J Algebr Comb (2007) 26: 529–552
DOI 10.1007/s10801-007-0070-7

Biplanes with flag-transitive automorphism groups of almost simple type, with classical socle

Eugenia O'Reilly-Regueiro

Received: 31 October 2005 / Accepted: 9 March 2007 /
Published online: 21 April 2007

Abstract In this paper we prove that if a biplane D admits a flag-transitive automorphism group G of almost simple type with classical socle, then D is either the unique (11,5,2) or the unique (7,4,2) biplane, and $G \leq PSL_2(11)$ or $PSL_2(7)$, respectively. Here if X is the socle of G (that is, the product of all its minimal normal subgroups), then $X \trianglelefteq G \leq \mathrm{Aut}\, G$ and X is a simple classical group.

Keywords Automorphism group · Biplanes · Flag-transitive

1 Introduction

A *biplane* is a $(v, k, 2)$-symmetric design, that is, an incidence structure of v points and v blocks such that every point is incident with exactly k blocks, and every pair of blocks is incident with exactly two points. Points and blocks are interchangeable in the previous definition, due to their dual role. A *nontrivial* biplane is one in which $2 < k < v - 1$. A *flag* of a biplane D is an ordered pair (p, B) where p is a point of D, B is a block of D, and they are incident. Hence if G is an automorphism group of D, then G is *flag-transitive* if it acts transitively on the flags of D.

The only values of k for which examples of biplanes are known are $k = 3$, 4, 5, 6, 9, 11, and 13 [7, pp. 76]. Due to arithmetical restrictions on the parameters, there are no examples with $k = 7$, 8, 10, or 12.

For $k = 3$, 4, and 5 the biplanes are unique up to isomorphism [6], for $k = 6$ there are exactly three non-isomorphic biplanes [13], for $k = 9$ there are exactly four non-isomorphic biplanes [26], for $k = 11$ there are five known biplanes [3, 10, 11], and for $k = 13$ there are two known biplanes [1], in this case, it is a biplane and its dual.

E. O'Reilly-Regueiro (✉)
Instituto de Matemáticas, Universidad Nacional Autónoma de México, Mexico, DF 04510, Mexico
e-mail: eugenia@matem.unam.mx

In [24] it is shown that if a biplane admits an imprimitive, flag-transitive automorphism group, then it has parameters (16,6,2). There are three non-isomorphic biplanes with these parameters [4], two of which admit flag-transitive automorphism groups which are imprimitive on points, (namely 2^4S_4 and $(\mathbb{Z}_2 \times \mathbb{Z}_8)S_4$ [24]). Therefore, if any other biplane admits a flag-transitive automorphism group G, then G must be primitive. The O'Nan-Scott Theorem classifies primitive groups into five types [22]. It is shown in [24] that if a biplane admits a flag-transitive, primitive, automorphism group, it can only be of affine or almost simple type. The affine case was treated in [24]. The almost simple case when the socle of G is an alternating or a sporadic group was treated in [25], in which it is shown that no such biplane exists. Here we treat the almost simple case when the socle X of G is a classical group. We now state the main result of this paper:

Theorem 1 (Main Theorem) *If D is a nontrivial biplane with a primitive, flag-transitive automorphism group G of almost simple type with classical socle X, then D has parameters either* (7,4,2), *or* (11,5,2), *and is unique up to isomorphism.*

This, together with [24, Theorem 3] and [25, Theorem 1] yield the following:

Corollary 1 *If D is a nontrivial biplane with a flag-transitive automorphism group G, then one of the following holds*:

(1) *D has parameters* (7,4,2),
(2) *D has parameters* (11,5,2),
(3) *D has parameters* (16,6,2),
(4) *$G \leq A\Gamma L_1(q)$, for some odd prime power q, or*
(5) *G is of almost simple type, and the socle X of G is an exceptional group of Lie type.*

For the purpose of proving our Main Theorem, we will consider D to be a nontrivial 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).

For this we will proceed as in [27], in which the case for finite linear spaces with almost simple flag-transitive automorphism groups of Lie type is treated.

2 Preliminary results

In this section we state some preliminary results we will use throughout this paper.

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

Proof The result follows from [24, Lemma 3]. □

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

Proof The equality $k(k-1) = 2(v-1)$, implies $k^2 = 2v - 2 + k$, so clearly $2v < k^2$. The result follows from $v = |G : G_x|$ and $k \leq |G_x|$. □

From [9] we get the following two lemmas:

Lemma 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.*

Lemma 5 *If G is a flag-transitive automorphism group of a biplane D, then k divides $2 \cdot \gcd(v-1, |G_x|)$.*

Lemma 6 (Tits Lemma [28, 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 7 *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 $[X : H]_2 \leq 2$ is contained in a parabolic subgroup of X.*

Proof First assume $X = Cl_n(q)$ is classical (q a power of 2), and take H maximal in X. By Aschbacher's Theorem [2], 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, and 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 $2|H|_2 < |X|_2$, except when H is parabolic.

Now we take $H \in \mathcal{S}$. Then by [18, Theorem 4.2], $|H| < q^{2n+4}$, or H and X are as in [18, Table 4]. If $|X|_2 \leq 2|H|_2 \leq q^{2n+4}$, then either $X = L_n^\epsilon(q)$ and $n \leq 6$, or $X = Sp_n(q)$ or $P\Omega_n^\epsilon(q)$ and $n \leq 10$. We check the list of maximal subgroups of X for $n \leq 10$ in [15, Chapter 5], and we see that no group H satisfies $2|H|_2 \leq |X|_2$. We then check the list of groups in [18, Table 4], and again, none of them satisfy this bound.

Finally, assume X to be an exceptional group of Lie type in characteristic 2. By [20], if $2|H| \geq |X|_2$, then H is either contained in a parabolic subgroup, or H and X are as in [20, Table 1]. Again, we check all the groups in [20, Table 1], and in all cases $2|H|_2 < |X|_2$. □

As a consequence, we have a strengthening of Corollary 3:

Corollary 8 *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 then 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 3 that $|G| < |G_x|^3$. Now, by Lemma 6, 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 $|G| < 2|G_x||G_x|_{p'}^2$. □

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

Lemma 9 *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 The assumption that p divides v and the fact that k divides $2(v-1)$ imply $(k, p) \leq (2, p)$. Also, we know $k = [G_x : G_{x,B}]$ (where B is a block incident with x), so $[H : H_B]$ divides k, and therefore $([H : H_B], p) \leq (2, p)$. By Lemmas 6 and 7 we conclude that H_B is contained in a parabolic subgroup P of H, and P maximal in H implies that H_B is contained in P, so k is divisible by $[H : P]$. □

Lemma 10 ([21, 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.*

3 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 11 *If the group X is $PSL_2(q)$, then it is one of the following*:

(1) *$PSL_2(7)$ acting on the* (7,4,2) *biplane with point stabiliser S_4, or*
(2) *$PSL_2(11)$ 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 [12]: (Note that $|G_x|$ divides $(2, q-1)m|X_x|$):

(1) A solvable group of index $q+1$.
(2) $D_{(2,q)(q-1)}$.
(3) $D_{(2,q)(q+1)}$.
(4) $L_2(q_0)$ if $(r > 2)$, or $PGL_2(q_0)$ if $(r = 2)$, where $q = q_0^r$, r prime.
(5) S_4 if $q = p \equiv \pm 1 \pmod 8$.
(6) A_4 if $q = p \equiv 3,5,13,27,37 \pmod{40}$.
(7) A_5 if $q \equiv \pm 1 \pmod{10}$.

(1) Here $v = q+1$, so $k(k-1) = 2(v-1) = 2q$, hence $q = 3$, but $PSL_2(3)$ is not simple.

(2) and (3) 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.

(4) First assume $r > 2$. Clearly, q_0 divides $v = q_0^{r-1}(\frac{q_0^{2r}-1}{q_0^2-1})$, so k divides $2(v-1, mq_0(q_0^2-1))$, hence $k = \frac{2m(q_0^2-1)}{n}$ for some n. Say $q_0 = p^b$, so $m = br$ and (except for $p = 2$ and $2 \leq b \leq 4$), we have $b < \sqrt{q_0}$, (since $b^2 < p^b = q_0$).

Now, $k^2 > 2v$ implies

$$\frac{4m^2(q_0^2-1)^2}{n^2} > 2q_0^{r-1}\left(\frac{q_0^{2r}-1}{q_0^2-1}\right),$$

so

$$n^2 < \frac{2m^2(q_0^2-1)^3}{(q_0^{2r}-1)q_0^{r-1}}.$$

First consider $r > 3$, so $(r \geq 5)$. Here $q_0^r > b^2r^2 = m^2$. On the other hand, $2m^2 > \frac{q_0^{r-1}(q_0^{2r}-1)}{(q_0^2-1)^3}$, therefore

$$2q_0^r < \frac{q_0^{r-1}(q_0^{2r}-1)}{(q_0^2-1)^3},$$

which is a contradiction.

Next consider $r = 3$. From $k^2 > 2v$, we obtain $18b^2(q_0^2-1)^3 > n^2q_0^2(q_0^6-1)$, this together with $b^2 < q_0$, imply $n^2(q_0^6-1) < 18q_0^5$, therefore $q_0 \leq 17$. We check for all possible values of q_0 that $8v-7$ is not a square, contradicting Lemma 2.

Now assume $r = 2$. Then $v = \frac{q_0(q_0^2+1)}{(2,q-1)}$. As $q = q_0^2 \neq 2$, we have $m^2 < q$, so $4b^2 < q_0^2$, which implies $q_0 \neq 2$.

First consider q even. From $2(v-1) = k(k-1)$, we have $2(q_0^3+q_0-1) = \frac{2m(q_0^2-1)}{n}\big(\frac{2m(q_0^2-1)}{n}-1\big)$, however $\gcd(q_0^3+q_0-1, q_0^2-1)$ divides 3, which implies $k = \frac{6m}{t}$, with $t = 1, 3$.

If $t = 3$ then $q_0^3+q_0-1 = 2m^2-m = m(2m-1) < 2m^2$, but $m < q_0$, so this is a contradiction.

If $t = 1$ then $q_0^3+q_0-1 = 18m^2-6m$, which implies $q_0 < 18$, that is $q_0 = 4, 8$, or 16. However $m = 2b$ implies $k = 12b$, so $v-1$ is divisible by 6, but this is not the case for any of these values of q_0.

Now consider q odd. The equality $2(v-1) = k(k-1)$ yields $q_0^3+q_0-2 = \frac{4m^2}{n^2}(q_0^2-1)^2 - \frac{2m}{n}(q_0^2-1)$, and the inequality $k^2 > 2v$ implies $\frac{4m^2}{n^2}(q_0^2-1)^2 > q_0(q_0^2+1)$. In this case $m = 2b$, so $k = \frac{4b(p^{2b}-1)}{n}$, and $v = \frac{p^{3b}+p^b}{2} > \frac{b^6+b^2}{2}$, hence we have the following inequalities:

$$b^6+b^2 < p^{3b}+p^b < \frac{4b(p^{2b}-1)}{n} < \frac{4b\cdot p^{2b}}{n}.$$

This implies $\frac{n(p^{3b}+p^b)}{p^{2b}} < 4b$, so $n(p^b+p^{\frac{b}{2}}) < 4b < 4p^{\frac{b}{2}}$, therefore $n(p^{\frac{b}{2}}+1) < 4$ which implies $n = 1 = b$, and $p = 3$, 5, or 7, but in all these cases $k > v$, which is a contradiction.

(5) In this case $q = p \equiv \pm 1 \pmod 8$, and $m = 1$, so $G_0 \cong S_4$. We have q odd, $v = \frac{q(q^2-1)}{48}$, and k divides $2\big(\frac{q(q^2-1)-48}{48}, 24\big)$, so $k \mid 48$. Now $k^2 > 2v$ implies $q \leq 37$, hence $q = 7$, 17, 23, or 31. The only one of these values for which $8v-7$ is a square (Lemma 2) is $q = 7$, so $v = 7$ and $k = 4$, that is, we have the (7,4,2) biplane and $G = X \cong PSL_2(7)$.

(6) Here $q = p \equiv 3, 5, 13, 27$, or $37 \pmod{40}$, 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, contradicting Lemma 2.

(7) Here $q = p$ or $p^2 \equiv \pm 1 \pmod{10}$, and $v = \frac{q(q^2-1)}{120}$, so k divides $120m$, with $m = 1$ or 2. The inequality $2v < k^2$ implies $q^3 - q < 60k^2 < 60(120)^2 m^2$, 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 11.

Lemma 12 *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 Aschbacher's Theorem [2], the stabiliser 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 G_x is 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 by Kantor [14].

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 see k divides

$$\frac{2q(q^i - 1)(q^{n-i} - 1)}{(q - 1)^2}.$$

Also,

$$v = \frac{(q^n - 1)\ldots(q^{n-i+1} - 1)}{(q^i - 1)\ldots(q - 1)} > q^{i(n-i)},$$

but $k^2 > 2v$, so either $i = 3$ and $n < 10$, or $i = 2$.

First assume $i = 3$ and $q = 2$.

If $n = 9$ then $k = 2^2 \cdot 3^2 \cdot 7^2$, but the equation $k(k - 1) = 2(v - 1)$ does not hold.

If $n = 8$ then $k = 4 \cdot 7 \cdot 31$ but again the equation $k(k - 1) = 2(v - 1)$ does not hold.

For $n = 7$ $k = 420$ or 210, but again, k does not divide $2(v - 1)$.

Finally, if $n = 6$ then $k = 196$ or 98, but neither is a divisor of $2(v - 1)$.

Now assume $i = 3$ and $q > 2$. Then $n = 6$ or 7.

If $n=7$ then k divides

$$2\left(\frac{q(q^3-1)(q^4-1)}{(q-1)^2}, \frac{(q^7-1)(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)(q-1)}-1\right),$$

but then $k^2 < v$, which is a contradiction.

If $n=6$ then k divides

$$2\left(\frac{q(q^3-1)^2}{(q-1)^2}, \frac{(q^6-1)(q^5-1)(q^4-1)}{(q^3-1)(q^2-1)(q-1)}-1\right),$$

But again $k^2 < 2v$.

Hence $i=2$. Here $v=\frac{(q^n-1)(q^{n-1}-1)}{(q^2-1)(q-1)}$, and G has suborbits with sizes:

$|\{2\text{-subspaces } H : \dim(H\cap W)=1\}| = \frac{q(q+1)(q^{n-2}-1)}{q-1}$ and

$|\{2\text{-subspaces } H : H\cap W=\overline{0}\}| = \frac{q^4(q^{n-2}-1)(q^{n-3}-1)}{(q^2-1)(q-1)}$.

If n is even then k divides $\frac{q(q^{n-2}-1)}{(q^2-1)}$, since $q+1$ is prime to $\frac{(q^{n-3}-1)}{q-1}$, this implies $k^2 < v$, which is a contradiction.

Hence n is odd, and k divides $\frac{2q(q^{n-2}-1)}{q-1}(q+1, \frac{n-3}{2})$.

First assume $n=5$. Then $v=(q^2+1)(q^4+q^3+q^2+q+1)$, and k divides $2q(q^2+q+1)$. The fact that $k^2 > 2v$ forces $k=2q(q^2+q+1)$.

The condition $k(k-1)=2(v-1)$ implies

$$4q^2(q^2+q+1)^2-2q(q^2+q+1)=2(q^6+q^5+2q^4+2q^3+2q^2+q),$$

so

$$(q^2+q+1)\left(2q(q^2+q+1)-1\right)=(q^5+q^4+2q^3+2q^2+2q+1).$$

If we expand we get the following equality:

$$q^5+3q^4+4q^3+q^2-q-2=0,$$

which is a contradiction. Therefore $n\geq 7$. Here

$$v=(q^{n-1}+q^{n-2}+\cdots+q+1)(q^{n-3}+q^{n-5}+\cdots+q^2+1),$$

and k divides $2dc$, where $d=q(q^{n-3}+q^{n-4}+\cdots+q+1)$ and $c=(q+1, \frac{n-3}{2})$. Say $k=\frac{2dc}{e}$, then $v<k^2$ forces $e\leq 2q$. We have the following equality:

$$\frac{v-1}{d}=q^{n-2}+q^{n-4}+\cdots+q^3+q+1,$$

and also, since $k(k-1)=2(v-1)$, we have

$$k=\frac{2(v-1)}{k}+1=\frac{2e(v-1)}{2dc}=\frac{eq^{n-2}+eq^{n-4}+\cdots+eq^3+eq+e+c}{c}.$$

Now, (kc, d) divides d, and also
$(kc, q(eq^{n-3} + eq^{n-5} + \cdots + eq^2 + e))$
$= (eq^{n-2} + eq^{n-4} + \cdots + eq + e + c, q(eq^{n-3} + eq^{n-5} + \cdots + eq^2 + e))$
$= (eq^{n-2} + \cdots + eq + e + c, e + c)$, and
$(kc, \frac{ed}{q})$
$= (eq^{n-2} + \cdots + eq + e + c, eq^{n-3} + eq^{n-4} + \cdots + eq + e)$
$= (eq^{n-2} + \cdots + eq + e + c, (2e + c)q + e + c)$.

Therefore k divides $c(e + c)((2e + c)q + e + c)$, 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, again contradicting Lemma 2.

$\mathcal{C}_1'$) 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 Lemma 10, 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 $(k, p) \leq 2$. First assume $i = 1$. If $x = \{\langle v_1\rangle, \langle v_2 \ldots v_n\rangle\}$, then consider $y = \{\langle v_1, \ldots, v_{n-1}\rangle, \langle v_n\rangle\}$, so $[G_x : G_{xy}] = \frac{q^{n-2}(q^{n-1}-1)}{q-1}$ and k divides $\frac{2(q^{n-1}-1)}{q-1}$. However $v = \frac{q^{n-1}(q^n-1)}{q-1} > q^{2(n-1)}$, which implies $k^2 < v$, a contradiction.

Now assume $i > 1$. Consider $x = \{\langle v_1, \ldots, v_i\rangle, \langle v_{i+1}, \ldots, v_n\rangle\}$ and $y = \{\langle v_1, \ldots, v_{i-1}, v_i + v_n\rangle, \langle v_{i+1}, \ldots, v_n\rangle\}$. Then $[G_x^0 : G_{xy}^0]_{p'}$ divides $2(q^i - 1)(q^{n-i} - 1)$, which implies $k < 2q^n$, but $v > q^{2i(n-i)}$, so again $k^2 < v$, a contradiction.

$\mathcal{C}_2$) Here G_x preserves a partition $V = V_1 \oplus \cdots \oplus V_a$, with each V_i of the same dimension, say, b, and $n = ab$.

First consider the case $b = 1$ and $n = a$, and let $x = \{\langle v_1\rangle, \ldots, \langle v_n\rangle\}$ and $y = \{\langle v_1 + v_2\rangle, \langle v_2\rangle, \ldots, \langle v_n\rangle\}$. Since $n > 2$, we see k divides $4n(n - 1)(q - 1) = 2[G_x : G_{xy}]$. Now $v > \frac{q^{n(n-1)}}{n!}$ and $k^2 > v$, so $n = 3$ and $q \leq 4$, that is $v = \frac{q^3(q^3-1)(q+1)}{(3,q-1)6!}$. 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 $x = \{\langle v_1, \ldots, v_b\rangle, \langle v_{b+1}, \ldots, v_{2b}\rangle, \ldots\}$ and $y = \{\langle v_1, \ldots, v_{b-1}, v_{b+1}\rangle, \langle v_b, v_{b+2}, \ldots, v_{2b}\rangle, \ldots, \langle v_{n-b+1}, \ldots, v_n\rangle\}$. Then k divides $\frac{2a(a-1)(q^b-1)^2}{q-1}$, so $v > \frac{q^{n(n-b)}}{a!}$, forcing $n = 4$, $q \geq 5$, and $a = 2 = b$. In none of these cases can we obtain $k > 2$.

$\mathcal{C}_3$) In this case G_x is an extension field subgroup. Since $2|G_x||G_x|_{p'}^2 > |G|$ by Corollary 8, either:

(1) $n = 3$ and $X \cap G_x = \hat{}(q^2 + q + 1) \cdot 3 < PSL_3(q) = X$, or
(2) n is even and $G_x = N_G(\hat{}PSL_{\frac{n}{2}}(q^2))$.

First consider case (1). Here $v = \frac{q^3(q^2-1)(q-1)}{3}$, so k divides $6(q^2+q+1)(\log_p q)$, and $k^2 > v$ implies $q = 3, 4, 5, 8, 9, 11, 13$, or 16. In none of these cases is $8v - 7$ a square.

Now consider case (2) and write $n = 2m$. As p divides v, we have $(k, p) \leq 2$. 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 then 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 $2(q^n - 1)(q^{n-2} - 1)$, contrary to $2v < k^2$, which is a contradiction.

Now let $n = 6$. Then since $(k, p) \leq 2$, Lemma 9 implies 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 $v = \frac{q^4(q^3-1)(q-1)}{2}$, and so k is odd and prime to $q - 1$. The fact that $(v - 1, q + 1) = 1$ implies 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 all these cases $v > k^2$.

$\mathcal{C}_5$) In this case G_x is the stabiliser in G of a subfield space. So $G_x = N_G(PSL_n(q_0))$, with $q = q_0^m$ and m 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 $v = \frac{(q_0^3+1)(q_0^2+1)q_0^3}{(q_0+1,3)}$.

Since p divides v, we have $(k, p) \leq 2$, so Lemma 9 implies 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 9 we see $q_0^2 + 1$ 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 see k divides $2(q_0^n - 1)(q_0^{n-1} - 1)$, 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 either $2^4 A_6$ or $3^2 Q_8$, 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 obtain $p \leq 13$. If $p = 7$ then the action is 2-transitive. The remaining cases 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 $v = \frac{q^4(q^2+1)(q^3-1)}{x} > \frac{q^9}{x}$, with $x = 2$ unless $q \equiv 1 \pmod 4$, in which case $x = 4$. Hence $4 \nmid k$, and so k divides $2(q^2 - 1)\log_p q$, and if q is odd then k divides $\frac{(q^2-1)\log_p q}{32}$.

If q is odd, then $k^2 < \frac{q^9}{32} < \frac{q^9}{x} = v$, a contradiction. Hence q is even, and so

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

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 $2(v-1)$.

$\mathcal{C}_8$) Now consider G_x to be a classical group.

(1) First assume G_x is a symplectic group, so n is even. By Lemma 6 k is divisible by a parabolic index in G_x. If $n = 4$ then $v = \frac{q^2(q^3-1)}{(2,q-1)}$, and $\frac{q^4-1}{q-1}$ divides k, however $(v-1, q^2+1)$ divides 2, which is a contradiction.

If $n = 6$ then $v = \frac{q^6(q^5-1)(q^3-1)}{(3,q-1)}$ and q^3+1 divides k, but q^3+1 divides $2(v-1)$ only if $q = 2$, so $k = 9$, too small.

Now suppose $n \geq 8$. If we consider the stabilisers of a 4-dimensional subspace of G_x and G, we see that k divides twice the odd part of $(q^n-1)(q^{n-2}-1)$. Also, $(k, q-1) \leq 2$, so k divides $2\frac{(q^n-1)(q^{n-2}-1)}{(q-1)^2}$, and therefore $k \leq 8q^{2n-4}$. The inequality $k^2 > 2v$ forces $n = 8$. In this case $v = \frac{q^{12}(q^7-1)(q^5-1)(q^3-1)}{(q-1,4)}$ which implies $q \leq 3$, and in neither of these two cases is $8v-7$ a square.

(2) Now let G_x be orthogonal. Then q is odd, since that is the case with odd dimension, and with even dimension it is a consequence of the maximality of G_x in G. The case in which $n = 4$ and G_x is of type O_4^+ will be investigated later, in all other cases Lemma 6 implies that k is divisible by a parabolic index in G_x and is therefore even, but it is not divisible by 4 since v is also even and $(k, v) \leq 2$. This and the fact that q does not divide k implies $k < v$, a contradiction.

(3) Finally let G_x be a unitary group over the field of q_0 elements, where $q = q_0^2$. If $n \geq 4$ then considering the stabilisers of a nonsingular 2-subspace of V in G and G_x, we see k divides $2(q_0^n - (-1)^n)(q_0^{n-1} - (-1)^{n-1})$. The inequality $k^2 > 2v$ forces $n = 4$, and in this case $v = \frac{q_0^6(q_0^4+1)(q_0^3+1)(q_0^2+1)}{(q_0-1,4)}$. Since k divides $2(q_0^4-1)(q_0^3+1)$ and $(k, (q_0^2+1)(q_0-1) \leq 2$, we see k divides $2(q_0^3+1)(q_0+1)$, so $k^2 \leq 2v$, a contradiction. Therefore $n = 3$, and by Lemma 6 $q_0^2 - q_0 + 1$ divides k, and k divides $2(v-1)$ with $v = \frac{q_0^3(q_0^3-1)(q_0^2+1)}{x}$ with x either 1 or 3. This implies $q_0 = 2$, but then $v = 280$, and $8v-7$ is not a square.

$\mathcal{S}$) 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 [18, Theorem 4.2] we have the possibilities $|G_x| < q^{2n+4}$, $G_x' = A_{n-1}$ or A_{n-2}, or $G_x \cap X$ and X are as in [18, Table 4].

Also, $|G| < |G_x|^3$ by Corollary 3 and $|G| \leq q^{n^2-n-1}$, so $n \leq 7$, and by the bound $2|G_x||G_x|_{p'}^2 > |G|$ we need only to consider the following possibilities [15, 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 12.

4 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 $\beta = \{e_1, f_1, \dots, e_m, f_m\}$.

Lemma 13 *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 $(p, 2m) = (2, 4)$ 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

$$v = \frac{(q^{2m} - 1)(q^{2m-2} - 1) \dots (q^{2m-2i+2} - 1)}{(q^i - 1)(q^{i-1} - 1) \dots (q - 1)}.$$

From this we see $v \equiv q + 1 \pmod{pq}$, so q is the highest power of p dividing $v - 1$. By Lemma 10 there is a subdegree which is a power of p, and since k divides twice every subdegree, 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 it preserves a partition $V = V_1 \oplus \cdots \oplus V_a$ 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 G_x maximal implies q is odd [17]. 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

$$y = \{\langle e_1, \dots, e_{m-1}, f_m\rangle, \langle f_1, \dots, f_{m-1}, e_m\rangle\}.$$

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 $G_x \cap X = \hat{}Sp_{2i}(q) \,\mathrm{wr}\, S_t$, with $it=m$. Let

$$x=\{\langle e_1, f_1, \dots, e_i, f_i\rangle, \langle e_{i+1}, f_{i+1}, \dots, e_{2i}, f_{2i}\rangle, \dots\},$$

and take

$$y=\{\langle e_1, f_1, \dots, e_i, f_i+e_{i+1}\rangle, \langle e_{i+1}, f_{i+1}-e_i, e_{i+2}, \dots, e_{2i}, f_{2i}\rangle, \dots\}.$$

Considering the size of the G_x-orbit containing y, we see k divides

$$\frac{t(t-1)(q^{2i}-1)^2}{q-1}.$$

Now,

$$\frac{q^{2i^2t(t-1)}}{t!}<v,$$

so $v<k^2$ implies $t!t^4>q^{2i^2t(t-1)+2-8i}$, hence $q^{2t(t-1)-6}<t^{t+4}$ and therefore $t<4$.

First assume $t=3$. Then by the above inequalities $i=1$ and $q=2$, but then G_x is not maximal [8, p. 46], a contradiction.

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 k divides $(q^2(q^2+1)-2, 2(q+1)^2(q-1))$, that is, k divides

$$((q^2+2)(q^2-1), 2(q+1)^2(q-1))=(q^2-1)(q^2+2, 2(q+1))\leq 6(q^2-1).$$

Therefore

$$k=\frac{6(q^2-1)}{r},$$

with $1\leq r\leq 6$. Now $2(v-1)=(q^2+2)(q^2-1)$, 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 obtain $t=2$ or 3.

If $t=3$, then $v<k^2$ implies $i=1$, 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 9 to $PSp_2(q^3)$ yields 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 $Sp_{2i-2}(q^2)$ 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 $i \le 2$.

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 $(k,v)\le 2$ and q^2-1 divides v, we see 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 $G_x \cap X = PSp_2(q^2).2 < PSp_4(q) = X$, Therefore k divides $4q^2(q^4-1)$, but since $(k,v)\le 2$, then k divides $4(q^2+1)$, so $k=\frac{4(q^2+1)}{r}$ for some $r\le 8$ (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

$$r^2(q^2-2) = 16(q^2+1)-4r,$$

that is,

$$(r+4)(r-4)q^2 = 2(8+r(r-2)).$$

This implies $4<r\le 8$, but solving the above equation for each of these possible values of r gives non-integer values of q, a contradiction.

Now assume $G_x \cap X = \hat{\ } GU_m(q).2$, with q odd. Since v is even, 4 does not divide k. Also, k is prime to p, so by the Lemma 9, 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

$$v = \frac{q^{\frac{m^2}{2}}(q^m+1)\dots(q+1)}{(2, q-1)} > \frac{q^{\frac{m(2m+1)}{2}}}{2}.$$

Now G_x stabilises a $GF(q_0)$-subspace W of V. Considering a nonsingular 2-dimensional subspace of W we see

$$Sp_2(q_0) \circ Sp_{2m-2}(q_0) < Sp_2(q) \circ Sp_{2m-2}(q) < X.$$

If we take $g \in Sp_2(q) \setminus Sp_2(q_0)$ then $Sp_{2m-2}(q_0) < G_x \cap G_x^g$. This implies that there is a subdegree of X with the p'-part dividing $q_0^{2m} - 1$, so 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 $a \leq 2$. The inequality $|G| < |G_x|^3$ implies $s \leq 3$, 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 $G_x = N_G(PSp_{2a}(q)^{2r}2^{r-1}A_r)$ 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 when $q = 2$ the action is 2-transitive and that has been done in [14]. Here

$$v = \frac{q^m(q^m+\epsilon)}{2},$$

and from the proof of [23, Prop. 1] 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 4 that k divides $2(q^m - \epsilon)(q - 2, q^{m-1} + \epsilon)$. However, Lemma 9 implies k is divisible by the index of a parabolic subgroup in $O_{2m}^\epsilon(q)$, which is not the case.

$p = m = 2$. Here $2m = 4$ and q is even, 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, contrary to $v < k^2$.

$G_x \cap X = D_{2(q\pm1)} \operatorname{wr} S_2$. So k divides $2(q \pm 1)^2 \log_2 q$, 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 [15] for $2m \leq 10$.

First assume $2m = 4$, so we have one of the following possibilities:

(1) $G_x \cap X = Sz(q)$ with q even,
(2) $G_x \cap X = PSL_2(q)$ with $q \geq 5$, or
(3) $G_x \cap X = A_6.a$ with $a \leq 2$ and $q = p \geq 5$.

In case (1) $v = q^2(q^2 - 1)(q + 1)$. Applying Lemma 9 to $Sz(q)$, we see $q^2 + 1$ divides k. Now $(v - 1, q^2 + 1) = (q - 2, 5)$, so $q = 2$, contrary to our initial assumptions.

In case (2), since $(k, v) \leq 2$, we have $k \leq 2\log_p q$, contrary to $v < k^2$.

In case (3), 4 does not divide 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 [15] 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 9 to $G_2(q)$ we see that $\frac{q^6-1}{q-1}$ divides k, a contradiction.

If $2m = 8$ or 10, then by [15] either $G_x = S_{10} < Sp_8(2) = G$ or $G_x = S_{14} < Sp_{12}(2) = G$. In the first case k divides $2(v - 1, |G_x|) = 70$, which is too small. In the second case $(k, v) \leq 2$ implies that k divides $2 \cdot 7^2 \cdot 11 \cdot 13$, also too small.

If $2m \geq 12$, then by [18] we have $|G_x| \leq q^{4(m+1)}$, $G'_x = A_{n+1}$ or A_{n+2}, or X or $G_x \cap X$ 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 13.

5 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 14 *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 $v - 1$. By Lemma 10 there is a subdegree which is a power of p, therefore 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 and 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 $G_x \cap G_x^g$ contains $SO_{i-1}(q) \times SO_{n-i-1}(q)$. This implies $k \le 4q^m \log_p q$, but $v > q^{\frac{i(n-i)}{4}}$ implies q is odd and $m \ge 3$, 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 either:

$G_x \cap X = 2^6 A_7 < \Omega_7(q)$ with q either 3 or 5, or
$G_x \cap X = 2^{n-1} A_n < \Omega_n(3)$ 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

$$|G_x|_{p'} = t \prod_{i=1}^{r} (q^{2it} - 1),$$

and since k divides $2(|G_x|_{p'}, v-1)$, 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 $a \le 2$ with $a = 2$ if and only $b = 2$. The inequality $|G| < |G_x||G_x|_{p'}^2$ forces $b = 2$. If $n = 2m+1$ then 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 therefore $(v-1, (q^{2m} - 1)\dots(q_0^2 - 1))$ is too small.

$\mathcal{C}_6$), $\mathcal{C}_7$), and $\mathcal{C}_8$) In the cases $\mathcal{C}_6$ and $\mathcal{C}_8$, the classes are empty, and for $\mathcal{C}_7$ we see $G_x \cap X$ 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:

(1) $G_x \cap X = G_2(q) < \Omega_7(q) = X$ with q odd,
(2) $G_x \cap X = Sp_6(2) < \Omega_7(p)$ with p either 3 or 5, or
(3) $G_x \cap X = S_9 < \Omega_7(3)$.

In all three cases as k divides $2(v-1, |G_x|)$ it is too small. □

This completes the proof of Lemma 14.

6 X is an orthogonal group of even dimension

In this section $X = P\Omega_{2m}^{\epsilon}(q)$, with $m \ge 4$. 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 15 *The group X is not $P\Omega_{2m}^{\epsilon}(q)$, with $m \ge 4$.*

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 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

$$x=\langle e_1,\dots,e_m\rangle,\ \ y=\langle f_1,\dots,f_m\rangle$$

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 $v=(q^{m-1}+1)(q^{m-2}+1)\dots(q+1)>q^{\frac{m(m-1)}{2}}$. Let

$$x=\langle e_1,\dots,e_m\rangle,\ \ y=\langle e_1,f_2,\dots,f_m\rangle.$$

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. The highest power of p dividing $v-1$ is q so k divides $2q(q^m-1)$, and the inequality $v<k^2$ implies $m=5$. In this case the action is of rank three, with nontrivial subdegrees

$$\frac{q(q^2+1)(q^5-1)}{q-1}\quad\text{and}\quad\frac{q^6(q^5-1)}{q-1}.$$

Therefore k divides

$$\frac{2q(q^5-1)}{q-1},$$

and $v<k^2$ implies k is either $2q(q^4+q^3+q^2+q+1)$ or $q(q^4+q^3+q^2+q+1)$, but neither of these satisfies the equality $k(k-1)=2(v-1)$.

Now suppose $G_x=N_i$. First let $i=1$. The subdegrees of X are (see [5]):

$q^{2m-2}-1$, $\frac{q^{m-1}(q^{m-1}+\epsilon)}{2}$, $\frac{q^{m-1}(q^{m-1}-\epsilon)(q-1)}{4}$, and $\frac{q^{m-1}(q^{m-1}+\epsilon)(q-3)}{4}$ if $q\equiv 1 \bmod 4$,
$q^{2m-2}-1$, $\frac{q^{m-1}(q^{m-1}-\epsilon)}{2}$, $\frac{q^{m-1}(q^{m-1}-\epsilon)(q-3)}{4}$, and $\frac{q^{m-1}(q^{m-1}+\epsilon)(q-3)}{4}$ if $q\equiv 3 \bmod 4$,
and
$q^{2m-2}-1$, $\frac{q^{m}(q^{m-1}-\epsilon)}{2}$, and $\frac{q^{m-1}(q^{m-1}+\epsilon)(q-2)}{2}$ if q is even.

Here k divides twice the 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 $SO_{i-1}(q)\times SO_{n-i-1}(q)\leq G_x\cap G_x^g$ for some

$g \in G \setminus G_x$. Since k and p are coprime $k < 8q^m \log_p q$, contrary to $v < k^2$. Now assume 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 $2(q - \epsilon_1)(q^{m-1} - \epsilon\epsilon_1)(\log_2 q)_{2'}$, 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

$$\big(q^{\frac{i}{2}} - \epsilon_1\big)\big(q^{\frac{i-2}{2}} + \epsilon_1\big)\big(q^{\frac{n-i}{2}} + \epsilon_2\big)\big(q^{\frac{n-i-2}{2}} + \epsilon_2\big)(\log_2 q)_{2'},$$

forcing $k^2 < v$, a contradiction.

$\mathcal{C}_2$) If $G_x \in \mathcal{C}_2$ then G_x stabilises a decomposition $V = V_1 \oplus \cdots \oplus V_a$ of subspaces of equal dimension, say b, so $n = ab$. Here we have three possibilities.

First assume all the V_i are nonsingular and isometric. (Also, if b is odd then so is q). If $b = 1$ then the inequality $|G| < 2|G_x||G_x|^2_{p'}$ implies $G_x \cap X = 2^{n-2}A_n$, 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 $G \leq X.2$ ([16]), 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 $V_3 \oplus \cdots \oplus V_a$. From this it follows that $k \leq 2a(a-1).(2(q+1))^2|\operatorname{Out} X|$, and from $v < k^2$ we obtain $n = 8$ 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 $V_4 \oplus \cdots \oplus V_a$, and in this case k is at most $2a(a-1)(a-2)(2(q+1))^3|\operatorname{Out} X|$, and so $n = 8$ or 10. Using the condition that k divides $2(v-1)$ we rule out these three cases.

Finally let $b > 2$. The inequality $|G| < 2|G_x||G_x|^2_{p'}$ forces $b = m$, (and so $\epsilon = +$). Let δ be the type of the V_i if m is even. Assume first that $m = 4$. Then

$$v = \frac{q^8(q^2+1)^2(q^4+q^2+1)}{4}$$

if $\delta = +$, and

$$v = \frac{q^8(q^6-1)(q^2-1)}{4}$$

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 $3(q^2+1)^2 \log_p q$, 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

$$v = \frac{q^{\frac{m(m-1)}{2}}(q^{m-1}+1)(q^{m-2}+1)\ldots(q+1)}{2^e},$$

where e is either 0 or 1 ([17, 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 $2(q^m-1)(q^{m-1}-1)\log_p q$, and in fact $(k,v) \leq 2$ implies k divides twice the odd part of $\frac{(q^m-1)(q^{m-1}-1)\log_p q}{q+1}$, 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 ([17]).

First assume $G_x = N_G(\Omega^{\delta}_{\frac{n}{s}}(q^s))$, with s a prime and $\delta = \pm$ if $\frac{n}{s}$ is even (and empty otherwise). The inequality $|G| < |G_x|^3$ forces $s = 2$. If q is odd, then by Lemma 9 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

$$v = \frac{q^{\frac{m^2}{2}}(q^{2m-2}-1)(q^{2m-2}-1)\dots(q^2-1)}{2^e},$$

with $e \leq 2$ ([17, 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.

Now let $G_x = N_G(\hat{\ }GU_m(q))$, with $\epsilon = (-1)^m$. If q is odd, then as in the symplectic case $q+1$ 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 k divides $2(q^m-(-1)^m)(q^{m-1}-(-1)^{m-1})\log_p q$, 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 $n = ab$. The inequality $|G| < 2|G_x||G_x|^2_{p'}$ implies $n = 8$ 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. The inequality $|G| < 2|G_x||G_x|^2_{p'}$ implies $G_x \cap X = P\Omega^{\delta}_{2m}(q_0).2^e < P\Omega^+_{2m}(q) = X$, with $q = q_0^2$ and $e \leq 2$ ([17, 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 an element $g \in G \setminus G_x$ that stabilises $U^\perp$ pointwise, from this it follows that $G_x \cap G_x^g$ involves $P\Omega^\delta_{2m-2}(q_0)$. This implies that k divides $2(q_0^m - \delta)(q_0^{m-1} + \delta)|\operatorname{Out} X|$, which contradicts the inequality $v < k^2$.

$\mathcal{C}_6$) If $G_x \in \mathcal{C}_6$, it is an extraspecial normaliser. From $|G| < |G_x|^3$ we have $G_x \cap X = 2^6 A_8 < P\Omega_8^+(3) = X$. 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 $n \le 10$, the subgroups G_x are listed in [15] and [16]. Since $|G| < 2|G_x||G_x|^2_{p'}$, we have one of the following:

(1) $\Omega_7(q) < P\Omega_8^+(q)$,
(2) $\Omega_8^+(q) < P\Omega_8^+(q)$ with $q = 3, 5$, or 7, or
(3) $A_9 < \Omega_8^+(q)$, $A_{12} < \Omega_{10}^-(2)$, $A_{12} < P\Omega_{10}^+(3)$.

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 the fact that k divides $2(|G_x|, v-1)$ implies 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 k is too small.

So $n \ge 12$. If $n > 14$, then by [18, Theorem 4.2] we need only to 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 conclude 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 k divides $2(v-1, |G_x|)$, so $k^2 < v$, a contradiction. If X is not alternating, then again since $|G_x| < q^{2n+4}$ by [18, Theorem 4.2] it follows that $|G_x| < q^{28}$, respectively $|G_x| < q^{32}$. On the other hand, from $|G| < 2|G_x||G_x|^2_{p'}$ we obtain $|G_x|_{p'} > \frac{q^{19}}{\sqrt{2}}$, respectively $|G_x|_{p'} > q^{29}$. We can now see (cf. [19, Sections 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 [16]. 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

$$v = \frac{(q^6-1)(q^4-1)}{(q-1)^3} > q^{11},$$

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 10), we have $k < 2q(3, q)$, which contradicts $v < k^2$.

Now, by [16] and $|G| < |G_x||G_x|^2_{p'}$, 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,

$$v = \frac{q^6(q^4-1)^2}{(q-1,2)^2},$$

and Lemma 9 applied to $G_2(q)$ implies 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 15.

7 *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 16 *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 throughout, 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

$$v = \frac{(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1}) \ldots (q^{n-2i+1} - (-1)^{n-2i+1})}{(q^{2i} - 1)(q^{2i-2} - 1) \ldots (q^2 - 1)}.$$

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 k divides
$2(q^i - (-1)^i)(q^{n-i} - (-1)^{n-i})$. However in this case

$$v = \frac{q^{i(n-1)}(q^n - (-1)^n) \ldots (q^{n-i+1} - (-1)^{n-i+1})}{(q^i - (-1)^i) \ldots (q+1)},$$

and $v < k^2$ implies $i = 1$. Therefore k divides $2(q+1)(q^{n-1} - (-1)^{n-1})$. Applying Lemma 9 to $U_{n-1}(q)$, we see k is divisible by the degree of a parabolic action of $U_{n-1}(q)$. We check the subdegrees, and by the fact that k divides $|G_x|^2$ as well as $k^2 > v$ we conclude $n \leq 5$.

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 $V = V_1 \oplus \cdots \oplus V_a$ 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 k divides $2a(a-1)(q^b - (-1)^b)^2$. From the inequality $v < k^2$ we have $n = 4$ and $b = 2$. Therefore

$$v = \frac{q^4(q^4-1)(q^3+1)}{2(q^2-1)(q+1)},$$

and k divides $4(q^2-1)^2$. 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 $q \le 17$, but by 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 k divides $n(n-1)(q+1)^2$, contrary to $v < k^2$. If $q \le 3$ 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 $n \le 6$ if $q = 2$, or $n \le 4$ 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 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 $|G| < 2|G_x||G_x|_{p'}^2$ 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 $|G| < |G_x|^3$ implies $b = 3$. 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 6 k is divisible by the degree of a parabolic action of G_x. Here $q+1$ 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 $G_x = N(PSp_n(q))$, with n even, then by Lemma 9 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 $G_x \cap X = 3^2 Q_8$, $2^4 A_6$, or $2^4 S_6$, and $X = U_3(5)$, $U_4(3)$, and $U_4(7)$ respectively. In all cases the fact that k divides $2(|G_x|, v-1)$ 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 $t \geq 3$, we see $|G_x|$ is too small to satisfy $|G| < |G_x|^3$.

$\mathcal{C}_8$) This class is empty.

$\mathcal{S}$) 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 [15, 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 $k^2 < v$ 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 [18] we have $|G| > |G_x|^3$, a contradiction. Hence $n = 11, 12$, or 13. By [18], $|G_x|$ is bounded above by q^{4n+8}, and $|G| < 2|G_x||G_x|^2_{p'}$ implies $|G_x|_{p'}$ is bounded below by q^{33}, q^{43}, or q^{53} respectively. Using the methods in [18, 19] we rule out all the almost simple groups G_x. □

This completes the proof of Lemma 16, and hence if X is a simple classical group, then it is either $PSL_2(7)$ or $PSL_2(11)$.

Acknowledgements The results in the present paper were obtained with a grant from the Dirección General de Asuntos del Personal Académico, UNAM, during the course of my Ph.D. under the supervision of Martin W. Liebeck. I am very grateful to Martin for his most helpful ideas and guidance. I would also like to thank Jan Saxl for allowing me to view his notes before [27] was published, and Sasha Ivanov for providing me with these notes. Finally I thank the referees for their observations and suggestions, which have greatly improved this article.

References

1. Aschbacher, M. (1971). On collineation groups of symmetric block designs. *J. Comb. Theory*, *11*, 272–281.
2. Aschbacher, M. (1984). On the maximal subgroups of the finite classical groups. *Invent. Math.*, *76*, 469–514.
3. Assmus, E. F. Jr., Mezzaroba, J. A., & Salwach, C. J. (1977). Planes and biplanes. In *Proceedings of the 1976 Berlin Combinatorics Conference*. Vancerredle.
4. Assmus, E. F. Jr., & Salwach, C. J. (1979). The (16,6,2) designs. *Int. J. Math. Math. Sci.*, *2*(2), 261–281.
5. Bannai, E., Hao, S., & Song, S.-Y. (1990). Character tables of the association schemes of finite orthogonal groups on the non-isotropic points. *J. Comb. Theory Ser. A*, *54*, 164–200.
6. Cameron, P. J. (1973). Biplanes. *Math. Z.*, *131*, 85–101.
7. Colbourn, C. J., & Dinitz, J. H. (1996). *The CRC handbook of combinatorial designs*. Boca Raton: CRC.
8. Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., & Wilson, R. A. (1985). *Atlas of finite groups*. London: Oxford University Press.
9. Davies, H. (1987). Flag-transitivity and primitivity. *Discret. Math.*, *63*, 91–93.
10. Denniston, R. H. F. (1980). On biplanes with 56 points. *Ars. Comb.*, *9*, 167–179.
11. Hall, M. Jr., Lane, R., & Wales, D. (1970). Designs derived from permutation groups. *J. Comb. Theory*, *8*, 12–22.
12. Huppert, B. (1967). *Endliche Gruppen*. Berlin: Springer.
13. Hussain, Q. M. (1945). On the totality of the solutions for the symmetrical incomplete block designs $\lambda = 2$, $k = 5$ or 6. *Sankhya*, *7*, 204–208.
14. Kantor, W. (1985). Classification of 2-transitive symmetric designs. *Graphs Comb.*, *1*, 165–166.
15. Kleidman, P. B. (1987). *The subgroup structure of some finite simple groups*. PhD thesis, University of Cambridge.
16. Kleidman, P. B. (1987). The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra*, *110*, 172–242.
17. Kleidman, P. B., & Liebeck, M. W. (1990). *The subgroup structure of the finite classical groups*. *London math. soc. lecture note series*, Vol. *129*. Cambridge: Cambridge Univ. Press.
18. Liebeck, M. W. (1985). On the orders of maximal subgroups of the finite classical groups. *Proc. Lond. Math. Soc.*, *50*, 426–446.
19. Liebeck, M. W. (1987). The affine permutation groups of rank 3. *Proc. Lond. Math. Soc.*, *54*, 477–516.
20. Liebeck, M. W., & Saxl, J. (1987). On the orders of maximal subgroups of the finite exceptional groups of Lie type. *Proc. Lond. Math. Soc.*, *55*, 299–330.
21. Liebeck, M. W., Saxl, J., & Seitz, G. M. (1987). On the overgroups of irreducible subgroups of the finite classical groups. *Proc. Lond. Math. Soc.*, *55*, 507–537.
22. Liebeck, M. W., Praeger, C. E., & Saxl, J. (1988). On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Aust. Math. Soc. (Ser. A)*, *44*, 389–396.
23. Liebeck, M. W., Praeger, C. E., & Saxl, J. (1988). On the 2-closures of finite permutation groups. *J. Lond. Math. Soc.*, *37*, 241–264.
24. O'Reilly Regueiro, E. (2005). On primitivity and reduction for flag-transitive symmetric designs. *J. Comb. Theory Ser. A*, *109*, 135–148.
25. O'Reilly Regueiro, E. (2005). Biplanes with flag-transitive automorphism groups of almost simple type, with alternating or sporadic socle. *Eur. J. Comb.*, *26*, 577–584.
26. Salwach, C. J., & Mezzaroba, J. A. (1978). The four biplanes with $k = 9$. *J. Comb. Theory Ser. A*, *24*, 141–145.
27. Saxl, J. (2002). On finite linear spaces with almost simple flag-transitive automorphism groups. *J. Comb. Theory Ser. A*, *100*(2), 322–348.
28. Seitz, G. M. (1973). Flag-transitive subgroups of Chevalley groups. *Ann. Math.*, *97*(1), 27–56.