1}}. \end{aligned}$$

If $3.04^m + 1 \leq (q - 1)^{t-1}$ then the result follows. Thus we assume that $3.04^m + 1 > (q - 1)^{t-1}$; in particular $m \geq t > 20$ and $n \geq 400$.

- (5) **No conjugates of g_k in P_k .** By assumption $g_k \in P_k$ is chosen so that $|T_k : C_{T_k}(g_k)|_{p'}$ is minimal. Suppose that there were no other T_k -conjugates of g_k in P_k . Then Theorem 3.27 implies that $g_k \in Z^*(T_k)$ and so $g \in Z^*(T)$. In particular

$$|H : C_H(g)|_{p'} \leq |T : C_T(g)|_{p'} \cdot |Z_2(T/O(T))|$$

where $Z_2(T/O(T))$ is the unique maximal elementary abelian 2-subgroup of $Z(T/O(T))$. (Recall that $O(T)$ is the largest odd-order normal subgroup of T .) Now, since

$$|T : C_T(g)|_{p'} = \prod_{i=1}^k |T_i : C_{T_i}(g_i)|_{p'} \leq \frac{(q^m - 1)^t}{(q - 1)^t}.$$

the result follows unless $|Z_2(T/O(T))| \geq (q - 1)^{t-1}$. Thus assume that this is the case and let W be the pre-image of $Z_2(T/O(T))$ in $H \cap N$ and let P' be a Sylow 2-subgroup of W . Clearly $W = O(T)P'$ and P' is elementary abelian. Take g, h to be distinct elements of $P' \setminus \{1\}$ and observe that Lemma 2.1 implies that $|T : C_T(g)| = |O(T) : C_{O(T)}(g)|$ (similarly for h).

Observe that $\langle O(T), g, h \rangle$ is isomorphic to a subgroup of $\text{GL}_{mk}(q)$ and that $\langle g, h \rangle$ is a Klein 4-group. We apply Lemma 3.21 to the group $\langle O(T), g, h \rangle$ and (by relabelling g and h if necessary) conclude that

$$|T : C_T(g)|_{p'} = |O(T) : C_{O(T)}(g)|_{p'} \leq \sqrt{q^{\frac{3mk}{2}} c_{mk}} \leq 3^{\frac{mk}{6}} \cdot q^{\frac{3mk}{4}}.$$

If $t = k$, then $T = H \cap N$ and P is isomorphic to a 2-subgroup of $\text{GL}_m(q)$. Now Lemma 2.6 and the fact that $m \geq t \geq 20$ imply that

$$|H : C_H(g)|_{p'} \leq 3^{\frac{n}{6}} \cdot q^{\frac{3n}{4}} \cdot 3.04^m < q^{\frac{29n}{30}} < q^{n-1}$$

and we are done.

If $t < k$, then $q = 7$ and $k = t - 1$. Now observe that W is normal in $H \cap N$ and that $|W : C_W(g)| = |T : C_T(g)|$. Applying Lemma 2.2 we have

$$|H \cap N : C_{H \cap N}(g)|_{p'} = |T : C_T(g)|_{p'} \frac{|g^{H \cap N} \cap P'|}{|g^W \cap P'|}.$$

Now P' is isomorphic to an elementary abelian 2-subgroup of $\text{GL}_m(q)$, thus Lemma 3.29 implies that $|P'| \leq 2^m$ and we have

$$|H \cap N : C_{H \cap N}(g)|_{p'} < \sqrt{q^{\frac{3m(t-1)}{2}} c_{m(t-1)}} \cdot 2^m$$

Since P is isomorphic to a 2-subgroup of $\text{GL}_m(q) \times \text{GL}_m(q)$, Lemma 2.6 implies that

$$\begin{aligned} |H : C_H(g)|_{p'} &< \sqrt{q^{\frac{3m(t-1)}{2}} c_{m(t-1)}} \cdot 2^m \cdot 3.04^{2m} \\ &\leq 3^{\frac{n-m}{6}} q^{\frac{3n-3m}{4}} \cdot 2^m \cdot 3.04^{2m} \\ &\leq 3^{\frac{n}{6} - \frac{n}{120}} q^{\frac{3n}{4} - \frac{3n}{80}} \cdot 12.16^{\frac{n}{10}} \\ &< q^{0.94n} < q^{n-1} \end{aligned}$$

and the result follows.

- (6) **Conjugates of g_k in P_k .** Suppose, instead, that P_k contains other T_k -conjugates of g_k in P_k . Then P contains other T -conjugates of g in P . Now Theorem 3.28 implies that there exists a T -conjugate $h \in P_k$ such that $\langle g, h \rangle$ is a Klein 4-subgroup of P .

Let V be the normal subgroup of T that is the pre-image of T_{k-1} . Observe that $\langle V, g, h \rangle$ is isomorphic to an odd order subgroup of $\text{GL}_{m(k-1)}(q)$. We apply Lemma 3.21 to the group $\langle V, g, h \rangle$ and (by relabelling g and h if necessary) conclude that

$$|V : C_V(g)|_{p'} \leq \sqrt{q^{\frac{3m(k-1)}{2}} c_{m(k-1)}} \leq 3^{\frac{m(k-1)}{6}} \cdot q^{\frac{3m(k-1)}{4}}.$$

If $t = k$, then $T = H \cap N$ and Lemma 2.1 implies that

$$\begin{aligned} |H \cap N : C_{H \cap N}(g)|_{p'} &= |V : C_V(g)|_{p'} |T_k : C_{T_k}(g_k)|_{p'} \\ &\leq 3^{\frac{m(t-1)}{6}} \cdot q^{\frac{3m(t-1)}{4}} (q^{m-1} + \cdots + q + 1). \end{aligned}$$

Then, since P is isomorphic to a subgroup of $\text{GL}_m(q)$, Lemma 2.2 and 2.6 imply that

$$\begin{aligned} |H : C_H(g)|_{p'} &\leq 3^{\frac{m(t-1)}{6}} \cdot q^{\frac{3m(t-1)}{4}} (q^{m-1} + \cdots + q + 1) 3.04^m \\ &< 3^{\frac{n}{6} - \frac{n}{120}} q^{\frac{3n}{4} + \frac{n}{80}} 3.04^{\frac{n}{20}} \\ &< q^{\frac{39n}{40}} < q^{n-1} \end{aligned}$$

and we are done.

If $t = k - 1$, then

$$\begin{aligned} |T : C_T(g)|_{p'} &\leq \sqrt{q^{\frac{3m(k-1)}{2}} c_{m(k-1)}} (q^{m-1} + \cdots + q + 1) \\ &\leq 3^{\frac{m(t-2)}{6}} \cdot q^{\frac{3m(t-2)}{4}} (q^{m-1} + \cdots + q + 1). \end{aligned}$$

Now, since $P \cap T$ is isomorphic to a subgroup of $\text{GL}_m(q)$, Lemma 2.2 and 2.6 imply that

$$|H \cap N : C_{H \cap N}(g)|_{p'} \leq 3^{\frac{m(t-2)}{6}} \cdot q^{\frac{3m(t-2)}{4}} (q^{m-1} + \cdots + q + 1) 3.04^m.$$

Similarly, since P is isomorphic to a subgroup of $\text{GL}_m(q) \times \text{GL}_m(q)$, Lemma 2.2 and 2.6 imply that

$$\begin{aligned} |H : C_H(g)|_{p'} &\leq 3^{\frac{m(t-2)}{6}} \cdot q^{\frac{3m(t-2)}{4}} (q^{m-1} + \cdots + q + 1) 3.04^m 3.04^{2m} \\ &\leq 3^{\frac{n}{6} - \frac{n}{60}} q^{\frac{3n}{4} - \frac{3n}{40}} q^{\frac{n}{20}} 3.04^{\frac{3n}{20}} \\ &< q^{0.98n} < q^{n-1} \end{aligned}$$

and the result is proved. \square

This completes our proof of Lemma A, and thereby proves Theorem A.

4. THEOREM B AND ITS COROLLARIES

Our first task is to prove Theorem B. We begin by recalling the statement of Hypothesis 1.

Hypothesis 1. *Suppose that a group G acts transitively upon the points of a non-Desarguesian projective plane \mathcal{P} of order $x > 4$. If G contains any involutions then each fixes a Baer subplane; in particular they fix $u^2 + u + 1$ points where $x = u^2$, $u > 2$. Furthermore in this case any non-trivial element of G fixing at least u^2 points fixes either $u^2 + u + 1$, $u^2 + 1$ or $u^2 + 2$ points of \mathcal{P} .*

In this section we operate under Hypothesis 1, which we recall represents the conditions under which a group may act transitively on the points of a non-Desarguesian projective plane (see p.7).

Our proof of Theorem B will require a background result and a lemma. The background result follows from the comments in [Gor68, p377] and the results in [WG64].

Proposition 4.1. *If a group H has generalized quaternion Sylow 2-subgroups then $H/O(H)$ is isomorphic to one of the following groups:*

- (1) S , i.e. H has a normal 2-complement.
- (2) $2.A_7$, a double cover of A_7 .
- (3) $SL_2(q).D$, where q is odd and D is cyclic.

Lemma B. *Suppose that G has generalized quaternion Sylow 2-subgroups and is insoluble. Then G has a subgroup of index at most 2 equal to $O(G) \rtimes K$ where K is a group isomorphic to $SL_2(5)$. Furthermore if N_t is a Sylow t -subgroup of $F(G)$, for some prime t , then one of the following holds:*

- (i) t divides $u^2 + u + 1$;
- (ii) t divides $u^2 - u + 1$, $N_G(N_t)$ contains a subgroup H such that $H \cong SL_2(5)$, H fixes a point of \mathcal{P} , $N_t \rtimes H$ is a Frobenius group, and N_t is abelian.

Furthermore there exists a prime t dividing both $|F(G)|$ and $u^2 - u + 1$.

We defer the proof of Lemma B until the next subsection; first we demonstrate that Lemma B implies Theorem B. We need a little notation which will hold throughout this section: for a group $H \leq G$, define $\overline{H} = H/(H \cap O(G))$.

Proof that Lemma B implies Theorem B. Let S be a Sylow 2-subgroup of G ; Theorem A implies that S is cyclic or generalized quaternion. Note that, since S contains exactly one involution, the Frattini argument implies that $G = O(G)C_G(g)$ for any involution $g \in G$.

If S is cyclic then [Asc00, 39.2] implies that $\overline{G} \cong S$, i.e. G has a normal 2-complement and Theorem B holds.

If S is generalized quaternion then Proposition 4.1 gives the structure of \overline{G} . Clearly if (1) holds, then Theorem B holds. Similarly if (3) holds with $q = 3$, then Theorem B holds. Thus, to prove Theorem B we must deal

with the remaining cases. Equivalently it is sufficient to assume that G has generalized quaternion Sylow 2-subgroups and is insoluble. Now Lemma B applies and Theorem B follows immediately. \square

4.1. A proof of Lemma B. Throughout this subsection we operate under the supposition of Lemma B, as well as under Hypothesis 1. In particular this means that $F^*(\overline{G})$ is a quasisimple group with centre of order 2. We start with a background result.

Lemma 4.2. [Asc00, (5.21)] *Let a group J be transitive on a set X , $x \in X$, H the stabilizer in J of x , and $K \leq H$. Then $N_J(K)$ is transitive on $\text{Fix}(K)$ if and only if $K^J \cap H = K^H$.*

Lemma 4.3. *For g an involution in G , $C_G(g)$ acts transitively on the set of points of $\text{Fix}(g)$, a Baer subplane of \mathcal{P} .*

Proof. This is immediate from Lemma 4.2. Take G to be the group J , X to be the set of points of \mathcal{P} ; thus $H = G_\alpha$, the stabilizer of a point α . Define K to be a subgroup of G_α of order 2, say $K = \{1, g\}$. Now g is the unique involution in a particular Sylow 2-subgroup of G_α and so $K^G \cap G_\alpha = K^{G_\alpha}$. Hence $N_G(K) = C_G(g)$ is transitive on $\text{Fix}(K) = \text{Fix}(g)$, a Baer subplane of \mathcal{P} . \square

For a fixed involution $g \in G$, define the subgroup

$$T_g = \{h \in C_G(g) \mid \text{Fix}(h) = \text{Fix}(g)\}.$$

Thus T_g is the kernel of the action of $C_G(g)$ on $\text{Fix}(g)$.

Lemma 4.4. *For g an involution in G , $\overline{T_g}$ contains a normal subgroup isomorphic to $F^*(\overline{G})$.*

Proof. Suppose first that $\text{Fix}(g)$ is Desarguesian. There are two possibilities for the structure of $C_G(g)/T_g$: either $C_G(g)/T_g$ is soluble or $C_G(g)/T_g$ has socle $\text{PSL}_3(u)$ where $u > 2$ is the order of $\text{Fix}(g)$. Now, since $u > 2$, $\text{PSL}_3(u)$ has Sylow 2-subgroups that are neither cyclic nor dihedral and so they cannot form a section of a quaternion group. Hence we conclude that $C_G(g)/T_g$ is soluble.

Now suppose that $\text{Fix}(g)$ is not Desarguesian. Recall that the quotient of a quaternion group Q by a normal subgroup containing the unique central involution of Q must be either dihedral or cyclic. We conclude that $C_G(g)/T_g$ must have dihedral or cyclic Sylow 2-subgroups. The former is not possible by Theorem A and the latter implies that $C_G(g)/T_g$ is soluble. Hence this conclusion holds in all cases.

Since $G = O(G)C_G(g)$, we know that $\overline{C_G(g)}$ must contain a normal subgroup isomorphic to $F^*(\overline{G})$. Since $C_G(g)/T_g$ is soluble, we conclude that $\overline{T_g}$ must contain a normal subgroup isomorphic to $F^*(\overline{G})$. \square

Now we will need a background result which is originally due to Zassenhaus [Zas36]; it is discussed fully in [Pas68].

Theorem 4.5. *Let F be an insoluble Frobenius complement. Then F has a normal subgroup F_0 of index at most 2 such that $F_0 = SL_2(5) \times M$ with M a group of order prime to 2, 3 and 5.*

We are now in a position to prove Lemma B and hence Theorem B:

Proof of Lemma B. Lemma 2.7 implies that any prime dividing $|F(G)|$ divides

$$u^4 + u^2 + 1 = (u^2 + u + 1)(u^2 - u + 1).$$

Hypothesis 1, Proposition 2.12 and Lemma A together imply that there is a prime t dividing $|F(G)|$ that does not divide $u^2 + u + 1$. We conclude that t divides $u^2 - u + 1$ and we write N_t for the Sylow t -subgroup of $F(G)$.

Let g be an involution in G . Since N_t acts semi-regularly on the points of \mathcal{P} (see Lemma 2.7), we know that $T_g \cap N_t$ is trivial; we also know that T_g acts (by conjugation) on N_t .

Suppose that T_g does not act semi-regularly on N_t . This implies that there exists $h \in T_g, h \neq 1$ such that $C_{N_t}(h)$ is non-trivial. Now $C_{N_t}(h)$ acts on the fixed set of h and, since $h \in T_g$, we know that the fixed set of h is a Baer subplane. We know, furthermore, that N_t acts semi-regularly on the points of \mathcal{P} . This implies that t divides $u^2 + u + 1$ which is a contradiction.

We conclude that T_g acts semi-regularly on N_t , i.e. that $N_t \rtimes T_g$ is a Frobenius group with Frobenius complement T_g and Frobenius kernel N_t .

We can now apply Theorem 4.5; thus T_g has a subgroup $T_{g,0}$ of index at most 2 such that $T_{g,0} = H \times M$ where $H \cong SL_2(5)$ and $(|M|, 60) = 1$. Note that H is the unique normal quasisimple subgroup of T_g . Observe that $N_t \rtimes H$ is a subgroup of G that is also a Frobenius group and so, in particular, N_t is abelian [Isa08, Theorem 6.3]. What is more $N_t \leq T_g$, thus N_t fixes a point of \mathcal{P} .

Now Lemma 4.4 implies that $F^*(\overline{G}) \cong SL_2(5)$; Proposition 4.1 implies that \overline{G} is a cyclic extension of $SL_2(5)$. Since $\text{Aut}(SL_2(5)) = \text{PSL}_2(5).2$, this extension must have size at most 2; thus $\overline{G} \cong SL_2(5)$ or $SL_2(5).2$.

Finally, since T_g has a subgroup isomorphic to $SL_2(5)$ it is clear that G contains a split extension, $O(G) : SL_2(5)$, and the result follows. \square

4.2. Corollary 1.2.

Proof of Corollary 1.2. As we pointed out in the introduction, the statement is true for Desarguesian projective planes. Assume that \mathcal{P} is non-Desarguesian. Write v for the number of points in \mathcal{P} and let $H = O^2(G)$, the largest normal subgroup of G such that $|G/H|$ is a (possibly trivial) power of 2. Since v is odd, it is clear that H acts transitively on the set of points of \mathcal{P} .

Now apply Theorem B. If (1) applies, then $H = O(G)$, an odd-order group and we are done. If (2) applies, then $H = O(H).SL_2(3)$ and $O(H)$ lies inside an odd-order subgroup M of index 8 in H ; then M acts transitively on the set of points of \mathcal{P} and we are done. Finally if (3) applies, then Theorem B implies that $H = O(H) \rtimes K$ where $K \cong SL_2(5)$ and, moreover, K fixes a

point of \mathcal{P} . Thus $O(H)$ acts transitively on the set of points of \mathcal{P} and we are done. \square

REFERENCES

- [Asc84] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514.
- [Asc00] Michael Aschbacher, *Finite group theory*, Cambridge studies in advanced mathematics, no. 10, Cambridge University Press, 2000.
- [BGL77] N. Burgoyne, R. Griess, and R. Lyons, *Maximal subgroups and automorphisms of Chevalley groups*, Pacific J. Math. **71** (1977), no. 2, 365–403.
- [Col08] Michael J. Collins *Modular analogues of Jordan’s theorem for finite linear groups*, J. Reine Angew. Math. **624** (2008), 143–171.
- [CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985.
- [Dem97] P. Dembowski, *Finite geometries*, Springer-Verlag, 1997.
- [Dic58] Leonard Eugene Dickson, *Linear groups: With an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958.
- [Gil06] Nick Gill, *Nilpotent singer groups*, Electronic Journal of Combinatorics **13** (2006), R94.
- [Gil07] ———, *Transitive projective planes*, Adv. Geom. **7** (2007), 475–528.
- [Gla66] George Glauberman, *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420.
- [GLS94] Daniel Gorenstein, Richard Lyons, and Ronald Solomon, *The classification of the finite simple groups, number 3*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, 1994.
- [Gor68] Daniel Gorenstein, *Finite groups*, Harper & Row Publishers, New York, 1968.
- [Gor94] Daniel M. Gordon, *The prime power conjecture is true for $n < 2,000,000$* , Electron. J. Combin. **1** (1994), Research Paper 6, approx. 7 pp. (electronic).
- [Isa08] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008.
- [Kan87] W. Kantor, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.
- [KL90] P. Kleidman and M. Liebeck, *The subgroup structure of the finite simple groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.
- [Mar05] A. Maróti, *Bounding the number of conjugacy classes of a permutation group*, J. Group Theory **8** (2005), no. 3, 273–289.
- [OW59] T.G. Ostrom and A. Wagner, *On projective and affine planes with transitive collineation groups*, Math. Z. **71** (1959), 186–199.
- [Pal82] Pálffy, P. P., *A polynomial bound for the orders of primitive solvable groups*, J. Algebra **77** (1982), no. 1, 127–137.
- [Pas68] Donald Passman, *Permutation groups*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.
- [PS80] Cheryl E. Praeger and Jan Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), no. 4, 303–307.
- [Tha03] K. Thas, *Finite flag-transitive projective planes: a survey and some remarks*, Discrete Math. **266** (2003), 417–429.
- [TZ08] Koen Thas and Don Zagier, *Finite projective planes, Fermat curves, and Gaussian periods*, J. Eur. Math. Soc. (JEMS) **10** (2008), no. 1, 173–190.
- [Wag59] A. Wagner, *On perspectivities of finite projective planes*, Math. Z. **71** (1959), 113–123.

- [WG64] John H. Walter and D. Gorenstein, *The characterisation of finite groups with dihedral sylow 2-subgroups*, J. Algebra **2** (1964), 85–151, 218–270, 354–393.
- [Zas36] H. Zassenhaus, *Über endliche fastkörper*, Abh. Math. Sem. Hamburg **11** (1936), 187–220.

DEPARTMENT OF MATHEMATICS, THE OPEN UNIVERSITY, WALTON HALL, MILTON
KEYNES, MK7 6AA, UK

E-mail address: `n.gill@open.ac.uk`