Flag-Transitive Symmetric Designs

Eugenia O'Reilly Regueiro

Thesis submitted for the degree of
Doctor of Philosophy
and the
Diploma of Imperial College

September 2002

Imperial College

ABSTRACT

This thesis is a contribution to the theory of symmetric designs. A (v, k, λ)-*symmetric design* is an incidence structure consisting of a set P of v points, a set of B of v blocks, and an incidence relation between them, in which every block is incident with exactly k points, and every pair of points is incident with exactly λ blocks.

A $flag$ in a design is a pair (p, B_0) such that the point p is incident with the block B_0. In this thesis we will focus on symmetric designs that have flag-transitive automorphism groups, that is, automorphism groups that act transitively on the flags of the design.

Our results focus on (v, k, λ)-symmetric designs with λ small. When $\lambda = 1$, these are *projective planes*, on which much work has been done. It is conjectured that for a given $\lambda > 1$, there are only a finite number of (v, k, λ)-symmetric designs. When $\lambda = 2$ they are called *biplanes*, and it is this case that the present work is mainly concerned with.

Let G be a flag-transitive automorphism group of a (v, k, λ)-symmetric design D. Here we show that if $\lambda \leq 7$, then either G is primitive, or (v, k, λ) is one of the following: (16,6,2), (45,12,3), (15,8,4), (96,20,4), (175,30,5), (16,10,6), (36,15,6), (288,42,6), (27,14,7), (247,42,7), or (441,56,7). We also show that if D is a biplane and G is primitive on the set of points, then G is of affine or almost simple type, and we then have classification results for flag-transitive biplanes for the affine and almost simple cases.

CONTENTS

ACKNOWLEDGEMENTS

I would like to acknowledge the financial support of the Dirección General de Apoyo al Personal Académico, UNAM, without which I could not have even started my studies at Imperial College. I am deeply and most sincerely grateful for this support.

I would like to thank my Supervisor, Martin W. Liebeck, for his guidance, ideas, support, and also his sense of humour. His invaluable help was vital and without it I could not possibly have completed this thesis.

During the course of my studies, I received great help both mathematically and in LaTeX. I cannot mention here every individual who contributed to this work, but I should emphasize my gratitude to Sasha Ivanov, Peter Cameron, Alan Camina, Dima Pasechnik, Alain Reuter, Katia Babbar, Fieke Dekkers, Annelies Gerber, Francisco Hernández Quiroz, Ara Minassian (to whom all credit should go for the first figure in this thesis), Péter Török, who so many times helped me out of computing trouble; and many friends at Imperial College.

I have many friends and relatives both in the UK and abroad whose company, enthusiasm and support have made these years a wonderful experience. Their names do not fit here, but they are certainly all included.

Undoubtedly the person who has spent the most time helping me not only with LaTeX and mathematics, but also and more importantly putting up with my neurosis, lack of patience, bad temper, and giving me love and unconditional support in every sense, is Matěj Stehlík. I have no words to express my immense love and gratitude.

I dedicate this thesis to my parents. My father's love of mathematics was certainly the greatest influence in my choice of profession. My mother's love of art was certainly the greatest influence in my devotion to music, which has always enriched my life enormously. Their love, enthusiasm and support have made all the difference.

1. INTRODUCTION

We begin this chapter by giving definitions and some of the background results on symmetric designs, flag-transitivity, and biplanes. In the next section we state the O'Nan-Scott Theorem, which is used in the proof of one of our results, and in the final section we state the results that will be proved throughout this work.

1.1 Symmetric Designs

Incidence structures appear in many branches of mathematics. An incidence structure consists of a set of points P, a set of blocks B, and an incidence relation between them. One particular class of incidence structures are the symmetric designs, defined as follows:

Definition 1.1. $D = (P, B, I)$ an incidence structure is a (v, k, λ)-*symmetric design* if and only if:

(*i*) $|P| = |B| = v$

(*ii*) Every block is incident with exactly k points.

(*iii*) Every pair of points is incident with exactly λ blocks.

We will show later that these conditions imply that every point is incident with exactly k blocks, and every pair of blocks is incident with exactly λ points. To avoid trivial examples, we will assume $k > \lambda$.

We now mention a few of the many examples of symmetric designs.

Examples 1.2. The projective plane $PG(2,2)$, or the *Fano Plane*, is a (7,3,1)-symmetric design; where P is the set of 1-dimensional subspaces of a 3-dimensional vector space over $GF(2)$, B is the set of 2-dimensional subspaces, and incidence is given by containment. We can verify the definition given above. There are 7 subspaces of dimension 1 in $PG(2,2)$, and 7 subspaces of dimension 2; so $v = 7$. There are three different non-zero vectors in each 2-dimensional subspace, and every non-zero vector is in three different subspaces of dimension 2; so $k = 3$. Finally, every two non-zero vectors are linearly independent, hence a basis of one 2-dimensional subspace; and dually every two 2-dimensional subspaces intersect in one 1-dimensional subspace.

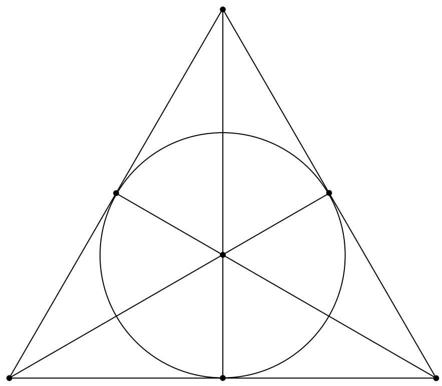

Figure 1.1: $PG(2,2)$

In general, projective spaces $PG(n,q)$ are examples of symmetric designs; taking $V = V_{n+1}(q)$ an n-dimensional vector space over the field of q elements, the points as the 1-dimensional subspaces, and the blocks as the hyperplanes. The parameters will then be $v = q^n + q^{n-1} + \ldots + q + 1$, $k = q^{n-1} + \ldots + q + 1$, and $\lambda = q^{n-2} + \ldots + q + 1$.

Another kind of symmetric designs are those constructed from difference sets. Let $(G,+)$ be an abelian group, and S a proper non-empty subset of G. Then we say S is a λ-*difference set* if and only if the list of all non-zero differences $s - s'$ $(s, s' \in S)$ contains every non-zero element of G exactly λ

times. From a λ-difference set, we can construct a (v, k, λ)-symmetric design as follows: Let $P = G$, and $B = \{S + g : g \in G\}$. Then $v = |P| = |B|$, and $k = |S|$.

One particular type of difference sets are the *Paley Difference Sets*:

Let $q \equiv 3 \pmod 4$ be a prime power, $G = (GF(q), +)$, and S the set of non-zero squares of G. Then $P = G$, $B = \{S + g : g \in G\}$, and we have $|P| = |B| = v = q$, $k = \frac{q-1}{2}$, and $\lambda = \frac{q-3}{4}$. In particular, when $q = 7$, with this construction we get the Fano Plane, mentioned above.

Definition 1.3. The *complement* D' of D a (v, k, λ)-symmetric design is a $(v, v-k, v-2k+\lambda)$-symmetric design whose set of points is the same as the set of points of D, and whose blocks are the complements of the blocks of D. That is, take the same set of points, and replace incidence by non-incidence and vice-versa.

Definition 1.4. If D is a (v, k, λ)-symmetric design (or its complement), we call $n = k - \lambda$ the order of D. (Note that the order of D is the same as that of D').

Before stating some results giving arithmetical conditions on the parameters of a symmetric design, we give the following:

Definition 1.5. A *flag* in a symmmetric design is a pair (p, B_0), where p is a point, B_0 is a block, and they are incident.

Lemma 1.6. *[38, 1.1] Let D be a (v, k, λ)-symmetric design. Then every point is incident with exactly k blocks, and every pair of blocks is incident with exactly λ points.*

We now state three conditions on the parameters of a symmetric design that are necessary (but not sufficient!) for its existence.

Lemma 1.7. *If D is a (v, k, λ)-symmetric design, then the following equation holds: $\lambda(v-1) = k(k-1)$.*

Proof. Fix a point x of D. Now we count the number of flags (p, B_i) of D such that p is different from x, and x is incident with the block B_i, in two different ways.

Each block incident with x is also incident with $k-1$ other points, and since there are exactly k blocks incident with x (by previous lemma), we have $k(k-1)$ such flags.

On the other hand, for each point p of D different from x, the pair $\{p, x\}$ is incident with exactly λ blocks, and since there are $v-1$ points different from x in D, there are $\lambda(v-1)$ such flags. Hence $\lambda(v-1) = k(k-1)$. □

Theorem 1.8 (Schutzenberger.). *[58] If D is a (v, k, λ)-symmetric design with v even, then $n = k - \lambda$ is a square.*

Theorem 1.9 (Bruck-Ryser-Chowla.). *[38, Theorem. 2.1] If D is a (v, k, λ)-symmetric design with v odd, then the equation*

$$(k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2 = z^2$$

has a non-trivial integral solution.

Lemma 1.10. *[6, Proposition 3.11] Let D be a (v, k, λ)-symmetric design, with $n = k - \lambda$. Then $4n - 1 \leq v \leq n^2 + n + 1$.*

Proof. Since $\lambda(v-1) = k(k-1)$, we have that

$$v - 1 = \frac{k(k-1)}{\lambda} = \lambda + 2n + \frac{n(n-1)}{\lambda},$$

so

$$\lambda = \frac{1}{2}\left(v - 2n \pm \sqrt{(v-2n)^2 - 4n(n-1)}\right).$$

The two solutions correspond to D and D'. As λ and $\lambda' \geq 1$, we need $v - 2n - 2 \geq \sqrt{(v-2n)^2 - 4n(n-1)}$, which yields the upper bound for v.

Also, $(v-2n)^2 \geq \sqrt{4n(n-1)}$, so $v - 2n \geq 2n - 1$. (Note $v \geq 2n$, and $(2n-1)^2$ is the least square integer which is greater than or equal to $4n(n-1)$). □

The upper bound for v is achieved if and only if D or D' is a projective plane, and the lower bound is achieved if and only if D or D' has parameters $v = 4n-1$, $k = 2n-1$, and $\lambda = n-1$. (This is a *Hadamard* design).

An *automorphism* of a design D is a permutation on the set of points that also permutes the blocks, preserving the incidence relation; that is, a permutation of the points that leaves the set of blocks invariant. The set of automorphisms of a design, with the composition of functions form a group.

Note that since automorphisms of symmetric designs preserve the incidence relation, an automorphism of a symmetric design is also an automorphism of the complement, therefore it suffices to consider designs in which $2k \leq v$.

One way to approach the problem of classifying symmetric designs is by imposing conditions on the automorphism group. One such condition is 2-transitivity on points. This classification was completed by Kantor (1985):

Theorem 1.11 (Kantor.). *[28] If D is a (v,k,λ)-symmetric design with $v > 2k$ and a 2-transitive automorphism group, then D is one of the following:*

(*i*) *$PG(n,q)$.*

(*ii*) *A unique (11,5,2)-symmetric design.*

(*iii*) *A unique (176,50,14)-symmetric design, or*

(*iv*) *A $(2^{2m}, 2^{m-1}(2^m-1), 2^{m-1}(2^{m-1}-1))$-symmetric design, of which there is one for each $m \geq 2$.*

Another condition that can be imposed on the automorphism group is flag-transitivity:

Definition 1.12. An automorphism group G of a symmetric design D is *flag-transitive* if for any two flags (p_1, B_1), (p_2, B_2) of D, there is a $g \in G$

such that $(p_1)^g = p_2$ and $(B_1)^g = B_2$; or equivalently, $(p_1, B_1)^g = (p_2, B_2)$. That is, there is an element in the automorphism group of the design that takes any point and any block it is incident with, to any other point and any of the blocks with which it is incident.

There are of course, other conditions that can be imposed on the automorphism group of a design; (for example point-transitivity, block-transitivity, point-primitivity, block-primitivity), and indeed work has been done with these conditions, particularly for $(v, k, 1)$-designs, that is, *linear spaces.* In the case of point-transitivity, if no other condition is imposed the admissible designs and groups appear to be too many to be classified. As stated previously, Kantor completed the classification of symmetric designs with automorphism groups that are transitive on pairs of points. For further discussion on these conditions see [7].

Symmetric designs with $\lambda = 1$ are *projective planes.* When $k = 3$, the only flag-transitive linear spaces besides the affine spaces and projective spaces are the *Netto systems* [16, p.98]. In the case of flag-transitivity much work has been done for projective planes, and Kantor proved the following:

Theorem 1.13. *[29] If D is a projective plane of order n admitting a flag-transitive automorphism group G, then either:*

(*i*) *D is Desarguesian and $G \rhd PSL(3, n)$, or*

(*ii*) *G is a sharply flag-transitive Frobenius group of odd order $(n^2 + n + 1)(n + 1)$ and $n^2 + n + 1$ is a prime.*

In the latter case, only two examples are known, namely $PG(2, 2)$ and $PG(2, 8)$; and any other would necessarily be non-Desarguesian due to a result by Higman and McLaughlin [20], and also by Dembowski [17], which states that the only Desarguesian planes admitting a sharply flag-transitive automorphism group are $PG(2, 2)$ and $PG(2, 8)$.

But we now consider $\lambda > 1$. There is a considerable difference between these two cases in that for $\lambda = 1$ there are infinitely many symmetric designs, whereas for any given $\lambda > 1$ there are only finitely many known examples, and indeed, it is conjectured that for any given $\lambda > 1$ only finitely many exist.

1.2 Biplanes

Definition 1.14. A *biplane* is a symmetric design with $\lambda = 2$, that is, a $(v, k, 2)$-symmetric design.

Regarding the conjecture that for a given $\lambda > 1$ only finitely many symmetric designs exist, biplanes are a natural case to consider, not only because 2 is the first value of λ in this category, but also because among symmetric designs with $\lambda > 1$ biplanes behave in a special way [10]. For example, in any symmetric design if we define the *line* through two points to be the set of points incident with every block through those two points, then if $\lambda > 2$, the lines carry information about the design. However, for $\lambda \leq 2$ the lines are automatically determined, in projective planes they are the blocks, and in biplanes they are the set of those two points, and hence they carry no information.

Also, the class of symmetric designs such that the number of blocks incident with three points takes only two values has only finitely many designs for a given $\lambda > 2$ [10], however all projective planes and biplanes are in this class. Projecive planes and biplanes are unique among symmetric designs in that any three points are incident with at most one block.

As we will see in the next chapter, the only known examples of biplanes so far are for $k = 3, 4, 5, 6, 9, 11$, and 13. It can be seen from the parameter restrictions (Lemma 1.7, and Theorems 1.8, and 1.9) that there are no examples for $k = 7, 8, 10$ or 12.

For $k = 3$, 4, and 5 the biplanes are unique up to isomorphism, for $k = 6$ there are exactly three non-isomorphic biplanes, for $k = 9$ there are exactly four non-isomorphic biplanes, and for $k = 11$ and 13 there are in each case, two known biplanes. In the latter case, it is a biplane and its dual.

We conclude this section with the following result, which is a consequence of the parameter restrictions on symmetric designs given earlier in this chapter.

Lemma 1.15. *If D is a $(v, k, 2)$-biplane, then $8v - 7$ is a square.*

Proof. We know from Lemma 1.7 that for any (v, k, λ)-symmetric design, $\lambda(v-1) = k(k-1)$. So, in the case of a biplane, we have $2(v-1) = k(k-1)$. If we solve this equation for k, we have that

$$k = \frac{1 + \sqrt{8v - 7}}{2},$$

and since this must be an integer, $8v - 7$ must be a square. □

1.3 Results

In this section we state the main results that will be proved in this thesis. First, we give a summary of the known examples of biplanes with flag-transitive automorphism groups. We focus on the biplanes with parameters (16,6,2), they play a special role in our study (see below), and only a biplane with these parameters can (and does) admit a flag-transitive, imprimitive, automorphism group. Thus, we have the following:

Theorem 1. *There are exactly three non-isomorphic (16,6,2) biplanes D_1, D_2, and D_3. Exactly two, say D_1 and D_2 admit flag-transitive automorphism groups. Moreover:*

(i) Both D_1 and D_2 admit imprimitive, flag-transitive automorphism groups, which are $G_1 = 2^4 S_4$ and $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_8)S_4$ respectively.

(*ii*) *Only* D_1 *has a primitive flag-transitive automorphism group of affine type, namely,* $G \leq 2^4S_6 < AGL_4(2)$.

We then see that flag-transitive automorphism groups of symmetric designs with small λ are almost always necessarily primitive:

Theorem 2. *If* G *is a flag-transitive automorphism group of a* (v,k,λ)*-symmetric design* D*, with* $\lambda \leq 7$*, then either* G *is primitive, or* D *has parameters (16,6,2), (45,12,3), (15,8,4), (96,20,4), (175,30,5), (16,10,6), (36,15,6), (288,42,6), (27,14,7), (247,42,7), or (441, 56, 7).*

It is important to note that although the above result refers to admissible parameters, it by no means asserts the existence of such designs. Symmetric designs with parameters (288,42,6) and (247,42,7) are not known to exist, the rest of the admissible parameters correspond to designs whose existence is known, mainly as difference sets. It is natural to ask here whether these designs admit flag-transitive automorphism groups, but that is something that has not been investigated in this thesis, except for the case of biplanes. We include in this case symmetric designs with $v < 2k$ because although a design and its complement have the same automorphism group, flag-transitivity in one design does not imply flag-transitivity in the complement.

We then apply the O'Nan-Scott Theorem (see Chapter 3), which classifies primitive groups, to obtain the following result:

Theorem 3. *If* G *is a primitive, flag-transitive automorphism group of a biplane* D*, then either* G *is affine, or almost simple.*

We analyse each of the two cases separately.

Theorem 4 (Affine case). *If* D *is a biplane with a primitive, flag-transitive automorphism group* G *of affine type, then one of the following holds:*

(*i*) D *has parameters (4,3,2).*

(*ii*) D *has parameters (16,6,2).*

(iii) $G \leq A\Gamma L_1(q)$, *for some prime power* q.

Theorem 5 (Almost simple case). *If D is a biplane with a primitive, flag-transitive automorphism group of almost simple type, then D has parameters either (7,4,2), or (11,5,2), and is unique up to isomorphism.*

And now combining all these results, we state the main result of this work:

Theorem 6 (Main Theorem). *If D is a biplane with a flag-transitive automorphism group G, then one of the following holds:*

(i) *D has parameters (16,6,2), and either* $G \leq 2^4 S_6 \leq AGL_4(2)$, *or* $G \leq (\mathbb{Z}_2 \times \mathbb{Z}_8)\,(S_4.2) \leq AGL_4(2)$.

(ii) $G \leq A\Gamma L(1, q)$ *for some prime power* q.

(iii) *D is the unique (4,3,2) biplane, and* $G \leq S_4$.

(iv) *D is the unique (7,4,2) biplane, and* $G = PSL_2(7)$.

(v) *D is the unique (11,5,2) biplane, and* $G = PSL_2(11)$.

2. GRAPHS AND BIPLANES

In this chapter we present a summary of the known examples of biplanes, but before that it is convenient to mention some related results, so we begin by defining Hussain graphs.

2.1 Hussain Graphs

There is a one-to-one correspondence between the unordered pairs of points incident with a given block B_0 of a biplane, and the blocks of the biplane different to B_0. To see this, note that every block different to B_0 meets B_0 in exactly two points; and, conversely, every pair of points incident with B_0 is also incident with exactly one other block. Hence, we can represent the blocks of a biplane different to a given block B_0 as the set of unordered pairs of points incident with B_0. How can we represent the points not incident with B_0? Take p to be such a point, and define a graph $\langle p \rangle$ as follows:

The vertex set V of $\langle p \rangle$ is the set of k points incident with B_0; and two vertices q, r are adjacent in $\langle p \rangle$ if and only if the unique block other than B_0 with which they are incident is also incident with p.

Now, if q is incident with B_0, q and p are each incident with exactly two blocks, B_1 and B_2; each of which meets B_0 in another point, and these two points are different. Hence, the graph $\langle p \rangle$ has exactly two edges on each vertex.

Given two points p_1 and p_2 not incident with B_0, they are both incident with two blocks; so the graphs $\langle p_1 \rangle$ and $\langle p_2 \rangle$ have two edges in common; and these two edges do not have a common vertex, since the two blocks on p_1 and p_2 do not have any other common point.

So now, given a block B_0 of a biplane, we have defined $v-k$ divalent graphs corresponding to the $v-k$ points not incident with B_0, and each two of them have two common edges that have no common vertex.

Definition 2.1. [21, 3.6] A set of divalent graphs on a vertex set V such that any two have exactly two common edges, and these do not have a common vertex is called a set of *Hussain Graphs.*

Notice that for a biplane D, if we fix a block B_0, then the set of graphs

$$\{\langle p \rangle \mid p \text{ is not incident with } B_0\}$$

defined above is a set of Hussain Graphs.

Similarly, if K is a set of k vertices, and $G_1, G_2, \ldots, G_{\frac{(k-1)(k-2)}{2}} (= G_{v-k})$ is a set of divalent graphs with vertex set K such that for $i \neq j$, G_i and G_j have two edges in common, then the following structure $D = (P, B, I)$ is a biplane with block size k:

The points in P are the vertices of K and the symbols (i), for $i = 1, 2, \ldots, \frac{(k-1)(k-2)}{2} = v-k$. The blocks in B are the symbol K and the unordered pairs $[p, q]$ of distinct vertices $p, q \in K$. The incidence rules are: A vertex p of K is incident with K and with every block $[p, q]$ for every $q \neq p$; a point (i) is incident with $[p, q]$ if pq is an edge of G_i.

Notice the set of graphs G_i is a set of Hussain graphs, that is, $G_i = \langle i \rangle$.

A biplane is completely determined by a single block and its set of Hussain graphs, hence two biplanes D_1 and D_2 are isomorphic if and only if for any block B_1 of D_1 there is a block B_2 of D_2 such that the graphs in the set of Hussain graphs of B_1 are isomorphic to the graphs in the set of Hussain graphs of B_2. (That is, there is a bijection between the set of Hussain graphs of B_1 and the set of Hussain graphs of B_2 which maps simultaneously all the

Hussain graphs of B_1 to those of B_2, such that every graph is isomorphic to its image). In particular, there is an automorphism of the biplane D sending the block B_1 to the block B_2 if and only if the graphs in the complete set of Hussain graphs corresponding to the block B_1 are isomorphic to the graphs in the complete set of Hussain graphs corresponding to the block B_2.

Observation 2.2. In general, unless the group of automorphisms of a biplane D is transitive on the blocks of D, the graphs in the sets of Hussain graphs of two different blocks are not necessarily isomorphic.

2.2 Known Examples of Biplanes

As we mentioned earlier, from the parameter restrictions on symmetric designs it can be shown that there are no biplanes with $k = 7$, 8, 10, or 12, and the only examples known so far are for $k = 3$, 4, 5, 6, 9, 11, and 13. We give here a brief summary[21].

2.2.1 The Three Smallest Biplanes

There is exactly one biplane for each k, $(3 \leq k \leq 5)$; this can be seen because the set of Hussain graphs for each of these values of k is unique (up to isomorphism).

We start with $k = 3$. As the size of the set of Hussain graphs for a block is $v - k$, for $k = 3$, we need 1 graph on $k = 3$ points, which is a unique triangle. This is the (4,3,2) biplane, constructed on the set of points $P = \{1, 2, 3, 4\}$. Take $B_0 = \{1, 2, 3\}$ a difference set in $\mathbb{Z}_4$, and $B_i = B_0 + i,\ i = 1, 2, 3, 4$. That is, the blocks are the 3-subsets of P. The automorphism group is S_4, which is flag-transitive.

For $k = 4$ we need $v - k = 3$ divalent graphs on 4 points, that is three 4-gons. It is straightforward to see that the set in Figure 2.1 is unique. Here we have the (7,4,2) biplane, on the set of points $P = \mathbb{Z}_7$. Take $B_0 = \{3, 5, 6, 7\}$

a difference set, so $B_i = B_0 + i$, for $i = 1, \ldots, 7$. This is the complement of the Fano Plane. The automorphism group is $PSL_2(7)$, also flag-transitive.

In the case $k = 5$, we need six divalent graphs on 5 points, so they must be six pentagons, and because the two common edges between any two graphs do not have a common vertex, the set in Figure 2.2 is unique. We have the (11,5,2) biplane, the set of points is $P = \mathbb{Z}_{11}$, and $B_0 = \{1, 3, 4, 5, 9\}$ is a Paley Difference Set, (the set of squares modulo 11). The automorphism group is $PSL_2(11)$, also flag-transitive.

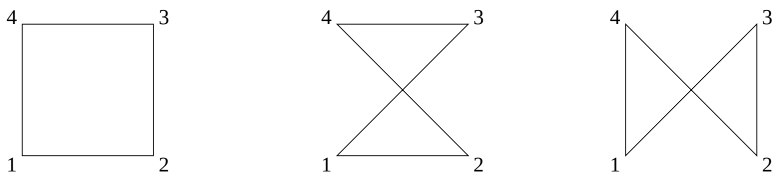

Figure 2.1: $k = 4$.

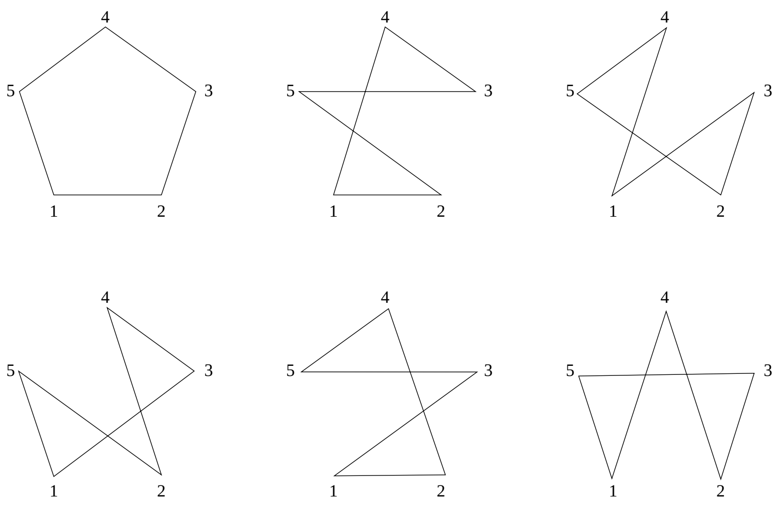

Figure 2.2: $k = 5$.

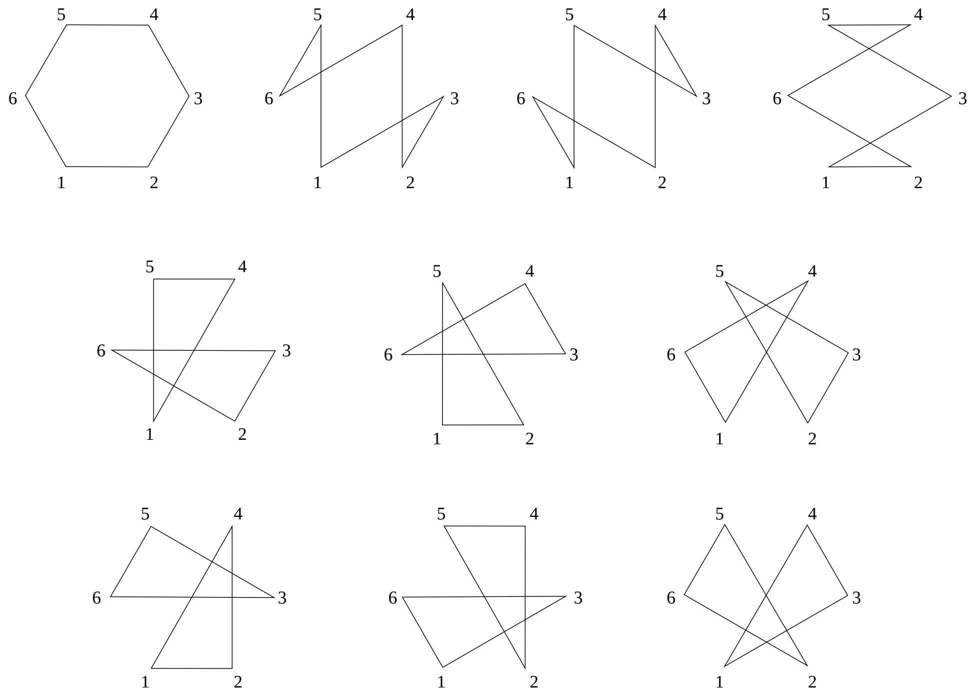

Figure 2.3: $k = 6$.

2.2.2 Biplanes with $k = 6$

It was established by Hussain [23] that there are exactly three non-isomorphic (16,6,2) biplanes, here we give a brief description [4, 21]. We need $v - k = 10$ divalent graphs on a set of six points. Hence each graph can be a hexagon, or a pair of triangles. It is not hard to show that the three non-isomorphic sets of Hussain graphs on six points are:

(i) Ten pairs of triangles.

(ii) Four hexagons and six pairs of triangles (Figure 2.3).

(iii) Six hexagons and four pairs of triangles (Figure 2.4).

For case (i), consider the set of ten pairs of triangles, any two of which must meet in two edges. Since any permutation of the six vertices is also a permutation of the pairs of triangles; the stabiliser of a block is the symmmetric group S_6. If the set of Hussain graphs of a block is a set of ten pairs

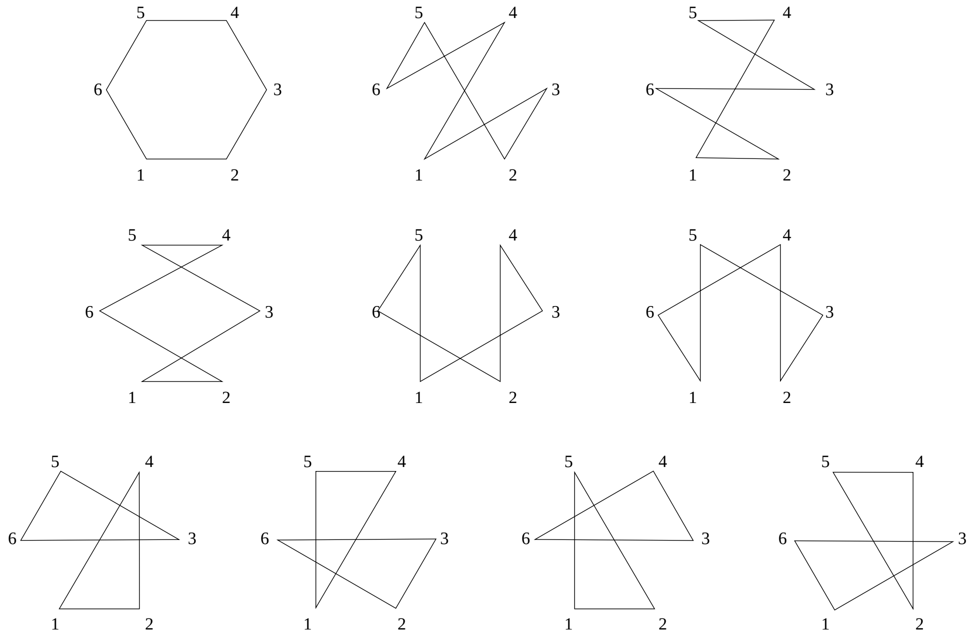

Figure 2.4: $k = 6$.

of triangles, then so is the set corresponding to any other block, therefore the automorphism group G is transitive on the blocks of the design, and has order $16 \cdot 6!$. This biplane arises from a difference set in $\mathbb{Z}_2^4$: Take the set of points $P = \mathbb{Z}_2^4$, and the set of blocks $B = \{B_0 + p : p \in P\}$, where $B_0 = \{\overline{0}, e_1, e_2, e_3, e_4, \sum_{i=1}^4 e_i\}$, and e_i is the vector with 1 in the i-th place, and 0 elsewhere, so $\{e_1, \ldots, e_4\}$ is the canonical basis for $\mathbb{Z}_2^4$. The automorphism group is $2^4 S_6 < 2^4 GL_4(2)$. Since the stabiliser $G_{\overline{0}}$ is transitive on all the blocks incident with $\overline{0}$, and the group of translations 2^4 acts regularly on the points of P, G is flag-transitive.

In case (*ii*) consider the set of graphs consisting of four hexagons and six pairs of triangles, (Figure 2.3). The following are automorphisms of the resulting biplane:

$$\alpha = (123456),\ \beta = (26)(35),\ \gamma = (23)(56),\ \delta = (36).$$

The permutation α shows that the stabiliser of the block $B_0 = \{1, 2, 3, 4, 5, 6\}$ is transitive on the points of B_0. By looking at the triangles containing 1 we see that the subgroup fixing 1 also fixes 4, in the same way 2 and 5 are fixed together, as are 3 and 6.

The group $\langle \beta, \gamma \rangle$ has order 4, and is transitive on the points 2, 3, 5, and 6. The subgroup fixing 1 and 2 also fixes 4 and 5, it is $\langle (3, 6) \rangle$, of order 2. Hence, the stabiliser of the block B_0 has order $2 \cdot 4 \cdot 6 = 48$. Also, G_{B_0} has three orbits on points, namely, the points incident with B_0, those corresponding to the hexagons, and those corresponding to the pairs of triangles. It too has three orbits on blocks, namely, B_0, those corresponding to the unordered pairs $\{1, 4\}$, $\{2, 5\}$ and $\{3, 6\}$, and the other twelve. The set of Hussain graphs for every block is isomorphic to that of B_0, hence the automorphism group G is transitive and has order $16 \cdot 48$. This biplane arises from a difference set in $\mathbb{Z}_2 \times \mathbb{Z}_8$, and the stabiliser of order 48 acts as the full group of symmetries of the cube, hence is a central extension of the symmetric group S_4 by a group of order 2. The group $\mathbb{Z}_2 \times \mathbb{Z}_8$ acts regularly, and hence the full automorphism group is flag-transitive.

Finally, we have case (*iii*). The biplane can be seen as a difference set in $Q \times \mathbb{Z}_2$, where Q is the quaternion group. The stabiliser of a block has two orbits on the points of the block, of size 2 and 4, therefore since the stabiliser is not transitive on the points of the block, we have that the full automorphism group is not flag-transitive. The order of the stabiliser is 24, and it acts as the inverse image of A_4 in the central extension of S_4 by a cyclic group of order 2 described in the previous case. The order of the automorphism group is $16 \cdot 24$, and it is not flag-transitive.

We can now proceed to state the following:

Theorem 1. *There are exactly three non-isomorphic (16,6,2) biplanes D_1, D_2, and D_3. Exactly two, say, D_1 and D_2 admit flag-transitive automorphism groups. Moreover:*

(i) *Both* D_1 *and* D_2 *admit imprimitive, flag-transitive automorphism groups, which are* $G_1 = 2^4S_4$ *and* $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_8)S_4$ *respectively.*

(ii) *Only* D_1 *has a primitive flag-transitive automorphism group of affine type, namely,* $G \leq 2^4S_6 < AGL_4(2)$.

Proof. We have seen above that there are exactly three non-isomorphic (16,6,2) biplanes, of which exactly two (D_1 and D_2) admit flag-transitive automorphism groups, and these are 2^4S_6, and $(\mathbb{Z}_2 \times \mathbb{Z}_8)\,(S_4.2)$. Now, both of these are affine groups contained in $AGL_4(2)$, where S_6 and $S_4.2$ are the point stabilisers in $GL_4(2)$. The group S_4 is contained in both of these stabilisers, and is transitive on the six cosets of V_4, so it is transitive on the six blocks containing the fixed point. Therefore the subgroups 2^4S_4 and $(\mathbb{Z}_2 \times \mathbb{Z}_8)\,(S_4)$ are still flag-transitive on the respective biplanes.

However S_4 fixes a subspace of dimension 2 in 2^4, so it is not irreducible, and therefore these subgroups are imprimitive. □

2.2.3 Biplanes with $k = 9$

There are exactly four (37,9,2) biplanes, [59]. The set of Hussain graphs corresponding to a fixed block, in general, depends on the choice of block. The ways in which nine vertices can be a disjoint union of polygons are:

(i) One 9-gon.

(ii) One hexagon and one triangle.

(iii) Three triangles.

(iv) One pentagon and one 4-gon.

The possible sets and number of blocks to which they correspond are as follows:

(*i*) 1 block with 28 graphs of type (3,3,3).

36 blocks with 21 graphs (9) and 7 graphs (6,3).

(*ii*) 9 blocks with 21 graphs (6,3).

28 blocks with 27 graphs (9) and 1 (3,3,3).

(*iii*) 37 blocks with 19 graphs (9) and 9 (5,4).

(*iv*) 27 blocks with 23 graphs (9), 4 (6,3), and 1 (5,4).

9 blocks with 27 graphs (9), and 1 (6,3).

1 block with 27 graphs (9), and 1 (3,3,3).

The only case in which all the blocks have the same set of Hussain graphs is (*iii*), so in all other cases the automorphism group is not transitive on blocks, and therefore is not flag-transitive.

Case (*i*): This biplane was first found by Hussain [24], the graphs are given by the elements of order 3 in $PSL_2(8)$. The full automorphism group is $P\Gamma L_2(8)$.

Case (*ii*): This is the dual of the previous biplane, and hence has the same automorphism group.

Case (*iii*): This biplane can be constructed from the difference set of nine quartic residues modulo 37. The automorphism group is $\mathbb{Z}_{37} \cdot \mathbb{Z}_9$, and it is flag-transitive, with the stabiliser of a point $G_0 \cong \mathbb{Z}_9$.

Case (*iv*): This biplane has an automorphism group of order 54, which fixes a unique point.

2.2.4 Biplanes with $k = 11$

There are five known (56,11,2) biplanes. The possible union of disjoint polygons on 11 vertices are as follows:

(*i*) One 11-gon.

(*ii*) One octagon and one triangle.

(*iii*) One heptagon and one 4-gon.

(*iv*) One hexagon and one pentagon.

(*v*) One pentagon and two triangles.

(*vi*) Two 4-gons and one triangle.

The possible sets of Hussain graphs, as well as the number of blocks to which they correspond in each of the five biplanes are as follows:

(*i*) All 56 blocks have 45 graphs of type (4,4,3).

(*ii*) 2 blocks with 45-(4,4,3).

18 blocks with 13-(4,4,3), 8-(5,3,3), and 24-(7,4).

36 blocks with 13-(4,4,3), 8-(7,4), 8-(8,3), and 16-(11).

(*iii*) 2 blocks with 36-(11) and 9-(7,4).

18 blocks with 4-(4,4,3), 8-(7,4), 17-(8,3), and 16-(11).

36 blocks with 5-(4,4,3), 8-(6,5), 12-(7,4), 8-(8,3), and 12-(11).

(*iv*) 32 blocks with 7-(4,4,3), 4-(5,3,3), 2-(6,5), 10-(7,4), 4-(8,3), and 18-(11).

16 blocks with 5-(4,4,3), 4-(5,3,3), 4-(6,5), 8-(7,4), 6-(8,3), and 18-(11).

4 blocks with 21-(4,4,3), and 24-(11).

4 blocks with 13-(4,4,3), 8-(5,3,3), and 24-(7,4).

(*v*) 8 blocks with 3-(5,3,3), 3-(6,5), 6-(7,4), 6-(8,3), and 27-(11).

6 blocks with 5-(4,4,3), 4-(5,3,3), 4-(6,5), 8-(7,4), 2-(8,3), and 22-(11).

12 blocks with 4-(5,3,3), 6-(6,5), 10-(7,4), 7-(8,3), and 18-(11).

24 blocks with 1-(4,4,3), 1-(5,3,3), 4-(6,5), 6-(7,4), 8-(8,3), and 25-(11).

6 blocks with 1-(4,4,3), 4-(5,3,3), 8-(7,4), 2-(3), and 30-(11).

Only in case (*i*) all the blocks have the same set of Hussain graphs, so in the other four cases the automorphism group is not transitive, and hence is not flag-transitive.

Case (*i*) was found first by Hall, Lane, and Wales [19] in terms of a rank-3 permutation group, and its associated strongly regular graph. The group of automorphisms is a subgroup of index 3 of Aut $(PSL_3(4))$, represented on the 56 cosets of A_6, which is the full stabiliser of a block. As we will see in following chapters, if the automorphism group G is flag-transitive, then k divides twice the order of G_0, but in this case $G_0 \cong A_6$, and 11 does not divide 720. Hence the group is not flag-transitive.

Case (*ii*) was found by a computer search by Assmus, Mezzaroba and Salwach [3]. The automorphism group has order 288.

Cases (*iii*) and (*iv*) were found by R. H. F. Denniston [18]. His constructions are based on $GF(9)$, and two other symbols A and B. As the points he takes the 55 unordered pairs of these symbols, and a further point (which he denotes - -), and assumes that addition and multiplication in $GF(9)$ (taking as its elements $a + bi,\ a, b \in GF(3)$) carry over to a biplane. Multiplication can be done by two methods, either fixing or interchanging A and B. The automorphism groups of (*iii*) and (*iv*) have orders 144 and 64 respectively.

Case (*v*) was constructed by Zvonimir Janko, assuming that a group of order 6 acts on the biplane. The full automorphism group is of order 24.

2.2.5 Biplanes with $k = 13$

There are only two known (79,13,2) biplanes. One was constructed by Michael Aschbacher [1] in 1970, and the other is its dual.

If we consider the elements of $GF(11)$ and two further elements A and B, we can take the unordered pairs of these elements to be the points of the biplane, plus one other point X. Addition and multiplication in $GF(11)$ fix A and B, but multiplication by a primitive root exchanges X and AB. The full group of automorphisms is $G = \langle x, y, z; x^2 = y^5 = z^{11}, x^y = x^4, x^z = x^{-1}, yz = zy\rangle$ which is of order 110, and is the only possible group of automorphisms for a biplane with $k = 13$ that has at least $v = 79$ points. Here k does not divide twice the order of the group so the group cannot be flag-transitive.

2.3 Flag-Transitive Biplanes

We give here a summary of the six known biplanes which do admit a flag-transitive automorphism group.

For $k = 3$, we have the unique (4,3,2) biplane, constructed from a difference set in $\mathbb{Z}_4$, with full automorphism group S_4, and point stabiliser S_3.

For $k = 4$, we have the unique (7,4,2) biplane, complement of $PG(2, 2)$, constructed from a difference set in $\mathbb{Z}_7$, with full automorphism group $PSL_2(7)$, and point stabiliser S_4.

For $k = 5$, we have the also unique (11,5,2) biplane, constructed from the difference set of squares in $\mathbb{Z}_{11}$, with full automorphism group $PSL_2(11)$, and point stabiliser A_5.

For $k = 6$, we have two non-isomorphic (16,6,2) biplanes admitting a flag-transitive automorphism group. The first of these is constructed from a difference set in $\mathbb{Z}_2^4$, with full automorphism group $\mathbb{Z}_2^4 \cdot S_6$, where $\mathbb{Z}_2^4$ is the group of translations, and S_6 is the point stabiliser, transitive on the 6 blocks containing 0.

The second arises from a difference set in $\mathbb{Z}_2 \times \mathbb{Z}_8$, and the full automorphism group is $(\mathbb{Z}_2 \times \mathbb{Z}_8)\,(S_4.2)$. Again, $\mathbb{Z}_2 \times \mathbb{Z}_8$ is the group of translations acting regularly, and the point stabiliser is $S_4.2$.

For $k = 9$, we have only one of the four (37,9,2) biplanes, namely the one constructed from the difference set of the quartic residues in $\mathbb{Z}_{37}$. The full automorphism group is $\mathbb{Z}_{37} \cdot \mathbb{Z}_9$, where $\mathbb{Z}_{37}$ is the group of translations, and $\mathbb{Z}_9$ is the point stabiliser, transitive on the nine blocks containing 0.

Finally we list the parameters of the six known flag-transitive biplanes, with their full automorphism groups and point stabilisers:

(i) (4,3,2), S_4, S_3.

(ii) (7,4,2), $PSL_2(7)$, S_4.

(iii) (11,5,2), $PSL_2(11)$, A_5.

(iv) (16,6,2), 2^4S_6, S_6.

(v) (16,6,2), $(\mathbb{Z}_2 \times \mathbb{Z}_8)\,(S_4.2)$, $(S_4.2)$.

(vi) (37,9,2), $\mathbb{Z}_{37} \cdot \mathbb{Z}_9$, $\mathbb{Z}_9$.

3. PRIMITIVITY AND REDUCTION

The fact that not many examples of biplanes are known, by no means rules out the possibility of more biplanes yet to be discovered. It is in this light that the present classification is made.

3.1 Primitivity

Firstly, we state the following:

Theorem 2. *If G is a flag-transitive automorphism group of a (v, k, λ)-symmetric design D, with $\lambda \leq 7$, then G is primitive, or D has parameters (16,6,2), (45,12,3), (15,8,4), (96,20,4), (175,30,5), (16,10,6), (36,15,6), (288,42,6), (27,14,7), (247,42,7), or (441,56,7).*

Before proving the theorem, we give the following,

Definition 3.1. If G is a permutation group and G_α is the stabiliser of a point, then the size of each non-trivial orbit of G_α is a *subdegree* of G.

and state the following:

Lemma 3.2. *If D is a (v, k, λ)-symmetric design with a flag-transitive automorphism group G, then k divides λd_i for every subdegree d_i of G.*

Proof. Let D be a (v, k, λ)-symmetric design with a flag-transitive automorphism group G. Fix a point α, and consider a non-trivial orbit of G_α, call it, say, Δ. Now count all flags (p, B_j) such that $p \in \Delta$, and both p and α are incident with B_j.

Let $|\Delta| = \delta$. Then there are δ points in Δ, each of which, together with α, is incident with λ blocks. Hence there are $\lambda\delta$ such flags.

Also, there are k blocks incident with α. The fact that G is flag-transitive implies that G_α is transitive on the k blocks through α, therefore they are all incident with the same number of points in Δ. Hence the result. $\square$

Combining this with Lemma 1.7, we get the following:

Corollary 3.3. *If G is a flag-transitive automorphism group of a (v, k, λ)-symmetric design D, then k divides $\lambda \cdot hcf\,(v-1, |G_\alpha|)$, for every point stabiliser G_α.*

This is a a fact which will prove very useful in the course of this thesis. And now, we proceed to prove Theorem 2, applying the methods by Davies in [14]:

Proof of Theorem 2. Suppose we have a (v, k, λ)-symmetric design D, with a flag-transitive automorphism group G which is imprimitive. Then P, the set of points is partitioned into n non-trivial blocks of imprimitivity Δ_j, $j = 1, \ldots, n$, each of size c. Now, as G is flag-transitive, we have that each block of D and each block of imprimitivity that intersect non trivially, do so in a constant number of points, say d, since G permutes these intersections transitively. Therefore, for each $i = 1, \ldots, v$, $j = 1, \ldots, n$ we have that $|B_i \cap \Delta_j| \in \{0, d\}$, where $B_1, \ldots B_v$ are the blocks of D. We claim the the following equations hold,

(*i*) $v = cn$

(*ii*) $k = ds$

(*iii*) $\lambda(v-1) = k(k-1)$

(*iv*) $\lambda(c-1) = k(d-1)$

with c, n, d, s integers greater than 1, and s the number of blocks of imprimitivity intersected by each block of the design. Equation (*i*) is a consequence of the imprimitivity of G. Equation (*ii*) is a consequence of the non-empty intersections of blocks of imprimitivity and blocks of B having a constant number of points (d). Equation (*iii*) is Lemma 1.7. For Equation (*iv*), fix a point α. Now count flags (p, B_i) such that p and α are in the same block of imprimitivity, (say, Δ), and both p and α are incident with B_i. Since each block of imprimitivity has constant size c, there are $c-1$ such points, and each of them is, together with α, incident with λ blocks, which gives us the left hand side of the equation. On the other hand, there are k blocks through α, and each of them intersects Δ in d points (as they are incident with α we already know the intersection is non-empty), of which $d-1$ are not α, and this gives us the right hand side of the equation.

From Equation (*iv*):

$$\lambda n(c-1) = kn(d-1),$$

and from Equations (*i*) and (*iii*) we have that

$$v = cn = \frac{k(k-1)+\lambda}{\lambda},$$

which together with (*iv*) yields

$$c = \frac{k(d-1)+\lambda}{\lambda}.$$

Subtracting the first equation from the second we get $\lambda(n-1) = k(k-1-n(d-1))$. Let $x = k-1-n(d-1)$. Then x is a positive integer, and we have $\lambda(n-1) = kx$, hence

$$n = \frac{kx+\lambda}{\lambda}.$$

Combining the above equations we get that

$$cn = \frac{k(k-1)+\lambda}{\lambda} = \frac{(k(d-1)+\lambda)(kx+\lambda)}{\lambda^2},$$

and solving for k we get the following equation:

$$k = \frac{\lambda(x+d)}{\lambda - x(d-1)}.$$

Therefore $\lambda > x(d-1)$, which is a positive integer. We now analyse for each value of λ:

$\lambda = 2$: We have that $2 > x(d-1) > 0$. This forces $x(d-1) = 1$, so $x = 1$ and $d = 2$, so from the last equation we see that $k = 6$ (and so $n = c = 4$, and $s = 3$). Therefore the only possible parameters for $\lambda = 2$ are (16,6,2).

$\lambda = 3$: Here we have $3 > x(d-1) > 0$, which gives us the following possible values for x and d:

(*i*) $x = 1$ and $d = 2$,

(*ii*) $x = 1$ and $d = 3$, or

(*iii*) $x = 2$ and $d = 2$.

The first case gives a non-integer value of k, which is impossible. The second and third cases yield $k = 12$, which gives the admissible parameters (45,12,3).

$\lambda = 4$: We have that $4 > x(d-1) > 0$, which gives us the following possible combinations of values for x and d:

(*i*) $x = 1$ and $d = 2, 3, 4$,

(*ii*) $x = 2$ and $d = 2$, or

(*iii*) $x = 3$ and $d = 2$.

These give us the following values for k: 4,8, and 20. We immediately rule out $k = 4$, as having $k = \lambda$ gives us a trivial design.

For $k = 8$, we would have (from Lemma 1.7) $56 = 4(v - 1)$, which means $v = 15$, and this yields the possible set of parameters (15,8,4).

For $k = 20$, we have $380 = 4(v - 1)$, so $v = 96$, and hence the possible set of parameters is (96,20,4).

$\lambda = 5$**:** Here we have $5 > x(d - 1) > 0$, with the following possible combinations of values of x and d:

(*i*) $x = 1$ and $d = 2, 3, 4, 5$,

(*ii*) $x = 2$ and $d = 2, 3$,

(*iii*) $x = 3$ and $d = 2$, or

(*iv*) $x = 4$ and $d = 2$.

For $x = 1$, the only integer value of k is 30, when $d = 5$. For $x = 2$, the only integer value for k is 25, when $d = 3$, but then d does not divide k, so this case is ruled out. In the third case the value of k is not an integer, and in the last case we obtain, again, $k = 30$; hence $5(v - 1) = 870$ and so $v = 175$. So the admissible parameters in this case are (175,30,5).

$\lambda = 6$**:** In this case $6 > x(d - 1) > 0$, so we have the following possiblities:

(*i*) $x = 1$ and $d = 2, 3, 4, 5, 6$,

(*ii*) $x = 2$ and $d = 2, 3$,

(*iii*) $x = 3$ and $d = 2$,

(*iv*) $x = 4$ and $d = 2$, or

(*v*) $x = 5$ and $d = 2$.

In the first case, the only integer value of k greater than λ, with d dividing k is $k = 42$ (when $d = 6$). In the second case, we get $k = 15$, which gives the possible set of parameters (36,15,6). For $x = 3$ we get $k = 10$, and this gives us the possible set of parameters (16,10,6). For $x = 4$, we obtain $k = 18$, which implies $v = 52$, but Theorem 1.8 states that if v is even, then $n = k - \lambda$ is a square, and in this case $n = 12$, which is not a square. In the last case, we obtain $k = 42$, and hence the possible set of parameters (288,42,6).

$\lambda = 7$: Here we have $7 > x(d-1) > 0$, so the possible values of x and d are as follows:

(*i*) $x = 1$ and $d = 2, 3, 4, 5, 6, 7$,

(*ii*) $x = 2$ and $d = 2, 3, 4$,

(*iii*) $x = 3$ and $d = 2, 3$,

(*iv*) $x = 4, 5, 6$ and $d = 2$.

For $x = 1$, the only case in which k has an integer value divisible by d is when $d = 7$ and $k = 56$. In this case we have $v = 441$, with the possible set of parameters (441,56,7). When $x = 2$, there are no integer values of k divisible by d. For the next case, the only integer value of k we obtain that is divisible by d is 42, when $d = 3$, and this gives us the set of parameters (247,42,7). When $x = 4$ and $d = 2$, we obtain the set (27,14,7). For $x = 5$ the value of k is not an integer; and for the last case, again, we obtain (441,56,7).

□

Corollary 3.4. *If a biplane D has an imprimitive, flag-transitive automorphism group, then D has parameters (16,6,2). And by Theorem 1, there are exactly two such biplanes.*

3.2 The O'Nan-Scott Theorem

In view of the above corollary, we know that except for the two (16,6,2) examples, flag-transitive automorphism groups of biplanes are necessarily primitive, hence we can apply the O'Nan-Scott Theorem [44], which classifies primitive groups into five types. Of these, we shall prove that primitive flag-transitive automorphism groups of biplanes can only be affine or almost simple.

Let X be a primitive permutation group on a finite set Ω, and suppose that N is a minimal normal subgroup of X. Then N is transitive. (Otherwise, its orbits would be blocks of imprimitivity of X). The centraliser $\mathrm{C}_X(N)$ is also normal in X. If such centraliser is not trivial, then it is also transitive; and regular, as well as N. If N is abelian, then N and $\mathrm{C}_X(N)$ have the same elements, if N is not abelian, then they are not equal as sets; and X has no more minimal normal subgroups, (since they centralise each other). Also, since N and $\mathrm{C}_X(N)$ are right and left regular representations of the same group, they are isomorphic. If, on the other hand, $\mathrm{C}_X(N)$ is trivial, then N is the unique minimal normal subgroup of X, and X is isomorphic to a subgroup of $\mathrm{Aut}(N)$. Let B be the socle of X, that is, the product of its minimal normal subgroups. Then, in either case, B is a direct product of isomorphic simple groups. That is, $B \cong T^c$, with $c \geq 1$ and T a simple group.

The O'Nan-Scott Theorem states that the action of any finite primitive permutation group is of one of the following five types:

(*i*) Affine.

(*ii*) Almost simple.

(*iii*) Simple diagonal.

(*iv*) Product.

(v) Twisted wreath.

We will now explain briefly each of these actions. In what follows, as above, X will be a primitive permutation group acting on a finite set Ω of size n, α will be a point in Ω, and B will be the socle of X, isomorphic to T^k, with T a simple group and $k \geq 1$.

Affine groups In this case we have $T = \mathbb{Z}_p$, where p is a prime; and B is the unique minimal normal subgroup of X with a regular action on Ω of degree $n = p^c$. Hence, Ω can be identified with $B \cong \mathbb{Z}_p^c$ so that $X \leq AGL_c(p)$, with B the translation group and $X_\alpha = X \cap GL_c(p)$ irreducible on B. In the remaining four cases, T is nonabelian.

Almost simple groups Here we have $c = 1$, $T \leq X \leq \text{Aut}\ T$, and $T_\alpha \neq 1$. For the following three types, we have $c \geq 2$.

Simple diagonal action Let

$$W = \{(a_1, \ldots, a_c) \cdot \pi \ \mid \ a_i \in \text{Aut}\ T,\ \pi \in S_c,\ a_i \equiv a_j \text{ mod Inn } T\ \forall\ i, j\},$$

where $\pi \in S_c$ permutes the components naturally. Then with the obvious multiplication W is a group, its socle is $B \cong T^c$, and $W = B \cdot (\text{Out}\ T \times S_c)$ is a (not necessarily split) extension of B by $\text{Out}\ T \times S_c$. Now define Ω as the set of cosets of $\text{Aut}T \times S_c$ of W, and we define an action of W on Ω as follows:

Let $W_\alpha = \{(a, \ldots, a) \cdot \pi \ \mid \ a \in \text{Aut}\ T,\ \pi \in S_c\}$. Then $W_\alpha \cong \text{Aut}\ T \times S_c$, $B_\alpha \cong T$, and $n = |T|^{c-1}$.

Now, for $1 \leq i \leq c$, let T_i be the subgroup of B consisting of all the c-tuples with 1 in all except the ith component, so that $T_i \cong T$, and $B = T_1 \times \ldots \times T_c$. Let $\mathcal{T} = \{T_1, \ldots, T_c\}$, so W acts on $\mathcal{T}$. Then the subgroup $X \leq W$ is of simple diagonal type if $B \leq X$, and the action of X on $\mathcal{T}$ is primitive, or $X^{\mathcal{T}} = 1$ and $c = 2$.

If the action of X on $\mathcal{T}$ is primitive, then B is the unique minimal normal subgroup of X; if it is trivial, then X has two minimal normal subgroups, T_1 and T_2, both acting regularly on Ω. In either case, $X_\alpha \lesssim \mathrm{Aut}\ T \times X^{\mathcal{T}}$, and $X \leq B \cdot (\mathrm{Out}\ T \times X^{\mathcal{T}})$.

Product action Take H to be a primitive permutation group, almost simple, or with simple diagonal action on a finite set Γ. For $l > 1$, let $W = H \text{ wr } S_l$, and take W to act on $\Omega = \Gamma^l$ in its natural product action, that is, for $(\gamma_1, \ldots, \gamma_l) \in \Omega$, the base group H^l acts coordinatewise, and S_l acts by permuting the coordinates. Then for $\gamma \in \Gamma$ and $\alpha \in \Omega$, $W_\alpha = H_\gamma \text{ wr } S_l$, and $n = |\Gamma|^l$. If K is the socle of H, then the socle of W is $B = K^l$, and $B_\alpha = (K_\gamma)^l \neq 1$.

Now W acts naturally on the l factors in K^l, and we say that the group $X \leq W$ has a product action if $B \leq X$ and X acts transitively on these l factors. If H is almost simple, then $K \cong T$, $c = l$, and B is the unique minimal normal subgroup of X, and if H has a simple diagonal action, then $K \cong T^{\frac{c}{l}}$, and both X and H have m minimal normal subgroups, with $m \leq 2$; if $m = 2$ then each of the two minimal normal subgroups of X acts regularly on Ω.

Twisted wreath action Let P be a transitive permutation group acting on $\{1, \ldots, c\}$ and let Q be the stabiliser P_1. Suppose there is a homomorphism $\phi : Q \to \mathrm{Aut}\ T$ such that $\mathrm{Inn}\ T \subseteq \mathrm{Im}\ \phi$.

Now define $B = \{f : P \to T \mid f(pq) = f(p)^{\phi(q)}\ \forall p \in P,\ q \in Q\}$. Then B is a group under pointwise multiplication, and $B \cong T^c$. Let P act on B by the following rule: $f^p(x) = f(px)$ for all $p, x \in P$.

We define $X = T \text{ twr}_{\phi}\ P$ to be the semidirect product of B by P with this action, and define the action of X on Ω by setting $X_\alpha = P$. Then we have $n = |T|^c$, and B is the unique minimal normal subgroup of X, which acts regularly on Ω. We say that X has a twisted wreath action if it acts primitively on Ω.

Observation 3.5. Although the above described actions are pairwise disjoint (consider the structures and actions of the socles B on Ω), the group X described with a twisted wreath action is in fact contained in the wreath product H wr S_k, which has a product action on Ω. Here $H = T \times T$ is of diagonal type, and the socle of H wr S_k is isomorphic to $B \times B$.

We now state, without proof, the O'Nan-Scott Theorem:

Theorem 3.6 (O'Nan-Scott). *[44] If X is a primitive permutation group acting on a finite set Ω, then it is permutation equivalent to one of the following types:*

(*i*) *Affine.*

(*ii*) *Almost simple.*

(*iii*) *Simple diagonal.*

(*iv*) *Product.*

(*v*) *Twisted wreath.*

3.3 Reduction

We now apply the O'Nan Scott Theorem to prove the following:

Theorem 3. *If G is a flag-transitive, primitive automorphism group of a biplane D, then G is of affine or almost simple type.*

Proof. Let G be a flag-transitive, primitive automorphism group of a biplane D. Since G is primitive, by the O'Nan-Scott Theorem it must be of one of the following five types: product, diagonal, twisted wreath, affine, or almost simple. To prove the theorem, we will assume G has a simple diagonal or product action, and arrive at a contradiction. In view of the earlier observation that twisted wreath groups are contained in wreath products with a product action on Ω, and the fact that in our proof for groups with product action we also rule out their subgroups, it is not necessary in this proof to analyse the twisted wreath product case.

1) First assume G is of simple diagonal type. Then

$$\text{Soc}\,(G) = N = T^m,\ m \geq 2$$

for some non-abelian simple group T, and

$$T \cong \langle t, \ldots, t \rangle \cong \{(t, \ldots, t) : t \in T\},$$

which is the stabiliser $N_\alpha \lhd G_\alpha \leq$ Aut $T \times S_m$.

Here we have that $v = |T|^{m-1} = |N_\alpha|^{m-1}$.

Now, the fact that G is flag-transitive implies that G_α is transitive on the k blocks through α, so $N_\alpha \lhd G_\alpha$ implies that the orbits of N_α on the set of k blocks through α all have the same size.

Let l be the size of these orbits. Then $l \mid k$, so $l \mid k(k-1) = 2(v-1)$, and l divides $|N_\alpha| = |T|$. Hence $l \mid (|T|, 2\,(|T|^{m-1} - 1)) = 2$. Therefore $l = 1$, or $l = 2$.

Since T is a non-abelian simple group, there is an odd prime r which divides $|T|$. Pick $t \in N_\alpha$ such that $o(t) = r$. Then t fixes every block through α, as the orbits have length 1 or 2. Now suppose t sends a point β to a point γ. Then the pair $\{\alpha, \beta\}$ lies in exactly two blocks which are fixed by t, so γ must also be in each of those blocks; but every pair of blocks intersects in exactly two points. So $\beta = \gamma$, hence t fixes every point; which is a contradiction since $o(t) = r > 2$.

Hence G is not of simple diagonal type.

2) Now assume G has a product action. Then there is a group H acting primitively on Γ (with $|\Gamma| \geq 5$) of almost simple or diagonal type, where:

$$\Omega = \Gamma^l, \text{ and } G \leq H^l \rtimes S_l = H \text{ wr } S_l.$$

Take $x \in P$. If $x = (\gamma_1, \ldots, \gamma_l)$, define for $1 \leq j \leq l$ the *cartesian line of the j^{th} parallel class* through x to be the set:

$$\mathcal{G}_{x,j} = \{(\gamma_1, \ldots, \gamma_{j-1}, \gamma, \gamma_{j+1}, \ldots, \gamma_l) \mid \gamma \in \Gamma\},$$

that is,

$$\mathcal{G}_{x,j} = \{\gamma_1\} \times \ldots \times \{\gamma_{j-1}\} \times \Gamma \times \{\gamma_{j+1}\} \times \ldots \times \{\gamma_l\}.$$

(So there are l cartesian lines through x).

Denote $|\Gamma| = m$.

By the primitivity of G, we have that G_x is transitive on the l cartesian lines through x. Denote by Δ the union of those lines (excluding x). Then Δ is a union of orbits of G_x, and so every block through x intersects it in the same number of points. Hence k divides $2l(m-1)$. Also, we have $k^2 > 2m^l$, so $2m^l < 4l^2(m-1)^2$.

Hence $m^l \leq 2l^2(m-1)^2$.

As we stated before that $m \geq 5$, we have then that $2 \leq l \leq 3$.

First assume $l = 2$. Then k divides $4(m-1)$. But we also have that $k(k-1) = 2(v-1)$, and $2(v-1) = 2(m^2-1) = 2(m-1)(m+1)$. So, as $m < k$, we have that $k = \frac{4(m-1)}{r}$, with $1 \leq r \leq 3$. If $r = 1$, then $k(k-1) = 4(m-1)(4m-5)$, and $2(v-1) = 2(m-1)(m+1)$, so

$$8m - 10 = m + 1,$$

which implies that $7m = 11$, a contradiction.

If $r = 2$, then $k(k-1) = 2(m-1)(2m-3)$, so

$$2m - 3 = m + 1,$$

which implies that $m = 4$, contradicting the fact that $m \geq 5$.

Finally, if $r = 3$ then

$$4(m-1)(4m-5) = 18(m-1)(m+1),$$

so $8m - 10 = 9m + 9$, which implies that $m = -19$, another contradiction.

Now assume $l = 3$. Then $m < 18$, and k divides $2(3(m-1), m^3 - 1)$, so k divides

$$2(m-1)(3, 1 + m + m^2).$$

Now $(3, 1 + m + m^2) = 3$ only when $m \equiv 1 \pmod 3$, that is, when $m = 7, 10, 13$, or 16. In the first three of these cases we have that $8v - 7$ is not a square, contradicting Lemma 1.15. If $m = 16$ then v is even, but $k - \lambda = 89$ is not a square, contradicting Theorem 1.8. Therefore $k = 2(m-1)$, and so

$$2m - 3 = m + 1,$$

which implies that $m = 4$, a contradiction.

Hence G is of affine or almost simple type. □

4. BIPLANES WITH AUTOMORPHISM GROUPS OF AFFINE TYPE

In this chapter we will prove the following:

Theorem 4. *If D is a biplane with a primitive, flag-transitive automorphism group G of affine type, then one of the following holds:*

(*i*) *D has parameters (4,3,2).*

(*ii*) *D has parameters (16,6,2).*

(*iii*) *$G \leq A\Gamma L_1(q)$, for some prime power q.*

For this purpose we consider biplanes which have a flag-transitive automorphism group G of affine type, that is, the points of the biplane can be identified with the vectors in a vector space $V = V_d(p)$ of dimension d over the field $\mathbb{F}_p$, (with p prime), so that $G = TG_x \leq AGL_d(p) = AGL(V)$, where $T \cong (\mathbb{Z}_p)^d$ is the translation group, and G_x (the stabiliser of the point x) is an irreducible subgroup of $GL_d(p)$.

Now, for each divisor n of d, there is a natural irreducible action of the group $\Gamma L_n\left(p^{\frac{d}{n}}\right)$ on V. Choose n to be the minimal divisor of d such that $G_x \leq \Gamma L_n(p^{\frac{d}{n}})$ in this action, and write $q = p^{\frac{d}{n}}$. Hence we have $G_x \leq \Gamma L_n(q)$, and $v = p^d = q^n$.

4.1 Preliminary Results

In this section we state some results (some of which have been stated previously in this work) and definitions which will be useful throughout the following chapters.

Throughout, D will be a $(v, k, 2)$-biplane with a primitive automorphism group G, and G_x the point-stabiliser, which is maximal in G, since G is primitive.

We begin by recalling the following lemma and corollary from Chapter 1:

Lemma 4.1. *If D is a $(v, k, 2)$-biplane, then $2(v-1) = k(k-1)$.*

Solving the previous equation for k, we have that $k = \frac{1+\sqrt{8v-7}}{2}$, and hence the following

Corollary 4.2. *If D is a $(v, k, 2)$-biplane, then $8v-7$ is a square.*

Also, from the previous lemma, we have the following

Corollary 4.3. *If D is a flag-transitive $(v, k, 2)$-biplane, then $v < k^2$, and hence $|G| < |G_x|^3$.*

Proof. Since $k(k-1) = 2(v-1)$, we have that $k^2 = 2v - 2 + k$, so clearly $v < k^2$. Since $v = |G : G_x|$, and $k \leq |G_x|$, the result follows. □

From Lemma 3.2 we get the following:

Lemma 4.4. *If D is a biplane with a flag-transitive automorphism group G, then k divides $2d_i$ for every subdegree d_i of G.*

Corollary 4.5. *If G is a flag-transitive automorphism group of a biplane D, then k divides $2 \cdot \mathrm{hcf}\,(v-1, |G_x|)$.*

The following result restricts the possibilities for biplanes where v is a power of 2:

Theorem 4.6 (Ramanujan-Nagell). *[64, p.99] The only integer solutions for the equation $x^2 + 7 = 2^a$ are the following:*

$$(\pm x, a) = (1,3), (3,4), (5,5), (11,7), (181,15).$$

If D is a $(2^b, k, 2)$ biplane, then by Corollary 4.2 we have that $2^{b+3} - 7$ is necessarily a square, so by Theorem 4.6 the only pair of solutions for which there can be a biplane with $v = 2^b = 2^{a-3}$ are (5,5) and (11,7), (which correspond to the parameters (4,3,2) and (16,6,2), respectively). The first two imply a value of v that is too small, and the last implies $k = 91$, but then $k - \lambda = 89$, which is not a square, contradicting Theorem 1.8. Hence we have the following:

Corollary 4.7. *If D is a $(2^b, k, 2)$-biplane, then b=2 or 4.*

The proof of Theorem 4 will use the following result by Aschbacher [2]:

Theorem 4.8 (Aschbacher). *Let G be a group such that $X \trianglelefteq G \leq \Gamma$, with $X = Cl_n(q)$, and $\Gamma = \Gamma L_n(q)$. Let H be a maximal subgroup of G not containing X. Then there is a collection $\mathcal{C}$ of subgroups of Γ described below such that either H is contained in a member of $\mathcal{C}$, or the last term of the derived series of H, that is, $H^{(\infty)}$, is absolutely irreducible, not realisable over any proper subfield of $\mathbb{F}_q$, and quasisimple.*

By quasisimple we mean that $L = H^{(\infty)}/Z\left(H^{(\infty)}\right)$ is a non-abelian simple group, and we define $V = V_n(q)$, an n-dimensional vector space over the field of q elements. The collection $\mathcal{C}$ of subgroups of Γ has eight members, we now give a brief description [33]:

$\mathcal{C}_1$) Stabilizers of totally singular or non-singular subspaces of V.

$\mathcal{C}_2$) Stabilizers of decompositions $V = \bigoplus_{i=1}^{t} V_i$, where all the subspaces have the same dimension.

$\mathcal{C}_3$) Stabilizers of extension fields of $\mathbb{F}_q$ of prime index b.

$\mathcal{C}_4$) Stabilizers of tensor product decompositions $V = V_1 \otimes V_2$.

$\mathcal{C}_5$) Stabilizers of subfields of $\mathbb{F}_q$ of prime index b.

$\mathcal{C}_6$) Normalizers of symplectic-type r-groups (r prime) in absolutely irreducible representations.

$\mathcal{C}_7$) Stabilizers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, with all the subspaces of equal dimension.

$\mathcal{C}_8$) Classical subgroups.

For a more precise description of this collection of subgroups, see [33].

We also have the following lemma:

Lemma 4.9. *[41, 2.8] Let $r \leq 11$ be a prime, and let q be a prime power as in Table 4.1. Then the order of r modulo q (i.e., the order of r in the group of units of $\mathbb{Z}_q$) is as given in Table 4.1.*

	$q=$	8	16	32	64	9	27	81	5	25	125	7	49	11	13	17	19	23	29	31
$r=2$						6	18	54	4	20	100	3	21	10	12	8	18	11	28	5
$r=3$		2	4	8	16				4	20	100	6	42	5	3	16	18	11	28	30
$r=5$		2	4	8	16	6	18	54				6	42	5	4	16	9	11	14	30
$r=7$		2	2	4	8	3	9	27	4	4	20			10	12	16	3	22	14	15
$r=11$		2	4	8	16	6	18	54	2	10	50	3	21		12	16	3	22	28	30

Table 4.1:

4.2 Reduction to Quasisimple Groups

By Theorem 1 and the fact that there is a unique (4,3,2) biplane, we can assume D to not have parameters (4,3,2) nor (16,6,2), and by Theorem 4.6 we have that if q is even then necessarily it is either 4 or 16, therefore we need only consider $p > 2$. Since the case $G \leq A\Gamma L_1(q)$ is a conclusion of Theorem 4, we may also assume $G \nleq A\Gamma L_1(q)$.

Also, since Theorem 1.11 classifies all symmetric designs with 2-transitive automorphism groups, we will assume that G_x is not transitive on $V \setminus \{x\}$.

So, for the proof of Theorem 4, we assume $p > 2$, $n > 1$, and G_x not transitive on $V \setminus \{x\}$.

The work in the rest of this chapter will be mainly group theoretic. We will assume $G \leq AGL_d(p)$ to be a flag-transitive automorphism group of a biplane D. By Theorem 4.8, there is a collection $\mathcal{C}$ of subgroups of $\Gamma L_n(q)$ (where $q^n = p^d$) such that either G_x is contained in a member of $\mathcal{C}$, or the last term of the derived series of G_x, that is $G_x^{(\infty)}$, is irreducible and quasisimple. Denote $H = G_x^{(\infty)}$, and $L = H/Z(H)$.

We begin by stating a group-theoretic proposition, then analyse the cases in which G_x is contained in a member of the collection $\mathcal{C}$, and finally handle the cases in which L is an alternating group, a sporadic group, a group of Lie type in characteristic p, and finally a group of Lie type in characteristic p'. We will use representation theory as well as arithmetic conditions, most of which have already been stated in previous chapters.

In this section, we see that if a biplane D has a flag-transitive, primitive, automorphism group of affine type, (as described above), then H is quasisimple.

Theorem 4.10. *Let $G \leq AGL_d(p)$ $(p > 2)$ be a flag-transitive, affine, primitive automorphism group of a biplane D which is not 2-transitive, with $G_x \leq \Gamma L_n\left(p^{\frac{d}{n}}\right)$, ($n$ minimal, $n > 1$). (So $v = p^d = q^n$). Then $H = G_x^{(\infty)}$ is quasisimple, and its action on $V = V_n(q)$ is absolutely irreducible and not realisable over any proper subfield of $\mathbb{F}_q$.*

The starting point for the proof of Theorem 4.10 is the group-theoretic proposition [41, 3.1]:

Proposition 4.11. *Under the assumptions of Theorem 4.10, one of the following holds:*

(i) *G_x contains a unitary group $SU_n(q^{\frac{1}{2}})$ or an orthogonal group $\Omega_n(q)$ in its natural action on $V = V_n(q)$.*

(ii) *G_x lies in a tensor product subgroup of $GL_d(p)$, either*

(a) *$V_d(p) = V_a \otimes V_c$ and $G_x \leq GL_a(p) \otimes GL_c(p)$ in its natural action on V, where V_a, V_c are spaces over $\mathbb{F}_p$ of dimension a, c and $d = ac$, $a > c \geq 2$, or*

(b) *$V_d(p) = V_a \otimes \cdots \otimes V_a$ ($m > 1$ copies), $d = a^m$, and $G_x \leq N(GL_a(p) \otimes \cdots \otimes GL_a(p))$.*

(iii) *G_x lies in the normaliser of an irreducible symplectic-type s-group R, (where s is a prime, $s \neq p$), and $R \leq G_x$, either*

(a) *$G_x \leq \mathbb{F}_q^* \circ s^{1+2m} \cdot Sp_{2m}(s) \cdot \log_p(q)$, $n = s^m$ and $s \mid (q-1)$, or*

(b) *$G_x \leq \mathbb{F}_q^* \circ 2_{\pm}^{1+2m} \cdot O_{2m}^{\pm}(2) \cdot \log_p(q)$ and $n = 2^m$. Further, if $s = 2$ then $q = p$ or p^2.*

(iv) *$G_x^{(\infty)}$ is a quasisimple group, and its action on $V = V_n(q)$ is absolutely irreducible and not realisable over any proper subfield of $\mathbb{F}_q$.*

We must mention here that although [41] classifies linear spaces, the proof of the above proposition is still valid when considering $\lambda = 2$, and hence it is still relevant in this case. If X is a classical group and G_x contains X, then (i) holds, since G_x is not transitive on $V \setminus \{x\}$. If G_x does not contain X, then by Theorem 4.8, either (iv) holds, or G_x is in a member of one of the families $\mathcal{C}_i$ $(1 \leq i \leq 7)$ of subgroups of $N_{\Gamma L_n(q)}(X)$.

Members of $\mathcal{C}_1$ are reducible on V, so G_x does not lie in one of these. Members of $\mathcal{C}_2$ permute the subspaces in a direct sum decomposition of V, so in the language of [7] they are of affine cartesian type, contradicting Theorem 3. By definition of q, G_x is not contained in a member of $\mathcal{C}_3$. Members of $\mathcal{C}_4$, $\mathcal{C}_5$, and $\mathcal{C}_7$ satisfy (ii), and members of $\mathcal{C}_6$ satisfy (iii).

Lemma 4.12. *Case 4.11 (i) does not hold.*

Proof. First consider the unitary case. Here, $G_x \rhd SU_n(s)$, $s^2 = q$, and $v = s^{2n}$. As $k(k-1) = 2(s^{2n}-1) = 2(v-1)$, we have that $k > s^n$. Also, k divides twice the size of any G_x orbit on V, and G_x is transitive on the singular vectors of V.

First suppose n is even. Then G_x has an orbit of size $(s^n-1)(s^{n-1}+1)$; so we have that $k \mid 2(s^n-1)(s^{n-1}+1)$, and $k \mid 2(s^{2n}-1) = 2(v-1)$. Hence we have that k divides

$$2(s^n-1)\cdot \mathrm{hcf}(s^{n-1}+1, s^n+1) = 2^2(s^n-1).$$

Therefore $k = \frac{1}{r}2^2(s^n-1)$ for some r. Since $k > s^n$, we have that $1 \leq r \leq 3$. Now $s > 2$, $k(k-1) = 2(v-1)$ implies

$$s^{2n}-1 = \frac{1}{r^2}\left(2(s^n-1)(4s^n-4-r)\right)$$

with $1 \leq r \leq 3$, so

$$r^2(s^n+1) = 2(4s^n-4-r).$$

If $r = 1$ then $s^n = \frac{11}{8}$, which is a contradiction. If $r = 2$ then $s^n = 4$, a contradiction since $s > 2$. Finally, if $r = 3$ then $s^n = -23$, another contradiction.

Now assume n is odd. Then the size of the orbit of singular vectors is $(s^n+1)(s^{n-1}-1)$, and so k divides

$$2\cdot\mathrm{hcf}\left((s^n+1)(s^{n-1}-1), s^{2n}-1\right) = 2(s^n+1)(s^{n-1}-1, s^n-1) = 2(s^n+1)(s-1).$$

Since $s^n < k$, we have that $k = \frac{1}{r}2(s-1)(s^n+1)$ with $1 \leq r \leq 2(s-1)$, and so we have

$$k(k-1) = \frac{1}{r^2}2(s-1)(s^n+1)\left(2(s-1)(s^n+1)-r\right)$$

and

$$2(v-1) = 2(s^{2n}-1),$$

hence

$$(s-1)\left(2(s-1)(s^n+1)-r\right) = r^2(s^n-1)$$

and so

$$2(s-1)^2(s^n+1) = r\left(r(s^n-1)+(s-1)\right).$$

As $r \leq 2(s-1)$, we have that

$$2(s-1)^2(s^n+1) = r\left(r(s^n-1)+(s-1)\right) \leq 2(s-1)\left(r(s^n-1)+(s-1)\right)$$

so

$$(s-1)(s^n+1) \leq r(s^n-1)+(s-1)$$

which implies

$$s^n(s-1-r)+(s-1) \leq s-1-r$$

and hence

$$s^n(s-1-r) \leq -r < 0$$

therefore $s-1 < r$.

We know $k^2 > 2(v-1)$, so $k^2r^2 > r^2 2(v-1)$, hence

$$4(s-1)^2(s^n+1)^2 > 2r^2(s^n+1)^2(s^n-1)^2$$

so

$$2(s-1)^2 > r^2(s^n-1)^2 > (s-1)^2(s^n-1)^2$$

which implies $2 > (s^n-1)^2$. This is only possible if $n=1$ and $s=2$, or $n=0$; again, a contradiction.

Now consider the orthogonal case. Here $G_x \rhd \Omega_n^{\epsilon}(q)$.

First assume n is odd, say, $n = 2m+1$. Then $v = q^{2m+1}$, and the number of singular vectors in V is $q^{2m}-1$, so k divides $2(q^{2m}-1)$ which is twice the size of a G_x-orbit. Also, as before, $k(k-1)=2(v-1)$, hence k divides $2(q^{2m+1}-1, q^{2m}-1)=2(q-1)$, which is a contradiction, since $q^{\frac{2m+1}{2}}<k$.

Now assume n is even, say, $n=2m$ with $m\geq 2$. If $\epsilon=-$, then the number of singular vectors in V is $(q^m+1)(q^{m-1}-1)$, so

$$k \mid 2\left(q^{2m}-1,(q^m+1)(q^{m-1}-1)\right)=2(q^m+1)(q-1)$$

If $\epsilon=+$, then

$$k \mid 2\left(q^{2m}-1,(q^m-1)(q^{m-1}+1)\right)=2(q^m-1)(q^m+1,q^{m-1}+1).$$

In both cases the same calculations as for the unitary groups lead to a contradiction. □

Lemma 4.13. *Case 4.11 (ii)b does not hold.*

Proof. Assume case 4.11 (*ii*)b. Then $G_x \leq N\left(GL_a(p)\otimes\ldots\otimes GL_a(p)\right)$, $V_d(p)=V_a\otimes\ldots\otimes V_a$, $d=a^m$, and $v=p^{a^m}$; so k divides $2(p^{a^m}-1)$ and $k>p^{\frac{a^m}{2}}$, with $2\leq a$, and $2\leq m$. The vectors $v_1\otimes\ldots\otimes v_m$ form a union of G_x-orbits that has size $\frac{(p^a-1)^m}{(p-1)^{m-1}}$, so k divides $\frac{2(p^a-1)^m}{(p-1)^{m-1}}$. Hence,

$$k \,\Big|\, 2\left(\frac{(p^a-1)^m}{(p-1)^{m-1}},p^{a^m}-1\right).$$

Therefore $k\leq\frac{2(p^a-1)^m}{(p-1)^{m-1}}<2p^{am}\leq p^{am+1}$, and $p^{\frac{a^m}{2}}<k$, hence $\frac{a^m}{2}<am+1$, which implies $a=2$, and $3\leq m\leq 4$.

So, we have that k divides $2^m(p^2-1)$, but $k>p^{2^{m-1}}$, which is a contradiction. □

Lemma 4.14. *Case 4.11 (ii)a with $c\geq 3$ does not hold.*

Proof. Assume 4.11 (*ii*)a, with $c\geq 3$. Then $G_x\leq N\left(GL_a(p)\otimes GL_c(p)\right)$,

$d = ac$, $V_d(p) = V_a \otimes V_c$, and $v = p^{ac}$ with $2 \le c < a$. So, as above,

$$k \mid 2\left(\frac{(p^a-1)(p^c-1)}{p-1}, p^{ac}-1\right).$$

As $p^{\frac{ac}{2}} < k$, we have $p^{\frac{ac}{2}} < \frac{2(p^a-1)(p^c-1)}{p-1}$, so $c \le 4$ and we have the following possibilities:

(i) $c = 3,\ a = 5,\ 2 < p \le 5$

(ii) $c = 3,\ a = 4$

For none of the values in (i), do we have that $8v-7$ is a square. Now suppose $c = 3$, and $a = 4$. Then $p^6 < k$, and k divides

$$2\left(\frac{(p^3-1)(p^4-1)}{p-1}, p^{12}-1\right) = 2(p^3-1)(p+1)(p^2+1).$$

So $k = \frac{2}{r}(p^3-1)(p^2+1)(p+1)$, with $1 \le r < p$.

Assume $r = 1$. Then

$$2(v-1) = 2(p^{12}-1) = 2(p^6+1)(p^3+1)(p^3-1),$$

and

$$k(k-1) = 2(p^3-1)(p^2+1)(p+1)\left(2(p^3-1)(p^2+1)(p+1)-1\right)$$

so $(p^4-p^2+1)(p^2-p+1) = 2(p^3-1)(p^2+1)(p+1)-1$ which is a contradiction, and hence $r \ge 2$.

Therefore $k = \frac{2}{r}(p^3-1)(p^2+1)(p+1) \le (p^3-1)(p^2+1)(p+1)$, and so

$$2(p^6+1)(p^3+1)(p^3-1) < (p^3-1)^2(p^2+1)^2(p+1)^2,$$

so $2p^3(p^2-1)(p-1) < 2(p^4-p^2+1)(p^2-p+1) < p^3(p^2+1)(p+1)$ and hence $2(p-1)^2 < (p^2+1)$, so we have that $p^2-4p+1 < 0$ which implies

$p(p-4) < -1$, so $p = 3$; but $8 \cdot 3^{12} - 7$ is not a square. Hence $c \ngeq 3$. □

Lemma 4.15. *Case 4.11 (ii)a with $c = 2$ does not hold.*

Proof. Suppose $c = 2$. Then we have $p^a < k$, and k divides

$$2\left(\frac{(p^a-1)(p^2-1)}{p-1}, p^{2a}-1\right) = 2(p^a-1)(p+1, p^a+1).$$

So $k = \frac{2}{r}(p^a-1)(p+1)$, with $1 \leq r < 2(p+1)$. Now,

$$2(v-1) = 2(p^a+1)(p^a-1),$$

and

$$k(k-1) = \frac{1}{r^2}2(p^a-1)(p+1)\left(2(p^a-1)(p+1)-r\right),$$

so

$$r^2(p^a+1) = (p+1)\left(2(p^a-1)(p+1)-r\right),$$

which implies

$$r\left(r(p^a+1)+(p+1)\right) = 2(p^a-1)(p+1)^2.$$

Hence $r(p^a+1)+(p+1) > (p^a-1)(p+1)$, that is $r(p^a+1) > (p^a-2)(p+1)$, which implies that $p^a(p+1-r) < r+2(p+1) < 4(p+1)$. Therefore $p+1 \leq r$.

First assume $p+1 = r$. Then $k = 2(p^a-1)$, so

$$k(k-1) = 2(p^a-1)\left(2(p^a-1)-1\right)$$

and

$$2(v-1) = 2(p^a-1)(p^a+1),$$

therefore

$$2(p^a-1)(p^a+1) = 2(p^a-1)\left(2(p^a-1)-1\right).$$

Hence $p^a+1 = 2p^a-3$, so $p^a = 4$, which again contradicts our initial assumptions, and so $p+1 < r$. So we have that k divides

$$2\left(\frac{(p^a-1)(p^2-1)}{p-1}, p^{2a}-1\right) = 2(p^a-1)(p+1, p^a+1)$$

hence

$$k = \frac{2(p^a-1)(p+1)}{r}$$

with $p+1 < r$. This implies a is odd, since if a is even then we would have that $\text{hcf}(p+1, p^a+1) = 1$ or 2.

Therefore, since $k(k-1) = 2(p^{2a}-1)$, we have that $k = \frac{1}{2}(1+\sqrt{8p^{2a}-7})$ and hence

$$r = \frac{4(p^a-1)(p+1)}{1+\sqrt{8p^{2a}-7}} \cdot \frac{\sqrt{8p^{2a}-7}-1}{\sqrt{8p^{2a}-7}-1} = \frac{(p+1)(\sqrt{8p^{2a}-7}-1)}{2(p^a+1)}.$$

So

$$\sqrt{8p^{2a}-7} - 1 = 2r\left(\frac{p^a+1}{p+1}\right),$$

and

$$\sqrt{8p^{2a}-7} + 1 = 2r\left(\frac{p^a+1}{p+1}\right) + 2.$$

Multiplying the previous 2 equations we get

$$8(p^{2a}-1) = 4r^2\left(\frac{p^a+1}{p+1}\right)^2 + 4r\left(\frac{p^a+1}{p+1}\right) = 4r\left(\frac{p^a+1}{p+1}\right)\left(\frac{r(p^a+1)}{p+1}+1\right),$$

so

$$2(p^a-1)(p+1) = r\left(\frac{r(p^a+1)}{p+1}+1\right) = r^2\left(\frac{p^a+1}{p+1}\right) + r =$$

$$r^2\left(\sum_{i=0}^{a-1} p^i\right) - 2r^2\left(\sum_{j=1}^{\frac{a-1}{2}} p^{2j-1}\right) + r$$

and hence, dividing by $\sum_{i=0}^{a-1} p^i$,

$$2(p^2-1) = r^2 - \left(\frac{2r^2 \left(\sum_{j=1}^{\frac{a-1}{2}} p^{2j-1} \right) - r}{\sum_{i=0}^{a-1} p^i} \right),$$

so

$$\frac{2r^2 \left(\sum_{j=1}^{\frac{a-1}{2}} p^{2j-1} \right) - r}{\sum_{i=0}^{a-1} p^i}$$

is an integer.

So we have that

$$\sum_{i=0}^{a-1} p^i \;\Big|\; r \left(2r \sum_{j=1}^{\frac{a-1}{2}} p^{2j-1} - 1 \right)$$

Now,

$$\mathrm{hcf} \left(\sum_{i=0}^{a-1} p^i, 2r \sum_{j=1}^{\frac{a-1}{2}} p^{2j-1} - 1 \right)$$

divides

$$2r \sum_{i=0}^{a-1} p^i - \left(2rp \sum_{j=1}^{\frac{a-1}{2}} p^{2j-1} - p \right) = 2r \left(\sum_{i=0}^{a-1} p^i - \sum_{j-1}^{\frac{a-1}{2}} p^{2j} \right) + p =$$

$$2r \left(\sum_{i=1}^{\frac{a-1}{2}} p^{2i-1} + 1 \right) + p$$

and hence divides

$$\left(2r\left(\sum_{i=1}^{\frac{a-1}{2}} p^{2i-1}+1\right)+p\right)-\left(2r\sum_{j=1}^{\frac{a-1}{2}} p^{2j-1}-1\right)=2r+p+1$$

Therefore

$$r(2r+p+1)=b\left(\sum_{i=0}^{a-1} p^i\right),$$

with $b \in \mathbb{Z}$. As $r < 2(p+1)$, we have that

$$b\sum_{i=0}^{a-1} p^i < 6(p+1)^2.$$

Therefore $a = 3$.

So, as $p+1 < r < 2(p+1)$, we have that $3(p+1)^2 < b(p^2+p+1) < 6(p+1)^2$, and hence $3 < b < 8$.

First suppose that $b = 7$. Then $7\left(p^2+p+1\right) < 6p^2+12p+6$, so $p(p-5) < -1$, which forces $p = 3$. Then $v = 3^6$, but then $8v-7$ is not a square. Hence $b = 4$, 5, or 6, and $p > 3$.

Now, if $p > 3$ then $2r < p^2$, so $(2r+p+1) < (p^2+p+1)$, and since $r(2r+p+1) = b\left(p^2+p+1\right)$, we have that $b < r$. Since $p+1 < r$, we have that

$$3r^2 > b\left(p^2+p+1\right) > r\left(p^2+p+1\right),$$

so $3r > p^2+p+1$, and since $r < 2(p+1)$, we have that $p^2+p+1 < 6(p+1)$, which forces $p = 5$. Hence $v = 5^6$, but then $8v-7$ is not a square.

□

Lemma 4.16. *Case 4.11 (iii) does not occur.*

Proof. Assume G_x is as in 4.11 (*iii*). Then either:

(*i*) $G_x \leq \mathbb{F}_q * \circ s^{1+2m}.Sp_{2m}(s)\log_p q$, $n = s^m$, $s|q-1$ or

(*ii*) $G_x \leq \mathbb{F}_q * \circ 2\pm^{1+2m}.O^+_{2m}(2)\log_p q$, $n = 2^m$, $s = 2$, $q = p$ or p^2.

First assume s is odd. Then $|G_x|$ divides

$$(q-1)s^{m^2+2m}(s^{2m}-1)\dots(s^2-1)\log_p q,$$

so k divides

$$2\left((q-1)s^{m^2+2m}(s^{2m}-1)\dots(s^2-1)\log_p q, q^{s^m}-1\right),$$

that is, k divides

$$2(q-1)\left(s^{m^2+2m}(s^{2m}-1)\dots(s^2-1)\log_p q, \sum_{i=0}^{s^m-1} q^i\right).$$

Now, $\left(\sum_{i=0}^{s^m-1} q^i, s^{m^2+2m}\right)$ divides s^m, so

$$q^{\frac{s^m}{2}} < k \leq 2(q-1)s^m(s^{2m}-1)\dots(s^2-1)\log_p q.$$

As $1+s \leq q$, and $\log_p q \leq q^{\frac{1}{2}}$, we have that $(s+1)^{\frac{s^m-3}{2}} < 2s^{m(m+2)}$, which implies that $s^m \leq 9$.

If $s^m = 9$, then $q \equiv 1 (\mathrm{mod}\ 3)$, and k divides

$$2(q-1)\left(\sum_{i=0}^{s^m-1} q^i, 3^2(3^4-1)(3^2-1)\log_p q\right) = 2(q-1)\left(\sum_{i=0}^{s^m-1} q^i, 2^7\cdot 3^2\cdot 5\log_p q\right).$$

We have that $\sum_{i=0}^{s^m-1} q^i$ is odd and coprime to 5, so k divides

$$2(q-1)3^2\log_p q < q^{\frac{9}{2}} < k,$$

which is a contradiction. Similarly, s^m is not 7 or 5. $\square$

Proof of Theorem 4.10.

Proof. By Proposition 4.11, and Lemmas 4.12, 4.13, 4.14, 4.15, and 4.16, H is a quasisimple group, and its action on $V = V_n(q)$ is absolutely irreducible, and not realisable over any proper subfield of $\mathbb{F}_q$. This completes the proof of Theorem 4.10. □

4.3 L is an Alternating Group

Now we examine the case in which $L = H/Z(H) = A_c$, an alternating group of degree $c \geq 5$, and prove the following:

Theorem 4.17. *If D is a biplane with a flag-transitive, primitive automorphism group $G \leq A\Gamma L_n(q)$ of affine type, with $n > 1$, q odd, and $L = H/Z(H)$ is simple, as in Theorem 4.10, (where $H = G_x^{(\infty)}$), then L is not an alternating group.*

Assume D is a biplane with an affine, primitive, flag-transitive automorphism group $G < A\Gamma L_n(q)$, with $n > 1$, q odd, and $L \cong A_c$, an alternating group with $c \geq 5$.

First consider V to be the *fully deleted permutation module*, defined as follows: Let $q = p$, and A_c act on $(\mathbb{F}_p)$ by permuting the coordinates naturally. Also, let

$$X = \{(a_1, \ldots a_c) \in (\mathbb{F}_p)^c \mid \sum a_i = 0\}$$

of dimension $c - 1$, and

$$Y = \{(a, \ldots, a) \mid a \in \mathbb{F}_p\}.$$

Then $V = X/X \cap Y$ is the fully deleted permutation module.

Lemma 4.18. *If $H = A_c$, then V is not the fully deleted permutation module for A_c.*

Proof. Suppose V is the fully deleted permutation module. If $p \mid c$, then $X \cap Y = Y$, V is of dimension $c-2$, and G_x has an orbit of size $\frac{c(c-1)}{2}$ (take $(a, -a, 0, \ldots, 0)$).

If $p \nmid c$, then $X \cap Y = \{\overline{0}\}$, $V = X$ of dimension $c-1$, and G_x has an orbit of size c. (Take $(1, 1, \ldots, 1-c)$).

We look first at the case $p = 3$:

First consider $c \equiv 0 \pmod 3$. Then we have that $3^{\frac{c-2}{2}} < k$, and k divides $(2(3^{c-2}-1), c(c-1)) \leq c(c-1)$, which implies that $c \leq 9$. Also, $k^2 - k + 2(3^{c-2}-1) = 0$, so

$$k = \frac{1}{2}\left(1 + \sqrt{1 + 8(3^{c-2}-1)}\right)$$

and we have that $8 \cdot 3^{c-2} = r^2 + 7$, which has no integer solutions for $c \leq 9$, $c \equiv 0 \pmod 3$.

Now consider $3 \nmid c$. We have that $3^{\frac{c-1}{2}} < k$, and k divides $2\left((3^{c-1}-1), c\right)$, so $k \leq 2c$, hence $c \leq 5$. So $c = 5$, which means $k \mid 10$, and $k(k-1) = 2(3^4-1)$, which is a contradiction.

Now we present the case $p \geq 5$:

If $p \nmid c$ then $q^{\frac{c-1}{2}} < 2c$, which is a contradiction.

If $p \mid c$ then $q^{\frac{c-2}{2}} < c(c-1)$, hence $c \leq 6$, and we have that $q = 5$, so $c = 5$, and $k \mid 20$, but $k(k-1) = 2(5^3-1)$ which is, again, a contradiction.

Therefore, if $H = A_c$, then V is not the fully deleted permutation module.

□

Lemma 4.19. *We have that $c \leq 16$.*

Proof. Assume $c \geq 15$, and $H = A_c$. Then by [26, Theorem 7] and the previous lemma we have that $n \geq \frac{c(c-5)}{4}$, and the inequality $q^{\frac{c(c-5)}{8}} < (q-1)(c!)_{p'}$ implies $c \leq 16$.

Now assume $c \geq 9$ and $H = 2A_c$. Then by [65] $n \geq 2^{\frac{(c-s-1)}{2}}$, where s is the number of terms in the 2-adic expansion of c, and so $(q-1)(c!)_{p'} > q^{\frac{n}{2}}$, which implies that $c \leq 16$. □

Lemma 4.20. *We have that* $c \leq 11$

Proof. Suppose $12 \leq c \leq 16$, and assume $H = A_c$. Since $12 \leq c$ then by [27] and [42, 2.5] $n \geq 43$. But $q^{\frac{n}{2}} < k \leq 2(q-1)(c!)_{p'}$, which can only happen if $q = 3$, $c = 16$, and $43 \leq n \leq 46$. But in these cases $2\,(3^n - 1, 2.(16!)) < 3^{\frac{n}{2}}$, which is a contradiction.

Now assume $H = 2A_c$. Then by [65], $16 \mid n$, and $32 \mid n$ if $c \geq 14$. But, as above, $n \leq 46$, so $c \leq 13$ and $n = 16$, or $n = 32$. In either case, $2(q^n - 1, (q-1)(c!)) < q^{\frac{n}{2}}$. Hence $c \leq 11$. □

Lemma 4.21. *We have that* $c \leq 7$.

Proof. First suppose $c = 8, 9$. We have that $q^9 > 2(q-1)(9!)_{p'}$ for q odd, so $n < 18$. Hence by [27] $n = 8, 13, 14$. But $q^{\frac{13}{2}} > 2(q^{13} - 1, (q-1)(9!))$, and $2(q^{14} - 1, (q-1)(9!)) < q^7$; so $n = 8$. For $q \geq 5$, $q^4 > 2(q^8 - 1, (q-1)(9!))$, so $q = 3$; but $8 \cdot 3^8 - 7$ is not a square, contradicting Corollary 4.2.

Now assume $c = 10, 11$. Then $2(q^{13} - 1, (q-1)(11!)) < q^{13}$, so $n < 26$. Hence by [27] $n = 8, 16$. But $q^{\frac{n}{2}} < 2(q^n - 1, (q-1)(11!))$ forces $q = 3$, $n = 8$. Yet, as before, $8 \cdot 3^8 - 7$ is not a square. □

Lemma 4.22. *We have that c is not 7.*

Proof. Assume $c = 7$. The fact that $q^{\frac{n}{2}} < 2(q-1)(7!)_{p'}$ forces $n < 12$, (except for the case $q = 3$, but for $12 \leq n \leq 14$, $8 \cdot 3^n - 7$ is not a square, contradicting Corollary 4.2). So by the ordinary and modular characters of A_7 and its covering groups in [9, 27], $n = 3, 4, 6, 8, 9, 10$.

If $n = 3$, then $q = 25$, and $H = 3A_7$ ([27]). But $8 \cdot 5^6 - 7$ is not a square, contradicting Corollary 4.2.

If $n = 4$, then $H = 2A_7$, and $q = p$ or p^2. First consider $q = p^2$, then $k \mid 2((p^8 - 1), (p^2 - 1)7!)$, so $k \mid 40(p^2 - 1)$. Since $p^4 < k$, $p = 3, 5$. We know already that $8 \cdot 3^8 - 7$ is not a square, and $8 \cdot 5^8 - 7$ is not a square either.

If $n = 6$, then $k \mid 2(q^6 - 1, (q-1)7!)$, so $q^3 < k \mid 42(q^2 - 1)$, hence $q < 42$. We check that for all possible values of q, $8q^6 - 7$ is not a square.

If $n = 8$, 9, or 10, then $q^{\frac{n}{2}} < 2(q^n - 1, (q-1)(7!))$, so $q = 3$ and $n = 8$; but we know $8 \cdot 3^8 - 7$ is not a square. □

Hence $c < 7$.

Lemma 4.23. *We have that c is not 6.*

Proof. Suppose $c = 6$. Then $q^{\frac{n}{2}} < (q-1)(2 \cdot 6!)_{p'}$, which forces $n < 9$. Again we refer to [9, 27] for the ordinary and modular character tables for A_6 and its covering groups.

First assume $p = 3$. Then $n \neq 2, 3$, or 4, as each one of these would give $H = SL_2(9)$, $\Omega_3(9)$, $\Omega_4^-(3)$ respectively, and we have seen in the previous section that these do not occur. So $n = 6$ and by [27] $q = 9$; but $8 \cdot 9^6 - 7$ is not a square.

Now assume $p \geq 5$, which by [9, 27] implies that $n = 3, 4, 6$, or 8. If $n = 3$, then $k \mid 6(q-1)$. So $q^{\frac{3}{2}} < 6(q-1)$, which implies that $q^{\frac{1}{2}} < 6$. Hence $q \leq 31$. But for $5 \leq q \leq 31$, we have that $8 \cdot q^3 - 7$ is not a square. Now consider $n = 6$. Then $k \mid 6(q^2 - 1)$, which implies that $q = 5$, but $8 \cdot 5^6 - 7$ is not a square. Next consider $n = 8$, so $k \mid 40(q^2 - 1) < q^4$, a contradiction. Finally consider $n = 4$. Here $q = p$ so k divides $2\left((p-1)5!, p^4 - 1\right) \leq 240(p-1)$. Since $k^2 > v$, we have that $p < 240$, but then for every possibility we have that $8p^4 - 7$ is not a square, which is a contradiction. □

Lemma 4.24. *We have that c is not 5.*

Proof. If $c = 5$, then by [9, 27] $n = 2$, 3, 4, 5, or 6. If $n = 3$, 5, or 6, then $q^{\frac{n}{2}} > (q^n - 1, (q-1)5!)$, so $n = 2$ or 4. If $n = 2$ then $q = p$ or p^2, and if $n = 4$ then $q = p$. We have that k divides $240(q-1)$. If $n = 4$ or $q = p^2$, then we check that for all the possibilities for p, we have that $8v - 7$ is not a square.

If $n = 2$ and $q = p$, then k divides $2(p-1)\,(p+1, 120)$, which divides $120(p-1)$, since 119 is not prime. So $k = \frac{120(p-1)}{r}$, and since $v < k^2$, we have $p, r < 120$. Now, from the equation $k(k-1) = 2(v-1)$, we get that

$$p = \frac{7200 + 60r + r^2}{7200 - r^2}.$$

The fact that p is positive forces $r \leq 84$ (by the denominator), and $p > 2$ forces $r \geq 41$. We check all possible values of r, and the only values for which p is a prime are $r = 75$, and 80, which give the parameters (121,16,2) and (529,33,2) respectively. (So $p = 11$ or 23). The case $p = 23$ is ruled out by the fact that if $A_5 \cong SL_2(5) \leq SL_2(p)$, then 5 divides $p(p^2-1)$ (Lagrange's Theorem), and this is not the case. For $p = 11$, the action is 2-transitive [40], and by Theorem 1.11 the only 2-transitive biplane has parameters (11,5,2). □

Proof of Theorem 4.17

Proof. By Lemmas 4.18, 4.19, 4.20, 4.21, 4.22, 4.23, and 4.24, we have that the group L is not an alternating group. □

4.4 L is a Sporadic Group

In this section we will assume that $L = H/Z(H)$ is a sporadic group, and arrive at a contradiction, proving the following:

Theorem 4.25. *If D is a biplane with an affine, primitive, flag-transitive automorphism group $G \leq A\Gamma L_n(q)$, with $n > 1$, q odd, and $L = H/Z(H)$ where $H = G_x^{(\infty)}$ is simple, as in Theorem 4.10, then the group L is not a sporadic group.*

Assume D is a biplane with an affine, primitive, flag-transitive automorphism group $G < A\Gamma L_n(q)$, with $n > 1$, q odd, and $L = H/Z(H)$ a sporadic group.

Lemma 4.26. *The sporadic group L is not J_4, L_y, Fi_{23}, Fi'_{24}, BM, or M. Moreover, $N_l \leq n \leq N_u$ and $q \leq Q$, where N_l, N_u, and Q are as in Table 4.2.*

Proof. The lower bounds for n are given by [43, 2.3.2]. Everything else follows from the inequality $2(q-1) \cdot |\text{Aut } L|_{p'} > q^{\frac{n}{2}}$ (*). □

L	$\|\text{Aut } L\|$	N_l	N_u	Q
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	5	19	811
M_{12}	$2^7 \cdot 3^3 \cdot 5 \cdot 11$	23	719	
M_{22}	$2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	6	25	1447
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	11	35	73
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	11	39	149
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	7	39	673
J_2	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7$	6	27	2887
J_3	$2^8 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	9	39	311
HS	$2^{10} \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	20	33	3
McL	$2^8 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	21	47	7
He	$2^{11} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	18	45	13
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	28	49	5
Suz	$2^{14} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	12	53	293
$O'N$	$2^{10} \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	31	65	5
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	24	85	7^2
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	22	53	23
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	22	61	13
Fi_{22}	$2^{18} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	27	61	11
HN	$2^{15} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	56	71	2
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	48	85	3

Table 4.2:

Given that q, n must satisfy the inequality

$$2\left(q^n - 1, (q-1)|\text{Aut}L|\right) > q^{\frac{n}{2}} \quad (**),$$

all through this section we will be calculating $2\left(q^n - 1, (q - 1 \cdot |\text{Aut } L|\right)$ for different values of q, n, and L. For this we use Lemma 4.9, which gives the orders of 2, 3, 4, 5, and 11 modulo several powers of small primes, and since $n \geq 5$.

Lemma 4.27. *L is not HN or Th.*

Proof. The fact that L is not HN is immediate from the bound $q \leq 2$. Now suppose $L = Th$. Then $q = 3$. Now,

$$2^2|\text{Aut } Th|_{3'} = 2^{17} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31 > 3^{\frac{n}{2}}$$

implies that $n \leq 53$. But by Lemma 4.9, for $48 \leq n \leq 53$ we have $2\,(3^n - 1, 2|Th|) < 3^{\frac{n}{2}}$, which is a contradiction. □

Lemma 4.28. *L is not He.*

Proof. Suppose L is He. Then $18 \leq n \leq 45$, and $q \leq 13$. We have that $|\text{Aut } He| = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$. First suppose $q = 13$. Then $n \leq 21$. Hence $2^3 \nmid n$, so $2^5 \nmid (|\text{Aut } He|, q^n - 1)$. Also, $3^4 \nmid (|\text{Aut } He|, q^n - 1)$, as well as 7^2 and 17.

So we have $2(q-1)\,(|\text{Aut } He|, q^n - 1) \leq 24 \cdot 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 < 13^{\frac{12}{2}}$, and hence $q \leq 11$. For $q = 11$ we have $2^8, 7^3 \nmid (|\text{Aut } He|, q^n - 1)$, so $k \leq 20(2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 17) < 11^{\frac{18}{2}}$ and hence $q \leq 9$.

If $q = 7$, then $2^9 \nmid (|\text{Aut } He|, q^n - 1)$, so we have that the inequalities $k < 12(2^8 \cdot 3^3 \cdot 5^2 \cdot 17) < 7^{\frac{18}{2}}$ imply that $q \neq 7$.

If $q = 5$, then $2^8, 7^3 \nmid (|\text{Aut } He|, q^n - 1)$, so $k \leq 8(2^7 \cdot 3^3 \cdot 7^2 \cdot 17) < 5^{\frac{22}{2}}$, so $n \leq 21$. Therefore $2^5, 7^2, 17 \nmid (|\text{Aut } He|, q^n - 1)$, so $k \leq 8(2^4 \cdot 3^3 \cdot 7) < 5^{\frac{16}{2}}$, and hence $q \neq 5$.

Therefore we have $p = 3$. Then $k \leq 2 \cdot 8 \cdot 2^8 \cdot 5^2 \cdot 7^2 \cdot 17 < 9^{\frac{17}{2}} = 3^{\frac{34}{2}}$. Hence $q \neq 9$, so $q = 3$ and $k \leq 4 \cdot 2^7 \cdot 5^2 \cdot 7^2 \cdot 17 < 3^{\frac{30}{2}}$, so $n \leq 29$. But then $2^6, 7^2$, and 17 do not divide $(|\text{Aut } He|, q^n - 1)$, so $k \leq 2^7 \cdot 5^2 \cdot 7 < 3^{\frac{19}{2}}$. Hence $n = 18$, but by [41, lem 2.8] $k \leq 2^5 \cdot 7 < 3^{\frac{18}{2}}$. □

Lemma 4.29. *L is not Fi_{22}.*

Proof. Assume L is Fi_{22}. Then $27 \leq n \leq 61$, and $q \leq 11$. By Lemma 4.9, for $5 \leq q \leq 11$ we have $2(q-1)\left(|\mathrm{Aut}\ Fi_{22}|, q^n - 1\right) < q^{\frac{N_l}{2}}$, so we have $q = 3$.

In this case, we have $2(q-1)\left(|\mathrm{Aut}\ Fi_{22}|, q^n - 1\right) \leq 2^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 < 3^{\frac{30}{2}}$, so $27 \leq n \leq 29$; so again by Lemma 4.9, $2^5, 5^2$, 7 and 11 do not divide $(|\mathrm{Aut}\ Fi_{22}|, q^n - 1)$. Hence $k \leq 2^4 \cdot 5 \cdot 13 < 3^{\frac{14}{2}}$, so $q \neq 3$. □

Lemma 4.30. *L is not $O'N$.*

Proof. Suppose $L = O'N$. Then $31 \leq n \leq 65$, and $q \leq 5$. By Lemma 4.9, $2^9, 7^3 \nmid (|\mathrm{Aut}\ O'N|, q^n - 1)$. If $3^4 \mid (|\mathrm{Aut}\ O'N|, q^n - 1)$, then $n = 54$, (and $p = 5$); so $k \leq 2^6 \cdot 3^4 \cdot 7 \cdot 19 < 5^{\frac{17}{2}}$, which is a contradiction. So $n \neq 54$, and $3^4 \nmid (|\mathrm{Aut}\ O'N|, q^n - 1)$.

If $3^3, 19 \mid (|\mathrm{Aut}\ O'N|, q^n - 1)$, then $n = 36$ (again, $p \neq 3$). If $p = 5$, then $k \leq 2^7 \cdot 3^3 \cdot 7 \cdot 19 < 5^{\frac{18}{2}}$; so this value is not possible, and therefore $n \neq 36$, and $3^3, 19 \nmid (|\mathrm{Aut}\ O'N|, q^n - 1)$.

If $31 \mid k$, then $n = 60$, and $k \leq 2^7 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 < 3^{\frac{28}{2}}$, which is a contradiction. Therefore $n \neq 60$, and $31 \nmid k$; so $k \leq 2^{11} \cdot 3^2 \cdot 7^2 \cdot 11 < 3^{\frac{30}{2}}$, which is also a contradiction. □

Lemma 4.31. *L is not HS.*

Proof. Suppose L is HS. Then $20 \leq n \leq 23$, and $q = 3$. If $n = 32$, then $k \mid 2^9 \cdot 5$, and hence $k < q^{\frac{n}{2}}$, so the highest power of 2 dividing n is 2^3. Therefore, by Lemma 4.9, $2^6 \nmid (q^n - 1, |\mathrm{Aut}\ HS|)$, and for the same reason $5^3 \nmid (q^n - 1, |\mathrm{Aut}\ HS|)$. If $5^2 \mid k$, then by Lemma 4.9 20 divides n, so $n = 20$, but then $2\left(3^{10} - 1, 2|\mathrm{Aut}\ HS|\right) < 3^{10}$.

If $n \neq 20$, then 25 does not divide k, and $5 \cdot 11 \nmid k$, so we have that $2\left(q^n - 1, (q^n - 1)|\mathrm{Aut}\ HS|\right) < q^{\frac{N_l}{2}}$, which is a contradiction. □

Lemma 4.32. *L is not McL.*

Proof. Assume L is McL. Then $21 \leq n \leq 47$, and $q \leq 7$. By Lemma 4.9, $2^8, 3^5$, and 5^3 do not divide $(q^n - 1, |\mathrm{Aut}\ McL|)$, and if $q \neq 4$, then 3^4 does not divide $(q^n - 1, |\mathrm{Aut}\ McL|)$ either.

So we have $k \leq 2^9 \cdot 3^4 \cdot 5^2 \cdot 11 < 2^{\frac{47}{2}}, 3^{\frac{30}{2}}$, and $5^{\frac{21}{2}}$. Hence $q = 3$, and $k \leq 2^9 \cdot 5^2 \cdot 7 \cdot 11 < 3^{\frac{26}{2}}$, so $21 \leq n \leq 25$; but then by Lemma 4.9 2^7 and 5^2 do not divide k, so $k \leq 2^6 \cdot 5 \cdot 7 \cdot 11 < 3^{\frac{20}{2}}$, which is a contradiction. □

Lemma 4.33. *L is not Ru.*

Proof. Suppose $L = Ru$. Then $28 \leq n \leq 29$, and $q \leq 5$. By Lemma 4.9, we have 2^8 and 5^3 do not divide $(q^n - 1, |\mathrm{Aut}\ Ru|)$.

First consider $q = 5$. Then $k \leq 2^{10} \cdot 3^3 \cdot 7 \cdot 13 \cdot 29 < 5^{\frac{23}{2}}$, which is a contradiction, and so $q < 5$.

Now consider $q = 3$. Then we have $k \leq 2^9 \cdot 5^2 \cdot 7 \cdot 13 \cdot 29 < 3^{\frac{32}{2}}$, so $n \leq 31$. But then $2^3 \nmid n$, so $2^5 \nmid (3^n - 1, |\mathrm{Aut}\ Ru|)$; and 20 does not divide n, so 25 does not divide k. Therefore $k \leq 2^6 \cdot 5 \cdot 7 \cdot 13 \cdot 29 < 3^{\frac{26}{2}}$, which is a contradiction. □

Lemma 4.34. *L is not a Conway group.*

Proof. Suppose L is a Conway group. If $p \nmid |L|$, then from the character tables in [9] we have that $n = 23$ if $L = Co_2$ or Co_3, and $n = 24$ if $L = Co_1$. But then if $n = 23$ we have that k divides $46(q-1)$, and if $n = 24$ then k divides $2 \cdot 3 \cdot 7 \cdot 13(q^2 - 1)$, so that $k < q^{\frac{n}{2}}$, which is contradiction.

So p divides L, and hence $p \leq 13$ or $p = 23$. Write $q = p^a$. Now assume that $q^n - 1$ is divisible by at least one of the following: $2^8, 3^4, 5^3, 7^2$. Then by Lemma 4.9 and some extra calculations for $p = 13$ or 23, we have that an is divisible by 16, 27, 20, or 21 respectively. Also, $q^{\frac{n}{2}} < (q-1)|\mathrm{Aut}\ L|$, so we have $an \leq 92$. Hence an is one of the following numbers:

$$27, 32, 40, 42, 48, 54, 60, 64, 80, 81.$$

Using Lemma 4.9 we see that for all these values of an, and $p \leq 13$ or 23, $(p^{an} - 1, (p^a - 1)|\mathrm{Aut}\ L|) < p^{\frac{an}{2}}$.

Hence k divides $2(q-1)2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23$.

If $p = 3$, then k divides $(q-1)2^8 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23 < 3^{18}(q-1)$, and hence $q = 3$ and $n < 36$.

Now, if $23 \mid k$, then $11 \mid an$, and one of the following holds:

(*i*) $q = 3$, $n = 22$, or 33.

(*ii*) $q = 5$ or 7, $n = 22$.

In all of the above cases we have

$$2(q^n - 1, (q-1)2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23) < q^{\frac{n}{2}}.$$

Therefore 23 does not divide k. Similarly, 11 does not divide k, and hence k divides $(q-1)2^8 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$. This implies that if $p \geq 3$, then $q = 3$, and $n < 26$. But none of these possible values of n satisfy (**). □

Lemma 4.35. *L is not J_1.*

Proof. Let L be J_1. By Lemma 4.26, $n \leq 39$, and if $p \geq 5$ then by the inequality $2(q-1) \cdot |J_1| > q^{\frac{n}{2}}$ we have that $n < 18$. Hence from the p-modular tables for J_1 given in [9, 27] we see that $n = 7$ and $q = 11$. But $8 \cdot 11^7 - 7$ is not a square. □

Lemma 4.36. *L is not J_2.*

Proof. Suppose $L = J_2$, and assume first that $n = 6$. As 5^2 does not divide $|L_6(q)|$ for $q = 3$, or 7, we have that $q \neq 7$ and $q \geq 5$. Also, we have that k divides $2\,(q^6 - 1, (q-1)|\mathrm{Aut}L|)$, so it divides $42(q^2-1)$, and as $k > q^3$, we have $q \leq 41$. But for all these values of q, $8q^6 - 7$ is not a square.

Hence $7 \leq n \leq 27$. From the tables in [9, 27] for $J - 2$ and its covering group we have that either $n = 14$ and $q = p$ or p^2, $n = 21$ and $q = p$ or p^2, or $n = 13$ and $q = 9$. We check that for all of these values, $8v - 7$ is not a square. □

Lemma 4.37. *L is not J_3.*

Proof. Suppose that $L = J_3$. The subgroup $L_2(16)$ of J_3 shows that $n \geq 15$, by [37]. Now, the inequality (*) forces $q \leq 17$, and $n \leq 26$. If $q > 5$ then by the character tables of J_3 and its covering group in [9] we have that $n = 18$, but for none of the possible values of q do we have that $8q^{18} - 7$ is a square.

Hence $q = 3$ or 5. If k is divisible by $2^5, 3^2$, 17, or 19, then n is divisible by 8, 6, 16, or 9, so $n = 16$, 18, or 24; but none of these values of n satusfy (**). Therefore $k \mid 2^4 \cdot 3 \cdot 5$, which implies $k < q^{\frac{n}{2}}$, which is a contradiction. □

Lemma 4.38. *L is not Suz.*

Proof. Suppose $L = Suz$. As $12 \leq n \leq 53$, we know that p is odd. First assume $n = 12$. We have that k divides $2\,(q^{12} - 1, (q-1)|\mathrm{Aut}L|)$, and so divides $2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13(q^2 - 1)$, and we also have that $k > q^6$, hence $q \leq 11$. But we check for each of these values of q that $8q^{12} - 7$ is not a square.

So $13 \leq n \leq 53$. By [9], there is no such irreducible representation of Suz (or any covering group) in characteristic not dividing $|Suz|$, so $p \leq 13$. Write $q = p^a$. If either 2^7 or 3^4 divides r, then 2^4 or 3^3 divides an, so $an = 16$, 27, 32, or 48, but we check that none of these values of an satisfy (**) for $p \leq 13$. Therefore $k \mid 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13(q-1)$. If $p \geq 5$ this implies $n < 18$ and $q = p$, but we check that with none of the values for $13 \leq n \leq 17$ and $5 \leq p \leq 13$ is (**) satisfied.

Hence $p = 3$, and since $k > p^{\frac{an}{2}}$ we have $an \leq 28$. If k is divisible by $2^5, 5^2$, 11, or 13, then an is divisible by 8, 20, 6, or 5, so $an = 16$, 18, 20, 24, or 25 and therefore $a = 1$, but we check that $8 \cdot 3^n - 7$ is not a square for these values of n. Hence k divides $2^4 \cdot 5 \cdot 13$, but then $k < 3^{\frac{n}{2}}$, which is a contradiction. □

Lemma 4.39. *L is not a Mathieu group.*

Proof. Suppose L is a Mathieu group. From the tables in [9, 27] and the inequality (**), we see that (n, q) is as in the following table:

L	possibilities for (n,q)
M_{11}	$(5,3),(10,p),(11,p)$
M_{12}	$(10,p),(10,p^2),(11,p),(12,p),(5,3)$
M_{22}	$(10,p),(10,p^2),(21,3)$
M_{24}	(22,3), (23,5)

The only case satisfying (**) is (n,q)=(5,3), but $8 \cdot 3^5 - 7$ is not a square.

□

Proof of Theorem 4.25

Proof. The proof is a consequence of Lemmas 4.26 to 4.39. □

4.5 L is a Group of Lie Type in Characteristic p

Here we assume $L = H/Z(H)$ is a group of Lie type in characteristic p, and prove the following:

Theorem 4.40. *If a biplane D has a primitive, affine, flag-transitive automorphism group $G \leq A\Gamma L_n(q)$, where $q = p^n$ (with $p > 2$ and $n > 1$) and $L = H/Z(H)$ where $H = G_x^{(\infty)}$, then L is not a simple group of Lie type in characteristic p.*

Assume D is a biplane with an affine, primitive, flag-transitive automorphism group $G < A\Gamma L_n(q)$, with $n > 1$, q odd, and L a group of Lie type in characteristic p, and $V = V_n(q)$ is an absolutely irreducible module for H, not realisable over any proper subfield of $\mathbb{F}_q$. Write $q = p^a$, and suppose that $L = L(s)$ is of Lie type over $\mathbb{F}_s$, where s is a power of p.

First we state the following result, which will be useful in this section:

Lemma 4.41. *There is a positive integer u, and a faithful irreducible projective $\overline{\mathbb{F}_p}L$-module of dimension t, such that at least one of the following holds:*

(*i*) $s = q^u$, *and* $dimV = n = t^u$.

(*ii*) L *is of type* ${}^2A_l$, ${}^2D_l$, *or* ${}^2E_6$; u *is odd,* $s = q^{\frac{u}{2}}$, *and* $n = t^u$.

(*iii*) L *is of type* ${}^3D_4$, $s = q^{\frac{u}{3}}$, $3 \nmid u$, *and* $n = t^u$.

(*iv*) L *is of type* ${}^2B_2$, ${}^2G_2$, *or* ${}^2F_4$; $s = q^u$, *and* $n \geq t^u$.

Proof. Consequence of [33, 5.4.6 and 5.4.7]. □

Lemma 4.42. *If U is a Sylow p-subgroup of L, then k divides* $2(q-1) \cdot |L : N_L(U)|$. *In particular,* $2(q-1)|L : N_L(U)| > q^{\frac{n}{2}}$.

Proof. Let $\overline{G_x} = G_x/(G_x \cap \mathbb{F}_q^*)$, so $L \lhd \overline{G_x}$. By [13, 4.3(c)], U fixes a unique 1-space in V, which is therefore fixed by $N_{\overline{G_x}}(U)$. By the Frattini argument, we deduce that $\overline{G_x}$ has an orbit on $P_1(V)$ (the 1-spaces of V) of size dividing $|L : N_L(U)|$. Since k divides twice the size of any G_x-orbit on $V \setminus \{x\}$, we have that k divides $2(q-1)|L : N_L(U)|$. As $k^2 > v$, we have that $q^{\frac{n}{2}} < 2(q-1)|L : N_L(U)|$, and this completes our proof. □

Now, $N_L(U)$ is a Borel subgroup of L. Let l be the rank of the simple algebraic group over $\overline{\mathbb{F}_p}$ corresponding to L, and N the number of positive roots in the corresponding root system.

Lemma 4.43. *We have that* $(q-1) \mid L : N_L(U) \mid < q^{u(N+l)}$.

Proof. By 4.41, we have $s \leq q^u$. If L is of untwisted type, then

$$|L : N_L(U)| = \prod_{i \in X} \frac{s^i - 1}{s - 1},$$

where X is a set of positive integers with sum $N + l$; hence the result.

If L is of type ${}^2A_l$, ${}^2D_l$, or ${}^2E_6$, then some of the factors are replaced by $\frac{s^i+1}{s+1}$, which is even less than $\frac{s^i-1}{s-1}$.

If L is of type ${}^3D_4$, ${}^2B_2$, ${}^2G_2$, or ${}^2F_4$; then $|L : N_L(U)|$ is at most $(s^8 + s^4+1)(s^6-1)(s^2-1)$, (s^2+1), (s^3+1), or $(s^6+1)(s^4-1)(s^3+1)$ respectively; and the result follows. □

Lemma 4.44. *If $q \geq 5$, then $n = dimV \leq 2u(N + l)$. If $q = 3$, then $n \leq 2u(N + l) + 1$.*

Proof. By 4.42, we have $q^{\frac{n}{2}} < 2(q-1)|L : N_L(U)|$, and by 4.43 we have $(q-1)|L : N_L(U)| < q^{u(N+l)}$. Therefore we have:

$$q^{\frac{n}{2}} < 2(q-1)|L : N_L(U)| < 2q^{u(N+l)},$$

and so $n < 2\log_q(2) + 2u(N + l)$. Hence the result. □

Now let $R_p(L)$ denote the minimal dimension of a faithful projective representation of L in characteristic p. The values of $R_p(L)$ are given by [33, 5.4.13], and are recorded, with the values of $N+l$, in the following table [41, Table III]:

Type of L	$N + l$	$R_p(L)$
A_l^ϵ	$l(l + 3)/2$	$l + 1$
B_l, C_l, ${}^2B_2$	$l^2 + l$	$\geq 2l$
D_l^ϵ $(l > 4)$	L^2	$2l$
G_2^ϵ	8	≥ 6
F_4^ϵ	28	≥ 25
E_6^ϵ	42	27
E_7	60	56
E_8	128	248

Table 4.3:

Lemma 4.45. *We have $u = 1$.*

Proof. By 4.41, $n \geq R_p(L)^u$, so by 4.44:

$R_p(L)^u \leq 2u(N+l)$ if $q \geq 5$, and

$R_p(L)^u \leq 2u(N+l)+1$ if $q = 3$.

Suppose $u \geq 2$. From Table 4.3 we see that L must be of type A_l^ϵ, B_l, C_l, ${}^2B_2$, or D_l^ϵ with $u = 2$ and $q = 3$.

If $L = B_l(q^u)$, and $l = 3$, then $R_p(L) = 2l+1$ which contradicts the above equations; and if $L = {}^2B_2(q^u)$ then $|L : N_L(U)| = q^{2u}+1$, so $n > 2(2u+1)$ by Lemma 4.42, and $n \geq R_p(L)^u = 4^u$, which is a contradiction.

Hence L is of type A_l^ϵ, C_l, or $D_l^\epsilon(q^2)$ with $q = 3$.

If $L = D_l^\epsilon(q^2)$ $(l \geq 4)$, then $R_p(L)^2 = 4l^2 \geq n$, and by Lemma 4.44 we have $n \leq 4(N+l)+1 = 4l^2+1$. From Lemma 4.41, $n = t^u$, so $n = (2l)^2$.

So we have that $n = 4l^2$, $u = 2$, and $L = P\Omega_{2l}(q^2)$, and therefore $V \otimes F_{q^2} = W \otimes W^{(q)}$, where $W = V_{2l}(q^2)$; that is, the usual (projective) module for L.

Now assume $L = A_l^\epsilon$. If $l = 1$, then $L = L_2(q^u)$, and by Lemma 4.42 we have $(q-1)(q^u+1) > q^{\frac{n}{2}}$, so $n > 2(u+1)$. Now $n = t^u \geq 2^u$, so $u = 2$ and $n = 4$; therefore $L = P\Omega_4^-(q)$, which does not occur (by Lemma 4.12). So $l \geq 2$. From above equations, $(l+1)^u < ul(l+3)$, so either $u = 2$, or $u = 3$ and $l = 2$.

In the latter case, by Lemma 4.42 we have $n \leq 24$, but $n \geq (l+1)^u = 27$. Hence $u = 2$, so $n = t^2 \leq 2l(l+3)+1$, which forces $t < \frac{(l+1)^2}{2}$ and also $t < \frac{l(l+1)}{2}$ when $l \geq 3$. Hence by [39, 1.1] we have that $t = l+1$, and so [33, 5.4.6] implies that $L = A_l(q^2)$ and $V \otimes \mathbb{F}_{q^2} = W \otimes W^{(q)}$, where $W = V_{l+1}(q)$, the usual (projective) module for L.

When $L = C_l(q^u)$ with $l \geq 2$, we have that $(2l)^u \leq t^u = n < 2u(N+l)$ if $q \geq 5$, and $(2l)^u \leq t^u = n \leq 2u(N+l)+1$ if $q = 3$. Hence we have that $(2l)^u \leq t^u < 2u(l^2+l)$ if $q \geq 5$, and $(2l)^u \leq t^u \leq 2u(l^2+l)+1$ otherwise. In any case, we have that $u = 2$, and $t = 2l$. So, as above, $V \otimes \mathbb{F}_{q^2} = W \otimes W^{(q)}$, where $W = V_{2l}(q^2)$, the usual (projective) module for L.

So, in any case we have $L = L_d(q^2)$ or $PSp_d(q^2)$, and $V \otimes \mathbb{F}_{q^2} = W \otimes W^{(q)}$, where $W = V_d(q^2)$. A basis for the $\mathbb{F}_q$-realisation of V is given in the proof of [40, 2.4], it contains elements of the form $v \otimes v$. So G_x on the vectors has an orbit of size $\frac{(q^{2d}-1)(q-1)}{q^2-1}$, and so k divides twice this number. Therefore $q^{\frac{n}{2}} < k < q^{2d-\frac{1}{2}}$, and since $n = d^2$, we have that $d \leq 3$. We have already dealt with the case $d = 2$, so here $L = L_3(q^2)$, $n = 9$, and k divides $2(q^6-1, q^9-1)$, and hence divides $2(q^3-1)$, but in that case we have $k < q^{\frac{n}{2}}$, which is a contradiction. □

The previous two lemmas give the following:

$$n = dimV \leq 2(N+l) \text{ if } q \geq 5$$

and

$$n = dimV \leq 2(N+l)+1 \text{ if } q = 3.$$

The next lemma lists all the possibilities for the module V satisfying this bound for $q \geq 5$. The notation is standard, explained in [33, Section 5.4]. In particular, $M(\lambda)$ denotes the irreducible module with high weight λ. By "quasiequivalent", we mean "equivalent, up to automorphisms of L".

Lemma 4.46. *If $q \geq 5$, then as a projective $\mathbb{F}_q L$-module, V is quasiequivalent to one of the modules $M(\lambda)$ listed in Table 4.4 below.*

Proof. Since dim $V \leq 2(N+l)$, the result follows directly from [40, 2.10] and [39, 1.1], except when L is of type A_l^{ϵ}, C_l, or E_6^{ϵ}, but in these cases we have dim $V < l^2+3l$, $2l^2+2l$, or 84 respectively, so we require slight improvements on the bounds in [40, 2.2, 2.7, 2.10]. These have been achieved in [56].

Note that the modules $M(\lambda_1)$ for classical groups L are not listed in the table, this is because if $V = M(\lambda_1)$, then G_x is in the class $\mathcal{C}_8$ of subgroups of $\Gamma L_n(q)$, which we have dealt with already in Section 4.2 □

type of L	λ	$\dim M(\lambda)$
A_l^ϵ	$\lambda_2 (l \geq 3)$	$\frac{l(l+1)}{2}$
	$\lambda_3 (l \geq 5)$	$\frac{l(l^2-1)}{6}$
	$2\lambda_1 (p \text{ odd})$	$\frac{(l+1)(l+2)}{2}$
	$(1+p^i)\lambda_1,\ \lambda_1 + p^i\lambda_l\ (i>0)$	$(l+1)^2$
	$\lambda_1 + \lambda_l$	$\lambda^2 + 2l - \delta$ ($\delta = 0$ or 1
B_l (p odd , $l \geq 3$)	λ_2	$l(2l+1)$
	λ_l	2^l
C_l $(l \geq 2)$, ${}^2B_2$	λ_2	$l(2l-1) - \delta$ ($\delta = 1$ or 2)
	$2\lambda_1$ (p odd)	$2l^2 + 2 \leq \dim M(\lambda) \leq 2l^2 + l$
	λ_3 $(l = 3, p \text{ odd})$	14
D_l^ϵ $(l \geq 4)$	λ_2	$l(2l-1) - \delta$ $(0 \leq \delta \leq 2)$
	λ_{l-1}, λ_l	2^{l-1}
G_2^ϵ	λ_1, λ_2	$7 - \delta_{p,2},\ 14 - 7\delta_{p,3}$
F_4^ϵ	λ_4, λ_1	$26 - \delta_{p,3},\ 52 - 26\delta_{p,2}$
E_6^ϵ	λ_1, λ_2	27, 78-$\delta_{p,3}$
E_7	λ_7, λ_1	56, 133-$\delta_{p,2}$
E_8	λ_8	248

Table 4.4:

Lemma 4.47. *L is not a classical group.*

Proof. Suppose L is classical and write $L = Cl_d(s)$, with d the minimal dimension of a natural projective L-module in characteristic p. By Lemmas 4.41 and 4.45, we have $s = q^x$, with $x = 1$ except when L is of type U or $P\Omega^-$, in which case $x = 1$ or $\frac{1}{2}$.

By [40, 2.3], the stabiliser in L of a maximal 1-space of V is a parabolic subgroup that corresponds to the set of fundamental roots on which λ does not vanish. Call this subgroup P_λ. Then k divides $2(q-1)|L : P_\lambda|$.

First supose $\lambda = \lambda_2$. When L is unitary, we have $L = U_d(q^{\frac{1}{2}})$ rather than $U_d(q)$, as in this case $M(\lambda_2)$ is realised over $\mathbb{F}_s$ only when $d = 4$, so $n = 6$ and $L = P\Omega_6^-(q)$, which has already been dealt with.

Thus, $(q-1)|L : P_\lambda|$ is as follows:

type of L	$(q-1)\|L : P_\lambda\|$
L^{ϵ}_{δ}	divides $\frac{(q^d-1)(q^{d-1}-1)}{q^2-1}$
$C_l,\ B_l$	$\frac{(q^{2l}-1)(q^{2l-2}-1)}{q^2-1}$
D^{ϵ}_l	$\frac{(q^{2l-2}-1)(q^l-\epsilon)(q^{l-2}+\epsilon)}{q^2-1}$

If $L = L^{\epsilon}_d(q^x)$, then since k divides $2(q-1)|L : P_\lambda|$ and $q^{\frac{n}{2}} < k$, we have $q^{\frac{n}{2}} = q^{\frac{d(d-1)}{4}} < 2q^{2d-1}$, so $\frac{d(d-1)}{4} < 2d - 2 + \log_q 2$, therefore $\frac{d(d-1)}{4} \leq 2d-2$, and hence $d \leq 8$. (And $d \geq 4$, by Table 4.4). Also, as noted above, $d \neq 4$, since $L \neq P\Omega^{\epsilon}_6(q)$. So we have $5 \leq d \leq 8$.

First assume $d = 5$. Then we have that k divides $2\left((q^5-1)(q^2+1), q^{10}+1\right)$, so $k \mid 4(q^5-1)$, and hence $k = \frac{4(q^5-1)}{r}$, with $1 \leq r \leq 3$, as $q^5 < k$. Then

$$\frac{4(q^5-1)}{r} \cdot \frac{4(q^5-1)-r}{r} = 2(q^{10}-1)$$

(recall $k(k-1) = 2(v-1)$), and so

$$8(q^5-1) - 2r = r^2(q^5+1).$$

But substituting $r = 1$, 2, or 3 we get $q^5 = \frac{11}{7}$, 4, and -23 respectively, which is a contradiction.

Now assume $d = 6$. Then k divides $2\left((q^5-1)(q^4+q^2+1), q^{15}-1\right)$, and so

$$q^{\frac{15}{2}} < k \mid 2(q^5-1)(q^2+q+1),$$

which implies that $q \leq 5$, and

$$k = \frac{2(q^5-1)(q^2+q+1)}{r},$$

with $1 \leq r \leq 2$. But for none of these possible values of r and q is the equation $k(k-1) = 2(v-1)$ satisfied.

If $d = 7$, then k divides $2(q^7-1)(q^2+q+1)$. As $k > q^{\frac{n}{2}}$, this forces $q = 2$, which is a contradiction.

Finally, suppose $d = 8$.Then k divides $2\left(\frac{(q^8-1)(q^7-1)}{q^2-1}, q^{28}-1\right)$, so we have that

$$k \mid 2(q^7-1)\left((q^4+1)(q^2+1), (q^{14}+1)(q^7+1)\right).$$

Hence we have that $q^{14} < k \le 2(q^7-1)(q^4+1)(q^2+1)$, which is a contradiction.

This completes the case $L = L_d^\epsilon,\ \lambda = \lambda_2$.

Now consider L to be of type $C_l,\ B_l$, or D_l^ϵ, still with $\lambda = \lambda_2$. If $l = 2$, then $L = P\Omega_5(q)$ with $n = 5$, which has already been seen to not occur. Hence $l \ge 3$. Since $k^2 > v$, from the above tables we have that

$$\frac{l(2l-1)-2}{2} \le \frac{n}{2} < 4l - 2 - \frac{3}{2},$$

which implies $l \le 3$. Therefore $l = 3$ and so L is of type C_3 or B_3. In this case k divides $2(q^6-1)(q^2+1)$, so $n \le 18$, and hence $L = C_3(q)$ and $n = 13$ or 14, but in both cases we have $2\left((q^6-1)(q^2+1), q^n-1\right) < q^{\frac{n}{2}}$, which is a contradiction. This completes the case $\lambda = \lambda_2$.

Now suppose $\lambda = 2\lambda_1$, so from Table 4.4 L is of type L_d^ϵ or C_l, with p odd. Here $|L : P_\lambda| = \frac{q^d-1}{q-1}$. So $q^{\frac{n}{2}} < k$, and k dividing $2(q^d-1)$ imply $d \ge \frac{n}{2}$, which forces $n = 2$ and $d = 3$, but then $L = P\Omega_3(q)$ with $n = 3$ has already been dealt with.

Suppose now that V is a spin module, so that $\lambda = \lambda_l$ for L of type B_l, and $\lambda = \lambda_{l-1}$ or λ_l for L of type D_l^ϵ. In the latter case, with $\epsilon = -$, we have $L = D_l^-(q^{\frac{1}{2}})$, as the spin modules for $D_l^-(q)$ are not realised over $\mathbb{F}_q$.

If L is of type B_l, then $|L : P_\lambda| = (q^l+1)(q^{l-1}+1)\ldots(q+1)$, and if L is of type D_l^ϵ, then $|L : P_\lambda|$ divides $(q^{l-1}+1)\ldots(q+1)$. As $q^{\frac{n}{2}} < k \le 2(q-1)|L : P_\lambda|$, we have that

$$2^{l-1} = \frac{n}{2} < 2 + l(l+1)$$

if L is of type B_l, and

$$2^{l-2} = \frac{n}{2} < 2 + l(l-1)$$

if L is of type D_l^ϵ. This forces $l \leq 6$ in the first case, and $l \leq 7$ if L is of type D_l^ϵ.

If $L = B_3(q),\ D_4(q)$, or $D_4^-(q^{\frac{1}{2}})$, then k divides $2\left((q^3+1)(q^4-1), q^8-1\right)$, so we have $k \mid 4(q^4-1)$, and hence $k = \frac{4(q^4-1)}{r}$, with $1 \leq r \leq 3$. But for each of these values of r the equality $k(k-1) = 2(v-1)$ yields non-integer values of q, which is a contradiction.

If $L = C_3(q)$, then $p = 2$, which is a contradiction.

If $L = B_4(q)$ or $D_5^\epsilon(q)$, then k divides $2\left((q^3+1)(q^8-1), q^{16}-1\right)$, so $k \mid 4(q^8-1)$, but as $q^8 < k$, we have that $k = \frac{4(q^8-1)}{r}$, with $1 \leq r \leq 3$, but then $k(k-1) = 2(v-1)$ taking each of these values of r forces q to have non-integer values, which is a contradiction.

Now, if $L = B_5(q)$, $C_5(q)$, or $D_6^\epsilon(q)$, then we have that k divides $2\left((q^8-1)(q^3+1)(q^5+1), q^{32}-1\right) < q^{16}$, a contradiction.

Similarly, if $L = B_6(q),\ C_6(q)$, or $D_7^\epsilon(q)$, then we have that k divides $2\left((q^8-1)(q^3+1)(q^5+1)(q^6+1), q^{64}-1\right) < q^{32}$, a contradiction.

By Lemma 4.46, the remaining cases are

$$L = L_d^\epsilon(q^x),\ \lambda = \lambda_3,\ (1+p^i)\lambda_1,\ \lambda_1 + p^i\lambda_{d-1},\ \lambda_1 + \lambda_{d-1},$$

and

$$L = C_3(q),\ (q \text{ odd}),\ \lambda = \lambda_3.$$

In the last case, $n = 14$ and $\mid L : P_\lambda \mid= (q^3+1)(q^2+1)(q+1)$, so k divides $2\left((q^4-1)(q^3+1), q^{14}-1\right) < q^7$, a contradiction.

Now consider $L = L_d^\epsilon(q^x)$. If $\lambda = \lambda_3$, then $d \geq 6$. If $d \geq 7$ then $L = L_d(q)$

or $U_d(q^{\frac{1}{2}})$, so that k divides

$$\frac{2(q^d-1)(q^{d-1}-1)(q^{d-2}-1)}{(q^3-1)(q^2-1)},$$

so

$$3d-7 \geq \frac{n}{2} = \frac{d(d-1)(d-2)}{12},$$

which is not true. Therefore $d = 6$, $L = L_6^{\epsilon}(q)$, and k divides $2\left((q^5-\epsilon)(q^3+1)(q^2+1), q^{20}-1\right)$, which implies $k < q^{10}$, a contradiction.

If $\lambda = (1+p^i)\lambda_1$, then $n = d^2$ and k divides $2(q^d-1)$, forcing $d^2 \leq 2d$, which can only happen if $d = 2$. In this case the equality $k(k-1) = 2(v-1)$ forces $(v,k,\lambda) = (16,6,2)$, which we have already assumed not to happen.

If $\lambda = \lambda_1 + p^i\lambda_{d-1}$, (with $d \geq 3$), then $n = d^2$ and we have that k divides

$$2\left(\frac{(q^d-1)(q^{d-1}-1)}{q-1}, q^{d^2}-1\right),$$

forcing $k < q^{\frac{n}{2}}$, again, a contradiction.

Finally, if $\lambda = \lambda_1 + \lambda_{d-1}$ $(d \geq 3)$, then $n = d^2 - \delta$ with $0 \leq \delta \leq 2$. Then k divides

$$\frac{2(q^d-\epsilon^d)(q^{d-1}-\epsilon^{d-1})(q-1)}{q-\epsilon},$$

so $2d-1 \geq \frac{n}{2} \geq \frac{d^2-2}{2}$, which is only possible if $d = 3$ or 4. If $d = 3$, then $n = 7$ or 8. If $\epsilon = +$ then k divides $2\left((q^3-1)(q^2-1), q^n-1\right)$, and if $\epsilon = -$ then k divides $2\left((q^3+1)(q-1)^2, q^n-1\right)$. In both cases we have $k < q^{\frac{n}{2}}$. If $d = 4$, then $n = 14$. If $\epsilon = +$ then k divides $2\left((q^4-1)(q^3-1), q^{14}-1\right)$, and if $\epsilon = -$ then k divides $2\left((q^3+1)(q^2+1)(q-1)^2, q^{14}-1\right)$. Here also, in both cases we have $k < q^7$, a contradiction. □

Lemma 4.48. *L is not an exceptional group of Lie type.*

Proof. Just as above, we have $V = M(\lambda)$, with λ as in Table 4.4, and k divides $2(q-1)|L : P_\lambda|$; so we see that k is as in the following table:

L	λ	k divides
$G_2(q)$	λ_1	$2(q^6-1, q^{7-\delta_{p,2}}-1)$
	λ_2	$2(q^6-1, q^{14-7\delta_{p,3}}-1)$
$F_4^{\epsilon}(q)$	λ_4	$2\left((q^{12}-1)(q^4+1), q^{26-\delta_{p,3}}-1\right)$
	λ_1	$2\left((q^{12}-1)(q^4+1), q^{52-26\delta_{p,2}}-1\right)$
$E_6^{\epsilon}(q^x)$	λ_1	$2\left((q^9-1)(q^8+q^4+1), q^{27}-1\right)$
	λ_2	$2(\frac{(q^{12}-1)(q^9-\epsilon)(q^4+1)(q-1)}{(q^3-\epsilon)(q-\epsilon)}, q^{78-\delta_{p,3}}-1)$
$E_7(q)$	λ_7	$2\left((q^{14}-1)(q^9+1)(q^5+1), q^{56}-1\right)$
	λ_1	$2(\frac{(q^{18}-1)(q^{14}-1)(q^6+1)}{q^4-1}, q^{133-\delta_{p,2}}-1)$
$E_8(q)$	λ_8	$2(\frac{(q^{30}-1)(q^{24}-1)(q^{10}+1)}{q^6-1}, q^{248}-1)$
${}^3D_4(q^x)$	$\lambda_4(x=\frac{1}{3})$	$2\left((q^4-1)(q^3+1), q^8-1\right)$
	$\lambda_2(x=1)$	$2\left((q^8+q^4+1)(q^6-1), q^{28-2\delta_{p,2}-1}\right)$
${}^2B_2(q)$	λ_2	$2\left((q^2+1)(q-1), q^4-1\right)$

It follows from the above table and from the inequality $q^{\frac{n}{2}} < k$ that if L is an exceptional group of Lie then one of the following holds:

(*i*) $L = {}^3D_4(q^{\frac{1}{3}})$ with $\lambda = \lambda_4$;

(*ii*) $L = {}^2B_2(q)$.

In the first case,, we have that k divides $4(q^4-1)$, and $k > q^4$, so $k = \frac{4(q^4-1)}{r}$, with $1 \leq r \leq 3$.

First assume $r = 1$. Then $k(k-1) = 4(q^4-1)(4q^4-5)$, and we have that $2(v-1) = 2(q^8-1)$, so $8q^4-10 = q^4+1$, so $7q^4 = 11$, which is a contradiction.

Now assume $r = 2$. Then $k = 2(q^4-1)$, so $k(k-1) = 2(q^4-1)(2q^4-3)$, and so $2q^4-3 = q^4+1$, hence $q^4 = 4$, which is also a contradiction.

If $r = 3$, then $k(k-1) = \frac{4(q^4-1)(4q^4-7)}{9}$, and since $k(k-1) = 2(q^8-1)$, we have that $q^4 = -23$, another contradiction.

Now consider the second case. Then L is the Suzuki group, and so $v = q^4$, with $p = 2$, but this is a contradiction. □

This completes the proof of Theorem 4.40.

4.6 L is a Group of Lie type in Characteristic p'

Here we complete this chapter by proving that $L = H/Z(H)$ is not a group of Lie type in characteristic p', that is:

Theorem 4.49. *If a biplane D has an affine, primitive, flag-transitive automorphism group $G \leq A\Gamma L_n(q)$, with $n > 1$, $q = p^n$ odd, and $H = G_x^{(\infty)}$, then $L = H/Z(H)$ is not a group of Lie type in characteristic p'.*

Assume L is a group of Lie type in characteristic p', and is not isomorphic to an alternating group. Then we have the following:

Lemma 4.50. *L is one of the following groups:*

$L_2(s),\ s \leq 59$

$L_3(s),\ s \leq 5$

$L_4(3)$

$PSp_4(s),\ s \leq 9,\ s \neq 8$

$PSp_6(s),\ s = 2, 3, 5$

$PSp_8(s),\ s = 2, 3$

$PSp_{10}(3)$

$U_3(s),\ s \leq 5$

$U_4(s),\ s \leq 3$

$U_l(2),\ l = 5, 6, 7$

$\Omega_7(3)$, $\Omega_8^{\pm}(2)$

${}^2B_2(8),\ G_2(3),\ G_2(4),\ {}^3D_4(2),\ {}^2F_4(2)',\ F_4(2).$

Proof. We know that $n \geq R_{p'}(L)$, which is the smallest degree of a faithful projective representation of L over a field of p'-characteristic. In [37] there are lower bounds for $R_{p'}(L)$, and we also have:

$$2(q-1) \mid \text{Aut } L \mid > q^{\frac{n}{2}} \geq q^{\frac{R_{p'}(L)}{2}}. \quad (*)$$

Substituting the lower bounds of [37] for $R_{p'}(L)$ we obtain that the groups satisfying the inequality are precisely those listed above. □

Lemma 4.51. *The group L is not $L_2(s)$.*

Proof. Suppose that $L = L_2(s)$. As $L \neq A_c$, we have that $s \neq 4, 5$, or 9. We see in the p'-modular character tables of $SL_2(s)$ (given in [8], and [27] for $s \leq 32$) that n is one of the numbers $\frac{s \pm 1}{2}$ (s odd), $s \pm 1$, or s. In particular, $n \geq \frac{s-1}{(2,s-1)}$.

If $s \geq 29$, then the inequality (*) forces $q \leq 3$ and $n = \frac{s \pm 1}{2}$, but for these values of q and n, and $29 \leq s \leq 59$, $2(q^n - 1, (q-1)|\text{Aut } L|) < q^{\frac{n}{2}}$.

If $L = L_2(27)$, then $n = 13, 14, 26, 27$, or 28, and by (*) we have that $q = 2$ or 4, a contradiction.

Now let $L = L_2(25)$. Then $n =$ 12, 13, 24, 25, or 36, and again (*) forces $q \leq 4$ or $(q, n) = (7, 12)$. But

$$2\,(q^n - 1, (q-1)|\text{Aut } L|) > q^{\frac{n}{2}} \quad (**)$$

only if $q = 2$, again, a contradiction.

Similarly, when $16 \leq s \leq 23$, (*) forces $q \leq 13$, and the only values which satisfy (**) are $(s, q, n) = (19, 4, 9)$ and (17,2,8), another contradiction.

If $L = L_2(13)$, then $n =$ 6, 7, 12, 13, or 14. Suppose $p \geq 3$. Then by (*) either $n \leq 7$ or $q = 3$. If $q = 3$ then (**) forces $n = 12$, but then $8v - 7$ is not a square. So $n = 6$ or 7, and by (*) $q = p$. If $n = 7$ then $k \mid 14(p-1)$, so $k < q^{\frac{n}{2}}$. Hence $n = 6$ and k divides $182(p^2-1)$. Since $p^3 < k$, we have that $p < 182$, but then for all possibilities of p we have that $8v - 7$ is not a square.

Next consider $L_2(11)$, so $|\mathrm{Aut}\ L| = 2^3 \cdot 3 \cdot 5 \cdot 11$. First assume $p \geq 3$. we have $n = 5, 6, 10, 11$, or 12, and k divides $110(q-1)$, $6(q^2-1)$, $110(q^2-1)$, $22(q-1)$, or $60(q-1)$ respectively. The only possibilities for $k > q^{\frac{n}{2}}$ are $(n, q) = (5, 3)$, (6,3), (6,5), and (10,3), but in none of these cases is $8v - 7$ a square.

If $s = 8$ then $n = 7$, 8, or 9, and k divides $14(q-1)$, $8(q^2-1)$, or $126(q-1)$ respectively. The only possibility for $k > q^{\frac{n}{2}}$ is $(n, q) = (9, 3)$, but in this case we have that $8v - 7$ is not a square.

Now let $L = L_2(7)$, so $|\mathrm{Aut}\ L| = 2^4 \cdot 3 \cdot 7$. As $L \cong L_3(2)$, we take $p \neq 7$. In this case $n =$ 3,4,6,7, or 8, and k divides $42(q-1)$, $4(q^2-1)$, $42(q^2-1)$, $14(q-1)$, or $8(q^2-1)$ respectively. Therefore $n \neq 7$ or 8. If $n = 4$ then $k = 2(q^2-1)$ or $4(q^2-1)$. First suppose $k = 2(q^2-1)$. As $2(v-1) = k(k-1)$, we have $2(q^4-1) = 4(q^2-1)^2 - 2(q^2-1)$, so $q^2 + 1 = 2(q^2-1) - 1$, which implies $q^2 = 4$, a contradiction. Now suppose $k = 4(q^2-1)$. Then, as above, $2(q^4-1) = 16(q^2-1)^2 - 4(q^2-1)$, so $q^2 + 1 = 8(q^2-1) - 2$, but this forces $q^2 = \frac{11}{7}$, which is another contradiction. Hence $n \neq 4$. If $n = 6$ then since $k > q^3$, we have $q \leq 41$, and (**) forces $q = 3$, 5, or 11, but for none of these values of q is $8q^6 - 7$ a square. Finally consider $n = 3$. From [27], we have $q = p$ or p^2, and $q = p$ if and only if -7 is a square in $\mathbb{F}_p$, which occurs only if $p \equiv 1$, 2, or 4 mod 7. If $q \leq 31$, then $q = 9$, 11, 23, or 25. For none of these values $8q^3 - 7$ is a square. If $q \geq 37$, as k divides $42(q-1)$ we have that $k = \frac{42(q-1)}{r}$, and as $k > q^{\frac{3}{2}}$ then $r < 7$. Solving the equation $2(q^3-1) = k(k-1)$ for q, with each $1 \leq r \leq 6$ we get a non-integer solution, which is a contradiction. ☐

Lemma 4.52. *L is not $L_3(s)$.*

Proof. Suppose L is $L_3(s)$, so by 4.50 $s \leq 5$. If $s = 5$ then by [27] $n \geq 30$, but this does not satisfy (*). If $s = 3$ then $n \geq 12$, but (*) forces $q = 2$, which cannot occur.

So $L = L_3(4)$, and $|\mathrm{Aut}\ L| = 2^8 \cdot 3^3 \cdot 5 \cdot 7$. First suppose $p \geq 5$. Then by (*) $n \leq 17$, so by [27] $n = 6, 8, 10, 12$, or 15. If $n = 8$, then k divides $40(q^2 - 1)$, and the condition $k > q^4$ forces $q = 5$, $k = 40(q^2 - 1)$, but $8 \cdot 5^8 - 7$ is not a square. For $n = 10, 12$, or 15 it is impossible with $p \geq 5$ to satisfy the conditions $q^{\frac{n}{2}} < k \mid 40(q^2 - 1)$. Now consider $n = 6$. Then k divides $42(q^2 - 1)$, and $q = p \leq 41$. If $p \geq 17$, then $k = \frac{42(q^2-1)}{r}$, with $1 \leq r \leq 2$. First suppose $r = 1$. Then $2(q^6 - 1) = (42)^2(q^2 - 1)^2 - 42(q^2 - 1)$, so $q^4 + q^2 + 1 = (21)(42)(q^2 - 1) - 21$, so $q^4 - 881q^2 + 904 = 0$, giving a non-integer value of q between 29 and 31, which is a contradiction. Now suppose $r = 2$. Then similarly, we have $2q^4 - 880q^2 + 904 = 0$, giving a non-integer value of q between 19 and 23, another contradiction. Hence $q < 17$, but we check that for $5 \leq q < 17$, $8q^6 - 7$ is not a square. Hence $p = 3$, and by (*) we have $n \leq 19$, and so by [9, 27] $n = 4, 6, 8, 10, 15$ or 16, and $q = 9, 3, 9, 9, 3$ or 9 respectively, but we check that for none of these values $8q^n - 7$ is a square. □

Lemma 4.53. *L is not $L_4(3)$ or $PSp_4(s)$.*

Proof. If $L = L_4(3)$, then (*) and [27] force $q = 2$ and $n = 26$, a contradiction.

Now suppose $L = PSp_4(s)$, then by 4.50 $s \leq 9$ and $s \neq 8$. If $s = 7$ or 9 then by [37] $n \geq 24$ or 40 respectively, so by (*) we have that $q \leq 3$ and $24 \leq n \leq 36$ for $s = 7$, and $q = 2$ and $40 \leq n \leq 45$ for $s = 9$. The latter case cannot occur, and for $q = 3$ we check that for all values of n we have $2\left((q^n - 1), (q - 1)|\mathrm{Aut}\ L|\right) < q^{\frac{n}{2}}$.

If $s = 5$ then by (*) and the character tables for L and $2.L$ in [9, 27] $n = 12$ or 13, so $((q^n - 1), (q - 1)|\mathrm{Aut}\ L|)$ divides $390(q^2 - 1)$ or $13(q - 1)$ respectively. The inequality $k > q^{\frac{n}{2}}$ forces $n = 12$ and $q^4 < 390$, so $q = 3$, but from [27] we see that if $p = 3$ then $q = 9$, a contradiction.

If $s = 4$ then by (*) and [9, 27] $n = 18$, but $2\,((q^n-1),(q-1)\mid \text{Aut } L\mid) < q^{\frac{n}{2}}$.

Finally, if $s = 3$ then $|\text{Aut } L| = 2^7 \cdot 3^4 \cdot 5$, and as $PSp_4(3) \cong U_4(2)$, we can assume $p \neq 3$. The inequality (*) forces $n \leq 11$, so by [9, 27] $n = 4$, 5, 6, or 10. If $n = 5$, 6, or 10 then k divides $10(q-1)$, $6(q-1)$, or $10(q^2-1)$, so $k < q^{\frac{n}{2}}$. Hence $n = 4$, and $q = p$ or p^2, with $q = p$ if and only if -3 is a square in $\mathbb{F}_p$. If $q = p^2$ then k divides $40(p^2-1)$, so $p = 5$ or 6. We check that in each case $8q^4 - 7$ is not a square. If $q = p$ then k divides $20(p^2-1)$, so $k = \frac{20(p^2-1)}{r}$, with $r < 20$. As $2(p^4-1) = k(k-1)$, we have that

$$\frac{400(p^2-1)^2}{r^2} - \frac{20(p^2-1)}{r} = 2(p^4-1),$$

which implies that

$$\frac{200(p^2-1)}{r^2} - \frac{10}{r} = p^2+1,$$

so

$$p^2 = \frac{r^2+10r+200}{200-r^2},$$

and hence $r \leq 14$. The only value of r that yields an integer value for p is $r = 10$, but this forces $p = 2$, a contradiction. □

Lemma 4.54. *L is not $PSp_6(s)$.*

Proof. First suppose $L = PSp_6(5)$. Then (*) forces $q = 2$ a contradiction.

Next suppose $L = PSp_6(3)$. In this case $|\text{Aut } L| = 2^{10} \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$, and by [37] $n \geq 13$. If p does not divide $|L|$ ($p > 13$ or $p = 11$), then by (*) and the tables in [9] we have $n = 13$ or 14, but neither case satisfies (**). If $p = 13$ then (*) forces $n \leq 18$, but we check that $2\,(13^n - 1, 12|\text{Aut } L|) < 13^{\frac{n}{2}}$ for $13 \leq n \leq 18$.

Hence $p \leq 7$. By (*) $an < 40$, where $q = p^a$. If 2^6 or 3^3 divides k, then 8 or 9 divides an, so $an = 16$, 18, 24, 27, 32, or 36. But none of these values of an satisfy (**) for $p = 5$ or 7. Therefore k divides $2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot (q-1)_{2',3'}$.

By (*) we have that with $p = 5$ or 7 $a \leq 2$, so $(q-1)_{2',3'} = 1$, and so $k < q^{\frac{13}{2}}$, which is a contradiction.

Finally, consider $L = PSp_6(2)$. In this case $|\mathrm{Aut}\ L| = 2^9 \cdot 3^4 \cdot 5 \cdot 7$. By (*) and the tables in [9, 27], we have that $n = 7$, 8, or 15 if $p \neq 3$, and $n = 7$, 8, 14, or 21 if $p = 3$, and in all cases we have $q = p$. The only possibility satisfying (**) is $(n, q) = 8, 3$, but $8 \cdot 3^8 - 7$ is not a square. □

Lemma 4.55. *L is not $PSp_8(s)$ or $PSp_{10}(3)$.*

Proof. If $L = PSp_8(3)$ or $PSp_{10}(3)$ then by [37], n is at least 40 or 121 respectively, but (*) forces $q = 2$, a contradiction.

Now consider the case $L = PSp_8(2)$. In this case we have by [37] that $n \geq 28$, and by (*) we have that either $q = 5$ and $n \leq 29$, or $q = 3$ and $n \leq 36$, but we check that none of these cases satisfy (**). □

Lemma 4.56. *L is not $U_3(s)$.*

Proof. Suppose $L = U_3(s)$. If $s = 5$, then by (*) and [9, 27] we have that $q = 3$ and $n = 20$ or 28, and if $s = 4$ then $n = 12$ or 13. None of these cases satisfy (**).

Now consider $s = 3$. Then $|\mathrm{Aut}\ L| = 2^6 \cdot 3^3 \cdot 7$, and by (*) and the tables in [9, 27] we have that $n = 6$, 7, or 14. In the last two cases k divides $14(q-1)$ and $14(q^2-1)$ respectively, forcing $q = 2$, a contradiction. Hence $n = 6$, and by [9, 27] $q = p$. In this case we have that k divides $42(p^2 - 1)$. We know $p \neq 3$, and if $p \geq 7$ then (**) is not satisfied. Hence $p = 5$, but $8 \cdot 5^6 - 7$ is not a square, which is a contradiction. □

Lemma 4.57. *L is not $U_4(3)$, or $U_r(2)$, $5 \leq r \leq 7$.*

Proof. If $L = U_4(3)$ then by (*) and [9, 27] we have that either $n = 15$, 20, or 21, or $(n, q) = (6, 4)$; and if $L = U_5(2)$ then for the same reason we have that $n = 10$ or 11. But we check that none of these possibilities satisfy (**).

If $L = U_6(2)$ then by (*) and [37] we have that either $q = p \leq 11$ and $21 \leq n \leq 32$, or $q = 13$ and $n = 21$; and if $L = U_7(2)$ we have that $q = 3$ or 5, and $42 \leq n \leq 45$. Again, none of these possibilities satisfy (**). □

Lemma 4.58. *L is not $\Omega_7(3)$ or $\Omega_8^{\pm}(2)$.*

Proof. If $L = \Omega_7(3)$, then by [37] we have $n \geq 27$, so by (*) $p = 5$. By (*) $q = 5$ and $n \leq 28$, but neither case satisfies (**).

Now consider $L = \Omega_8^{\epsilon}(2)$. By (*) and [9, 27] we have that either $\epsilon = -$, $q = 3$, and $n = 34$, or $\epsilon = +$, and $n = 8$ or 28. The only possibility satisfying (**) is $n = 8$. In this case $q = p$, and $k \mid 40(p^2 - 1)$, hence $p = 3$ or 5, but in both cases $8v - 7$ is not a square. □

Lemma 4.59. *L is not ${}^2B_2(8), G_2(3), G_2(4), {}^3D_4(2), {}^2F_4(2)'$, or $F_4(2)$.*

Proof. First suppose $L = F_4(2)$. Then by [37] we have $n \geq 44$, so (*) implies $q = 3$ and $n \leq 56$. we check that none of these values satisfy (**).

Now suppose L is one of the remaining groups. Then using the p-modular tables for L and its covering groups from [9, 27], and (*), we find that the possibilities are the following:

$$\begin{array}{ll} L = {}^2B_2(8): & n = 8 (q = 5) \text{ or } 14 \\ L = G_2(3): & n = 14 \\ L = G_2(4): & n = 12 \\ L = {}^3D_4(2): & n = 25 \text{ or } 26 \\ L = {}^2F_4(2)': & n = 26 \text{ or } 27 \end{array}$$

The only cases satisfying (**) are $(L, n, q) = ({}^2B_2(8), 8, 5)$, and $(G_2(4), 12, 3)$, but in both of them $8v - 7$ is not a square. □

This completes the proof of Theorem 4.49, and hence we have completed the proof of Theorem 4, namely:

Theorem 4. *If D is a biplane with a primitive, flag-transitive automorphism group G of affine type, then one of the following holds:*

(*i*) *D has parameters (4,3,2).*

(*ii*) *D has parameters (16,6,2).*

(*iii*) $G \leq A\Gamma L_1(q)$*, for some prime power* q*.*

4.7 Addendum

The proof of Theorem 4 can be greatly simplified using the following proposition, very helpfully provided by Peter Cameron:

Proposition 4.60. *Let* G *be an affine automorphism group of a biplane. Suppose that* $G = TH$*, where* T *is the translation group of* $V(d,p)$ *(acting regularly on the points of the biplane) and* $H \leq GL(d,p)$*, and p is odd. Then* $|G|$ *is odd.*

Proof. We have $v = p^d$, so

$$p^d = 1 + \frac{k(k-1)}{2}.$$

Suppose that $|G|$ is even. Then H contains an involution t. The fixed points of t form an e-dimensional subspace of V for some e, so t fixes p^e points. Also, $G_x = H$ permutes the k blocks incident with x. Suppose G_x has m transpositions and $k-2m$ fixed blocks. Then, since the points different from x correspond bijectively to pairs of blocks incident with x, we see that t has $1 + m + \frac{(k-2m)(k-2m-1)}{2}$ fixed points. Thus

$$p^e = 1 + m + \frac{(k-2m)(k-2m-1)}{2}.$$

Subtracting the two displayed equations gives

$$p^d - p^e = 2m(k - m - 1).$$

Note that the number of fixed points is at least $\frac{k+1}{2}$, with equality only if $k-2m=1$. So $p^e \geq \frac{k+1}{2}$.

It cannot happen that $p \mid m$ and $p \mid k-m-1$, for then $p \mid k-1$ and $p^d = 1+\frac{k(k-1)}{2} \equiv 1 \pmod{p}$. Hence either $p^e \mid m$ or $p^e \mid k-m-1$. The former is impossible since $m \leq \frac{k}{2}$ and $p^e \geq \frac{k+1}{2}$. We conclude that $p^e \mid k-m-1$, so that indeed

$$p^e = k-m-1.$$

Now we have $k-m-1 = p^d - 2m(k-m-1)$, so

$$(2m+1)(k-m-1) = p^d,$$

so $2m+1 = p^{d-e}$.

If $m = 0$, then p divides $k-1$ and $p^d = 1 + \frac{k(k-1)}{2} \equiv 1 \pmod{p}$, a contradiction. If $m \geq 1$, then p divides $2(k-m-1)+(2m+1) = 2k-1$, so p^2 divides $(2k-1)^2 = 8p^d - 7$, also a contradiction. This completes the proof. □

To prove Theorem 4, we only need Corollary 4.7, Theorem 4.10 and Proposition 4.60.

5. BIPLANES WITH AUTOMORPHISM GROUPS OF ALMOST SIMPLE TYPE

In this chapter we will prove Theorem 5, that is:

Theorem 5. *If D is a biplane with a primitive, flag-transitive automorphism group of almost simple type, then D has parameters either (7,4,2), or (11,5,2), and is unique up to isomorphism.*

For this purpose we will consider biplanes that admit a primitive, flag-transitive automorphism group G of almost simple type, that is, if X is the socle of G (the product of all its minimal normal subgroups), then we have that X is simple, and $X \trianglelefteq G \leq \mathrm{Aut}X$.

5.1 Preliminary Results

In this section we mention some results which will be useful throughout the rest of this chapter.

Assume that D is a biplane with a primitive, flag-transitive automorphism group G is of almost simple type, with socle (the product of its minimal normal subgroups) X, a simple group, so $X \trianglelefteq G \leq \mathrm{Aut}X$.

We have the following results:

Lemma 5.1 (Tits Lemma). *[61, 1.6] If X is a simple group of Lie type in characteristic p, then any proper subgroup of index prime to p is contained* *in a parabolic subgroup of X.*

Lemma 5.2. *If X is a simple group of Lie type in characteristic 2, ($X \ncong A_5$ or A_6), then any proper subgroup H such that $[G : H]_2 \leq 2$ is contained in a parabolic subgroup of X.*

Proof. First assume that $G = Cl_n(q)$ is classical (q a power of 2), and take H maximal in G. By Theorem 4.8, H is contained in a member of the collection $\mathcal{C}$ of subgroups of $\Gamma L_n(q)$, or in $\mathcal{S}$, that is, $H^{(\infty)}$ is quasisimple, absolutely irreducible, not realisable over any proper subfield of $\mathbb{F}_(q)$.

We check for every family $\mathcal{C}_i$ that if H is contained in C_i, then $2|H|_2 < |G|_2$, except when H is parabolic.

Now we take $H \in \mathcal{S}$. Then by [39, Theorem 4.2], $|H| < q^{2n+4}$, or H and G are as in [39, Table 4]. If $|G|_2 \leq 2|H|_2 \leq q^{2n+4}$, then if $G = L_n^\epsilon(q)$ we have $n \leq 6$, and if $G = SP_n(q)$ or $P\Omega_n^\epsilon(q)$ then $n \leq 10$. We check the list of maximal subgroups of G for $n \leq 10$ in [30, Chapter 5], and we see that no group H satisfies $2|H|_2 \leq |G|_2$. We then check the list of groups in [39, Table 4], and again, none of them satisfy this bound.

Finally, assume G to be an exceptional group of Lie type in characteristic 2. Then by [51], if $2|H| \geq |G|_2$, H is either contained in a parabolic subgroup, or H and G are as in [51, Table 1]. Again, we check all the groups in [51, Table 1], and in all cases $2|H|_2 < |G|_2$. □

As a consequence, we have a strengthening of Corollary 4.3:

Corollary 5.3. *Suppose D is a biplane with a primitive, flag-transitive almost simple automorphism group G with simple socle X of Lie type in characteristic p, and the stabiliser G_x is not a parabolic subgroup of G. If p is odd p does not divide k; and if $p = 2$ then 4 does not divide k. Hence $|G| < 2|G_x||G_x|_{p'}^2$.*

Proof. We know from Corollary 4.3 that $|G| < |G_x|^3$. Now, by Lemma 5.1, p divides $v = [G : G_x]$. Since k divides $2(v-1)$, if p is odd then $(k, p) = 1$, and if $p = 2$ then $(k, p) \leq 2$. Hence k divides $2|G_x|_{p'}$, and since $2v < k^2$, we have $|G| < 2|G_x||G_x|^2_{p'}$. □

From the previous results we have the following lemma, which will be quite useful throughout this chapter:

Lemma 5.4. *Suppose p divides v, and G_x contains a normal subgroup H of Lie type in characteristic p which is quasisimple and $p \nmid |Z(H)|$; then k is divisible by $[H : P]$, for some parabolic subgroup P of H.*

Proof. As p divides v, then since k divides $2(v-1)$ we have that $(k, p) \leq (2, p)$. Also, we have that $k = [G_x : G_{x,B}]$ (where B is a block incident with x), so $[H : H_B]$ divides k, and therefore $([H : H_B], p) \leq (2, p)$, so by Lemmas 5.1 and 5.2 H_B is contained in a parabolic subgroup P of G_x, and since P is maximal, we have $G_{x,B}$ is contained in P, so k is divisible by $[G_x : P]$. □

We will also use the following two lemmas:

Lemma 5.5. *[49] If X is a simple group of Lie type in odd characteristic, and X is not $PSL_d(q)$ nor $E_6(q)$, then the index of any parabolic subgroup is even.*

Lemma 5.6. *[47, 3.9] If X is a group of Lie type in characteristic p, acting on the set of cosets of a maximal parabolic subgroup, and X is not $PSL_d(q)$, $P\Omega^+_{2m}(q)$ (with m odd), nor $E_6(q)$, then there is a unique subdegree which is a power of p.*

Before stating the next result, we give the following [46]:

Definition 5.7. Let H be a simple adjoint algebraic group over an algebraically closed field of characteristic $p > 0$, and σ be an endomorphism of H such that $X = (H_\sigma)'$ is a finite simple exceptional group of Lie type over $\mathbb{F}_q$, where $(q = p^a)$. Let G be a group such that $\mathrm{Soc}(G) = X$. The group $\mathrm{Aut}X$ is generated by H_σ, together with field and graph automorphisms. If D is a σ-stable closed connected reductive subgroup of H containing a maximal torus T of H, and $M = N_G(D)$, then we call M a *subgroup of maximal rank* in G.

We now have the following theorem and table [52, Theorem 2, Table III]:

Theorem 5.8. *If X is a finite simple exceptional group of Lie type such that $X \leq G \leq \mathrm{Aut}(X)$, and G_x is a maximal subgroup of G such that $X_0 = \mathrm{Soc}(G_x)$ is not simple, then one of the following holds:*

(i) *G_x is parabolic.*

(ii) *G_x is of maximal rank.*

(iii) *$G_x = N_G(E)$, where E is an elementary abelian group given in [11, Theorem 1(II).].*

(iv) *$X = E_8(q)$, ($p > 5$), and X_0 is either $A_5 \times A_6$ or $A_5 \times L_2(q)$.*

(v) *X_0 is as in Table 5.1.*

X	X_0
$F_4(q)$	$L_2(q) \times G_2(q)$ $(p > 2, q > 3)$
$E_6^\epsilon(q)$	$L_3(q) \times G_2(q)$, $U_3(q) \times G_2(q)$ $(q > 2)$
$E_7(q)$	$L_2(q) \times L_2(q)$ $(p > 3)$, $L_2(q) \times G_2(q)$ $(p > 2, q > 3)$
	$L_2(q) \times F_4(q)$ $(q > 3)$, $G_2(q) \times PSp_6(q)$
$E_8(q)$	$L_2(q) \times L_3^\epsilon(q)$ $(p > 3)$, $G_2(q) \times F_4(q)$
	$L_2(q) \times G_2(q) \times G_2(q)$ $(p > 2, q > 3)$, $L_2(q) \times G_2(q^2)$ $(p > 2, q > 3)$

Table 5.1:

We will also use the following theorem [48, Theorem 3]:

Theorem 5.9. *Let X be a finite simple exceptional group of Lie type, with $X \leq G \leq \mathrm{Aut}(X)$. Assume G_x is a maximal subgroup of G, and $\mathrm{Soc}(G_x) = X_0(q)$ is a simple group of Lie type over $\mathbb{F}_q$ ($q > 2$) such that $\frac{1}{2}\mathrm{rk}(X) < \mathrm{rk}(X_0)$. Then one of the following holds:*

(i) G_x *is a subgroup of maximal rank.*

(ii) X_0 *is a subfield or twisted subgroup.*

(iii) $X = E_6(q)$ *and* $X_0 = C_4(q)$ *(q odd) or* $F_4(q)$.

Finally, we will use the following theorem [54, Theorem 1.2]:

Theorem 5.10. *Let* X *be a finite exceptional group of Lie type such that* $X \leq G \leq \mathrm{Aut}(X)$, *and* G_x *a maximal subgroup of* G *with socle* $X_0 = X_0(q)$ *a simple group of Lie type in characteristic* p. *Then if* $\mathrm{rk}(X_0) \leq \frac{1}{2}\mathrm{rk}(X)$, *we have the following bounds:*

(i) *If* $X = F_4(q)$ *then* $|G_x| < q^{20}.4\log_p(q)$,

(ii) *If* $X = E_6^{\epsilon}$ *then* $|G_x| < q^{28}.4\log_p(q)$,

(iii) *If* $X = E_7(q)$ *then* $|G_x| < q^{30}.4\log_p(q)$, *and*

(iv) *If* $X = E_8(q)$ *then* $|G_x| < q^{56}.12\log_p(q)$.

In all cases, $|G_x| < |G|^{\frac{5}{13}}.5\log_p(q)$.

5.2 The Case in which X is an Alternating Group

In this section we suppose there is a non-trivial biplane D that has a primitive, flag-transitive almost simple automorphism group G with socle X, where X is an alternating group, and arrive at a contradiction.

Lemma 5.11. *The group* X *is not* A_c.

Proof. We need only consider $c \geq 5$. Except for three cases (namely $c = 6$ and $G \cong M_{10}$, $PGL_2(9)$, or $P\Gamma L_2(9)$) G is an alternating or a symmetric group. The three exceptions will be dealt with at the end of this section.

The point stabiliser G_x acts on the points on the biplane as well as on the set $\Omega_c = \{1, 2, \ldots, c\}$. The action of G_x on this set can be one of the following three:

(i) Not transitive.

(ii) Transitive but not primitive.

(iii) Primitive.

We analyse each of these actions separately.

Case (i) Since G_x is a maximal subgroup of G, it is necessarily the full stabiliser of a proper subset S of Ω_c, of size $s \leq \frac{c}{2}$. The orbit of S under G consists of all the s-subsets of Ω_c, and G_x has only one fixed point in D, hence we can identify the points in D with the s-subsets of Ω_c. (We identify x with S).

Two points of the biplane are in the same G_x-orbit if and only if the corresponding s-subsets of Ω_c intersect S in the same number of points. Therefore G acting on the biplane has rank $s+1$, each orbit O_i corresponding to a possible size $i \in \{0, 1, \ldots, s\}$ of the intersection of an s-subset with S in Ω_c.

Now fix a block B in D incident with x. Since G is flag-transitive on D, B must meet every orbit O_i. Let $i < s$, and $y_i \in O_i \cap B$. Since D is a biplane, the pair $\{x, y_i\}$ is incident with exactly two blocks, B, and say, B_i. The group G_{xy_i} fixes the set of flags $\{(x, B), (x, B_i)\}$, and in its action on Ω_c stabilises the sets S and Y_i, as well as their complements S^c and Y_i^c. That is, G_{xy_i} is the full stabiliser in G of the four sets $S \cap Y_i$, $S \cap Y_i^c$, $S^c \cap Y_i$, and $S^c \cap Y_i^c$, so it acts as $S_{(s-i)}$ on $S^c \cap Y_i$, and at least as $A_{(c-2s+i)}$ on $S^c \cap Y_i^c$. Any element of G_{x,y_i} either fixes the block B, or interchanges B and B_i, so the index of $G_{x,y_i} \cap G_{xB}$ in G_{x,y_i} is at most 2, and therefore $G_{x,B} \cap G_{x,y_i}$ acts at least as the alternating group on $S^c \cap Y_i$, and $S^c \cap Y_i^c$. Since $G_{x,B}$

contains such an intersection for each i, we have that $G_{x,B}$ is transitive on the s-subsets of S^c, that is, on O_0. This implies that the block B is incident with every point in the orbit, so every other block intersects this orbit in only one point, (since for every point y in O_0 the pair $\{x, y\}$ is incident with exactly B and only one other block).

However, any pair of distinct points in O_0 is also incident with exactly two blocks, which is a contradiction.

Case *(ii)* Here we have that since G_x is maximal, then in its action on Ω_c it is the full stabiliser in G of some non-trivial partition of Ω_c into t classes of size s, (with $s, t \geq 2$). Since G acts transitively on all the partitions of Ω_c into t classes of size s, we may identify the points of the biplane D with the partitions of Ω_c into t classes of size s.

We fix a point x of the biplane, that is, a partition X of Ω_c into t classes $C_0, C_1, \ldots, C_{t-1}$ of size s. We call a partition Y of Ω_c *j-cyclic* (with respect to X) if X and Y have $t - j$ common classes, and if, numbering the other j classes $C_0, \ldots, C_{j-1}$, for each C_i $(i < j)$ there is a point c_i such that the j classes of Y which differ from those of X are $(C_i - \{c_i\}) \cup \{c_{i+1}\}$ for all $i = 0, \ldots, j-1$, with the subscripts computed modulo j. We define the *cycle* of Y to be the cycle $(C_0, \ldots, C_{j-1})$. As we have that X is fixed, if $s \geq 3$ then the points $c_0, \ldots, c_{j-1}$ are uniquely determined by Y, and are called the *special points* of Y. For every $j = 2, \ldots, t$ the set of j-cyclic partitions is an orbit O_j of G_x.

Now fix a block B incident with x. Since we can identify the points of the biplane D with the partitions of Ω_c into t classes of size s, for simplicity we will refer to partitions whose corresponding points of the biplane are incident with B simply as partitions incident with B.

For every $j = 2, \ldots, t$, the block B is incident with at least one j-cyclic partition Y_j, (since G is flag-transitive), and there is an even permutation of the elements of Ω_c that preserves X and Y_j, stabilising each of their $t - j$

common classes and acting as $\mathbb{Z}_j$ on the remaining j classes of X. Therefore G_{xB} acts as S_t on the t classes of X. As a consequence, we have that for any two classes C_0 and C_1 of X, the block B is incident with at least one 2-cyclic partition with cycle (C_0, C_1).

Now we claim that $s \geq 3$. Suppose to the contrary that the classes of X have size 2. Then there are only two 2-cyclic partitions with cycle (C_0, C_1), so B is incident with at least half of the points of the biplane corresponding to the 2-cyclic partitions, which implies that there are at most two blocks incident with x, which is a contradiction. Therefore $s \geq 3$.

Now we claim that any two 2-cyclic partitions incident with B have a common special point. Suppose to the contrary that for two points y, z incident with the block B, the corresponding 2-cyclic partitions Y and Z have cycle (C_0, C_1), with Y having special points $\{c_0, c_1\}$, which are both distinct from the special points of Z. There is an even permutation of Ω_c that stabilises the partitions Y and Z, and maps $\{c_0, c_1\}$ to any other disjoint pair $\{c_0', c_1'\}$ (where $c_i' \in C_i$). Therefore, the number m of 2-cyclic partitions with cycle (C_0, C_1) incident with B satisfies $m \geq s^2 - 2s + 1$. However, the flag-transitivity of G and the fact that G_{xB} acts as S_t on the t classes of X imply that m divides the total number s^2 of 2-cyclic partitions with cycle (C_0, C_1), so $m = s^2$. Therefore the block B is incident with the whole orbit O_2 under G_x of all 2-cyclic partitions, which implies that B is the only block incident with x, and this is a contradiction. Therefore any two 2-cyclic partitions incident with B have a common special point.

If $t \geq 3$, then since G_{xB} acts as S_t on the t classes of X, and since any 2-cyclic partitions incident with B have a common special point, we have that $t = 3$ and only one point c_i in each class C_i is a special point of some 2-cyclic partition incident with B. However there is an even permutation of Ω_c that preserves each of the classes C_0, C_1, C_2, fixing c_0 and c_1 but mapping c_2 into any other point of C_2, preserving x and B but not $\{c_0, c_1, c_2\}$, which is a contradiction. Therefore $t = 2$.

It follows that B is incident with only one partition, say Y, with special points $\{c_0, c_1\}$. If the size of C_0 and C_1 is greater than 3, then B is incident with a partition, say Z different to Y and X, and there is an even permutation of Ω_c which leaves X and Z invariant, but does not preserve $\{c_0, c_1\}$, which is a contradiction. Therefore $s = 3$.

Hence $c = 6$, and since the points of D can be identified with the partitions of Ω_6 into 2 classes of size 3, we have that $v = 10$. However, there is no biplane with 10 points, a contradiction.

Case *(iii)* Here first of all we mention that if $G \cong S_c$ then $G_x \ncong A_c$, since $[G : G_x] = v > 2$. If k, the number of blocks incident with a point is even, then the group G_x contains a Sylow 2-subgroup of G. Therefore G_x contains a subgroup acting transitively on 2 or 4 points of Ω_c, and fixing all other points, so by a theorem of Marggraf [66, Th.13.5], we have that $c \leq 8$. If we check all the divisors of $|S_c|$ for $5 \leq c \leq 8$, (since v divides G), the only possibilities such that $8v - 7$ is a square are $v = 2$, 4, 16, and 56. We rule out $v = 2$ because it is too small. For $v = 4$, $k = 3$ which is odd, and $v = 56$ forces $k = 11$ which is also odd. Finally by Theorem 1 we rule out $v = 16$.

If k is odd, then let p be a prime divisor of k, so p divides $2|G_x|$. Then G_x contains a Sylow p-subgroup of G, and so G_x acting on Ω_c contains an even permutation with exactly one cycle of length p and $c - p$ fixed points. By a result of Jordan [66, Th. 13.9], the primitivity of G_x on Ω_c yields $c - p \leq 2$. Since $c - 2 \leq p \leq c$, we have that p^2 does not divide $|G|$, so p^2 does not divide k. Therefore either k is a prime, namely $c - 2$, $c - 1$, or c, or the product of two twin primes, namely $c(c - 2)$. On the other hand, $k^2 > v$, and by a result of Bochert [66, Th. 14.2], we have that $v \geq \frac{\frac{c+2}{2}!}{2}$. From this and the previous conditions on k, we have that $c = 13 (k = 11 \cdot 13)$, 8,7,6, or 5.

If $c = 13$, then $k = 143$, so $k(k - 1) = 2(v - 1)$ forces $v = 10154$. But if v is even, $k - 2$ must be a square, however 141 is not a square, which is a contradiction.

As we have seen earlier in this proof, for $5 \leq c \leq 8$ the only possibilities with k odd are the (4,3,2) and the (56,11,2) biplanes. Given the above conditions on k we have that $k = 3$ and $c = 5$, but we check in [9] that there are no maximal subgroups of S_5 nor A_5 of index 4.

We know consider the case $c = 6$, and $G \cong M_{10}$, $PGL_2(9)$, or $P\Gamma L_2(9)$. Checking the divisors of $2^2|A_6|$, the only possibilities for v such that $8v-7$ is a square are $v = 4$ and 16, and by Section 2.2 we know this is not the case.

□

This completes the proof of Lemma 5.11, and hence X is not an alternating group.

5.3 The Case in which X is a Sporadic Group

Here we consider D to be a biplane with a primitive, flag-transitive, almost simple automorphism group G with simple socle X, with X a sporadic group.

Lemma 5.12. *If D is a non-trivial biplane with a flag-transitive, primitive, almost simple automorphism group G, then* $\mathrm{Soc}(G) = X$ *is not a sporadic group.*

Proof. The way we proceed is as follows: We assume that the automorphism group G of D is almost simple, such that $X \trianglelefteq G \leq \mathrm{Aut}X$ with X a sporadic group. Then $G = X$, or $G = \mathrm{Aut}X$. We know that $v = [G : G_x]$, and G_x is a maximal group of G. The lists of maximal subgroups of X and $\mathrm{Aut}X$ appear in [9, 34, 35, 55]. (They are complete except for the 2-local subgroups of the Monster group). For each sporadic group (and its automorphism group), we rule out the maximal subgroups the order of which is too small to satisfy $|G| < |G|^3$. In the remaining cases, for those $v > 2$, we check if $8v - 7$ is a square, or if $2\left(|G_x|\right)^2_{v'} > 2v$. If this does happen, we check the remaining arithmetic conditions (v even then $k-2$ a square, $k(k-1) = 2(v-1)$).

To illustrate this procedure, suppose $X = J_1$. Then $G = J_1$, since $|\mathrm{Out}J_1| = 1$. The maximal subgroups H of J_1, with their orders and indices are as follows:

$L_2(11)$, of order 660, $v = 266$,

$2^3.7.3$, of order 168, $v = 1045$,

$2 \times A_5$, of order 120, $v = 1463$,

$19 : 6$, of order 114, $v = 1540$,

$11 : 10$, of order 110, $v = 1596$,

$D_6 \times D_{10}$, of order 60, $v = 2926$, and

$7 : 6$, of order 42.

In the last case, the order of the group is too small to satisfy $|G_x|^3 > |G|$, and in all the remaining cases we have that $8v - 7$ is not a square.

Proceeding in the same manner with the other sporadic groups, the only cases in which all conditions are met are the following:

(*i*) $G = M_{23}$, $G_x = 2^4 : (A_5 \times 3) : 2$, $(v, k) = (1771, 60)$.

(*ii*) $G = M_{24}$, $G_x = 2^6 : (3 \cdot S_6)$, $(v, k) = (1771, 60)$.

In the first case we have that the subdegrees of M_{23} on $2^4 : (A_5 \times 3) : 2$ are 1, 60, 480, 160, 90, and 20 (calculated with GAP, my sincere thanks to A.A. Ivanov and D. Pasechnik), but 30 does not divide 20, contradicting the fact that k must divide twice the order of every subdegree.

In the second case, the subdegrees are 1,90, 240, and 1440 [25, pp.126], however M_{24} has only one conjugacy class of subgroups of index 1771 [9], so if x is a point and B is a block we have G_x is conjugate to G_B, so G_x

fixes a block, say, B_0. We have that x cannot be incident with B_0 since the flag-transitivity of G implies that G_x is transitive on the k blocks incident with x. Hence x and B_0 are not incident, so the points (or a subset of them) incident with the block B_0 are a G_x-orbit, which is a contradiction since the smallest non-trivial G_x-orbit has size 90, and B_0 is incident with 60 points.

□

This completes the proof of Lemma 5.12, and hence X is not a sporadic group.

5.4 The Case in which X is a Classical Group

Here we consider D to be a non-trivial biplane, with a primitive, flag-transitive, almost simple automorphism group G, with simple socle X, such that $X = X_d(q)$ is a simple classical group, with a natural projective action on a vector space V of dimension d over the field $\mathbb{F}_q$, where $q = p^e$, (p prime).

5.4.1 X is a Linear Group

In this case we consider the socle of G to be $PSL_n(q)$, and $\beta = \{v_1, v_2, \ldots, v_n\}$ a basis for the natural n-dimensional vector space V for X.

Lemma 5.13. *If the group X is $PSL_2(q)$, then it is one of the following:*

(*i*) $PSL_2(7)$ *acting on the (7,4,2) biplane, with point stabiliser* S_4.

(*ii*) $PSL_2(11)$ *acting on a (11,5,2) biplane, with point stabiliser* A_5.

Proof. Suppose $X \cong PSL_2(q)$, $(q = p^m)$ is the socle of a flag-transitive automorphism group of a biplane D, so $G \leq P\Gamma L_2(q)$. As G is primitive, G_x is a maximal subgroup of G, and hence X_x is isomorphic to one of the following [22]: (Note that $|G_x|$ divides $(2, q-1)m|X_x|$):

(i) A solvable group of index $q+1$.

(ii) $D_{(2,q)(q-1)}$.

(iii) $D_{(2,q)(q+1)}$.

(iv) $L_2(q_0)$ if ($r>2$), or $PGL_2(q_0)$ if ($r=2$), where $q=q_0^r$, r prime.

(v) S_4 if $q=p\equiv \pm 1$ (mod8).

(vi) A_4 if $q=p\equiv$ 3,5,13,27,37 (mod40).

(vii) A_5 if $q\equiv \pm 1$ (mod10).

(i) Here we have that $v=q+1$, so $k(k-1)=2(v-1)=2q$, hence $q=3$, but $PSL_2(3)$ is not simple.

(ii), and (iii) The degrees in these cases are a triangular number, but the number of points on a biplane is always one more than a triangular number.

(iv) First assume $r>2$. Here we clearly have that q_0 divides $v=q_0^{r-1}\left(\frac{q_0^{2r}-1}{q_0^2-1}\right)$, so $k \mid 2\left(v-1, mq_0(q_0^2-1)\right)$, which divides $2m\left(q_0^2-1\right)$, so $k=\frac{2m\left(q_0^2-1\right)}{n}$. Say $q_0=p^b$, so $m=br$ and (except for $p=2$ and $2\leq b\leq 4$), we have $b<\sqrt{q_0}$.

Now, as $k^2>2v$, we have

$$\frac{4m^2\left(q_0^2-1\right)^2}{n^2}>2q_0^{r-1}\left(\frac{q_0^{2r}-1}{q_0^2-1}\right),$$

so

$$n^2<\frac{2m^2\left(q_0^2-1\right)^3}{q_0^{r-1}}\left(q_0^{2r}-1\right).$$

First consider $r>3$, so ($r\geq 5$). Here $\frac{\left(q_0^2-1\right)^3}{\left(q_0^{2r}-1\right)}<\frac{1}{4}$, so

$$n^2<\frac{m^2}{2q_o^{r-1}}<\frac{q_0}{2},$$

(as $m = rb > 4$).

From $k(k-1) = 2(v-1)$, we get

$$2m^2\left(q_0^2-1\right)^3 - mn\left(q_0^2-1\right)^2 = n^2\left(q_0^{3r-1} - q_0^{r-1} - q_0^2 + 1\right).$$

Now,

$$2m^2\left(q_0^2-1\right)^3 - mn\left(q_0^2-1\right)^2 < 2m^2q_0^6,$$

and

$$n^2\left(q_0^{3r-1} - q_0^{r-1} - q_0^2 + 1\right) > n^2q_0^{3r-2},$$

so

$$n^2q_0^{3r-8} < 2m^2 < 2q_0^r \leq q_0^{r+1}.$$

This implies that $3r - 8 < r + 1$, so $2r < 9$, which is a contradiction.

Next consider $r = 3$. Here $\frac{\left(q_0^2-1\right)^3}{\left(q_0^{2r}-1\right)} < 1$, so

$$n^2 < \frac{2m^2}{q_0^2} = \frac{18b^2}{q_0^2},$$

hence $n < \frac{5b}{q_0}$.

As $q = q_0^3 \neq 2$, we have $m^2 < q_0^3$, so $9b^2 < q_0^3$, and therefore $q_0 \neq 2$, and $b^2 < q_0$. Hence $n^2 < \frac{18}{q_0} \leq 6$, so $n \leq 2$.

Since $\sqrt{q_0} < \frac{5}{n}$, we have that $n > 1$ implies $q_0 < 7$. Also, $n < \frac{5}{\sqrt{q_0}}$ implies $q_0 < 25$, so $b \leq 4$.

Assume $n = 1$. From $k(k-1) = 2(v-1)$, we have $2m^2\left(q_0^2-1\right)^3 - m\left(q_0^2-1\right)^2 = q_0^8 - 2q_0^2 + 1$. As $m = 3b$, we have

$$q_0^8 - 2q_0^2 + 1 = 18b^2\left(q_0^2-1\right)^3 - 3b\left(q_0^2-1\right)^2 < 18 \cdot 16q_0^6.$$

So $q_0^8 - 2^5 \cdot 3^2 q_0^6 \leq 2q_0^2$, hence $q_0^4\left(q_0^2 - 2^5 \cdot 3^2\right) \leq 2$. This implies $q_0^2 \leq 2^5 \cdot 3^2$, which forces $q_0 \leq 16$.

We check for all values of $q_0 = 3$, 4, 5, 7, 8, 9, 11, 13, and 16 that $8v - 7$

is not a square.

Now assume $r = 2$. Then $v = \frac{q_0\left(q_0^2+1\right)}{(2,q-1)}$. As $q = q_0^2 \neq 2$, we have $m^2 < q$, so $4b^2 < q_0^2$, which implies $q_0 \neq 2$.

Now, from $k^2 > 2v$, we get $\frac{(2,q-1)^2 \cdot 2m^2\left(q_0^2-1\right)^2}{q_0\left(q_0^2+1\right)} > n^2$. If q is even then $n^2 < 2m^2 = 8b^2$, so $n < 3b$. If q is odd then $n^2 < 8m^2 = 32b^2$ so $n < 6b$.

First consider q even. From $k(k-1) = 2(v-1)$, we have

$$16b^2\left(q_0^2-1\right)^2 - 4bn\left(q_0^2-1\right) = 2n^2\left(q_0^3+q_0-1\right) < 16b^2\left(q_0^3+q_0-1\right),$$

so

$$4b\left(q_0^2-1\right)^2 - 4b\left(q_0^3+q_0-1\right) < n\left(q_0^2-1\right) < 3b\left(q_0^2-1\right),$$

hence $\left(q_0^2-1\right)^2 - q_0^3 - q_0 + 1 < q_0^2 - 1$, which is a contradiction.

Now consider q odd. Then we have

$$16b^2\left(q_0^2-1\right)^2 - 4bn\left(q_0^2-1\right) = n^2\left(q_0^3+q_0-2\right) < 32b^2\left(q_0^3+q_0-2\right),$$

so

$$4b\left(q_0^2-1\right)^2 - 8b\left(q_0^3+q_0-2\right) < n\left(q_0^2-1\right) < 6b\left(q_0^2-1\right),$$

that is, $2\left(q_0^2-1\right) - 4\left(q_0^3+q_0-2\right) < 3\left(q_0^2-1\right)$, which forces $q_0 = 3$, and $q = 9$. However this implies $v = 12$, but there is no k such that $k(k-1) = 22$, which is a contradiction.

(v) In this case $q = p \equiv \pm 1 \pmod 8$, and $m = 1$, so $G_0 \cong S_4$. So, we have q odd, $v = \frac{q(q^2-1)}{48}$, and k divides $2\left(\frac{q(q^2-1)-48}{48}, 24\right)$, so $k \mid 48$. As $k^2 > 2v$, we have that $q \leq 37$, hence $q = 7$, 17, 23, or 31. The only one of these values for which $8v-7$ is a square is $q = 7$, so $v = 7$ and $k = 4$, that is, we have the (7,4,2) biplane and $G = X \cong PSL_2(7)$.

(vi) Here $q = p \equiv 3$, 5, 13, 27, or 37 (mod 40), so $m = 1$ and $G_x \cong A_4$. Here $v = \frac{q(q^2-1)}{24}$, and so k divides $2\left(\frac{q(q^2-1)-24}{24}, 12\right)$, so $k \mid 24$. As $2v < k^2$,

we have $q = 3$, 5, or 13. For $q = 3$ we have $v = 1$, which is a contradiction. For $q = 5$ we have $v = 5$, but there is no such biplane. Finally, $q = 13$ implies $v = 91$, but then $8v - 7$ is not a square.

(*vii*) Here $q = p$ or $p^2 \equiv \pm 1 \pmod{10}$, $v = \frac{q(q^2-1)}{120}$, and so k divides $120m$, with $m = 1$ or 2. As $2v < k^2$, $q^3 - q < 60k^2 < 60(120)^2m^2$, so $q = 9$, 11, 19, 29, 31, 41, 49, 59, 61, 71, 79, 81, 89, or 121. Of these, the only value for which $8v - 7$ is a square is $q = 11$. In this case, $v = 11$ and $k = 5$, that is, we have a (11,5,2) biplane, with $G = X \cong PSL_2(11)$, and $G_x \cong A_5$.

□

This completes the proof of Lemma 5.13.

Lemma 5.14. *The group X is not $PSL_n(q)$, with $n > 2$, and $(n, q) \neq (3, 2)$.*

Proof. Suppose $X \cong PSL_n(q)$, with $n > 2$ and $(n, q) \neq (3, 2)$ (since $PSL_3(2) \cong PSL_2(7)$). We have $q = p^m$, and take $\{v_1, \ldots, v_n\}$ to be a basis for the natural n-dimensional vector space V for X. Since G_x is maximal in G, then by Theorem 4.8 G_x lies in one of the families $\mathcal{C}_i$ of subgroups of $\Gamma L_n(q)$, or in the set $\mathcal{S}$ of almost simple subgroups not contained in any of these families. We will analyse each of these cases separately. In describing the Aschbacher subgroups, we denote by $\hat{}H$ the pre-image of the group H in the corresponding linear group.

$\mathcal{C}_1$) Here we have G_x reducible. That is, $G_x \cong P_i$ stabilises a subspace of V of dimension i.

Suppose $G_x \cong P_1$. Then G is 2-transitive, and this case has already been done (Theorem 1.11).

Now suppose $G_x \cong P_i$, $1 < i < n$ fixes W, an i-subspace of V. We will assume $i \leq \frac{n}{2}$ since our arguments are arithmetic, and for i and $n - i$ we have the same calculations. Considering the G_x-orbits of the i-spaces intersecting

W in $i-1$-dimensional spaces, we have that k divides

$$\frac{2q\left(q^{i}-1\right)\left(q^{n-i}-1\right)}{(q-1)^{2}}.$$

Also,

$$v=\frac{\left(q^{n}-1\right)\ldots\left(q^{n-i+1}-1\right)}{\left(q^{i}-1\right)\ldots(q-1)}>q^{i(n-i)},$$

but we have that $k^2 > 2v$, so either $i=3$ and $n=7$, or $i=2$.

First assume $(n,i)=(7,3)$. Then k divides

$$2\left(\frac{q\left(q^{3}-1\right)\left(q^{4}-1\right)}{(q-1)^{2}},\frac{\left(q^{7}-1\right)\left(q^{6}-1\right)\left(q^{5}-1\right)}{\left(q^{3}-1\right)\left(q^{2}-1\right)(q-1)}-1\right),$$

but then $k^2 < v$, which is a contradiction.

Hence $i=2$. Here $v=\frac{(q^n-1)\left(q^{n-1}-1\right)}{(q^2-1)(q-1)}$, and G has suborbits with sizes: $|\{2\text{-subspaces } H : \dim(H\cap W)=1\}| = \frac{q(q+1)\left(q^{n-2}-1\right)}{q-1}$ and $|\{2\text{-subspaces } H : H\cap W=\overline{0}\}| = \frac{q^4\left(q^{n-2}-1\right)\left(q^{n-3}-1\right)}{(q^2-1)(q-1)}$.

If n is even then k divides $\frac{q\left(q^{n-2}-1\right)}{(q^2-1)}$, since $q+1$ is prime to $\frac{\left(q^{n-3}-1\right)}{q-1}$, and so $k^2<v$, which is a contradiction.

Hence n is odd, and k divides $\frac{2q\left(q^{n-2}-1\right)}{q-1}\left(q+1,\frac{n-3}{2}\right)$.

First assume $n=5$. Then $v=(q^2+1)\left(q^4+q^3+q^2+q+1\right)$, and k divides $2q\left(q^2+q+1\right)$. The fact that $k^2>2v$ forces $k=2q\left(q^2+q+1\right)$.

From $k(k-1)=2(v-1)$, we have

$$4q^{2}\left(q^{2}+q+1\right)^{2}-2q\left(q^{2}+q+1\right)=2\left(q^{6}+q^{5}+2q^{4}+2q^{3}+2q^{2}+q\right),$$

so

$$\left(q^{2}+q+1\right)\left(2q\left(q^{2}+q+1\right)-1\right)=\left(q^{5}+q^{4}+2q^{3}+2q^{2}+2q+1\right).$$

If we expand we get the following equality:

$$q^5 + 3q^4 + 4q^3 + q^2 - q - 2 = 0,$$

which is, of course, a contradiction. Hence $n \geq 7$. Here we have

$$v = \left(q^{n-1} + q^{n-2} + \ldots + q + 1\right)\left(q^{n-3} + q^{n-5} + \ldots + q^2 + 1\right),$$

and k divides $2dc$, where $d = q\left(q^{n-3} + q^{n-4} + \ldots + q + 1\right)$ and $c = \left(q+1, \frac{n-3}{2}\right)$. Say $k = \frac{2dc}{e}$. The inequality $v < k^2$ forces $e \leq 2q$. We have that

$$\frac{v-1}{d} = q^{n-2} + q^{n-4} + \ldots + q^3 + q + 1,$$

and also, since $k(k-1) = 2(v-1)$, we have

$$k = \frac{2(v-1)}{k} + 1 = \frac{2eq^{n-2} + 2eq^{n-4} + \ldots + 2eq^3 + 2eq + 2e + c}{c}.$$

We have that $\left(\frac{kc}{2}, d\right)$ divides d, and also
$\left(eq^{n-2} + eq^{n-4} + \ldots + eq + e + c, q\left(eq^{n-3} + eq^{n-5} + eq^2 + e\right)\right) =$
$\left(eq^{n-2} + \ldots + eq + e + c, e + c\right)$, and
$\left(eq^{n-2} + \ldots + eq + e + c, eq^{n-3} + eq^{n-4} + \ldots + eq + e\right) =$
$\left(eq^{n-2} + \ldots + eq + e + c, (2e + c)q + e + c\right)$.

Therefore $\frac{kc}{2}$ divides $c^2(e + c)\left((2e + c)q + e + c\right)$, and since $e \leq 2q$ and $c = \left(q+1, \frac{n-3}{2}\right)$, the only possibilities for n and q are $n = 7$ and $q \leq 3$, or $n = 9$ and $q = 2$. However in none of these possibilities is $8v - 7$ a square.

$\mathcal{C}_1'$) Here G contains a graph automorphism and G_x stabilises a pair $\{U, W\}$ of subspaces of dimension i and $n - i$, with $i < \frac{n}{2}$. Write G^0 for $G \cap P\Gamma L_n(q)$ of index 2 in G.

First assume $U \subset W$. By 5.6, there is a subdegree which is a power of p. On the other hand, if p is odd then the highest power of p dividing $v - 1$ is

q, it is $2q$ if $q > 2$ is even, and is at most 2^{n-1} if $q = 2$. Hence $k^2 < v$, which is a contradiction.

Now suppose $V = U \oplus W$. Here p divides v, so $(k, p) \le 2$. First assume $i = 1$. If $x = \{\langle v_1 \rangle, \langle v_2 \dots v_n \rangle\}$, then consider $y = \{\langle v_1, \dots, v_{n-1} \rangle, \langle v_n \rangle\}$, so $[G_x : G_{xy}] = \frac{q^{n-2}\left(q^{n-1}-1\right)}{q-1}$, and k divides $\frac{2\left(q^{n-1}-1\right)}{q-1}$, so as $v = \frac{q^{n-1}(q^n-1)}{q-1} > q^{2(n-1)}$, we have $k^2 < v$, a contradiction.

Now assume $i > 1$. Consider $x = \{\langle v_1, \dots, v_i \rangle, \langle v_{i+1}, \dots, v_n \rangle\}$ and $y = \{\langle v_1, \dots, v_{i-1}, v_i + v_n \rangle, \langle v_{i+1}, \dots, v_n \rangle\}$. Then $[G_x^0 : G_{xy}^0]_{p'}$ divides $2\left(q^i - 1\right)\left(q^{n-i} - 1\right)$, so again we have $k^2 < v$, a contradiction.

$\mathcal{C}_2$) Here G_x preserves a partition $V = V_1 \oplus \dots \oplus V_a$, with each V_i of the same dimension, say, b, and $n = ab$.

First consider the case $b = 1$, $n = a$, and let $x = \{\langle v_1 \rangle, \dots, \langle v_n \rangle\}$ and $y = \{\langle v_1 + v_2 \rangle, \langle v_2 \rangle, \dots, \langle v_n \rangle\}$. As $n > 2$, we have that k divides $4n(n-1)(q-1) = 2[G_x : G_{xy}]$. We have $v > \frac{q^{n(n-1)}}{n!}$ and $k^2 > v$, so $n = 3$ and $q \le 4$. So $v = \frac{q^3(q^3-1)(q+1)}{(3,q-1)6!}$. As $k \mid 2(v-1)$, only for $q = 2$ can $k > 2$, so consider $q = 2$. Then $k \mid 6$, and $v = 28$, but there is no such value of k satisfying $k(k-1) = 2(v-1)$.

Now let $b > 1$, and consider $x = \{\langle v_1, \dots, v_b \rangle, \langle v_{b+1}, \dots, v_{2b} \rangle, \dots\}$ and $y = \{\langle v_1, \dots, v_{b-1}, v_{b+1} \rangle, \langle v_b, v_{b+2}, \dots, v_{2b} \rangle, \dots, \langle v_{n-b+1}, \dots, v_n \rangle\}$. Then k divides $\frac{2a(a-1)\left(q^b-1\right)^2}{q-1}$. Since $v > \frac{q^{n(n-b)}}{a!}$, we have $n = 4$, $q \ge 5$, and $a = 2 = b$. In none of these cases can we have $k > 2$.

$\mathcal{C}_3$) In this case G_x is an extension field subgroup. Since $2|G_x||G_x|_{p'}^2 > |G|$, we have that either:

(i) $n = 3$, and $X \cap G_x = \hat{}(q^2 + q + 1) \cdot 3 < PSL_3(q) = X$, or

(ii) n is even, and $G_x = N_G(\hat{}PSL_{\frac{n}{2}}(q^2))$.

First consider case (i). Here $v = \frac{q^3\left(q^2-1\right)(q-1)}{3}$, so k divides $6\left(q^2 + q + 1\right)(\log_p q)$. As $k^2 > v$, we have $q = 3, 4, 5, 8, 9, 11$, or 13. But in none of these cases is $8v-7$ a square.

Now consider case (ii), and write $n=2m$. As p divides v, we have that $(k,p)\leq 2$. First suppose $n\geq 8$, and let W be a 2-subspace of V considered as a vector space over the field of q^2 elements, so that W is a 4-subspace over a field of q elements. If we consider the stabiliser of W in G_x and in G we have that in $G_W\setminus G_{xW}$ there is an element g such that $G_x\cap G_x^g$ contains the pointwise stabiliser of W in G_x as a subgroup. Therefore k divides $2\left(q^n-1\right)\left(q^{n-2}-1\right)$, contrary to $2v<k^2$, which is a contradiction.

Now let $n=6$. Then since $(k,p)\leq 2$, by Lemma 5.4, we have that k is divisible by the index of a parabolic subgroup of G_x, so it is divisible by the primitive prime divisor q_3 of q^3-1, but this divides the index of G_x in G, which is v, a contradiction.

Hence $n=4$. Then $v=\frac{q^4\left(q^3-1\right)(q-1)}{2}$, and so k is odd and prime to $q-1$. As $(v-1,q+1)=1$, we have that k is also prime to $q+1$, and hence $k\mid(q^2+1)\log_p q$, contrary to $k^2>2v$, another contradiction.

$\mathcal{C}_4$) Here G_x stabilises a tensor product of spaces of different dimensions, and $n\geq 6$. In these cases we have $v>k^2$.

$\mathcal{C}_5$) In this case G_x is the stabiliser in G of a subfield space. So $G_x=N_G\left(PSL_n(q_0)\right)$, with $q=q_0^m$, m a prime.

If $m>2$ then $2|G_x||G_x|_{p'}^2>|G|$, forces $n=2$, a contradiction.

Hence $m=2$. If $n=3$ then $v=\frac{\left(q_0^3+1\right)\left(q_0^2+1\right)q_0^3}{(q_0+1,3)}$.

Since p divides v, we have $(k,p)\leq 2$, so by Lemma 5.4 we have that G_{xB} (where B is a block incident with x) is contained in a parabolic subgroup of G_x. Therefore $q_0^2+q_0+1$ divides k, and $(v-1,q_0^2+q_0+1)$ divides $2q_0+(q_0+1,3)$, forcing $q_0=2$ and $v=120$, but then $8v-7$ is not a square.

If $n=4$, then by Lemma 5.4 q_0^2+1 divides k, but q_0^2+1 also divides v, which is a contradiction.

Hence $n\geq 5$. Considering the stabilisers of a 2-dimensional subspace of

V, we have that k divides $2\left(q_0^n-1\right)\left(q_0^{n-1}-1\right)$, but then $k^2<v$, which is also a contradiction.

$\mathcal{C}_6$) Here G_x is an extraspecial normaliser. Since $2|G_x||G_x|_{p'}^2>|G|$, we have $n\leq 4$. Now, $n>2$ implies that $G_x\cap X$ is 2^4A_6 or 3^2Q_8, with X either $PSL_4(5)$ or $PSL_3(7)$ respectively. Since k divides $2(v-1,|G_x|)$, we check that $k\leq 6$, contrary to $k^2>2v$.

If $n=2$ then $G_x\cap X=A_4.a<L_2(p)=X$, with $a=2$ precisely when $p\equiv\pm 1 \pmod 8$, and $a=1$ otherwise, (and there are a conjugacy classes in X). From $|G|<|G_x|^3$ we have that $p\leq 13$. If $p=7$ then the action is 2-transitive. The remaining case are ruled out by the fact that k divides $2(v-1,|G_x|)$, and $k(k-1)=2(v-1)$.

$\mathcal{C}_7$) Here G_x stabilises the tensor product of a spaces of the same dimension, say, b, and $n=b^a$. Since $|G_x|^3>|G|$, we have $n=4$ and $G_x\cap X=(PSL_2(q)\times PSL_2(q))\,2^d<X=PSL_4(q)$, with $d=(2,q-1)$. Then $v=\frac{q^4\left(q^2+1\right)\left(q^3-1\right)}{x}>\frac{q^9}{x}$, with $x=2$ unless $q\equiv 1 \pmod 4$, in which case $x=4$. Hence $4\nmid k$, and so k divides $2\left(q^2-1\right)\log_p q$, and if q is odd then k divides $\frac{\left(q^2-1\right)\log_p q}{32}$.

If q is odd. Then $k^2<\frac{q^9}{32}<\frac{q^9}{x}=v$, a contradiction. Hence q is even, and so

$$k=\frac{2\left(q^2-1\right)^2\log_p q}{r},$$

and since $k^2>2v$ we have $r^2<\frac{4(q+1)^4\log_p q}{q^5}$, therefore $q\leq 32$.

However, the five cases are dismissed by the fact that k divides $2(v-1)$.

$\mathcal{S}$) We finally consider the case where G_x is an almost simple group, (modulo the scalars), not contained in the Aschbacher subgroups of G. From [39, Theorem 4.2] we have that $|G_x|<q^{2n+4}$, $G_x'=A_{n-1}$ or A_{n-2}, or $G_x\cap X$ and X are as in [39, Table 4].

Also, we have that $|G| < |G_x|^3$, and $|G| \leq q^{n^2-n-1}$, so $n \leq 7$, and by the bound $2|G_x||G_x|^2_{p'} > |G|$, we need only consider the following possibilities [30, Chapter 5]:

$n = 2$, and $G_x \cap X = A_5$, with $q = 11$, 19, 29, 31, 41, 59, 61, or 121.

$n = 3$, and $G_x \cap X = A_6 < PSL_3(4) = X$.

$n = 4$, and $G_x \cap X = U_4(2) < PSL_4(7) = X$.

In the first case, with $A_5 < L_2(11)$ the action is 2-transitive. In the remaining cases, the fact that k divides $2|G_x|$ and $2(v-1)$ forces $k^2 < v$, which is a contradiction.

□

This completes the proof of Lemma 5.14.

5.4.2 X is a Symplectic Group

Here the socle of G is $X = PSp_{2m}(q)$, with $m \geq 2$ and $(m, q) \neq (2, 2)$. As a standard symplectic basis for V, we have $\beta = \{e_1, f_1, \ldots, e_m, f_m\}$.

Lemma 5.15. *The group X is not $PSp_{2m}(q)$ with $m \geq 2$, and $(m, q) \neq (2, 2)$.*

Proof. We will consider G_x to be in each of the Aschbacher families of subgroups, and finally, an almost simple group not contained in any of the Aschbacher families of G. In each case we will arrive at a contradiction.

When $(p, n) = (2, 4)$, the group $Sp_4(2^f)$ admits a graph automorphism, this case will be treated separately after the eight Aschbacher families of subgroups.

$\mathcal{C}_1$) If $G_x \in \mathcal{C}_1$, then G_x is reducible, so either it is parabolic or it stabilises a nonsingular subspace of V.

First assume that $G_x = P_i$, the stabiliser of a totally singular i-subspace of V, with $i \leq m$. Then we have

$$v = \frac{(q^{2m}-1)(q^{2m-2}-1)\dots(q^{2m-2i+2}-1)}{(q^i-1)(q^{i-1}-1)\dots(q-1)}.$$

From this we see that $v \equiv q+1 \ (\mathrm{mod} pq)$, so q is the highest power of p dividing $v-1$. By Lemma 5.6 there is a subdegree which is a power of p, and as k divides twice every subdegree, we have that k divides $2q$, contrary to $v < k^2$.

Now suppose that $G_x = N_{2i}$, the stabiliser of a nonsingular $2i$-subspace U of V, with $m > 2i$. Then p divides v, so $(k,p) \leq 2$.

Take $U = \langle e_1, f_1, \dots e_i, f_i\rangle$, and $W = \langle e_1, f_1, \dots e_{i-1}, f_{i-1}, e_{i+1}, f_{i+1}\rangle$. The p'-part of the size of the G_x-orbit containing W is

$$\frac{(q^{2i}-1)(q^{2m-2i}-1)}{(q^2-1)^2}.$$

Since $v < q^{4i(m-i)}$, we can only have $v < k^2$ if $q = 2$ and $m = i+1$, which is a contradiction.

$\mathcal{C}_2$) If $G_x \in \mathcal{C}_2$ then in preserves a partition $V = V_1 \oplus \dots \oplus V_a$ of isomorphic subspaces of V.

First assume all the V_j's to be totally singular subspaces of V of maximal dimension m. Then $G_x \cap X = \hat{\ } GL_m(q).2$, and since G_x is maximal we have that q is odd [33]. Then

$$v = \frac{q^{\frac{m(m+1)}{2}}(q^m+1)(q^{m-1}+1)\dots(q+1)}{2} > \frac{q^{m(m+1)}}{2},$$

and $(k,p) = 1$.

Let

$$x = \{\langle e_1, \dots, e_m\rangle, \langle f_1, \dots f_m\rangle\},$$

and

$$y = \{\langle e_1, \ldots, e_{m-1}, f_m\rangle, \langle f_1, \ldots, f_{m-1}, e_m\rangle\}.$$

Then the p'-part of the G_x-orbit of y divides $2(q^m - 1)$, and so k divides $4(q^m - 1)$, contrary to $v < k^2$.

Now assume that each of the V_j's is nonsingular of dimension $2i$, so we have $G_x \cap X = \hat{}Sp_{2i}(q)\mathrm{wr}S_t$, with $it = m$. Let

$$x = \{\langle e_1, f_1, \ldots, e_i, f_i\rangle, \langle e_{i+1}, f_{i+1}, \ldots, e_{2i}, f_{2i}\rangle, \ldots\},$$

and take

$$y = \{\langle e_1, f_1, \ldots, e_1, f_i + e_{i+1}\rangle, \langle e_{i+1}, f_{i+1} - e_i, e_{i+2}, \ldots, e_{2i}, f_{2i}, \ldots\rangle\}.$$

Considering the size of the G_x-orbit containing y, we see that k divides

$$\frac{t(t-1)(q^{2i}-1)^2}{q-1}.$$

Now, we have that

$$\frac{q^{2i^2t(t-1)}}{t!} < v,$$

so from $v < k^2$ we have that $t!t^4 > q^{2i^2t(t-1)+2-8i}$, so $q^{2t(t-1)-6} < t^{t+4}$, and therefore $t < 4$.

First assume $t = 3$. Then by the above inequalities we have that $i = 1$ and $q = 2$, but then G_x is not maximal [9, p.46].

Now let $t = 2$. Then $k < 2q^{4i-1}$, so $q^{4i^2-8i+2} < 8$, and therefore $i \leq 2$.

If $i = 2$ then $q = 2$ and $v = 45696 = 2^7 \cdot 3 \cdot 7 \cdot 17$, but then $8v - 7$ is not a square, which is a contradiction.

If $i = 1$ then $X = PSp_4(q)$,

$$v = \frac{q^2(q^2+1)}{2},$$

and k divides $2(q+1)^2(q-1)$. Since k divides $2(v-1)$, we have that k divides $(q^2(q^2+1)-2, 2(q+1)^2(q-1))$, that is, k divides

$$\big((q^2+2)(q^2-1), 2(q+1)^2(q-1)\big) = (q^2-1)\left(q^2+2, 2(q+1)\right) \leq 6(q^2-1).$$

Therefore

$$k = \frac{6(q^2-1)}{r},$$

with $1 \leq r \leq 6$. We have that $2(v-1) = (q^2+2)(q^2-1)$, and also $2(v-1) = k(k-1)$, but we check that for all possible values of r this equality is not satisfied.

$\mathcal{C}_3$) If $G_x \in \mathcal{C}_3$, then it is an extension field subgroup, and there are two possibilities.

Assume first that $G_x \cap X = PSp_{2i}(q^t).t$, with $m = it$ and t a prime number. From $|G| < |G_x|^3$, we have that $t = 2$ or 3.

If $t = 3$, then since $v < k^2$ we have that $i = 1$, and so

$$G_x \cap X = PSp_2(q^3) < PSp_6(q) = X,$$

and

$$v = \frac{q^6(q^4-1)(q^2-1)}{3}.$$

This implies that k is coprime to $q+1$, but applying Lemma 5.4 to $PSp_2(q^3)$ we have that q^3+1 divides k, which is a contradiction.

If $t = 2$, then

$$v = \frac{q^{2i^2}(q^{4i-2}-1)(q^{4i-6}-1)\dots(q^6-1)(q^2-1)}{2}.$$

Consider the subgroup $Sp_2(q^2) \circ Sp_{2i-2}(q^2)$ of $G_x \cap X$. This is contained in $Sp_4(q) \circ Sp_{4i-4}(q)$ in X. Taking $g \in Sp_4(q) \setminus Sp_2(q^2)$, we see that $Sp_{2i-2}(q^2)$ is contained in $G_x \cap G_x^g$, so k divides $2(q^{4i}-1)\log_p q$. The inequality $v < k^2$

forces $i \leq 2$.

First assume $i = 2$. Then

$$v = \frac{q^8(q^6 - 1)(q^2 - 1)}{2}$$

and k divides $2(q^8 - 1)\log_p q$, but since $(k, v) \leq 2$ and $q^2 - 1$ divides v, we have that k divides $2(q^4 + 1)(q^2 + 1)\log_p q$, forcing $q = 2$. In this case $v = 2^7 \cdot 3^3 \cdot 7 = 24192$, and $k = 2 \cdot 5 \cdot 17 = 170$ (otherwise $k^2 < v$), but then k does not divide $2(v - 1)$, which is a contradiction.

Hence $i = 1$, so

$$v = \frac{q^2(q^2 - 1)}{2},$$

and $G_x \cap X = PSp_2(q^2).2 < PSp_4(q) = X$, so k divides $4q^2(q^4 - 1)$, but since $(k, v) \leq 2$, then k divides $4(q^2 + 1)$, so $k = \frac{4(q^2+1)}{r}$ for some $r \leq 8$ (since $v < k^2$). Now $2(v - 1) = k(k - 1)$, and also $2(v - 1) = (q^2 - 2)(q^2 + 1)$, so we have that

$$r^2(q^2 - 2) = 16(q^2 + 1) - 4r,$$

that is,

$$(r + 4)(r - 4)q^2 = 2(8 + r(r - 2)).$$

This implies that $4 < r \leq 8$, but solving the above equation for each of these possible values of r gives non-integer values of q, which is a contradiction.

Now assume that $G_x \cap X = \hat{}GU_m(q).2$, with q odd. Since v is even, 4 does not divide k. Also, k is prime to p, so by the Lemma 5.4, the stabiliser in $G_x \cap X$ of a block is contained in a parabolic subgroup. But then $q + 1$ divides the indices of the parabolic subgroups in the unitary group, so $q + 1$ divides k, but $q + 1$ also divides v, which is a contradiction.

$\mathcal{C}_4$) If $G_x \in \mathcal{C}_4$, then G_x stabilises a decomposition of V as a tensor product of two spaces of different dimensions, and G_x is too small to satisfy

$$|G| < 2|G_x||G_x|_{p'}^2.$$

$\mathcal{C}_5$) If $G_x \in \mathcal{C}_5$, then $G_x \cap X = PSp_{2m}(q_0).a$, with $q = q_0^b$ for some prime b and $a \leq 2$, (with $a = 2$ if and only if $b = 2$ and q is odd). The inequality $|G| < 2|G_x||G_x|_{p'}^2$ forces $b = 2$. Then

$$v = \frac{q^{\frac{m^2}{2}}(q^m + 1)\ldots(q + 1)}{(2, q - 1)} > \frac{q^{\frac{m(2m+1)}{2}}}{2}.$$

Now G_x stabilises a $GF(q_0)$-subspace W of V. Considering a nonsingular 2-dimensional subspace of W we see that

$$Sp_2(q_0) \circ Sp_{2m-2}(q_0) < Sp_2(q) \circ Sp_{2m-2}(q) < X.$$

If we take $g \in Sp_2(q) \setminus Sp_2(q_0)$ we see that $Sp_{2m-2}(q_0) < G_x \cap G_x^g$. This impies that there is a subdegree of X with the p'-part dividing $q_0^{2m} - 1$, so that k divides $2(q^m - 1)\log_p q$, contrary to $v < k^2$.

$\mathcal{C}_6$) If $G_x \in \mathcal{C}_6$, then $G_x \cap X = 2^{2^s}\Omega_{2^s}^{-}(2).a$, q is an odd prime, $2m = 2^s$, and $a \leq 2$. Since $|G| < |G_x|^3$, we have that $s \leq 3$, and if $s = 3$ then $q = 3$, but then k is too small. If $s = 2$, then $q \leq 11$, but again k is too small in each of these cases.

$\mathcal{C}_7$) If $G_x \in \mathcal{C}_7$ then $G_x = N_G\left(PSp_{2a}(q)^{2r}2^{r-1}A_r\right)$ and $2m = (2a)^r \geq 8$, but this is a contradiction since $|G| < |G_x|^3$.

$\mathcal{C}_8$) If $G_x \in \mathcal{C}_8$, then $G_x \cap X = O_{2m}^{\epsilon}(q)$, with q even, and $2m \geq 4$. We can assume $q > 2$ as in this case the action is 2-transitive, and that has been done in Theorem 1.11. Here

$$v = \frac{q^m(q^m+\epsilon)}{2},$$

and from the proof of [45, Prop.1] we have that the subdegrees of X are $(q^m-\epsilon)(q^{m+1}+\epsilon)$, and $\frac{(q-2)}{2}q^{m-1}(q^m-\epsilon)$. This implies by Lemma 3.2 that k divides $2(q^m-\epsilon)\,(q-2, q^{m-1}+\epsilon)$. However, by Lemma 5.4 k is divisible by the index of a parabolic subgroup in $O^{\epsilon}_{2m}(q)$, which is not the case.

$p = m = 2$ Here $2m = 4$, q is even, and we have the following possibilities:

G_x normalises a Borel subgroup of X in G. Then $v = (q+1)(q^3+q^2+q+1)$, so $2q$ is the highest power of 2 dividing $v-1$. But k is also a power of 2, conrtary to $v < k^2$.

$G_x \cap X = D_{2(q\pm1)}\mathrm{wr}S_2$. So k divides $2(q\pm1)^2\log_2 q$, too small to satisfy $v < k^2$.

$G_x \cap X = (q^2+1).4$, which is too small.

$\mathcal{S}$) Finally consider the case in which $G_x \in \mathcal{S}$ is an almost simple group (modulo scalars) not contained in any of the Aschbacher subgroups of G. These subgroups are listed in [30] for $2m \le 10$.

First assume $2m = 4$. then we have one of the following possibilities:

(*i*) $G_x \cap X = Sz(q)$, q even.

(*ii*) $G_x \cap X = PSL_2(q)$, $q \ge 5$, or

(*iii*) $G_x \cap X = A_6.a$, $a \le 2$ and $q = p \ge 5$.

In case (*i*), $v = q^2(q^2-1)(q+1)$. Applying Lemma 5.4 to $Sz(q)$, we see that q^2+1 divides k. Now, $(v-1, q^2+1) = (q-2, 5)$, so $q = 2$, contrary to our initial assumptions.

In case (*ii*), since $(k, v) \le 2$, we have $k \le 2\log_p q$, contrary to $v < k^2$.

In case (*iii*), 4 does not divides k, so k must divide 90, contrary to $v < k^2$.

Now let $2m = 6$. As $|G| < 2|G_x||G_x|^2_{p'}$, from [30] we have that either $G_x \cap X = J_2 < PSp_6(5) = X$, or $G_x \cap X = G_2(q)$ with q even. In the first case, k divides $2 \cdot 3^3 \cdot 7$, which is too small. In the second case, $v = q^3(q^4 - 1)4$, so $(k, q+1) = 1$. Applying Lemma 5.4 to $G_2(q)$, we see that $\frac{q^6-1}{q-1}$ divides k, a contradiction.

If $2m = 8$ or 10, then by [30] we have $G_x = S_{10} < Sp_8(2) = G$, or $G_x = S_{14} < Sp_{12}(2) = G$. In the first case, k divides $2(v-1, |G_x|) = 70$, which si too small. In the second case, since $(k, v) \leq 2$, we have that k divides $2 \cdot 7^2 \cdot 11 \cdot 13$, also too small.

If $2m \geq 12$, then by [39] we have $|G_x| \leq q^{4(m+1)}$, $G'_x = A_{n+1}$ or A_{n+2}, or X and $G_x \cap X$ are $E_7(q) \leq PSp_{56}(q)$. The latter is not possible as here $k^2 < v$, and the bound $|G_x| < q^{4(m+1)}$ forces $m < 6$.

The only possibilities for the alternating groups are $q = 2$, and $m = 7$, 8, or 9, however in all these cases k is too small. □

This completes the proof of Lemma 5.15.

5.4.3 X is an Orthogonal Group of Odd Dimension

Here we consider $X = P\Omega_{2m+1}(q)$, with q odd and $n = 2m+1 \geq 7$, (since $\Omega_3(q) \cong L_2(q)$, and $\Omega_5(q) \cong PSp_4(q)$).

Lemma 5.16. *The group X is not $P\Omega_{2m+1}(q)$, with $n \geq 7$.*

Proof. Here, as in the symplectic case, we will consider G_x to be in each of the Aschbacher families of subgroups, and then to be a subgroup of G not contained in any of these families, and arrive at a contradiction in each case.

$\mathcal{C}_1$) If $G_x \in \mathcal{C}_1$, then G_x is either parabolic or it stabilises a nonsingular subspace of V.

First assume $G_x = P_i$, the stabiliser of a totally singular i-subspace of V. Then, as in the symplectic case, $v \equiv q+1 \pmod{pq}$, so q is the highest power of p dividing $v-1$. As there is a subdegree which is a power of p, we have that k divides $2q$, contradicting $v < k^2$.

Now assume that $G_x = N_i^{\epsilon}$, the stabiliser of a nonsingular i-dimensional subspace W of V of sign ϵ (if i is odd ϵ is the sign of $W^{\perp}$).

First let $i = 1$. Then

$$v = \frac{q^m(q^m+\epsilon)}{2},$$

and the X-subdegrees are $(q^m-\epsilon)(q^m+\epsilon)$, $\frac{q^{m-1}(q^m-\epsilon)}{2}$, and $\frac{q^{m-1}(q^m-\epsilon)(q-3)}{2}$. This implies that k divides $q^m-\epsilon$, contrary to $v < k^2$.

Hence $i \geq 2$. Let W be the i-space stabilised by G_x, choose $w \in W$ with $\mathcal{Q}(w) = 1$, and $u \in W^{\perp}$ with $\mathcal{Q}(u) = -c$ for some non-square $c \in GF(q)$. Then $\langle v, w\rangle$ is of type N_2^-, and if $g \in G$ stabilises $W^{\perp}$ pointwise but does not fix neither u nor w, then we have $G_x \cap G_x^g$ contains $SO_{i-1}(q) \times SO_{n-i-1}(q)$. This implies that $k \leq 4q^m \log_p q$, but since $v > q^{\frac{i(n-i)}{4}}$, q is odd, and $m \geq 3$; this is contrary to $v < k^2$.

$\mathcal{C}_2$) If $G_x \in \mathcal{C}_2$, then G_x is the stabiliser of a subspace decomposition into isometric nonsingular spaces. From the inequality $|G| < 2|G_x||G_x|_{p'}^2$ it follows that the only possibilities are:

$G_x \cap X = 2^6 A_7 < \Omega_7(q)$ with q either 3 or 5, and

$G_x \cap X = 2^{n-1} A_n < \Omega_n(3)$ with $n = 7$, 9, or 11.

In each case the fact that k divides $2(v-1)$ forces $v < k^2$, a contradiction.

$\mathcal{C}_3$) If $G_x \in \mathcal{C}_3$, then $G_x \cap X = \Omega_a(q^t).t$ with $n = at$. Since a and t are odd, $a = 2r+1 < \frac{n}{2}$, so

$$|G_x|_{p'} = t\prod_{i=1}^{r}\left(q^{2it}-1\right),$$

and since k divides $2\left(|G_x|_{p'}, v-1\right)$, it is too small to satisfy $k^2 > v$.

$\mathcal{C}_4$) If $G_x \in \mathcal{C}_4$, then it stabilises a tensor product of nonsingular subspaces, but these have to be of odd dimension and so G_x is too small.

$\mathcal{C}_5$) If $G_x \in \mathcal{C}_5$, then $G_x \cap X = \Omega_n(q_0).a$, with $q = q_0^b$ for some prime b, and $a \leq 2$, with $a = 2$ if and only $b = 2$. The inequality $|G| < |G_x||G_x|^2_{p'}$ forces $b = 2$. If $n = 2m+1$, then we have that k divides $2|G_x \cap X| = q_0^{m^2}(q_0^{2m}-1)\dots(q_0^2-1)$, but $v = q^{m^2}(q_0^{2m}+1)\dots(q_0^2+1)$, so k is prime to q, and $(v-1, (q^{2m}-1)\dots(q_0^2-1))$ is too small.

$\mathcal{C}_6$), $\mathcal{C}_7$), and $\mathcal{C}_8$) In this cases $\mathcal{C}_6$ and $\mathcal{C}_8$, the classes are empty, and for $\mathcal{C}_7$ we have that $G_x \cap X$ stabilises the tensor product power of a non-singular space, but it is too small to satisfy $|G| < |G_x|^3$.

$\mathcal{S}$) Now consider the case in which G_x is a simple group not contained in any of the Aschbacher collection of subgroups of G. As in the symplectic section, we only need to consider the following possibilities:

(*i*) $G_x \cap X = G_2(q) < \Omega_7(q) = X$ with q odd,

(*ii*) $G_x \cap X = Sp_6(2) < \Omega_7(p)$ with p either 3 or 5, or

(*iii*) $G_x \cap X = S_9 < \Omega_7(3)$.

In all three cases we have that as k divides $2\,(v-1, |G_x|)$ it is too small.

□

This completes the proof of Lemma 5.16.

5.4.4 X is an Orthogonal Group of Even Dimension

In this section $X = P\Omega^\epsilon_{2m}(q)$, with $m \geq 4$. We write $\beta_+ = \{e_1, f_1, \dots, e_m, f_m\}$ for a standard basis for V in the O^+_{2m}-case, and $\beta_- = \{e_1, f_1, \dots, e_{m-1}, f_{m-1}, d, d'\}$ in the O^-_{2m}-case.

Lemma 5.17. *The group X is not $P\Omega^{\epsilon}_{2m}(q)$, with $m \geq 4$.*

Proof. As before, we take G_x to be in one of the Aschbacher families of subgroups of G, or a simple group not contained in any of these families, and analyse each case separately. We postpone until the end of the proof the case where $(m, \epsilon) = (4, +)$ and G contains a triality automorphism.

$\mathcal{C}_1$) If $G_x \in \mathcal{C}_1$, then we have two possibilities.

First assume that G_x stabilises a totally singular i-space, and suppose that $i < m$. If $i = m-1$ and $\epsilon = +$, then $G_x = P_{m,m-1}$, otherwise $G_x = P_i$. In any case there is a unique subdegree of X that is a power of p (except in the case where $\epsilon = +$, m is odd, and $G_x = P_m$ or P_{m-1}). On the other hand, the highest power of p dividing $v-1$ divides q^2 or 8, so k is too small.

Now consider $G_x = P_m$ in the case $X = P\Omega^{+}_{2m}(q)$, and note that in this case P_{m-1} and P_m are the stabilisers of totally singular m-spaces from the two different X-orbits. If m is even then

$$x = \langle e_1, \ldots, e_m \rangle,\ y = \langle f_1, \ldots, f_m \rangle$$

are in the same X-orbit, and the size of the G_x-orbit of y is a power of p. However, the highest power of p dividing $v-1$ is q, so k is too small.

If m is odd, $m \geq 5$, then $v = (q^{m-1}+1)(q^{m-2}+1)\ldots(q+1) > q^{\frac{m(m-1)}{2}}$. Let

$$x = \langle e_1, \ldots, e_m \rangle,\ y = \langle e_1, f_2, \ldots, f_m \rangle.$$

Then x and y are in the same X-orbit, and the index of G_{xy} in G_x has p'-part dividing $q^m - 1$. Since the highest power of p dividing $v-1$ is q, we have that k divides $2q(q^m-1)$. By the inequality $v < k^2$, we have that $m = 5$. In this case the action is of rank three, with nontrivial subdegrees

$$\frac{q(q^2+1)(q^5-1)}{q-1} \text{ and } \frac{q^6(q^5-1)}{q-1}.$$

Therefore k divides

$$\frac{2q\left(q^5-1\right)}{q-1},$$

and since $v<k^2$, then we have that k is either $2q\left(q^4+q^3+q^2+q+1\right)$, or $q\left(q^4+q^3+q^2+q+1\right)$, but neither of these satisfies the equality $k(k-1)=2(v-1)$.

Now suppose that $G_x=N_i$. First let $i=1$. The subdegrees of X are (see [5]):

$q^{2m-2}-1$, $\frac{q^{m-1}\left(q^{m-1}+\epsilon\right)}{2}$, $\frac{q^{m-1}\left(q^{m-1}-\epsilon\right)(q-1)}{4}$, and $\frac{q^{m-1}\left(q^{m-1}+\epsilon\right)(q-3)}{4}$ if $q\equiv 1 \bmod 4$,

$q^{2m-2}-1$, $\frac{q^{m-1}\left(q^{m-1}-\epsilon\right)}{2}$, $\frac{q^{m-1}\left(q^{m-1}-\epsilon\right)(q-3)}{4}$, and $\frac{q^{m-1}\left(q^{m-1}+\epsilon\right)(q-3)}{4}$ if $q\equiv 3 \bmod 4$, and

$q^{2m-2}-1$, $\frac{q^{m}\left(q^{m-1}-\epsilon\right)}{2}$, and $\frac{q^{m-1}\left(q^{m-1}+\epsilon\right)(q-2)}{2}$ if q is even.

We have that k divides twice highest common factor of the subdegrees, and in every case this is too small for k to satisfy $v<k^2$.

Now let $G_x=N_i^{\epsilon_1}$, with $1<i\leq m$, and $\epsilon_1=\pm$ present only if i is even. If q is odd, as in the odd-dimensional case we get that $SO_{i-1}(q)\times SO_{n-i-1}(q)\leq G_x\cap G_x^g$ for some $g\in G\backslash G_x$. Since k is prime to p, we have that $k<8q^m\log_p q$, contrary to $v<k^2$. Now assume that q is even. Then i is also even.

If $i=2$ then we can find $g_1,g_2\in G\setminus G_x\cap X$ such that $(G_x\cap X)\cap(G_x\cap X)^{g_1}\geq SO^{+}_{n-4}(q)$ and $(G_x\cap X)\cap(G_x\cap X)^{g_2}\geq SO^{-}_{n-4}(q)$. Therefore k divides $2(q-\epsilon_1)\left(q^{m-1}-\epsilon\epsilon_1\right)(\log_2 q)_{2'}$, so $k^2<v$.

If $2<i\leq m$ then we can find $g\in G\setminus G_x\cap X$ such that $(G_x\cap X)\cap(G_x\cap X)^{g}\geq SO^{\epsilon_1}_{i-2}(q)\times SO^{\epsilon_2}_{n-i-2}(q)$, with $\epsilon_2=\epsilon\epsilon_1$. It follows that k divides

$$\left(q^{\frac{i}{2}}-\epsilon_1\right)\left(q^{\frac{i-2}{2}}+\epsilon_1\right)\left(q^{\frac{n-i}{2}}+\epsilon_2\right)\left(q^{\frac{n-i-2}{2}}+\epsilon_2\right)(\log_2 q)_{2'},$$

forcing $k^2<v$, a contradiction.

$\mathcal{C}_2$) If $G_x \in \mathcal{C}_2$ then G_x stabilises a decomposition $V = V_1 \oplus \ldots \oplus V_a$ of subspaces of equal dimension, say b, so $n = ab$. Here we have three possibilities.

(1) First assume that all the V_i are nonsingular and isometric. (Also, if b is odd then so is q). If $b = 1$ then by the inequality $|G| < 2|G_x||G_x|^2_{p'}$ we have that $G_x \cap X = 2^{n-2}A_n$, with n being either 8 or 10 and X either $P\Omega^+_8(3)$ or $P\Omega^-_{10}(3)$ respectively. (Note that if $X = P\Omega^+_8(5)$, then the maximality of G_x in G forces $G \leq X.2$ ([31]), so G_x is too small). In the first case, k divides 112, and in the second it is a power of 2. Both contradict the inequality $v < k^2$.

Now let $b = 2$. If $q > 2$ then we can find $g \in G \setminus G_x$ so that $G_x \cap G_x^g$ contains the stabiliser of $V_3 \oplus \ldots \oplus V_a$. From this it follows that $k \leq 2a(a-1).\left(2(q+1)\right)^2 |\mathrm{Out}X|$, and from $v < k^2$ we get that $n = 8$ and $q = 3$. If $q = 2$ then we can find $g \in G \setminus G_x$ so that $G_x \cap G_x^g$ contains the stabiliser of $V_4 \oplus \ldots \oplus V_a$, and in this case k is at most $2a(a-1)(a-2)\left(2(q+1)\right)^3 |\mathrm{Out}X|$, and so $n = 8$ or 10. Using the condition that k divides $2(v-1)$ we rule out these three cases.

Finally let $b > 2$. From the inequality $|G| < 2|G_x||G_x|^2_{p'}$ we have that $b = m$, (and so $\epsilon = +$). Let δ be the type of the V_i if m is even. Assume first that $m = 4$. Then

$$v = \frac{q^8\left(q^2+1\right)^2\left(q^4+1^2+1\right)}{4}$$

if $\delta = +$, and

$$v = \frac{q^8\left(q^6-1\right)\left(q^2-1\right)}{4}$$

if $\delta = -$. In the first case, $(q^2-1, v-1) \leq 2$ and 4 does not divide $v-1$, so k divides $6(\log_p q)_{2'}$, contrary to $v < k^2$. In the latter case, v is even and divisible by (q^2-1), and k divides the odd part of $3\left(q^2+1\right)^2 \log_p q$, again contrary to v, k^2. Hence $m \geq 5$, and we argue as in $\mathcal{C}_1$.

In the case where m and q are odd, $a = 2$, and V_1, V_2 are similar but not isometric, we also argue as in $\mathcal{C}_1$.

Now consider the case $\epsilon = +$, $a = 2$, and V_1 and V_2 totally singular. If $m = 4$, then we can apply a triality automorphism of X to get to the case $G_x = N_2^+$, which we have ruled out in $\mathcal{C}_1$. Assume then that $m \geq 5$. Then

$$v = \frac{q^{\frac{m(m-1)}{2}}\left(q^{m-1}+1\right)\left(q^{m-2}+1\right)\ldots(q+1)}{2^e},$$

where e is 0 or 1 ([33, 4.2.7]), so

$$v > \frac{q^{m(m-1)}}{2}.$$

However, there exists $g \in G \setminus G_x$ such that $GL_{m-2}(q) \leq G_x \cap G_x^g$, and so k divides $2\left(q^m-1\right)\left(q^{m-1}-1\right)\log_p q$, and in fact, since $(k, v) \leq 2$, k divides twice the odd part of $\frac{(q^m-1)\left(q^{m-1}-1\right)\log_p q}{q+1}$, which is contrary to $k^2 < v$.

$\mathcal{C}_3$) If $G_x \in \mathcal{C}_3$, then G_x is an extension field subgroup, and there are two possibilities ([33]).

(1) First assume that $G_x = N_G(\Omega^{\delta}_{\frac{n}{s}}(q^s))$, with s a prime and $\delta = \pm$ if $\frac{n}{s}$ is even (and empty otherwise). Since $|G| < |G_x|^3$, we have $s = 2$. If q is odd, then by Lemma 5.4 we see that a parabolic degree of G_x divides k, and so it follows that k is even, but since v is even then 4 does not divide k, which is a contradiction.

If q is even then m is also even, and

$$v = \frac{q^{\frac{m^2}{2}}\left(q^{2m-2}-1\right)\left(q^{2m-2}-1\right)\ldots\left(q^2-1\right)}{2^e},$$

with $e \leq 2$ ([33, 4.3.14,4.3.16]). As k divides $2(v-1)$, it is prime to q^2-1, and it follows that $k^2 < v$, another contradiction.

(2) Now let $G_x = N_G(\tilde{G}U_m(q))$, with $\epsilon = (-1)^m$. If q is odd, then as in the symplectic case we have that $q+1$ divides v and k, which is a contradiction.

So let q be even. If $m = 4$ then applying a triality automorphism of X the action of G becomes that of N_2^-, which has been ruled out in the case $\mathcal{C}_1$. So let $m \geq 5$. Now, G_x is the stabiliser of a hermitian form $[,]$ on V over $GF(q^2)$ such that the quadratic form Q preserved by X satisfies $Q(v) = [v, v]$ for $v \in V$. Let W be a nonsingular 2-dimensional hermitian subspace over $GF(q^2)$. Then W over $GF(q)$ is of type O_4^+. The pointwise stabiliser of $W^\perp$ in $G_x \cap X$ is $GU_2(q)$, which is properly contained in the pointwise stabiliser of $W^\perp$ in X. Thus we can find $g \in G \setminus G_x$ so that $GU_{m-2}(q) \leq G_x \cap G_x^g$. Then we have that k divides $2\,(q^m - (-1)^m)\,(q^{m-1} - (-1)^{m-1}) \log_p q$, which is contrary to $v < k^2$.

$\mathcal{C}_4$) If $G_x \in \mathcal{C}_4$ then G_x stabilises an asymmetric tensor product, so either $G_x = N_G\,(PSp_a(q) \times PSp_b(q))$ with a and b distinct even numbers, or $G_x = N_G\,(P\Omega_a^{\epsilon_1}(q) \times P\Omega_b^{\epsilon_2}(q))$ with $a, b \geq 3$ and $n = ab$. From the inequality $|G| < 2|G_x||G_x|_{p'}^2$ we have that $n = 8$ and $G_x = N_G\,(PSp_2(q) \times PSp_4(q))$. Applying a triality automorphism of X, the action becomes that of N_3, a case that has been ruled out in $\mathcal{C}_1$.

$\mathcal{C}_5$) If $G_x \in \mathcal{C}_5$ then it is a subfield subgroup. From the inequality $|G| < 2|G_x||G_x|_{p'}^2$ we have that $G_x \cap X = P\Omega_{2m}^\delta(q_0).2^e < P\Omega_{2m}^+(q) = X$, with $q = q_0^2$ and $e \leq 2$ ([33, 4.5.10]), so

$$v > \frac{q_0^{2m^2-m}}{4}.$$

Now, G_x stabilises a $GF(q_0)$-subspace V_0 of V. Let U_0 be a 2-subspace of V_0 of type $O_2^+(q_0)$, and U a subspace of V of type $O_2^+(q)$ containing U_0. There exists and element $g \in G \setminus G_x$ that stabilises $U^\perp$ pointwise, from this it follows that $G_x \cap G_x^g$ involves $P\Omega_{2m-2}^\delta(q_0)$. This implies that k divides $2\,(q_0^m - \delta)\left(q_0^{m-1} + \delta\right)|\mathrm{Out}X|$, which contradicts the inequality $v < k^2$.

$\mathcal{C}_6$) If $G_x \in \mathcal{C}_6$, it is an extraspecial normaliser. From the inequality $|G| < |G_x|^3$ we have that $G_x \cap X = 2^6 A_8 < P\Omega_8^+(3) = X$. Applying a triality automorphism of X, we have one of the cases already ruled out in $\mathcal{C}_2$.

$\mathcal{C}_7$) If $G_x \in \mathcal{C}_7$, then it stabilises a symmetric tensor product of a spaces of dimension b, with $n = b^a$. Here G_x is too small.

$\mathcal{C}_8$) In this case this class is empty.

$\mathcal{S}$) Now consider the case in which G_x is an almost simple group (modulo scalars) not contained in any of the Aschbacher subgroups of G. For $n \leq 10$, the subgroups G_x are listed in [30] and [31]. Since $|G| < 2|G_x||G_x|_{p'}^2$, we have one of the following:

(i) $\Omega_7(q) < P\Omega_8^+(q)$,

(ii) $\Omega_8^+(q) < P\Omega_8^+(q)$ with $q = 3$, 5, or 7, or

(iii) $A_9 < \Omega_8^+(q), A_{12} < \Omega_{10}^-(2), A_{12} < P\Omega_{10}^+(3)$.

In the first case, applying a triality automorphism gives an action on N_1, which was excluded in $\mathcal{C}_1$. In the second case, from the fact that k divides $2\,(|G_x|, v-1)$ we have that k divides 20, 6, and $2 \cdot 3^5 \cdot 5^2$, and so is too small. In the third case since 6 divides v, again we have that k is too small.

So $n \geq 12$. If $n > 14$, then by [39, Theorem 4.2] we need only consider the cases in which G_x' is alternating on the deleted permutation module, and in fact $A_{17} < \Omega_{16}^+(2)$ is the only group which is big enough. Again, since v is divisible by $2 \cdot 3 \cdot 17$ we have that k is too small. Now let $n = 12$, respectively 14. If X is alternating, we only have to consider $A_{13} < \Omega_{12}^-(2)$, respectively $A_{16} < \Omega_{14}^+(2)$, however since k divides $2(v-1, |G_x|)$, we have that $k^2 < v$, a contradiction. If X is not alternating, then again since $|G_x| < q^{2n+4}$ by [39, Theorem 4.2], it follows that $|G_x| < q^{28}$, respectively $|G_x| < q^{32}$. However, from $|G| < 2|G_x||G_x|_{p'}^2$ we have that $|G_x|_{p'} > \frac{q^{19}}{\sqrt{2}}$, respectively $|G_x|_{p'} > q^{29}$. We can now see (cf. [40, Seccions 2,3, and 5]) that no sporadic or Lie type group will do for G_x.

Finally assume that $X = P\Omega_8^+(q)$, and G contains a triality automorphism. The maximal groups are determined in [31]. If $G_x \cap X$ is a parabolic subgroup of X, then it is either P_2 or P_{134}. The first was ruled out in $\mathcal{C}_1$, so consider the latter. In this case we have

$$v = \frac{(q^6-1)\,(q^4-1)}{(q-1)^3} > q^{11},$$

and $(3,q)q$ is the highest power of p dividing $v-1$. Since X has a unique suborbit of size a power of p (by Lemma 5.6), we have that $k < 2q(3,q)$, which contradicts $v < k^2$.

Now, by [31], and $|G| < |G_x||G_x|_{p'}^2$, the only cases we have to consider are $G_2(q)$ for any q, and $(2^9)\,L_3(2)$ for $q = 3$. In the first case, we have

$$v = \frac{q^6\,(q^4-1)^2}{(q-1,2)^2},$$

and by Lemma 5.4 applied to $G_2(q)$ we have that G_{xB} is contained a parabolic subgroup, so $\frac{(q^6-1)}{q-1}$ divides k, however k is prime to $q+1$, which is a contradiction. In the second case, k divides 28, which is too small.

□

This completes the proof of Lemma 5.17.

5.4.5 X is a Unitary Group

Here $X = U_n(q)$ with $n \geq 3$, and $(n,q) \neq (3,2),(4,2)$, since these are isomorphic to $3^2.Q_8$ and $PSp_4(3)$ respectively. We write $\beta = \{u_1,\ldots,u_n\}$ for an orthonormal basis of V.

Lemma 5.18. *The group X is not $U_n(q)$, with $n \geq 3$ and $(n, q) \neq (3, 2), (4, 2)$.*

Proof. As we have done all through this section, we will consider G_x to be in one of the Aschbacher families of subgroups of G, or a nonabelian simple group not contained in any of these families, and analyse each of these cases separately.

$\mathcal{C}_1$) If G_x is reducible, then it is either a parabolic subgroup P_i, or the stabiliser N_i of a nonsingular subspace.

First assume $G_x = P_i$ for some $i \leq \frac{n}{2}$. Then we have

$$v = \frac{(q^n - (-1)^n)\,(q^{n-1} - (-1)^{n-1}) \ldots (q^{n-2i+1} - (-1)^{n-2i+1})}{(q^{2i} - 1)\,(q^{2i-2} - 1) \ldots (q^2 - 1)}.$$

There is a unique subdegree which is a power of p. The highest power of p dividing $v - 1$ is q^2, unless n is even and $i = \frac{n}{2}$, in which case it is q, or n is odd and $i = \frac{n-1}{2}$, in which case it is q^3. If $n = 3$ then the action is 2-transitive, so consider $n > 3$. Then $v > q^{i(2n-3i)}$, and so $v < k^2$, which is a contradiction.

Now suppose that $G_x = N_i$, with $i < \frac{n}{2}$, and take $x = \langle u_1, \ldots, u_i \rangle$. If we consider $y = \langle u_1, \ldots, u_{i-1}, u_{i+1} \rangle$, then we see that k divides $2\,(q^i - (-1)^i)\,(q^{n-i} - (-1)^{n-i})$. But in this case we have

$$v = \frac{q^{i(n-1)}\,(q^n - (-1)^n) \ldots (q^{n-i+1} - (-1)^{n-i+1})}{(q^i - (-1)^i) \ldots (q + 1)},$$

and since $v < k^2$ we have that $i = 1$. Then k divides $2(q+1)\,(q^{n-1} - (-1)^{n-1})$. Applying Lemma 5.4 to $U_{n-1}(q)$, we have that k is divisible by the degree of a parabolic action of $U_{n-1}(q)$. We check the subdegrees, and the fact that k divides $|G_x|^2$ as well as $k^2 > v$, we get that $n \leq 5$.

If $n = 5$ then k divides $2(q + 1)\,(q^4 - 1)$ and is divisible by $q^3 + 1$, which can only happen if $q = 2$, but in this case none of the possibilities for k satisfy the equality $2(v - 1) = k(k - 1)$.

If $n = 4$ then $q^3 + 1$ divides k, but $(2(v-1), q^3+1) \leq 2\,(q^2 - q + 1)$, which is a contradiction.

Finally, if $n = 3$ then $q + 1$ divides k, but $q + 1$ is prime to $v - 1$, which is another contradiction.

$\mathcal{C}_2$) If $G_x \in \mathcal{C}_2$, then it preserves a partition $V = V_1 \oplus \ldots \oplus V_a$ of subspaces of the same dimension, say b, so $n = ab$ and either the v_i are nonsingular and the partition is orthogonal, or $a = 2$ and the V_i are totally singular.

First assume that the V_i are nonsingular. If $b > 1$, then taking

$$x = \{\langle u_1, \ldots u_b\rangle, \langle u_{b+1}, \ldots u_{2b}\rangle, \ldots\}$$

and

$$y = \{\langle u_1, \ldots u_{b-1}, u_{b+1}\rangle, \langle u_b, u_{b+2}, \ldots u_{2b}\rangle, \ldots\},$$

we see that k divides $2a(a-1)\left(q^b - (-1)^b\right)^2$. From the inequality $v < k^2$ we have that $n = 4$ and $b = 2$. Then we have that

$$v = \frac{q^4\,(q^4-1)\,(q^3+1)}{2\,(q^2-1)\,(q+1)},$$

and k divides $4\left(q^2-1\right)^2$. However, $(v-1, q+1) = (2, q+1)$, so k divides $16(q-1)^2$, which is contrary to $v < k^2$.

If $b = 1$ then $G_x \cap X = \hat{}(q+1)^{n-1} S_n$. First let $n = 3$, with $q > 2$. Then

$$v = \frac{q^3\,(q^3+1)\,(q^2-1)}{6(q+1)^2},$$

and k divides $12(q+1)^2 \log_p q$. The inequality $v < k^2$ forces $q \leq 17$, but from the fact that k divides $2(v-1)$ we rule out all these values. Now let $n > 3$, and let $x = \{\langle u_1\rangle, \langle u_2\rangle, \ldots, \langle u_n\rangle\}$. If $q > 3$ let $W = \langle u_1, u_2\rangle$. If we take $g \in G \setminus G_x$ acting trivially on $W^\perp$ we see that k divides $n(n-1)(q+1)^2$, contrary to $v < k^2$. If $q \leq 3$ then let $W = \langle u_1, u_2, u_3\rangle$. Taking $g \in G \setminus G_x$

acting trivially on $W^{\perp}$ we see that now k divides $\frac{n(n-1)(n-2)(q+1)^3}{3}$, so $n \leq 6$ if $q = 2$, or $n \leq 4$ if $q = 2$. By the fact that k divides $2(v-1)$ we rule these cases out.

Now assume that $a = 2$ and both the V_i's are totally singular. Let $\{e_1, f_1, \ldots, e_b, f_b\}$ be a standard unitary basis. Take

$$x = \{\langle e_1, \ldots, e_b \rangle, \langle f_1, \ldots, f_b \rangle\}, \text{ and } y = \{\langle e_1, \ldots, e_{b-1}, f_b \rangle, \langle f_1, \ldots, f_{b-1}, e_b \rangle\}.$$

Then we have that k divides $4\,(q^n - 1)$. The inequality $v < k^2$ forces $n = 4$, but then

$$v = \frac{q^4\,(q^3+1)\,(q+1)}{2},$$

so in fact k divides $2\,(q^2+1)\,(q-1)$, contrary to $v < k^2$.

$\mathcal{C}_3$) If $G_x \in \mathcal{C}_3$ then it is a field extension group for some field extension of $GF(q)$ of odd degree b. From the inequality $|G| < 2|G_x||G_x|^2_{p'}$ we have $b = 3$ and $n = 3$. Then

$$v = \frac{q^3\,(q^2-1)\,(q+1)}{3}.$$

Therefore 4 does not divide k, and so $k < 6q^2(\log_p q)_{2'}$. Since $v < k^2$, we have $q \leq 9$. With the condition that k divides $2(v-1)$ we rule out these cases.

$\mathcal{C}_4$) If $G_x \in \mathcal{C}_4$ then it is the stabiliser of a tensor product of two nonsingular subspaces of dimensions $a > b > 1$, but then the inequality $|G| < 2|G_x||G_x|^2_{p'}$ is not satisfied.

$\mathcal{C}_5$) If $G_x \in \mathcal{C}_5$ then it is a subfield subgroup. We have three possibilities:

If G_x is a unitary group of dimension n over $GF(q_0)$, where $q = q_0^b$ with b an odd prime, then since $|G| < |G_x|^3$ we have that $b = 3$. However $|G| < 2|G_x||G_x|^2_{p'}$ forces $q = 8$ and $n \leq 4$, but in these cases since k divides $2(v-1)$ it is too small.

If $G_x \cap X = PSO_n^{\epsilon}(q).2$, with n even and q odd, then by Lemma 5.1 k is divisible by the degree of a parabolic action of G_x. Here we have that $q+1$ divides k, and $\frac{q+1}{(4,q+1)}$ divides v.The fact that k divides $2(v-1)$ forces $q=3$, so $v=2835$, but then $8v-7$ is not a square, which is a contradiction.

Finally, if $G_x = N\left(PSp_n(q)\right)$, with n even, then by Lemma 5.4 G_{xB} is contained on some parabolic subgroup, so k is divisible by the degree of some parabolic action of G_x, and so is divisible by $q+1$. However, v is divisible by $\frac{q+1}{(q+1,2)}$, contradicting the fact that k divides $2(v-1)$

$\mathcal{C}_6$) If $G_x \in \mathcal{C}_6$, then it is an extraspecial normaliser, and since $|G| < |G_x|^3$, we only have to consider the cases $G_x \cap X = 3^2Q_8$, 2^4A_6, or 2^4S_6, and $X = U_3(5)$, $U_4(3)$, and $U_4(7)$ respectively. In all cases the fact that k divides $2\left(|G_x|, v-1\right)$ forces $k^2 < v$, a contradiction.

$\mathcal{C}_7$) If $G_x \in \mathcal{C}_7$, then it stabilises a tensor product decomposition of $V_n(q)$ into t subspaces V_i of dimension m each, so $n = m^t$. Since $m \geq 3$ and $t \geq 3$, $|G_x|$ is too small to satisfy $|G| < |G_x|^3$.

$\mathcal{S}$) Finally consider the case in which G_x is an almost simple group (modulo the scalars) not contained in any of the Aschbacher families of subgroups. For $n \leq 10$, the subgroups G_x are listed in [30, Chapter 5]. Since $|G| < |G_x|^3$, we only need to consider the following possibilities:

$L_2(7)$ in $U_3(3)$,

$A_6.2$, $L_2(7)$, and A_7 in $U_3(5)$,

A_6 in $U_3(11)$,

$L_2(7)$, A_7, and $L_2(4)$ in $U_4(3)$,

$U_4(2)$ in $U_4(5)$,

$L_2(11)$ in $U_5(2)$, and

$U_4(3)$ and M_{22} in $U_6(2)$.

Since k divides $2\,(|G_x|, v-1)$, we have that $k^2 < v$ in all cases except in the case $L_2(7) < U_3(3)$. In this last case, $v = 36$, but then there is no k such that $k(k-1) = 2(v-1)$, which is a contradiction.

If $n \geq 14$, then by [39] we have that $|G| < |G_x|^3$, a contradiction. Hence $n = 11$, 12, or 13. By [39], $|G_x|$ is bounded above by q^{4n+8}, and since $|G| < 2|G_x||G_x|^2_{p'}$, we have that $|G_x|_{p'}$ is bounded below by q^{33}, q^{43}, or q^{53} respectively. Using the methods in [39, 40] we rule out all the almost simple groups G_x.

□

This completes the proof of Lemma 5.18, and hence we have that if X is a simple classical group, it is either $PSL_2(7)$ or $PSL_2(11)$.

5.5 The Case where X is an Exceptional Group of Lie Type

In this section we consider the socle X of the group G to be a simple exceptional group of Lie type.

Lemma 5.19. *The group X is not a Suzuki group ${}^2B_2(q)$, with $q = 2^{2e+1}$.*

Proof. Suppose that the socle X is a Suzuki group ${}^2B_2(q)$, with $q = 2^{2e+1}$. Then $|G| = f|X| = f(q^2+1)q^2(q-1)$, where $f \mid 2e+1$, and so the order of any point stabiliser G_x is one of the following [62]:

(*i*) $fq^2(q-1)$

(*ii*) $4f(q+\sqrt{2q}+1)$

(*iii*) $4f(q-\sqrt{2q}+1)$

(*iv*) $f(q_0^2+1)q_0^2(q_0-1)$, where $8 \leq q_0^m = q$, with $m \geq 3$.

Case (i) Here $v = (q^2+1)$, so from $k(k-1) = 2(v-1)$ we get that $k(k-1) = 2q^2$, a power of 2, which is a contradiction.

Cases (ii) **and** (iii) From the inequality $|G| < |G_x|^3$, we get that

$$f \cdot \frac{7}{8} q^5 < f(q^2+1)q^2(q-1) < 4^4 f^3 (q \pm \sqrt{2q}+1)^3 < 4^4 f^3 (2q+1)^3 \leq 4^4 \left(\frac{17}{8} fq \right)^3 ,$$

so

$$q^2 < \frac{4^4 \cdot (17)^3 \cdot f^2}{8^2 \cdot 7} < 2808 f^2,$$

hence $q \leq 128$.

First assume $q = 128$. Then $v = 58781696$ in case (ii), and 75427840 in case (iii), and $|G_x| = 4060$ in case (ii), and 3164 in case (iii). Now we have that k divides $2(|G_x|, v-1)$, but here $(|G_x|, v-1) = 1015$ in case (ii), and 113 in case (iii). In both cases $k^2 < v$, which is a contradiction.

Next assume $q = 32$. Then $v = 198400$ in case (ii), and 325376 in case (iii). In case (ii), $(|G-x|, v-1) = 41$, and in case (iii) $(|G_x|, v-1) = 25$ or 125, depending on whether $f = 1$ or 5. In all cases we see $k^2 < v$, a contradiction.

Finally assume $q = 8$. Then $v = 560$ in case (ii), and 1456 in case (iii). In case (ii), $(|G_x|, v-1) = 13$, and in case (iii) $(|G_x|, v-1) = 5f$. Therefore k is again too small.

Case (iv) Here $|G_x| = f\,(q_0^2+1)\,q_0^2(q_0-1)$, so q_0 divides v and hence q_0 and $v-1$ are relatively prime, so from $|G| < 2|G_x||G_x|_{p'}^2$ we get:

$$\left(q_0^{2m}+1\right) q_0^{2m} \left(q_0^m - 1\right) < 4f^2 \left(q_0^2+1\right)^3 q_0^2 (q_0-1)^3.$$

Now, $q_0^{5m-1} < (q_0^{2m}+1)\, q_0^{2m}\, (q_0^m-1)$, and we have that also

$$4f^2 \left(q_0^2+1\right)^3 q_0^2 (q_0-1)^3 = 4f^2 q_0^2 \left(q_0^3 - q_0^2 + q_0 - 1\right)^3 < f^2 q_0^{13},$$

so

$$q_0^{5m-1} < f^2 q_0^{13} < q_0^{13+m}.$$

Therefore $5m-1 < 13+m$, which forces $m=3$. Then

$$v = \left(q_0^4 - q_0^2 + 1\right) q_0^4 \left(q_0^2 + q_0 + 1\right),$$

and so $k \leq 2(|G_x|, v-1) \leq 2fq_0^3 < 2q_0^{\frac{9}{2}}$. The inequality $v < k^2$ forces $q_0 = 2$, and so $q = 8$. Then $v = 1456$, and $|G_x| = 20f$, with $f = 1$ or 3. Then $(|G_x|, v-1) = 5f$, and so $k^2 < v$, which is a contradiction. □

This completes the proof of Lemma 5.19.

Lemma 5.20. *The point stabiliser G_x is not a parabolic subgroup of G.*

Proof. First assume $X \neq E_6(q)$. Then by Lemma 5.6 there is a unique subdegree which is a power of p. Therefore k divides twice a power of p, but it also divides $2(v-1)$, so it is too small.

Now assume $X = E_6(q)$. If G contains a graph automorphism or $G_x = P_i$ with $i = 2$ or 4, then there is a unique subdegree which is a power of p and again k is too small. If $G_x = P_3$, the A_1A_4 type parabolic, then

$$v = \frac{(q^3+1)(q^4+1)(q^{12}-1)(q^9-1)}{(q^2-1)(q-1)}.$$

Since k divides $2(|G_x|, v-1)$, we have that k divides $2q\left(q^5-1\right)(q-1)^5 \log_p q$, and hence $k^2 < v$, which is a contradiction. If $G_x = P_1$, then

$$v = \frac{(q^{12}-1)(q^9-1)}{(q^4-1)(q-1)},$$

and the nontrivial subdegrees are ([50]) $\frac{q\left(q^8-1\right)\left(q^3+1\right)}{(q-1)}$, and $\frac{q^8\left(q^5-1\right)\left(q^4+1\right)}{(q-1)}$. The fact that k divides twice the highest common factor of these forces $k^2 < v$, again, a contradiction. □

This completes the proof of Lemma 5.20.

Lemma 5.21. *The group X is not a Chevalley group $G_2(q)$.*

Proof. Assume $X = G_2(q)$, with $q > 2$ since $G_2(q)' = U_3(3)$. The list of maximal subgroups of $G_2(q)$ with q odd can be found in [32], and in [12] for q even.

First consider the case where $X \cap G_x = SL_3^{\epsilon}(q).2$. Here

$$v = \frac{q^3\left(q^3+\epsilon\right)}{2}.$$

From the factorization $\Omega_7(q) = G_2(q)N_1^{\epsilon}$ ([43]), it follows that the suborbits of $\Omega_7(q)$ are unions of G_2-suborbits, and so k divides each of the Ω_7-subdegrees. We have that q cannot be odd, since this is ruled out by the first case with $i = 1$ in the section of orthogonal groups of odd dimension in this chapter. For q even, the subdegrees for $Sp_6(q)$, given in the last case of the section on symplectic groups are $\left(q^3-\epsilon\right)\left(q^4+\epsilon\right)$ and $\frac{(q-2)q^2\left(q^3-\epsilon\right)}{2}$. This implies that k divides $2\left(q^3-\epsilon\right)\left(q-2, q^2+\epsilon\right)$, and since $v < k^2$ then $\epsilon = -$, and so

$$v = \frac{q^3\left(q^3-1\right)}{2}.$$

So we have that k divides $2\left(q^3+1\right)\left(q-2, q^2-1\right) \leq 6\left(q^3+1\right)$. Also, we have $k(k-1) = 2(v-1) = \left(q^3+1\right)\left(q^3-2\right)$. This is impossible.

If $X \cap G_x = G_2(q_0) < G_2(q)$ or ${}^2G_2(q) < G_2(q)$ then p does not divide $[G_x : G_{xB}]$, so by Lemma 5.4 k is divisible by the index of a parabolic subgroup of G_x which is $\frac{q_0^6-1}{q_0-1}$ in the case of $G_2(q_0)$, or q^3+1 in the case of ${}^2G_2(q)$. But this is not so since k also divides $2\left(v-1, |G_x|\right)$.

If $G_x = N_G\left(SL_2(q) \circ SL_2(q)\right)$, then we have that

$$v = \frac{q^4\left(q^6-1\right)}{q^2-1}.$$

Now k divides $2\left(q^2-1\right)^2 \log_p q$ but $\left(q^2-1, v-1\right) \leq 2$, so k is too small.

If $X \cap G_x = J_2 < G_2(4)$ then $v = 416$. But k divides $2(|G_x|, 415)$, which is too small.

Now suppose $X \cap G_x = G_2(2)$, with $p = q \geq 5$. Then the inequality $v < k^2$ forces $q = 5$ or 7. In both cases $(v-1, |G_x|)$ is too small.

If $X \cap G_x = PGL_2(q)$, or $L_2(8)$, then the inequality $|G| < |G_x|^3$ is not satisfied.

Next consider $X \cap G_x = L_2(13)$. Then the inequality $|G| < |G_x|^3$ forces $q \leq 5$. If $q = 5$ then $v = 2^3 \cdot 3^2 \cdot 5^6 \cdot 13 \cdot 31$, so $(v-1, |G_x|) \leq 7$, hence k is too small. If $q = 3$ then $v = 2^3 \cdot 3^5$, and k divides $2(v-1, |G_x|) \leq 2 \cdot 7 \cdot 13$, this does not satisfy the equation $k(k-1) = 2(v-1)$.

Finally, if $X \cap G_x = J_1$ with $q = 11$ then the inequality $v < k^2$ cannot be satisfied.

There is no other maximal subgroup G_x satisfying the inequality $|G| < |G_x|$. □

This completes the proof of Lemma 5.21.

Lemma 5.22. *The group X is not a Ree group ${}^2G_2(q)$, ($q > 3$).*

Proof. Suppose $X = {}^2G_2(q)$, with $q = 3^{2e+1} > 3$. A complete list of maximal subgroups of G can be found in [32, p.61]. First suppose $G_x \cap X = 2 \times SL_2(q)$. Then

$$v = \frac{q^2\left(q^2 - q + 1\right)}{2},$$

so $2(v-1) = q^4 - q^3 + q^2 - 2$, and k divides $2(|G_x|, v-1)$. But we have that $\left(q\left(q^2-1\right), q^4 - q^3 + q^2 - 1\right) = q - 1$, which is too small.

The groups $X \cap G_x = N_X(S_2)$, (where S_2 is a Sylow 2-subgroup of X of order 8), of order $2^3 \cdot 3 \cdot 7$ and $L_2(8)$ are not allowed since $|G| < |G_x|^3$ forces $q = 3$.

If $X \cap G_x = {}^2G_2(q_0)$, with $q_0^m = q$, m prime, then

$$v = q_0^{3(m-1)}\left(q_0^{3(m-1)} - q_0^{3(m-2)} + \ldots + (-1)^m q_0^3 + (-1)^{m-1}\right)\left(q_0^{m-1} + q_0^{m-2} + \ldots + 1\right).$$

Now k divides $2mq_0^3\,(q_0^3+1)\,(q_0-1)$, but since q_0 and $v-1$ are relatively prime, q_0 does not divide k, so in fact $k \leq 2m\,(q_0^3+1)\,(q_0-1)$, and the inequality $v < k^2$ forces $m = 2$, which is a contradiction.

If $X \cap G_x = \mathbb{Z}_{q\pm\sqrt{3q}+1} : \mathbb{Z}_6$, since $q \geq 27$ we have that the inequality $|G| < |G_x|^3$ is not satisfied.

Finally, if $X \cap G_x = \left(2^2 \times D_{\left(\frac{1}{2}\right)(q+1)}\right) : 3$, since $q \geq 27$ then the inequality $|G| < |G_x|^3$ is not satisfied. □

This completes the proof of Lemma 5.22.

Lemma 5.23. *The group X is not a Ree group ${}^2F_4(q)$.*

Proof. Suppose $X = {}^2F_4(q)$. Then from [57] we see that there are no maximal subgroups G_x that are not parabolic satisfying the inequality $|G| < 2|G_x||G_x|_{2'}^2$, except for the case $q = 2$. In this case $G_x \cap X = L_3(3).2$ or $L_2(25)$. In both cases, since k must divide $2(v-1, |G_x|)$ it is too small. □

Lemma 5.24. *The group X is not ${}^3D_4(q)$.*

Proof. Suppose $X = {}^3D_4(q)$. If $X \cap G_x = G_2(q)$ or $SL_2(q^3) \circ SL_2(q).(2, q-1)$ then $v = q^e\,(q^8+q^4+1)$, where $e = 6$ or 8 respectively. By Lemma 5.4, k is divisible by $q+1$, which forces $q = 3$ (since $q+1$ also divides $2(v-1)$), but then in neither case is $8v-7$ a square.

If $X \cap G_x = PGL_3^\epsilon(q)$ then the inequality $|G| < |G_x|^3$ is not satisfied. □

Lemma 5.25. *The group X is not $F_4(q)$.*

Proof. Suppose $X = F_4(q)$. First assume that $X_0 = \mathrm{Soc}(X \cap G_x)$ is not simple. Then by Theorem 5.8 and Table 5.1, $G_x \cap X$ is one of the following,

(*i*) Parabolic.

(*ii*) Maximal rank.

(*iii*) $3^3.SL_3(3)$.

or $X_0 = L_2(q) \times G_2(q)(p > 2, q > 3)$.

The parabolic subgroups have been ruled out by Lemma 5.20.

The possibilities for the second case are given in [46, Table 5.1]. We check that in every case there is a large power of q dividing v, and since $(k, v) \leq 2$, we have that q does not divide k (unless $q = 2$, but then 4 does not divide k). But then k divides $2\left(|G_x|, v-1\right)$, and in each case $(|G_x|_{p'}, v-1)$ is too small for k to satisfy $k^2 > v$.

The local subgroup is too small to satisfy the bound $|G_x|^3 > |G|$.

Finally, we have that $|L_2(q) \times G_2(q)| \leq q^7\left(q^2-1\right)^2\left(q^6-1\right) < |F_4(q)|^{\frac{1}{3}}$. Therefore X_0 is simple.

First suppose that $X_0 \notin \mathrm{Lie}(p)$. Then by [53, Table 1], it is one of the following:

A_7, A_8, A_9, A_{10}, $L_2(17)$, $L_2(25)$, $L_2(27)$, $L_3(3)$, $U_4(2)$, $Sp_6(2)$, $\Omega_8^+(2)$, ${}^3D_4(2)$, J_2, $A_{11}(p = 11)$, $L_3(4)(p = 3)$, $L_4(3)(p = 2)$, ${}^2B_2(8)(p = 5)$, $M_{11}(p = 11)$.

The only possibilities for X_0 that could satisfy the bound $|G_x|^3 > |G|$ are $A_9, A_{10}(q = 2)$, $Sp_6(2)(q = 2)$, $\Omega_8^+(2)(q = 2, 3)$, ${}^3D_4(2)(q = 3)$, $J_2(q = 2)$, and $L_4(3)(q = 2)$. However, since k divides $2\left(|G_x|, v-1\right)$, in all these cases $k^2 < v$.

Now assume $X_0 \in \mathrm{Lie}(p)$. First consider the case $\mathrm{rk}(X_0) > \frac{1}{2}\mathrm{rk}(G)$, where $X_0 = X_0(r)$. If $r > 2$, then by Theorem 5.9 it is a subfield subgroup. We have seen earlier that the only subgroups which could satisfy the bound $|G_x|^3 > |G|$ are $F_4\left(q^{\frac{1}{2}}\right)$ and $F_4\left(q^{\frac{1}{3}}\right)$. If $q_0 = q^{\frac{1}{2}}$, then

$$v = q^{12}\left(q^6+1\right)\left(q^4+1\right)\left(q^3+1\right)(q+1) > q^{26}.$$

We have that k divides $2F_4\left(q^{\frac{1}{2}}\right)$, and $(k, v) \leq 2$. Since $(q, k) \leq 2$, we have that k divides

$$2\left(2(q^6-1)(q^4-1)(q^3-1)(q-1), v-1\right) < q^{13},$$

so $k^2 < v$, a contradiction.

If $q_0 = q^{\frac{1}{3}}$, then

$$v = \frac{q^{16}\left(q^{12}-1\right)\left(q^4+1\right)\left(q^6-1\right)}{\left(q^{\frac{8}{3}}-1\right)\left(q^{\frac{2}{3}}-1\right)},$$

but $k < q^{10}$ so $k^2 < v$, which is a contradiction.

If $r = 2$, then the subgroups $X_0(2)$ with $\mathrm{rk}(X_0) > \frac{1}{2}\mathrm{rk}(G)$ that satisfy the bound $|G_x|^3 > |G|$ are $A_4^\epsilon(2)$, $B_3(2)$, $B_4(2)$, $C_3(2)$, $C_4(2)$, and $D_4^\epsilon(2)$. Again, in all cases the fact that k divides $2\left(|G_x|, v-1\right)$ forces $k^2 < v$, a contradiction.

Now consider the case $\mathrm{rk}(X_0) \leq \frac{1}{2}\mathrm{rk}(G)$. By Theorem 5.10 we have that $|G_x| < q^{20}.4\log_p q$. Looking at the orders of groups of Lie type, we see that if $|G_x| < q^{20}.4\log_p q$, then $|G_x|_{p'} < q^{12}$, so $2|G_x||G_x|^2_{p'} < |G|$, contrary to Corollary 5.3. □

This completes the proof of Lemma 5.25.

Lemma 5.26. *The group X is not $E_6^\epsilon(q)$.*

Proof. Suppose $X = E_6^\epsilon(q)$. As in the previous lemma, assume first that X_0 is not simple. Then by Theorem 5.8 $G_x \cap X$ is one of the following,

(*i*) Parabolic.

(*ii*) Maximal rank.

(*iii*) $3^6.SL_3(3)$.

or $X_0 = L_3(q) \times G_2(q)$, $U_3(q) \times G_2(q) (q > 2)$.

The first case was ruled out in Lemma 5.20.

The possibilities for the second case are given in [46, Table 5.1]. In some cases $|G_x|^3 < |G|$, and in each of the remaining cases, calculating $2\left(|G_x|, v-1\right)$ we get that $k^2 < v$.

The local subgroup for the third case is too small.

Finally, the order of the groups in the last case is less than $q^{17} < |E_6^\epsilon|^{\frac{1}{3}}$.

Now assume X_0 is simple. If $X_0 \notin \mathrm{Lie}(p)$, then we find the possibilities in [53, Table 1]. However, the only two cases which satisfy Corollary 4.3 have order that does not divide $|E_6^\epsilon|$. Hence $X_0 = X_0(r) \in \mathrm{Lie}(p)$.

If $\mathrm{rk}(X_0) > \frac{1}{2}\mathrm{rk}(G)$, then when $r > 2$ by Theorem 5.9 are $E_6^\epsilon\left(q^{\frac{1}{s}}\right)$ with $s = 2$ or 3, $C_4(q)$, and $F_4(q)$. In all cases we have that k is too small. When $q = 2$ then the possibilities satisfying $|G_x|^3 > |G|$ with order dividing $E_6^\epsilon(2)$ are $A_5^\epsilon(2)$, $B_4(2)$, $C_4(2)$, $D_4^\epsilon(2)$, and $D_5^\epsilon(2)$. However since k divides $2\left(|G_x|, v-1\right)$, in all cases we have that $k^2 < v$, a contradiction.

If $\mathrm{rk}(X_0) \leq \frac{1}{2}\mathrm{rk}(G)$, then by Theorem 5.10 we have that $|G_x| < q^{28}.4\log_p q$. Looking at the p and p' parts of the orders of the possible subgroups, we see that the p'-part is always less than q^{17}. Hence $|G_x|_{p'} < q^{17}$, so $2|G_x||G_x|_{p'}^2 < |G|$, contradicting Corollary 5.3. □

This completes the proof of Lemma 5.26.

Lemma 5.27. *The group X is not $E_7(q)$.*

Proof. Suppose $X = E_7(q)$. First assume X_0 is not simple. Then by Theorem 5.8, $G_x \cap X$ is one of the following,

(*i*) Parabolic.

(*ii*) Maximal rank.

(*iii*) $2^2.S_3$.

or $X_0 = L_2(q) \times L_2(q)(p > 3)$, $L_2(q) \times G_2(q)(p > 2, q > 3)$, $L_2(q) \times F_4(q)(q > 3)$, or $G_2(q) \times PSp_6(q)$.

The parabolic subgroups have been ruled out in Lemma 5.20. The subgroups of maximal rank can be found in [46, Table 5.1]. Of these, the only ones with order greater than $|E_7(q)|^{\frac{1}{3}}$ are $d.\left(L_2(q) \times P\Omega_{12}^+(q)\right).d$ and

$f.L_8^\epsilon(q).g.\left(2 \times \left(\frac{2}{f}\right)\right)$, where $d = (2, q-1)$, $f = \left(4, \frac{q-\epsilon}{d}\right)$, and $g = \left(8, \frac{q-\epsilon}{d}\right)$. However in both cases the fact that $(k, v) \leq 2$ forces $k^2 < v$, a contradiction.

The local subgroup is too small to satisfy $|G_x|^3 > |G|$.

In the last case, the only group that is not too small to satisfy $|G_x|^3 > |G|$ is $L_2(q) \times F_4(q)$, but here q^{38} divides v, and since $(v, k) \leq 2$, we have that $k^2 < v$. So X_0 is simple.

First assume $X_0 \notin \text{Lie}(p)$. Then by [53, Table 1], the possibilities are $A_{14}(p = 7)$, $M_{22}(p = 5)$, $Ru(p = 5)$, and $HS(p = 5)$. None of these groups satisfy Corollary 4.3.

Now assume $X_0 = X_0(r) \in \text{Lie}(p)$. If $\text{rk}(X_0) \leq \frac{1}{2}\text{rk}(G)$, then by Theorem 5.10 $|G_x|^3 < |G|$, which is a contradiction.

If $\text{rk}(X_0) > \frac{1}{2}\text{rk}(G)$ then if $r > 2$ by Theorem 5.9 $X \cap G_x = E_7\left(q^{\frac{1}{s}}\right)$, with $s = 2$ or 3. However in both cases $(v, k) \leq 2$ forces $k^2 < v$, a contradiction. If $r = 2$ then the possible subgroups satisfying the bound $|G_x|^3 > |G|$ and having order dividing $|E_7(2)|$ are $A_6^\epsilon(2)$, $A_7^\epsilon(2)$, $B_5(2)$, $C_5(2)$, $D_5^\epsilon(2)$, and $D_6^\epsilon(2)$. However in all of these cases $(v, k) \leq 2$ forces $k^2 < v$.

□

Lemma 5.28. *The group X is not $E_8(q)$.*

Proof. Suppose $X = E_8(q)$. First suppose that X_0 is not simple. Then by Theorem 5.8 $G_x \cap X$ is one of the following,

(*i*) Parabolic.

(*ii*) Maximal rank.

(*iii*) $(2^{15}).L_5(2)$ (q odd) or $5^3.SL_3(5)$ ($5|q^2-1$).

(*iv*) $G_x \cap X = (A_5 \times A_6).2^2$.

or $X_0 = L_2(q) \times L_3^\epsilon(q)(p > 3)$, $G_2(q) \times F_4(q)$, $L_2(q) \times G_2(q) \times G_2(q)(p > 2, q > 3)$, or $L_2(q) \times G_2(q^2)(p > 2, q > 3)$.

We know from Lemma 5.20 that the first case does not hold.

From [46, Table 5.1] we have that the only subgroups of maximal rank such that $|G_x|^3 \geq |G|$ are $d.P\Omega_{16}^{+}(q).d$, $d.\left(L_2(q) \times E_7(q)\right).d$, $f.L_9^{\epsilon}(q).e.2$, and $e.\left(L_3^{\epsilon}(q) \times E_6^{\epsilon}(q)\right).e.2$, (where $d = (2, q-1)$, $e = (3, q-\epsilon)$, and $f = \frac{(9,q-\epsilon)}{e}$). In all cases, since $(k, v) \leq 2$ we have $k^2 < v$, which is a contradiction.

In all other cases, for all possible groups we have that $|G_x|^3 < |G|$, a contradiction. Hence X_0 is simple.

First consider the case $X_0 \notin \mathrm{Lie}(p)$. Then by [53, Table 1] the possibilities are Alt_{14}, Alt_{15}, Alt_{16}, Alt_{17}, $Alt_{18}(p = 3)$, $L_2(16)$, $L_2(31)$, $L_2(32)$, $L_2(41)$, $L_2(49)$, $L_2(61)$, $L_3(5)$, $L_4(5)(p = 2)$, $PSp_4(5)$, $G_2(3)$, ${}^2B_2(8)$, ${}^2B_2(32)(p = 5)$, and $Th(p = 3)$. In every case the inequality $|G_x|^3 > |G|$ is not satisfied.

Now consider the case $X_0 \in \mathrm{Lie}(p)$. If $\mathrm{rk}(X_0) \leq \frac{1}{2}\mathrm{rk}(G)$, then by Theorem 5.10 we have $|G_x|^3 \geq |G|$, which is a contradiction.

So $\mathrm{rk}(X_0) > \frac{1}{2}\mathrm{rk}(G)$. If $r > 2$, then by Theorem 5.9 $G_x \cap X$ is a subfield subgroup. The only cases in which $|G_x|^3 > |G|$ can be satisfied are when $q = q_0^2$ or $q = q_0^3$, but in all cases since $(v, k) \leq 2$ we have that k is too small.

If $r = 2$, then $\mathrm{rk}(X_0) \geq 5$. The groups for which $|G| < |G_x|^3$ are $A_8^{\epsilon}(2)$, $B_8(2)$, $B_7(2)$, $C_8(2)$, $C_7(2)$, $D_8^{\epsilon}(2)$, and $D_7^{\epsilon}(2)$. However, in all cases $(v, k) \leq 2$ forces $k^2 < v$, which is a contradiction. □

This completes the proof of Lemma 5.28, and hence we have that X is not an exceptional group of Lie type, completing thus the proof of Theorem 5, namely:

Theorem 5. *If D is a biplane with a primitive, flag-transitive automorphism group of almost simple type, then D has parameters either (7,4,2), or (11,5,2), and is unique up to isomorphism.*

Thus the proof of our Main Theorem is now complete.

BIBLIOGRAPHY

[1] M. Aschbacher, "On Collineation Groups of Symmetric Block Designs.", *J. Combin. Theory* (11) (1971), 272-281.

[2] M. Aschbacher, "On the Maximal Subgroups of the Finite Classical Groups", *Invent. Math.* **76** (1984), 469-514.

[3] E.F. Assmus Jr., J.A. Mezzaroba, and C.J. Salwach, "Planes and Biplanes", *Proceedings of the 1976 Berlin Combinatorics Conference, Vancerredle, 1977.*

[4] E.F. Assmus Jr., and C.J. Salwach, "The (16,6,2) Designs", *International J. Math. and Math. Sci.* Vol. 2 No. 2 (1979), 261-281.

[5] E. Bannai, S.Hao, and S-Y. Song, "Character tables of the association schemes of finite orthogonal groups on the non-isotropic points", *J. Comb. Theory Ser. A* **54** (1990), 164-200.

[6] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Encycopledia of Mathematics and its Applications, Vol. 69, Cambridge University Press, UK, 1999.

[7] F. Buekenhout, A. Delandtsheer, J. Doyen, "Finite Linear Spaces with Flag-Transitive Automorphism Groups", *J. Combin. Theory Ser. A* **49** (1988), 269-293.

[8] R. Burkhardt, "Der Zerlegungsmatrizen der $PSL(2, p^f)$", *J. Algebra* **40** (1976), 75-96.

[9] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, London, 1985.

[10] P.J. Cameron, "Biplanes", *Math. Z.* **131** (1973), 85-101.

[11] A.M. Cohen, M.W. Liebeck, J. Saxl, and G.M. Seitz, "The Local Maximal Subgroups of Exceptional Groups of Lie Type, Finite and Algebraic", *Proc. London Math. Soc* (3) **64** (1992) 21-48.

[12] B. N. Cooperstein, "Minimal Degree for a Permutation Representation of a Classical Group", *Israel J. Math* **30** (1978), 213-235.

[13] C.W. Curtis, Modular Representations of Finite Groups with Split (B, N)-Pairs, *in* "Seminar on Algebraic Groups and Related Topics" (A. Borel *et al.*, Eds.), Lecture Notes in Math. Vol. 131, Springer-Verlag, Berlin, 1970.

[14] H.Davies, "Flag-Transitivity and Primitivity", *Discrete Mathematics* **63** (1987), 91-93.

[15] A. Delandtsheer, "Flag-Transitive Finite Simple Groups" *Arch. Math.* **47** (1986) 395-400.

[16] P. Dembowski, *Finite Geometries*, Springer Verlag, Berlin-Heidelberg-New York, 1968.

[17] P. Dembowski, "Scharf transitive und scharf fahnentransitive Kollineationsgruppen" *Math. Ann.* **149** (1963), 217-225.

[18] R.H.F. Denniston, "On Biplanes with 56 points.", *Ars. Combin.* **9** (1980), 167-179.

[19] M. Hall Jr., R. Lane, and D. Wales "Designs derived from Permutation Groups", *J. Combin. Theory* **8** (1970), 12-22.

[20] D.G. Higman and J.E. McLaughlin, "Geometric ABA-groups", *Illinois Journal of Math.* **5** (1961), 328-397.

[21] D.R. Hughes, and F.C. Piper, *Design Theory*, Cambridge University Press, Cambridge, UK, 1988.

[22] B.Huppert, *Endliche Gruppen*, Springer-Verlag, Berlin, 1967.

[23] Q.M. Hussain, "On the Totality of the Solutions for the Symmetrical Incomplete Block Designs $\lambda = 2$, $k = 5$ or 6", *Sankhya* **7** (1945), 204-208.

[24] Q.M. Hussain, "Symmetrical Incomplete Block Designs with $\lambda = 2$, $k = 8$ or 9.", *Bull. Calcutta Math. Soc.* **37** (1945) 115-123.

[25] A.A. Ivanov, *Geometry of Sporadic Groups I*, Cambridge University Press, 1999.

[26] G.D. James, "On the Minimal Dimensions of Irreducible Representations of Symmetric Groups", *Math. Proc. Cambridge Philos. Soc.* **94** (1983), 417-424.

[27] C. Jansen, K. Lux, R.A. Parker, and R.A. Wilson, *An Atlas of Brauer Characters*, London Math. Soc. Monographs, New Series 11, Clarendon, Oxford, 1995.

[28] W. Kantor, "Classification of 2-Transitive Symmetric Designs", *Graphs and Combinatorics* **1** (1985), 165-166.

[29] W. Kantor, "Primitive Permutation Groups of Odd Degree, and an Application to Finite Projective Planes", *J. Alg.* **106** (1987) 1, 15-45.

[30] P.B. Kleidman, *The Subgroup Structure of Some Finite Simple Groups*, Ph.D. Thesis, University of Cambridge, 1987.

[31] P. B. Kleidman, "The Maximal Subgroups of the Finite 8-dimensional Orthogonal Groups $P\Omega_8^+(q)$ and of their Automorphism Groups", *J. Algebra* **110** (1987), 172-242.

[32] P.B. Kleidman, "The Maximal Subgroups of the Chevalley Groups $G_2(q)$ with q Odd, the Ree Groups ${}^2G_2(q)$, and Their Automorphism Groups", *J. Algebra* **117** (1998), 30-71.

[33] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, Vol. 129, Cambridge Univ. Press, Cambridge, UK, 1990.

[34] P.B. Kleidman and R.A. Wilson, "The Maximal Subgroups of J_4" *Proc. London Math. Soc.* (3) **56** (1998), 484-510.

[35] P.B. Kleidman and R.A. Wilson, "The Maximal Subgroups of Fi_{22}" *Math. Proc. Cam. Phil. Soc.* **102** (1987), 17-23.

[36] P.B. Kleidman, R.A. Parker, and R.A. Wilson, "The Maximal Subgroups of the Fischer Groups Fi_{23}" *J. London Math. Soc.* (2) **39** (1989), 89-101.

[37] V. Landazuri and G.M. Seitz, "On the Minimal Degrees of Projective Representations of the Finite Chevalley Groups", *J. Algebra* **32** (1974), 418-443.

[38] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series, Vol. , Cambridge University Press, Cambridge, UK, .

[39] M.W. Liebeck, "On the Orders of Maximal Subgroups of the Finite Classical Groups", *Proc. London Math Soc.* **50** (1985), 426-446.

[40] M.W. Liebeck, "The Affine Permutation Groups of Rank 3", *Proc. London Math Soc.* **54** (1987), 477-516.

[41] M.W. Liebeck, “The Classification of Finite Linear Spaces with Flag-Transitive Automorphism Groups of Affine Type”, *Journal of Combinatorial Theory, Series A* **84** (1998), 196-235.

[42] M.W. Liebeck and C.E. Praeger, “Affine Distance-Transitive Groups with Alternating or Symmetric Point Stabiliser”, *European J. Combin.* **13** (1992), 489-501.

[43] M.W. Liebeck, C.E. Praeger, and J. Saxl, “The Maximal Factorizations of the Finite Simple Groups and their Automorphism Groups”, *Mem. Amer. Math. Soc.* **86** No. 432 (1990), 1-151.

[44] M.W. Liebeck, C.E. Praeger, J. Saxl, “On the O’Nan-Scott Theorem for Finite Primitive Permutation Groups”, *J. Austral. Math. Soc. (Series A)* **44** (1988), 389-396.

[45] M.W. Liebeck, C.E. Praeger, and J. Saxl, “On the 2-closures of Finite Permutation Groups”, *J. London Math. Soc.* **37** (1988), 241-264.

[46] M.W. Liebeck, J. Saxl, and G.M. Seitz, “Subgroups of Maximal Rank in Finite Exceptional Groups of Lie Type”, *Proc. London Math. Soc.* **65** (1992), 297-325.

[47] M.W. Liebeck, J. Saxl, and G.M. Seitz, “On the Overgroups of Irreducible Subgroups of the Finite Classical Groups”, *Proc. London Math. Soc.* **55** (1987), 507-537.

[48] M.W. Liebeck, J. Saxl, and D.M. Testerman, “Simple Subgroups of Large Rank in Groups of Lie Type”, *Proc. London Math. Soc.* (3) **72** (1996), 425-457.

[49] M.W. Liebeck and J. Saxl, “The Primitive Permutation Groups of Odd Degree” *J. London Math. Soc.* **31** (1985), 250-264.

[50] M.W. Liebeck and J. Saxl, "The Finite Primitive Permutation Groups of Rank Three" *Bull. London Math. Soc.* **18** (1986), 165-172.

[51] M.W. Liebeck and J. Saxl, "On the Orders of Maximal Subgroups of the Finite Exceptional Groups of Lie Type" *Proc. London Math. Soc.* **55** (1987), 299-330.

[52] M.W. Liebeck and G.M. Seitz, "Maximal Subgroups of Exceptional Groups of Lie Type, Finite and Algebraic", *Geometriae Dedicata* **35** (1990), 353-387.

[53] M.W. Liebeck and G.M. Seitz, "On Finite Subgroups of Exceptional Algebraic Groups", *J. reine. angew. Math.* **515** (1999), 25-72.

[54] M.W. Liebeck and A. Shalev, "The Probability of Generating a Finite Simple Group" *Geometriae Dedicata* **56** (1995), 103-113.

[55] S. Linton, "The Maximal Subgroups of the Thompson Group" *J. London Math. Soc.* (2) **39** (1989), 79-88.

[56] F. Lübeck, "Small Degree Representations of Finite Chevalley Groups in Defining Characteristic" *LMS J. Comput. Math.* **4** (2001) 135-169.

[57] G. Malle, "The Maximal Subgroups of ${}^2F_4(q^2)$", *J. Algebra* **139** (1991), 53-69.

[58] M.P. Schutzenberger, "A Nonexistence Theorem for an Infinite Family of Symmetrical Block Designs", *Annals of Eugenics* **14** (1949), 286-287.

[59] C.J. Salwach, and J.A. Mezzaroba, "The Four Biplanes with $k = 9$", *J. Combin. Theory, Ser. A* **24** (1978), 141-145.

[60] J. Saxl "On Finite Linear Spaces with Almost Simple Flag-Transitive Automorphism Groups" *Journal of Combin. Theory A*, **100** 2 (2002), 322-348.

[61] G.M. Seitz, "Flag-Transitive subgroups of Chevalley Groups" *Annals of Math.* **97** 1, (1973), 27-56.

[62] M. Suzuki, "On a Class of Doubly Transitive Groups", *Annals of Math.* **75** (1962), 105-145.

[63] M. Suzuki, *Group Theory I*, Springer-Verlag, 1981.

[64] I.N. Stewart and D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, 1979.

[65] A. Wagner, "An Observation on the Degrees of Projective Representations of the Symmetric and Alternating Groups over an Arbitrary Field", *Arch. Math.* **29** (1977), 583-589.

[66] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York-London, 1964.