Finite linear spaces admitting a two-dimensional projective linear group ☆

Weijun Liu

Department of Mathematics, Central South University, Changsha, Hunan 410075, People's Republic of China

Abstract

This article is a contribution to the study of linear spaces admitting a line-transitive automorphism group. We classify such linear spaces where $\mathrm{PSL}(2,q)$, $q > 3$ acts line transitively. We prove that the only cases which arise are projective planes, a Bose–Witt–Shrikhande linear space and one more space admitting $\mathrm{PSL}(2,2^6)$ as a line-transitive automorphism group.
© 2003 Elsevier Inc. All rights reserved.

Keywords: Line-transitive; Linear space; Automorphism; Projective linear group

1. Introduction

A *linear space* $\mathscr{S}$ is a set $\mathscr{P}$ of points, together with a set $\mathscr{L}$ of distinguished subsets called lines such that any two points lie on exactly one line. This paper will be concerned with linear spaces with an automorphism group which is transitive on the lines. This implies that every line has the same number of points and we shall call such a linear space a *regular linear space*. Moreover, we shall also assume that $\mathscr{P}$ is finite and that $|\mathscr{L}| > 1$.

Let G be a line-transitive automorphism group of a linear space $\mathscr{S} = (\mathscr{P}, \mathscr{L})$. Let the parameters of $\mathscr{S}$ be given by (b, v, r, k), where b is the number of lines, v is the number of points, r is the number of lines through a point and k is the number of

points on a line with $k > 2$. By Block [1], transitivity of G on lines implies transitivity of G on points.

The groups of automorphisms of linear spaces which are line-transitive have greatly been considered by Camina, Praeger, Neumann, Spiezia and others (see [4–7,9,19]). Recently, Camina and Spiezia proved the following theorem (see [9]):

Theorem 1.1. *Let G be a simple group acting line transitively, point primitively but not flag transitively on a linear space. Then G is not* $\mathrm{PSL}(n, q)$ *with q odd and* $n \geqslant 13$.

Therefore, it is necessary to consider the case where n is small. In this article, we prove the following theorem:

Main Theorem. *Let* $G = \mathrm{PSL}(2, q)$ *with* $q > 3$ *acting line transitively on a finite linear space* $\mathscr{S}$. *Then* $\mathscr{S}$ *is one of the following cases*:

(i) *A projective plane.*
(ii) *A regular linear space with parameters* $(b, v, r, k) = (32760, 2080, 189, 12)$, *in this case,* $q = 2^6$.
(iii) *A regular linear space with parameters* $(b, v, r, k) = (q^2 - 1, q(q-1)/2, q+1, q/2)$, *where q is a power of* 2. *It is called a Witt–Bose–Shrikhande space.*

The second section introduces notation and contains preliminary results about the group $\mathrm{PSL}(2, q)$ and regular linear spaces. In the third section, we shall prove the main theorem.

We shall continue this work in the forthcoming paper which will deal with other Lie-type simple group of rank one.

2. Some preliminary results

Our conventions for expressing the structure of groups are as follows. If X and Y are arbitrary finite groups, then $X \cdot Y$ denotes an extension of X by Y. The expressions $X : Y$ and $X \cdot Y$ denote split and non-split extensions, respectively. The expression $X \times Y$ denotes the direct product of X and Y. The symbol $[m]$ denotes an arbitrary group of order m while Z_m or simply m denotes a cyclic group of that order. The other notation for group structure is standard. In addition, we use symbol $p^i || n$ to denote $p^i | n$ but $p^{i+1} \nmid n$. Moreover, $\mathrm{Fix}_\Omega(K)$ denotes the set of fixed points in Ω of a subgroup K of $\mathrm{Sym}(\Omega)$. The greatest common divisor of two integers m and n is denoted as (m, n). For a finite transitive permutation group of degree n, the lengths of the orbits of one of the point stabilizer are said to be subdegrees.

We begin by recalling some fundamental properties of $\mathrm{PSL}(2, q)$. Let $G = \mathrm{PSL}(2, q)$ with $q = p^f > 3$, where p is a prime and f is a positive integer.

Lemma 2.1 (Theorem 8.2, Chapter II of [11]). *Let P be a Sylow p-subgroup of G, then*

(i) *P is isomorphic to the additive group of the finite field* $\mathrm{GF}(q)$;

(ii) *G has precisely $q+1$ Sylow p-subgroups and $|N_G(P)| = q(q-1)/d$, where $d = (2, q-1)$;*

(iii) *$P_1 \cap P_2 = \{1\}$, where P_i, $i = 1, 2$, is a Sylow p-subgroup and $P_1 \neq P_2$.*

Lemma 2.2 (Theorem 8.3, Chapter II of [11]).

(i) *G has a cyclic subgroup U of order $(q-1)/d$, where $d = (2, q-1)$;*

(ii) *$U \cap U^g = \{1\}$, where $g \in G$ but $g \notin N_G(U)$;*

(iii) *For any $u \in U$, $u \neq 1$, $N_G(\langle u \rangle)$ is a dihedral group of order $2(q-1)/d$.*

Lemma 2.3 (Theorem 8.4, Chapter II of [11]). (i) *G has a cyclic subgroup S of order $(q+1)/d$, where $d = (2, q-1)$;*

(ii) *$S \cap S^g = \{1\}$, where $g \in G$ but $g \notin N_G(S)$;*

(iii) *For any $s \in S$, $s \neq 1$, $N_G(\langle s \rangle)$ is a dihedral group of order $2(q+1)/d$.*

Lemma 2.4 (Theorem 8.27, Chapter II of [11]). *Every subgroup of $G = \mathrm{PSL}(2, p^f)$ is isomorphic to one of the following groups*:

(1) *An elementary abelian p-group of order at most p^f;*

(2) *A cyclic group of order z, where z divides $(p^f \pm 1)/d$ and $d = (2, q-1)$;*

(3) *A dihedral group of order $2z$, where z is as above;*

(4) *The alternating group A_4, in this case, $p > 2$ or $p = 2$ and $2 | f$;*

(5) *The symmetric group S_4, in this case, $p^{2f} - 1 \equiv 0 \pmod{16}$;*

(6) *The alternating group A_5, in this case, $p = 5$ or $p^{2f} - 1 \equiv 0 \pmod 5$;*

(7) *$Z_p^m : Z_t$, where t divides $(p^m - 1)/d$ and $q - 1$, and $m \leqslant f$;*

(8) *$\mathrm{PSL}(2, p^m)$, where $m | f$, and $\mathrm{PGL}(2, p^m)$, where $2m | f$.*

Remarks. (i) When p is even, S_4 cannot occur and so apart from the groups in (1) and (7) every subgroup of G has precisely one conjugacy class of involutions. When p is odd, every subgroup of G has precisely one conjugacy class of involutions except those described in (3), with z even, and (5) and $\mathrm{PGL}(2, p^m)$.

(ii) For a Sylow p-subgroup P, the normalizer $N_G(P)$ is a group of type (7) with $t = (p^f - 1)/d$, where $d = (2, q-1)$. For $U \cong Z_{(q-1)/d}$, with $d = (2, q-1)$, a group of type (2) as in Lemma 2.2, $N_G(U)$ is a dihedral group of type (3). For $S \cong Z_{(q+1)/d}$, with $d = (2, q-1)$, a group of type (2) as in Lemma 2.3, $N_G(S)$ is a dihedral group of type (3). Clearly, by Lemma 2.4, $N_G(P)$, $N_G(U)$ and $N_G(S)$ are maximal in $\mathrm{PSL}(2, q)$.

(iii) Let i be an involution of G. By Theorems 8.3 and 8.4, Chapter II of [11], we have $|N_G(\langle i \rangle)| = q - \varepsilon$, where $\varepsilon = \pm 1$ and $4 | (q - \varepsilon)$. When q is even, we have $|N_G(\langle i \rangle)| = q$.

Lemma 2.5 (See Praeger and Xu [18] and Faradzev and Ivanov [10]). *Let $G = \text{PSL}(2, q)$ acting on the set of cosets of its subgroup $H \cong D_h$, where $h = 2(q - \varepsilon)/d$ and $\varepsilon = \pm 1$ and $d = (2, q - 1)$. Then the subdegrees are as presented in* Table 1, *where a^b means that the subdegree a appears with multiplicity b.*

From now on we suppose that G is a line-transitive automorphism group of a linear space $\mathscr{S} = (\mathscr{P}, \mathscr{L})$ with parameters (b, v, r, k) and $k > 2$. Recall the basic equalities and inequalities for linear spaces.

$$vr = bk, \tag{1}$$

$$v = r(k - 1) + 1, \tag{2}$$

$$b \geqslant v \quad \text{(Fisher's inequality)}, \tag{3}$$

with equality if and only if the linear space is a projective plane.

Note that (2) implies that v and r are coprime. Let

$$b^{(v)} = (b, v), \quad b^{(r)} = (b, v - 1), \quad k^{(v)} = (k, v), \quad \text{and} \quad k^{(r)} = (k, v - 1).$$

Obviously,

$$k = k^{(v)}k^{(r)}, \quad b = b^{(v)}b^{(r)}, \quad r = b^{(r)}k^{(r)}, \quad \text{and} \quad v = b^{(v)}k^{(v)}.$$

In terms of these parameters, Fisher's inequality becomes $b^{(r)} \geqslant k^{(v)}$ with equality if and only if the linear space is a projective plane.

For a line L, let G_L be the setwise stabilizer of L in G.

The observation used often in this article is that if an involution in G does not fix a point then G acts flag transitively, see [8]. In particular, if $G = \text{PSL}(2, q)$ is flag-transitive on $\mathscr{S}$, then by [2] or [3] $\mathscr{S}$ is a Witt–Bose–Shrikhande linear space. Hence, we can ignore this possibility, and assume that every involution fixes a point.

We collect some results which are useful for the study of line-transitive linear spaces.

Lemma 2.6 (Lemma 2 of [8]). *Let G act as a line-transitive automorphism group of a linear space $\mathscr{S}$. Let L be a line and H a subgroup of G_L. Assume that H satisfies the following two conditions:*

(i) $|\text{Fix}_{\mathscr{P}}(H) \cap L| \geqslant 2$ *and*
(ii) *if $K \leqslant G_L$ and $|\text{Fix}_{\mathscr{P}}(K) \cap L| \geqslant 2$ and K is conjugate to H in G then H is conjugate to K in G_L.*

Table 1

H	q	Subdegrees
$D_{2(q-1)}$	Even	$1, (q-1)^{q/2-1}, 2(q-1)$
$D_{2(q+1)}$	Even	$1, (q+1)^{q/2-1}$
$D_{(q\pm1)}$	$q \equiv \pm 3 \pmod 8$	$1, (\frac{q\pm1}{4})^2, (\frac{q\pm1}{2})^{(q\pm1)/2-2}, (q\pm1)^{(q+2\mp5)/4}$
$D_{(q\pm1)}$	$q \equiv \mp 1 \pmod 8$	$1, (\frac{q\pm1}{4})^2, (\frac{q\pm1}{2})^{(q\pm1)/2-2}, (q\pm1)^{(q+2\mp5)/4}$

Then either (a) $\mathrm{Fix}_{\mathscr{P}}(H) \subseteq L$ or (b) *the induced structure on* $\mathrm{Fix}_{\mathscr{P}}(H)$ *is also a regular linear space with parameters* (b_0, v_0, r_0, k_0), *where* $v_0 = |\mathrm{Fix}_{\mathscr{P}}(H)|$, $k_0 = |\mathrm{Fix}_{\mathscr{P}}(H) \cap L|$. *Further,* $N_G(H)$ *acts as a line-transitive group on this linear space.*

Lemma 2.7 (Lemma 2.6 of [16]). *Let G act as a line-transitive automorphism group of a linear space* $\mathscr{S}$. *Let L be a line and v even. Assume that there exists a 2-subgroup P of order 2 of* G_L *such that* $\mathrm{Fix}_{\mathscr{P}}(P) \subseteq L$. *Then k divides v and G is flag-transitive.*

Lemma 2.8 (Lemma 2.7 of [16]). *Let G act as a line-transitive automorphism group of a linear space* $\mathscr{S}$. *Let L be a line and let i be an involution of* G_L. *Assume that* G_L *has a unique conjugacy class of involutions. If*

$$|\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle) \cap L| \geqslant 2$$

and v is even, then G is flag-transitive or the induced structure on $\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)$ *is a regular linear space with parameters* (b_0, v_0, r_0, k_0), *where* $v_0 = |\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)|$, $k_0 = |\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle) \cap L|$. *Further,* $N_G(\langle i \rangle)$ *acts as a line-transitive group on this linear space.*

Lemma 2.9 (Lemma 9 of [21]). *Let G act line transitively on a linear space* $\mathscr{S}$. *Let K be a subgroup of G. If* $K \nleqslant G_L$ *for any line* $L \in \mathscr{L}$, *and* $K \leqslant G_\alpha$ *for some point* $\alpha \in \mathscr{P}$, *then* $N_G(K) \leqslant G_\alpha$.

Lemma 2.10 (Lemma 2.8 of [16]). *Let G act line transitively on a linear space* $\mathscr{S}$. *If there exists a prime number p such that* $p | b$ *but* $p \nmid v$, *then for some* $\alpha \in \mathscr{P}$, $N_G(P) \leqslant G_\alpha$, *where P is a Sylow p-subgroup of G.*

Lemma 2.11 (Lemma 3.8 of [15]). *Let G act line transitively on a linear space* $\mathscr{S}$. *Assume that P is a Sylow p-subgroup of* G_α *for some* $\alpha \in \mathscr{P}$. *If P is not a Sylow p-subgroup of G, then there exists a line L through* α *such that* $P \subseteq G_L$.

The following result of Manning (see Theorem XIV of [17]) will prove useful in calculating the number of fixed points of an element.

Lemma 2.12 (Lemma 2.1 of [18]). *Let G be a transitive group on* Ω, *let* $H = G_\alpha$ *for some* $\alpha \in \Omega$, *and let* $K \leqslant H$. *If the set of G-conjugates of K which are contained in H form t conjugacy classes* $C_1, C_2, \ldots, C_t$ *with respect to conjugation in H, then K fixes*

$$\sum_{i=1}^{t} |N_G(K_i) : N_H(K_i)|$$

points of Ω, *where* $K_i \in C_i$ *for* $1 \leqslant i \leqslant t$. *In particular, if* $t = 1$, *that is, if every G-conjugate of K in H is conjugate to K in H, then K fixes* $|N_G(K) : N_H(K)|$ *points of* Ω.

Note that $|N_G(K_i)|$ is constant (equal to $|N_G(K)|$) since G is transitive on the set of G-conjugates of K.

Lemma 2.13. *Let G act line transitively on a linear space $\mathcal{S} = (\mathcal{P}, \mathcal{L})$. Let i be an involution of G_L, where L is a line of $\mathcal{S}$. Assume that i has at least two fixed points. Then*

$$k > \frac{v - |\mathrm{Fix}_{\mathcal{P}}(\langle i \rangle)|}{|\mathrm{Fix}_{\mathcal{L}}(\langle i \rangle)|}. \tag{4}$$

Proof. Consider the cycle decomposition of i acting on $\mathcal{P}$. We know that i has $(v - |\mathrm{Fix}_{\mathcal{P}}(\langle i \rangle)|)/2$ cycles of length 2. Write $|\mathrm{Fix}_{\mathcal{L}}(\langle i \rangle)| = e$. Then i fixes e lines of $\mathcal{S}$, say L_j, where $1 \leqslant j \leqslant e$. Let m_j denote the number of 2-cycles of i which lie in L_j, where $1 \leqslant j \leqslant e$. Then

$$2 \sum_{j=1}^{e} m_j = v - |\mathrm{Fix}_{\mathcal{P}}(\langle i \rangle)|.$$

Since i has at least two fixed points, we have

$$ek > 2 \sum_{j=1}^{e} m_j.$$

Thus,

$$k > \frac{v - |\mathrm{Fix}_{\mathcal{P}}(\langle i \rangle)|}{|\mathrm{Fix}_{\mathcal{L}}(\langle i \rangle)|}. \qquad \square$$

The following lemma is useful for the proof of the main theorem.

Lemma 2.14 (Le [13]). *The diophantine equation $x^2 = 4q^m + 4q^n + 1$, where q is a prime and $m \geqslant n$, has exactly the following solutions: $(m, n, x, q) = (2n, n, 2q^n + 1, q)$, $(1, 1, 5, 3), (3, 1, 11, 3), (1, 2, 5, 2), (3, 2, 7, 2)$ or $(7, 2, 23, 2)$.*

3. The proof of the main theorem

Firstly, we shall prove the following proposition.

Proposition 3.1. *Let G be a group of automorphisms of a linear space $\mathcal{S} = (\mathcal{P}, \mathcal{L})$. Suppose that $\mathcal{S}$ is not a projective plane and $G = \mathrm{PSL}(2, p^f)$ with $q = p^f > 3$. If G is line-transitive, then G is point-primitive. Further, for a point α of $\mathcal{P}$, the stabilizer G_α is isomorphic to one of the following groups: $N_G(P), Z_{(q-1)/d} : 2$ or $Z_{(q+1)/d} : 2$, where P is a Sylow p-subgroup of G and $d = (2, q - 1)$.*

Proof. Since G is line-transitive and $\mathcal{S}$ is not a projective plane, we know that there exists a prime t such that $t | b$ but $t \nmid v$. In fact, every prime divisor of $b^{(r)}$ satisfies the

above condition. Thus, by Lemma 2.10 we have $N_G(T) \leqslant G_\alpha$, where T is a Sylow t-subgroup of G and $\alpha \in \mathscr{P}$. It is clear that b divides $|G| = q(q^2 - 1)/d$, where $d = (2, q - 1)$. Hence, t divides $q(q^2 - 1)/d$. Now we divide the proof into three cases:

(i)   If $t | q$, then $t = p$ and $N_G(T)$ is a maximal subgroup of G by Remark (ii). Hence G is point-primitive.

(ii) If $t > 2$ and t divides $(q - \varepsilon)/d$, where $\varepsilon = \pm 1$, then by Lemmas 2.2 and 2.3 and Remark (ii), $N_G(T)$ is a maximal group of G. It means that G is point-primitive.

(iii) If $t = 2$ and t divides $(q - \varepsilon)/d$, where $\varepsilon = \pm 1$ and q is odd, then let $2^a || (q - \varepsilon)$, where $a \geqslant 2$ and $\varepsilon = \pm 1$. Then $2^a ||| G|$ and a 2-Sylow subgroup is the dihedral group $T = Z_{2^{a-1}} : 2$ by Theorem 8.10 of [11]. Since

$$Z_{2^{a-1}} \overset{\text{char}}{\leqslant} Z_{(q-\varepsilon)/2} \trianglelefteq Z_{(q-\varepsilon)/2} : 2,$$

we have $Z_{(q-\varepsilon)/2} : 2 \leqslant N_G(Z_{2^{a-1}})$. If $Z_{2^{a-1}} \nleqslant G_L$ for any line $L \in \mathscr{L}$, then by Lemma 2.9, G_α is maximal in G (recall that $Z_{2^{a-1}} \leqslant T \leqslant N_G(T) \leqslant G_\alpha$). Hence G is point-primitive. Therefore, we can assume that $Z_{2^{a-1}} \leqslant G_L$ for some line L. The assumptions $t | b$ and $t \nmid v$ imply $2 || b = b^{(r)} b^{(v)}$ and hence $2 || b^{(r)}$. If there is an odd divisor of $b^{(r)}$, then this case returns to the above case (ii). Hence, we can assume that $b^{(r)} = 2$. Since $\mathscr{S}$ is not a projective plane, Fisher's inequality implies $k^{(v)} = 1$. Since $bk = vr$, we have

$$\frac{|G|}{|G_L|} k^{(v)} k^{(r)} = \frac{|G|}{|G_\alpha|} b^{(r)} k^{(r)},$$

that is

$$|G_\alpha| k^{(v)} = b^{(r)} |G_L|.$$

Hence $|G_\alpha| = 2|G_L|$. Note that every Sylow 2-subgroup of G_L is a cyclic group and $p \neq 2$. Therefore, by Lemma 2.4 we get $G_L = Z_h$ and $G_\alpha = Z_h : 2$, where h divides $(q - \varepsilon)/2$ and $2^{a-1} || h$. In this case, G_L has exactly one involution i. Since h is even, the dihedral group $G_\alpha = Z_h : 2$ has three conjugacy classes of involutions. If we choose generators σ, τ with $\langle \sigma \rangle = Z_h$ and $\langle \sigma, \tau \rangle = G_\alpha$, then $i = \sigma^{h/2}$ is a central involution of G_α, whereas τ and $\sigma\tau$ lie in two different G_α-conjugacy classes of size $h/2$ each. Thus, by Lemma 2.12 we get

$$|\text{Fix}_{\mathscr{P}}(\langle i \rangle)| = \frac{q - \varepsilon}{2h} + 2 \cdot \frac{q - \varepsilon}{4} = \frac{(q - \varepsilon)(h + 1)}{2h}.$$

By Lemma 2.6, we know that either $\text{Fix}_{\mathscr{P}}(\langle i \rangle) \subseteq L$ or the induced structure on $\text{Fix}_{\mathscr{P}}(\langle i \rangle)$ is a regular linear space with parameters (b_0, v_0, r_0, k_0), where $v_0 = |\text{Fix}_{\mathscr{P}}(\langle i \rangle)|$ and $k_0 = |\text{Fix}_{\mathscr{P}}(\langle i \rangle) \cap L|$ and $N_G(\langle i \rangle)$ acts line transitively on this linear space. Thus, if the latter holds, then v_0 divides $|N_G(\langle i \rangle)|$, that is $h + 1$ divides $2h$. This forces that $h = 1$, which contradicts $h \geqslant 2$. Hence $\text{Fix}_{\mathscr{P}}(\langle i \rangle) \subseteq L$. In order to prove that our proposition is true, we use reduction to absurdity. Assume that G is point-imprimitive. Namely, G_α is not maximal in G (it is the case where $G_\alpha < Z_{(q-\varepsilon)/2} : 2$). Then there exists an imprimitive block C of G, such that $\alpha \in C$ and $G_C = Z_{(q-\varepsilon)/2} : 2$. Note that we can assume that the involution i lies in the center

of G_C. Thus $C \subseteq \mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)$. In fact, for any $\beta \in C$, there is an element $g \in G_C$ such that $\beta = \alpha^g$. Thus,

$$\beta^i = \alpha^{gi} = \alpha^{ig} = \alpha^g = \beta, \quad \text{that is,} \quad \beta \in \mathrm{Fix}_{\mathscr{P}}(\langle i \rangle).$$

Therefore, $C \subseteq \mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)$ and so $C \subseteq L$. This means that every line of $\mathscr{S}$ is uniquely determined by some imprimitive block, which leads to $b < v$, contradicting the fact that $b \geqslant v$. This completes the proof of our proposition. $\quad\square$

Now we can prove our main theorem stated in the introduction.

Proof of the Main Theorem. Suppose that $\mathscr{S}$ is not a projective plane. Then $b^{(r)} > 1$ and so for any prime divisor t of $b^{(r)}$, $N_G(T) \leqslant G_\alpha$, where T is a Sylow t-subgroup of G and $\alpha \in \mathscr{P}$. By Proposition 3.1, G_α is a group $N_G(P)$, $Z_{(q-1)/d} : 2$ or $Z_{(q-1)/d} : 2$, where $d = (2, q-1)$. By [12], $G_\alpha \ncong N_G(P)$. Now we divide the proof into subcases according to the parity of q, the type of a stabilizer of a point, and the number of conjugacy classes of involutions in a line-stabilizer.

(i) *q is even*. In this case, G_α is isomorphic to $Z_{(q+1)} : 2$ or $Z_{(q-1)} : 2$.

If $G_\alpha \cong Z_{(q+1)} : 2$, then $v = q(q-1)/2$ and $v - 1 = (q+1)(q-2)/2$. Since $|G_\alpha|$ and v are all even, we have G_α contains an involution i which fixes at least one more point of $\mathscr{S}$. Let L be the line containing α and this point. Then $i \in G_\alpha \cap G_L$ and $|\mathrm{Fix}_{\mathscr{P}}(H) \cap L| \geqslant 2$, where $H = \langle i \rangle$. According to Remark (iii) after Lemma 2.4, $|N_G(H)| = q$. Note that $G_\alpha \cong Z_{(q+1)} : Z_2$ has a unique conjugacy class of involutions (since q is even), and $|N_{G_\alpha}(H)| = 2$, and so by Lemma 2.12,

$$|\mathrm{Fix}_{\mathscr{P}}(H)| = |N_G(H) : N_{G_\alpha}(H)| = q/2. \tag{5}$$

Suppose that G_L has a unique conjugacy class of involutions. By Lemma 2.8, either G is flag-transitive or there exists a regular linear space with parameters (b_0, v_0, r_0, k_0), where $v_0 = |\mathrm{Fix}_{\mathscr{P}}(H)|$, $k_0 = |\mathrm{Fix}_{\mathscr{P}}(H) \cap L|$, and $N_G(H)$ acts line transitively on this regular linear space. If the latter holds, then $b_0 k_0 (k_0 - 1) = v_0 (v_0 - 1)$. But $v_0 = q/2$ and $b_0 = v_0$ or $2v_0$, and so $b_0 k_0 (k_0 - 1) \neq v_0 (v_0 - 1)$, a contradiction. Therefore G is flag-transitive. By [3], $\mathscr{S}$ must be a Witt–Bose– Shrikhande linear space with $b = q^2 - 1$. Thus $|G_L| = |G|/b = q$, and so G_L is an elementary abelian 2-group of order $q \geqslant 4$. This contradicts our hypothesis. Suppose that G_L has at least two conjugacy classes of involutions. Checking the groups in Lemma 2.4, we find that G_L is isomorphic to $(Z_2)^m : Z_l$ (note that here q is even), where l divides $2^m - 1$ and $l < 2^m - 1$. Since l is odd, the involutions of G_L all lie in Z_2^m. Clearly, the centralizer of an involution of G_L is Z_2^m, so the length of the conjugacy class of an involution of G_L is l, and hence G_L has exactly $e := (2^m - 1)/l$ conjugacy classes of involutions. Let $i_1, i_2, \ldots, i_e$ be representatives of these classes. Since $Z_2^f \leqslant N_G(\langle i_j \rangle)$, Lemma 2.4 implies that $N_G(\langle i_j \rangle) = Z_2^f$. By Lemma 2.12,

$H = \langle i \rangle$ fixes exactly

$$\sum_{j=1}^{e} |N_G(i_j) : N_{G_L}(i_j)| = \frac{2^m - 1}{l} \times \frac{2^f}{2^m} = \frac{2^{f-m}(2^m - 1)}{l} =: c$$

lines, say $L_1, L_2, \ldots, L_c$. By (5),

$$|\text{Fix}_{\mathscr{P}}(H)| = q/2,$$

and so we know that i has $(v - q/2)/2$ cycles of length 2 on $\mathscr{P}$. Let m_j denote the number of 2-cycles of i which lie in L_j, where $1 \leqslant j \leqslant c$. Then

$$2 \sum_{j=1}^{c} m_j = v - q/2$$

and so

$$ck \geqslant v - q/2,$$

that is

$$k \geqslant \frac{(v - q/2)l}{2^{f-m}(2^m - 1)} = \frac{(q(q-1)/2 - q/2)l}{2^{f-m}(2^m - 1)} = \frac{2^m(2^{f-1} - 1)l}{2^m - 1}.$$

Since

$$k(k - 1) = v(v - 1)/b = |G_L|(v - 1)/|G_\alpha|, \tag{6}$$

we have

$$k(k - 1) = 2^{m-1}(2^{f-1} - 1)l. \tag{7}$$

Therefore,

$$2^{m-1}(2^{f-1} - 1)l \geqslant \frac{2^m(2^{f-1} - 1)l}{2^m - 1}\left(\frac{2^m(2^{f-1} - 1)l}{2^m - 1} - 1\right).$$

Hence,

$$\frac{2^{m+1}(2^{f-1} - 1)l}{2^m - 1} \leqslant 2^m + 1 \tag{8}$$

and so

$$l \leqslant \frac{2^{2m} - 1}{2^{m+1}(2^{f-1} - 1)} < \frac{2^{m-1}}{2^{f-1} - 1} \leqslant 2.$$

This forces that $l = 1$. By (8) we get $f = m$. Again by (7) we get

$$k^2 - k - 2^{f-1}(2^{f-1} - 1) = 0. \tag{9}$$

Thus $k = q/2$ and so $k|v$. This means that G is flag-transitive. By [3], $\mathscr{S}$ must be a Witt–Bose–Shrikhande linear space. If $G_\alpha \cong Z_{(q-1)} : 2$, then $v = q(q + 1)/2$ and $v - 1 = (q - 1)(q + 2)/2$. Suppose that G_L has a unique conjugacy class of involutions. Let i be an involution of G_L and $H = \langle i \rangle$. Then by Lemma 2.8 we know that either G is flag-transitive or there exists a regular linear space with parameters (b_0, v_0, r_0, k_0), where $v_0 = |\text{Fix}_{\mathscr{P}}(H)|$, $k_0 = |\text{Fix}_{\mathscr{P}}(H) \cap L|$, and $N_G(H)$

acts line transitively on this regular linear space. By [2] or [3], G is not flag-transitive. Hence the latter occur. As in the case $G_\alpha \cong Z_{(q+1)} : 2$, we get $v_0 = |\text{Fix}_{\mathscr{P}}(H)| = q/2$. Since b_0 divides $|N_G(H)| = q$ and $b_0 \geqslant v_0$, we have $b_0 = v_0$ or $2v_0$, which contradicts $b_0 k_0(k_0 - 1) = v_0(v_0 - 1)$ (note that here v_0 is even). Suppose that G_L has at least two conjugacy classes of involutions. Then $G_L = Z_2^m : Z_l$. It is analogous to the case where $G_\alpha \cong Z_{(q+1)} : 2$ to get

$$k \geqslant \frac{2^{f+m-1}l}{2^m - 1}.$$

By (6), we have

$$k(k - 1) = 2^{m-1}(2^{f-1} + 1)l. \tag{10}$$

Therefore,

$$2^{m-1}(2^{f-1} + 1)l \geqslant \frac{2^{f+m-1}l}{2^m - 1}\left(\frac{2^{f+m-1}l}{2^m - 1} - 1\right).$$

Namely,

$$\frac{(2^m - 1)(2^{f-1} - 1)}{2^f} \geqslant \frac{2^{f+m-1}l}{2^m - 1} - 1.$$

Therefore,

$$\frac{2^{f+m-1}l}{2^m - 1} \leqslant \frac{(2^{f-1} + 1)(2^m - 1)}{2^f} + 1.$$

It follows that

$$2^{f+m-1}l \leqslant \frac{(2^{f-1} + 1)(2^m - 1)^2}{2^f} + 2^m - 1 < \frac{2^{f-1} + 1}{2^{f-2m}} + 2^m.$$

Thus, we have

$$l < \frac{2^{f-1} + 1}{2^{2f-m-1}} + \frac{1}{2^{f-1}} \leqslant \frac{2^{f-1} + 1}{2^{f-1}} + \frac{1}{2^{f-1}} \leqslant 2.$$

This forces that $l = 1$. Hence,

$$k(k - 1) = 2^{m-1}(2^{f-1} + 1) \tag{11}$$

and so the discriminant of (11)

$$\varDelta = 2^{f+m} + 2^{m+1} + 1 = x^2$$

for some positive integer x. By Lemma 2.14, we get

$$(m, f, x) = (m, m, 2^m + 1), \ (3, 0, 5), \ (3, 2, 7) \ \text{or} \ (3, 6, 23).$$

Remember that $f \geqslant m$ and k is a positive integer. Thus, the equation (11) has solutions $k = 2^{m-1} + 1$ or 12. When $k = 2^{m-1} + 1$, $k - 1$ does not divide $v - 1$ (since $k > 2$), a contradiction. Hence $k = 12$ and $f = 6$. We get a regular linear space with parameters $(b, v, r, k) = (32760, 2080, 189, 12)$. In this case, $G = \text{PSL}(2, 2^6)$.

(ii) *q is odd*: Again, G_α is a group $N_G(P)$ or $Z_{(q-\varepsilon)/2} : 2$, where $\varepsilon = \pm 1$. By Kantor's result [12], $G_\alpha \ncong N_G(P)$ and hence G_α is isomorphic to $Z_{(q-\varepsilon)/2} : 2$, and $v = (q+\varepsilon)q/2$ and $v - 1 = (q-\varepsilon)(q+2\varepsilon)/2$, where $\varepsilon = \pm 1$. We divide this case into two subcases:

(a) *G_L contains a unique conjugacy class of involutions*: Since q is odd, by [3], G is not flag-transitive. Thus by [8], every involution of G fixes at least a point of $\mathscr{S}$. Let i be an involution of G_α. Clearly, i fixes at least a line of $\mathscr{S}$, say L. Hence $i \in G_L \cap G_\alpha$. If $4 | (q+\varepsilon)$, then G_α has a unique conjugacy class of involutions, and so by Lemma 2.12, we have

$$|\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)| = |N_G(\langle i \rangle) : N_{G_\alpha}(\langle i \rangle)| = (q+\varepsilon)/2.$$

Let $H = \langle i \rangle$, then by Lemma 2.8, either G is flag-transitive or there exists a regular linear space with parameters (b_0, v_0, r_0, k_0), where $v_0 = |\mathrm{Fix}_{\mathscr{P}}(H)|$, $k_0 = |\mathrm{Fix}_{\mathscr{P}}(H) \cap L|$, and $N_G(H)$ acts line transitively on this regular linear space. By [3], G is not flag-transitive. Thus, the latter case must hold. Since H fixes every point of $\mathrm{Fix}_{\mathscr{P}}(H)$, we have b_0 divides $|N_G(H)|/|H|$. This leads to $b_0 = v_0 = (q+\varepsilon)/2$, i.e., the parameters of a projective plane, and hence $v_0 = k_0(k_0 - 1) + 1$. But v_0 is even, a contradiction. If $4 | (q-\varepsilon)$, then G_α has three conjugacy classes of involutions. Thus, by Lemma 2.12 we get

$$|\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)| = 2 \cdot (q-\varepsilon)/4 + 1 = (q-\varepsilon)/2 + 1. \tag{12}$$

Let $H = \langle i \rangle$, then by Lemma 2.6, either $\mathrm{Fix}_{\mathscr{P}}(H) \subseteq L$ or there exists a regular linear space with parameters (b_0, v_0, r_0, k_0), where $v_0 = |\mathrm{Fix}_{\mathscr{P}}(H)|$, $k_0 = |\mathrm{Fix}_{\mathscr{P}}(H) \cap L|$, and $N_G(H)$ acts line transitively on this regular linear space. Since $(q-\varepsilon)/2 + 1$ does not divide $q - \varepsilon = |N_G(H)|$, we have $\mathrm{Fix}_{\mathscr{P}}(H) \subseteq L$. This implies that apart from L, every line fixed by $\langle i \rangle$ either does not contain any point fixed by $\langle i \rangle$ or contains exactly one point fixed by $\langle i \rangle$. Suppose that the lines fixed by $\langle i \rangle$, except for L, do not contain any point fixed by $\langle i \rangle$, then $\langle i \rangle$ fixes exactly $(v - k)/k + 1$ lines of $\mathscr{S}$, which leads to $k | v$. Therefore, G is flag-transitive. By [3], this cannot occur. Hence, except for L, every line fixed by $\langle i \rangle$ contains precisely one point fixed by $\langle i \rangle$. It follows that i fixes exactly $(v - k)/(k - 1) + 1 = (v - 1)/(k - 1) = r$ lines of $\mathscr{S}$, that is, $|\mathrm{Fix}_{\mathscr{L}}(\langle i \rangle)| = (v - 1)/(k - 1)$. Since G_L has a unique conjugacy class of involutions, we have, by Theorem 3.5 of [20], that $N_G(\langle i \rangle)$ acts transitively on the set of lines fixed by $\langle i \rangle$. This leads to $|\mathrm{Fix}_{\mathscr{L}}(\langle i \rangle)| = (v - 1)/(k - 1)$ divides $|N_G(\langle i \rangle)|$. Note that here

$$\frac{v - 1}{k - 1} = \frac{(q-\varepsilon)(q+2\varepsilon)}{2(k - 1)}$$

and $|N_G(H)| = q - \varepsilon$, and q is odd, and so $q + 2\varepsilon$ divides $k - 1$. Since $b > v$, it follows that $r > k$ and so $r \geqslant k + 1$, that is

$$\frac{v - 1}{k - 1} \geqslant k + 1.$$

Hence $v \geqslant k^2$. This conflicts with $(q+2\varepsilon)|(k - 1)$ (since $q \geqslant 5$).

(b) *G_L has at least two conjugacy classes of involutions*: According to Remark (i) after Lemma 2.4, G_L is isomorphic to a group S_4, $PGL(2, p^m)$, where $2m$ divides f, or $Z_h : 2$, where h is even and divided $(q \pm 1)/2$. If $G_L \cong S_4$, then $b = |G|/|G_L| = q(q^2 - 1)/48$ and $b^{(r)} = (v - 1, b) = ((q - \varepsilon)(q + 2\varepsilon)/2, q(q^2 - 1)/48)$. Hence if $2||(q - \varepsilon)$, then $b^{(r)} = (q - \varepsilon)/2$ or $(q - \varepsilon)/6$; if $2||(q + \varepsilon)$, then $b^{(r)} = (q - \varepsilon)/8$ or $(q - \varepsilon)/24$. By Corollary 3.2(ii) of [14], $b^{(r)}$ divides the lengths of every orbit of G_α acting on $\mathscr{P} - \{\alpha\}$. Thus, by Lemma 2.5 $b^{(r)} \neq (q - \varepsilon)/2$ and $(q - \varepsilon)/6$. Hence we must have $2||(q + \varepsilon)$ and $4|(q - \varepsilon)$. Consider the numbers of points and lines fixed by i, respectively. Since $4|(q - \varepsilon)$, we have, by (12),

$$|\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)| = (q - \varepsilon)/2 + 1.$$

Since S_4 contains two conjugacy classes of involutions, by Lemma 2.12 and Remark (iii) after Lemma 2.4, we have

$$|\mathrm{Fix}_{\mathscr{L}}(\langle i \rangle)| = (q - \varepsilon)/8 + (q - \varepsilon)/4 = 3(q - \varepsilon)/8.$$

Consequently, by Lemma 2.13 we get

$$\begin{aligned}
k &\geqslant \frac{v - (q - \varepsilon)/2 - 1}{3(q - \varepsilon)/8} \\
&= \frac{(q - \varepsilon)(q + 2\varepsilon)/2 - (q - \varepsilon)/2}{3(q - \varepsilon)/8} \\
&= 4(q + \varepsilon 2 - 1)/3.
\end{aligned}$$

Thus

$$k(k - 1) \geqslant 4(q + 2\varepsilon - 1)/3(4(q + 2\varepsilon - 1)/3 - 1). \tag{13}$$

By (6), we have

$$k(k - 1) = |G_L|(v - 1)/|G_\alpha| = 12(q + 2\varepsilon). \tag{14}$$

Therefore, by (13) and (14), when $\varepsilon = +1$, we get

$$4q^2 - 22q - 53 < 0$$

and when $\varepsilon = -1$, we get

$$4q^2 - 54q + 99 < 0.$$

Recall that $q > 3$ and q odd and $2||(q + \varepsilon)$. We get $(q, \varepsilon) = (5, +1), (7, -1)$ and $(11, -1)$. But in these cases, Eq. (14) has no integer solutions. If $G_L \cong PGL(2, p^m)$, where $2m|f$, then $b = |G|/|G_L| = \frac{q(q^2 - 1)}{2p^m(p^{2m} - 1)}$ and $b^{(r)} = (v - 1, b) = (q - 1)/(p^{2m} - 1)$ or $(q + 1)/2$ according to ε is $+1$ or -1 (note that here $p^{2m} - 1$ divides $q - 1$). By Lemma 2.5 and Corollary 3.2(ii) of [14], $b^{(r)} = (q - 1)/(p^{2m} - 1)$. In this case, $k^{(v)} = p^m$, and so by (6) we have

$$k^{(r)}(p^m k^{(r)} - 1) = (p^{2m} - 1)(p^f + 2)/2.$$

Write $k^{(r)} = A$ and $q = p^f = p^{2mn} = Q^{2n}$, where $Q = p^m > 1$. Then

$$2QA^2 - 2A + Q^{2n} - 2Q^2 + 2 = Q^{2n+2}.$$

Write $A = BQ + 1$. We get

$$2B^2Q^2 + 4BQ + 2 - 2B + Q^{2n-1} - 2Q = Q^{2n+1}.$$

Write $B = CQ + 1$. Then we get

$$2C^2Q^3 + 4CQ^2 + 2Q + 4CQ + 2 - 2C + Q^{2n-2} = Q^{2n}.$$

Write $C = DQ + 1$. Then we get

$$2D^2Q^4 + 4DQ^3 + 2Q^2 + 4Q + 4DQ^2 + 6 + 4DQ$$
$$- 2D + Q^{2n-3} = Q^{2n-1}.$$

We continue this process and eventually find positive integers L and M such that

$$2L^2Q^{2n+1} - 2L + M = Q^2.$$

Clearly, when $n \geqslant 1$ and $Q > 1$, $2L^2Q^{2n+1} - 2L + M > Q^2$, and hence we get a contradiction. If $G_L \cong Z_h : 2$, where $h | (q \pm 1)/2$ and h even, then $b = |G|/|G_L| = q(q^2 - 1)/(2h)$ and $b^{(r)} = (v - 1, b) = (q - \varepsilon)/2$ or $(q - \varepsilon)/(2h)$ according to $2 || (q - \varepsilon)$ or $2 || (q + \varepsilon)$. By Corollary 3.2(ii) of [14] and Lemma 2.5, we know that $b^{(r)} = (q - \varepsilon)/(2h)$ and so $4 | (q - \varepsilon)$, $k^{(v)} = 1$. This leads to

$$k(k - 1) = h(q + 2\varepsilon). \tag{15}$$

On the other hand, we consider the number of lines fixed by $\langle i \rangle$. By Lemma 2.12, we get

$$|\mathrm{Fix}_{\mathscr{L}}(\langle i \rangle)| = 2(q - \varepsilon)/4 + (q - \varepsilon)/(2h).$$

Since $4 | (q - \varepsilon)$, we have, by (12),

$$|\mathrm{Fix}_{\mathscr{P}}(\langle i \rangle)| = (q - \varepsilon)/2 + 1.$$

Thus, by Lemma 2.13

$$k > \frac{(q - \varepsilon)(q + 2\varepsilon)/2 - (q - \varepsilon)/2}{(q - \varepsilon)/2 + (q - \varepsilon)/(2h)} = \frac{h(q + 2\varepsilon - 1)}{1 + h},$$

and so

$$k(k - 1) > \frac{h^2(q + 2\varepsilon - 1)^2}{(1 + h)^2} - \frac{h(q + 2\varepsilon - 1)}{1 + h}.$$

By (15) we get

$$h(q + 2\varepsilon - 1)^2 - (h + 1)^2(q + 2\varepsilon) - (1 + h)(q + 2\varepsilon - 1) < 0.$$

It follows that

$$h(q + 2\varepsilon)(q + 2\varepsilon - 3 - h) - 1 < 0.$$

Therefore, $q + 2\varepsilon - h - 3 \leqslant 0$. Note that h divides $(q - \varepsilon)/2$ and h is even. We get $(q, \varepsilon) = (7, -1)$. By Lemma 15, $(q, k, \varepsilon) = (7, 5, -1)$. In this case, $b^{(r)} = 1$, a contradiction. This completes the proof of the main theorem. $\quad\square$

References

[1] R.E. Block, On the orbits of collineation groups, Math. Z. 96 (1967) 33–49.
[2] F. Buekenhout, A. Delandtsheer, J. Doyen, Finite linear spaces with flag-transitive groups, J. Combin. Theory Ser. A 49 (1988) 268–293.
[3] F. Buekenhout, A. Delandtsheer, J. Doyen, P.B. Kleidman, M.W. Liebeck, J. Saxl, Linear spaces with flag-transitive automorphism groups, Geom. Dedicata 36 (1990) 89–94.
[4] A.R. Camina, Socle of automorphism-groups of linear-spaces, Bull. London. Math. Soc. 28 (1996) 269–272.
[5] A.R. Camina, S. Mischke, Imprimitive automorphism groups of linear spaces, Electron. J. Combin. 3 (1996), #R3.
[6] A.R. Camina, P.M. Neumann, C.E. Praeger, Alternating groups acting on linear spaces, to appear.
[7] A.R. Camina, C.E. Praeger, Line-transitive automorphism groups of linear spaces, Bull. London Math. Soc. 25 (1993) 309–315.
[8] A.R. Camina, J. Siemons, Block transitive automorphisms of $2 - (v, k, 1)$ block designs, J. Combin. Theory Ser. A 51 (1989) 268–276.
[9] A. Camina, F. Spiezia, Sporadic groups and automorphisms of linear spaces, J. Combin. Designs 8 (2000) 353–362.
[10] I.A. Faradzev, A.A. Ivanov, Distance-transitive representations of groups G with $PSL(2, q) \trianglelefteq G \leqslant P\Gamma L(2, q)$, European J. Combin. 11 (1990) 347–356.
[11] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[12] W.M. Kantor, Homogeneous designs and geometric lattices, J. Combin. Theory Ser. A 38 (1985) 66–74.
[13] M.H. Le, The diophantine equation $x^2 = 4q^m + 4q^n + 1$, Proc. Amer. Math. Soc. 106 (1989) 599–604.
[14] H.L. Li, W.J. Liu, Line-primitive linear spaces with $k/(k, v) \leqslant 10$, J. Combin. Theory, Ser. A 93 (2001) 153–167.
[15] W.J. Liu, The Chevalley groups $G_2(2^n)$ and $2 - (v, k, 1)$ designs, Algebra Colloq. 8 (2001) 471–480.
[16] W.J. Liu, H.L. Li, C.G. Ma, Suzuki groups $Sz(q)$ and $2 - (v, k, 1)$ designs, European J. Combin. 22 (2001) 513–519.
[17] W.A. Manning, On the order of primitive groups III, Trans. Amer. Math. Soc. 19 (1918) 127–142.
[18] C.E. Praeger, M.Y. Xu, Vertex-primitive graphs of order a product of two distinct primes, J. Combin. Theory, Ser. B 59 (1993) 245–266.
[19] F. Spiezia, Simple groups and automorphisms of linear spaces, Ph.D. Thesis, University of East Anglia, 1997.
[20] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.
[21] S. Zhou, H. Li, W. Liu, The Ree groups $^2G_2(q)$ and $2 - (v, k, 1)$ block designs, Discrete Math. 224 (2000) 251–258.