The classification of $\frac{3}{2}$-transitive permutation groups and $\frac{1}{2}$-transitive linear groups

Martin W. Liebeck, Cheryl E. Praeger and Jan Saxl

Abstract

A linear group $G \leq \text{GL}(V)$, where $V$ is a finite vector space, is called $\frac{1}{2}$-transitive if all the $G$-orbits on the set of nonzero vectors have the same size. We complete the classification of all the $\frac{1}{2}$-transitive linear groups. As a consequence we complete the determination of the finite $\frac{3}{2}$-transitive permutation groups – the transitive groups for which a point-stabilizer has all its nontrivial orbits of the same size. We also determine the $(k + \frac{1}{2})$-transitive groups for integers $k \geq 2$.

1 Introduction

The concept of a finite $\frac{3}{2}$-transitive permutation group – a non-regular transitive group in which all the nontrivial orbits of a point-stabilizer have equal size – was introduced by Wielandt in his book [16, §10]. Examples are 2-transitive groups and Frobenius groups: for the former, a point-stabilizer has just one nontrivial orbit, and for the latter, every nontrivial orbit of a point-stabilizer is regular. Further examples are provided by normal subgroups of 2-transitive groups; indeed, one of the reasons for Wielandt’s definition was that normal subgroups of 2-transitive groups are necessarily $\frac{3}{2}$-transitive.

Wielandt proved that any $\frac{3}{2}$-transitive group is either primitive or a Frobenius group ([16, Theorem 10.4]). Following this, a substantial study of $\frac{3}{2}$-transitive groups was undertaken by Passman in [13, 14], in particular completely determining the soluble examples. More recent steps towards the classification of the primitive $\frac{3}{2}$-transitive groups were taken in [3] and [8]. In [3] it was proved that primitive $\frac{3}{2}$-transitive groups are either affine or almost simple, and the almost simple examples were determined. For the affine case, consider an affine group $T(V)G \leq \text{AGL}(V)$, where $V$ is a finite vector space, $T(V)$ is the group of translations, and $G \leq \text{GL}(V)$; this group is $\frac{3}{2}$-transitive if and only if the linear group $G$ is $\frac{1}{2}$-transitive – that is, all the orbits of $G$ on the set $V^\sharp$ of nonzero vectors have the same size. The $\frac{1}{2}$-transitive linear groups of order divisible by $p$ (the characteristic of the field over which $V$ is defined) were determined in [8, Theorem 6].

The main result of this paper completes the classification of $\frac{1}{2}$-transitive linear groups. In the statement, by a semiregular group, we mean a permutation group all of whose orbits are regular.

Theorem 1 Let $G \leq \text{GL}(V) = \text{GL}_d(p)$ ($p$ prime) be an insoluble $p'$-group, and suppose $G$ is $\frac{1}{2}$-transitive on $V^\sharp$. Then one of the following holds:

(i) $G$ is semiregular on $V^\sharp$;

(ii) $d = 2$, $p = 11, 19$ or 29, and $\text{SL}_2(5) \triangleleft G \leq \text{GL}_2(p)$;

(iii) $d = 4$, $p = 13$, and $\text{SL}_2(5) \triangleleft G \leq \Gamma\text{L}_2(p^2) \leq \text{GL}_4(p)$.

In (ii) and (iii), the non-semiregular possibilities for $G$ are given in Table 1.
Table 1: Orbit sizes of $\frac{1}{2}$-transitive groups in Theorem 1(ii),(iii)

| $p^d$ | $|G|$ | orbit size on $V^d$ | number of orbits |
|-------|-------|---------------------|-----------------|
| $11^2$ | 600   | 120                 | 1               |
| $19^2$ | 360   | 120                 | 3               |
| $29^2$ | 1080  | 360                 | 1               |
| $13^3$ | 840   | 1680                | 17              |

Remarks

1. In conclusion (i) of the theorem, the corresponding affine permutation group $T(V)G$ (acting on $V$) is a Frobenius group, and $G$ is a Frobenius complement (see Proposition 2.1 for the structure of these).

2. In conclusion (ii), $F^*pR$ acts transitively on $V^d$, where $R = SL_2(5)$ and $F^*p$ is the group of scalars in $GL(V)$, and $G = Z_0R$ for some $Z_0 \leq F^*p$. Here $G \unlhd F^*pR$ (hence is $\frac{1}{2}$-transitive, since in general, a normal subgroup of a transitive group is $\frac{1}{2}$-transitive).

3. The $\frac{1}{2}$-transitive group $G$ in part (iii) is more interesting. Here $G = (Z_0R) \leq \Gamma L_2(13^2)$, where $R = SL_2(5)$ and $Z_0$ is a subgroup of $F^*13^2$ of order 28, and $G \cap GL_2(13^2) = Z_0R$ has orbits on 1-spaces of sizes 20, 30, 60, 60.

Combining Theorem 1 with the soluble case in [13, 14] and the $p$-modular case in [8, Theorem 6], we have the following classification of $\frac{1}{2}$-transitive linear groups. In the statement, for $q$ an odd prime power, $S_0(q)$ is the subgroup of $GL_2(q)$ of order $4(q-1)$ consisting of all monomial matrices of determinant $\pm 1$.

**Corollary 2** If $G \leq GL(V) = GL_d(p)$ is $\frac{1}{2}$-transitive on $V^d$, then one of the following holds:

(i) $G$ is transitive on $V^d$;

(ii) $G \leq \Gamma L_1(p^d)$;

(iii) $G$ is a Frobenius complement acting semiregularly on $V^d$;

(iv) $G = S_0(p^{d/2})$ with $p$ odd;

(v) $G$ is soluble and $p^d = 3^2, 5^2, 7^2, 11^2, 17^2$ or $3^4$;

(vi) $SL_2(5) \unlhd G \leq \Gamma L_2(p^{d/2})$, where $p^{d/2} = 9, 11, 19, 29$ or 169.

Together with the results of [3], Corollary 2 completes the solution of an old problem – namely, the classification of $\frac{1}{2}$-transitive permutation groups. For completeness, we state this classification here.

**Corollary 3** Let $X$ be a $\frac{1}{2}$-transitive permutation group of degree $n$. Then one of the following holds:

(i) $X$ is 2-transitive;

(ii) $X$ is a Frobenius group;

(iii) $X$ is affine: $X = T(V)G \leq AGL(V)$, where $G \leq GL(V)$ is a $\frac{1}{2}$-transitive linear group, given by Corollary 2;

(iv) $X$ is almost simple: either

(a) $n = 21$, $X = A_7$ or $S_7$ acting on the set of pairs in $\{1, \ldots, 7\}$, or

(b) $n = \frac{1}{2}q(q-1)$ where $q = 2^f \geq 8$, and either $G = PSL_2(q)$, or $G = PFG_2(q)$ with $f$ prime.
Turning to higher transitivity, recall (again from [16]) that for a positive integer \( k \), a permutation group is \((k + \frac{1}{2})\)-transitive if it is \( k \)-transitive and the stabilizer of \( k \) points has orbits of equal size on the remaining points. For \( k \geq 2 \) such groups are of course 2-transitive so belong to the known list of such groups. Nevertheless, their classification has some interesting features and we record this in the following result.

**Proposition 4** Let \( k \geq 2 \) be an integer, and let \( X \) be a \((k + \frac{1}{2})\)-transitive permutation group of degree \( n \geq k + 1 \). Then one of the following holds:

(i) \( X \) is \((k + 1)\)-transitive;

(ii) \( X \) is sharply \( k \)-transitive;

(iii) \( k = 3 \) and \( X = P\Gamma L_2(2^p) \) with \( p \) an odd prime, of degree \( 2^p + 1 \);

(iv) \( k = 2 \) and one of:

\[ L_2(q) \trianglelefteq X \leq P\Gamma L_2(q) \] of degree \( q + 1 \);

\[ X = \text{Sz}(q), \text{ a Suzuki group of degree } q^2 + 1; \]

\[ X = A\Gamma L_1(2^p) \text{ with } p \text{ prime, of degree } 2^p. \]

**Remarks**
1. The sharply \( k \)-transitive groups were classified by Jordan for \( k \geq 4 \) and by Zassenhaus for \( k = 2 \) or 3; see [6, §7.6].

2. In conclusion (iv), the groups \( \text{Sz}(q) \) and \( A\Gamma L_1(2^p) \) are Zassenhaus groups – that is, 2-transitive groups in which all 3-point stabilizers are trivial (so that all orbits of a 2-point stabilizer are regular). The groups \( X \) with socle \( L_2(q) \) are all \( \frac{3}{2} \)-transitive, being normal subgroups of the 3-transitive group \( P\Gamma L_2(q) \); some are 3-transitive, some are Zassenhaus groups, and some are neither.

The paper consists of two further sections, one proving Theorem 1, and the other Proposition 4. We offer a few observations on the proof of the main result, Theorem 1. Quite early in the proof is Lemma 2.3, which permits the use of inductive arguments. In order to use such arguments, some rather delicate analysis of small-dimensional cases is needed; most of this analysis is carried out theoretically, but for a few small cases we use computation through Magma [4]. We thank Eamonn O’Brien for assistance with these Magma computations.

## 2 Proof of Theorem 1

Throughout the proof, we shall use the following well-known result about the structure of Frobenius complements, due to Zassenhaus.

**Proposition 2.1** ([15, Theorem 18.6]) Let \( G \) be a Frobenius complement.

(i) The Sylow subgroups of \( G \) are cyclic or generalized quaternion.

(ii) If \( G \) is insoluble, then it has a subgroup of index 1 or 2 of the form \( SL_2(5) \times Z \), where \( Z \) is a group of order coprime to 30, all of whose Sylow subgroups are cyclic.

The following result is important in our inductive proof of Theorem 1.

**Proposition 2.2** Let \( R = SL_2(5) \) or \( A_5 \), let \( p > 5 \) be a prime, and let \( V \) be a faithful absolutely irreducible \( \mathbb{F}_q R \)-module, where \( q = p^a \). Regard \( R \) as a subgroup of \( GL(V) \), and let \( G \) be a group such that \( R \trianglelefteq G \leq GL(V) \).

(i) If \( R \) is semiregular on \( V^2 \), then \( \dim V = 2 \) and \( R = SL_2(5) \).

(ii) Suppose \( \dim V = 2 \) and \( G \) has no regular orbit on the set \( P_1(V) \) of 1-spaces in \( V \). Then either \( q \in \{p, p^2\} \) with \( p \leq 61 \), or \( q = 7^4 \).
(iii) If $\dim V = 2$ and $G$ is $\frac{1}{2}$-transitive but not semiregular on $V^2$, then $q = 11, 19, 29$ or $169$.

Conversely, for each of these values of $q$ there are examples of $\frac{1}{2}$-transitive, non-semiregular groups $G$, and they are as in Table 1 of Theorem 1.

Proof. (i) The irreducible $R$-modules and their Brauer characters can be found in [5], and have dimensions $2, 3, 4, 5$ or $6$. For those of dimension $3$ or $5$, the acting group is $R \cong A_5$, and involutions fix nonzero vectors; and for those of dimension $4$ or $6$, elements of order $3$ fix vectors.

(ii) Let $\dim V = 2$, and suppose $G$ has no regular orbit on $P_1(V)$. Assume for a contradiction that $q$ is not as in the conclusion of (ii). In particular, $q > 61$ (recall that $p > 5$).

Write $\overline{R} = R/Z(R) \cong A_5$ and $\overline{G} = G/(G \cap \mathbb{F}_q)$. Now $N_{\text{PGL}(V)}(\overline{R}) = \overline{R}$, so it follows that $\overline{G} = \overline{R}(\sigma)$ for some $\sigma \in \text{PGL}(V)$ (possibly trivial). Note that if $p \equiv \pm 2 \mod 5$ then $\mathbb{F}_{p^2} \subseteq \mathbb{F}_q$.

Consider the action of $\overline{R} \cong A_5$ on $P_1(V)$. As $A_5$ has $31$ nontrivial cyclic subgroups, and each of these fixes at most two $1$-spaces, it follows that $\overline{R}$ has at least $(q - 62)/60$ regular orbits on $P_1(V)$. Since $q > 61$, $\overline{R}$ has a regular orbit, and so $\overline{G} \neq \overline{R}$ by our assumption.

Let $r$ be the order of the element $\sigma$ modulo $\overline{R}$ (so that $\mathbb{F}_{p^r} \subseteq \mathbb{F}_q$). If there is a regular $\overline{R}$-orbit $\Delta_0$ on $P_1(V)$ that is not fixed by $\sigma^i$ for any $i$ with $1 \leq i \leq r - 1$, then $G\Delta_0 = \overline{R}$ and so $G(\langle v \rangle) = 1$ for $\langle v \rangle \in \Delta_0$ and $G$ has a regular orbit on $P_1(V)$, a contradiction. Hence $r > 1$, and for each regular $\overline{R}$-orbit $\Delta$, there is a subgroup $(\sigma^{(\Delta)})$, of prime order modulo $\overline{R}$, which fixes $\Delta$ setwise. Moreover, for $\langle v \rangle \in \Delta$, there exists $x \in \overline{R}$ such that $x\sigma^{(\Delta)}$ fixes $\langle v \rangle$. Since there are at least $q - 62$ elements of $P_1(V)$ in regular $\overline{R}$-orbits, it follows that

$$\left| \bigcup_{\langle x \sigma^j \rangle} \text{fix}_{P_1(V)}(x\sigma^j) \right| \geq q - 62, \quad (1)$$

where the union is over all $x \in \overline{R}$ and all $j$ dividing $r$ with $r/j$ prime. Let $s = r/j$ for such $j$, and let $x \in \overline{R}$. If $(x\sigma^j)^s \neq 1$ (then $(x\sigma^j)^s \in \overline{R}$ fixes at most two $1$-spaces, and so $|\text{fix}(x\sigma^j)| \leq 2$; and if $(x\sigma^j)^s = 1$, then $x\sigma^j$ is $\text{PGL}(V)$-conjugate to a field automorphism of order $s$, and $|\text{fix}(x\sigma^j)| = q^{1/s} + 1$. Hence (1) implies that

$$60 \sum_{s | r, s \text{ prime}} (q^{1/s} + 1) \geq q - 62. \quad (2)$$

Recall that $p > 5$ and $\mathbb{F}_{p^r} \subseteq \mathbb{F}_q$.

Suppose that $6 | r$. The terms in the sum on the left hand side of (2) with $s \geq 5$ add to at most $r(q^{1/5} + 1)$, which is easily seen to be less than $q^{1/2} + 1$. Hence (2) gives

$$2(q^{1/2} + 1) + (q^{1/3} + 1) \geq \frac{q - 62}{60}.$$ 

Putting $y = q^{1/6}$ this yields $120y^3 + 60y^2 + 242 \geq y^6$, which is false for $y \geq 7$. Similarly, when $\text{hcf}(r, 6) = 1$ or $3$, we find that (2) fails. Consequently $\text{hcf}(r, 6) = 2$, and (2) gives $2(q^{1/2} + 1) \geq (q - 62)/60$, which implies that $q^{1/2} \leq 121$. Hence (as $p > 5$ and $q = p^s$ with a even), either $q = p^2$ or $q = 7^2$ or $11^4$. Then further use of (2) gives $p \leq 61$ in the former case, and also shows that $q \neq 11^4$. But now we have shown that $q$ is as in (ii), contrary to assumption. This completes the proof.

(iii) Suppose $G$ is $\frac{1}{2}$-transitive but not semiregular on $V^2$. If $G$ has a regular orbit on $P_1(V)$, then it has a regular orbit on $V$, which is not possible by the assumption in the previous sentence. Hence $q$ must be as in the conclusion of part (ii). For these values of $q$, we use Magma [4] to construct $R \cong \text{SL}_2(5)$ in $\text{SL}_2(q)$, and for all subgroups of $\Gamma \text{L}_2(q)$ normalizing $R$, compute whether they are $\frac{1}{2}$-transitive and non-semiregular. We find that such groups exist precisely when $q$ is $11, 19, 29$ or $169$, and the examples are as in Table 1.

Note that part (ii) of the proposition follows from [11, Theorem 2.2] in the case where $R$ is $\mathbb{F}_p$-irreducible on $V$. We shall need the more general case proved above.

We now embark on the proof of Theorem 1. Suppose that $G$ is a minimal counterexample. That is,

- $G \leq \text{GL}_d(p) = \text{GL}(V)$ is an insoluble, $\frac{1}{2}$-transitive $p'$-group,
• $G$ is not semiregular on $V^2$, and $G$ is not as in (ii) or (iii) of the theorem, and

• $G$ is minimal subject to these conditions.

Observe that since $G$ is $\frac{1}{2}$-transitive and not semiregular, it cannot have a regular orbit on $V$.

The affine permutation group $VG \leq AGL(V)$ is $\frac{1}{2}$-transitive on $V$ and not a Frobenius group, hence is primitive by [16, Theorem 10.4]. It follows that $G$ is irreducible on $V$.

By [14, Theorem 1.1], $G$ acts primitively as a linear group on $V$. Choose $q = p^k$ maximal such that $G \leq \Gamma L_0(q) \leq GL_d(p)$, where $d = nk$. Write $V = V_n(q)$, $G_0 = G \cap GL_n(q)$, $K = F_q$ and $Z = G_0 \cap K^*$, the group of scalars in $G_0$. Since $G$ is insoluble, $n \geq 2$. Also $G_0$ is absolutely irreducible on $V$ (see [8, Lemma 12.1]), so $Z = Z(G_0)$.

**Lemma 2.3** Let $N$ be a normal subgroup of $G$ with $N \leq G_0$ and $N \not\leq Z$, and let $U$ be an irreducible $KN$-submodule of $V$. Then the following hold:

(i) $N$ acts faithfully and absolutely irreducibly on $U$;

(ii) $N$ is not cyclic;

(iii) $G_U$ acts $\frac{1}{2}$-transitively on $U^2$;

(iv) if $(G_U)^U$ is insoluble and not semiregular, and $(N^{(\infty)}, |U|) \neq (SL_2(5), q^3)$ with $q \in \{11, 19, 29, 169\}$, then $U = V$.

**Proof.** As $G$ is primitive on $V$, Clifford’s theorem implies that $V \downarrow N$ is homogeneous, so that $V \downarrow N = U \oplus U_2 \oplus \cdots \oplus U_r$ with each $U_i \cong U$. Hence $N$ is faithful on $U$; it is also absolutely irreducible, as in the proof of [8, Lemma 12.2]. Hence (i) holds, and (ii), (iii) follows.

To see (iii), let $v \in U^2$, $n \in N$ and $g \in G_v$. Then $vn = vgn = v'n'$ for some $n' \in N$. Hence $\{vn : n \in N\}$ is invariant under $G_v$. As $U$ is irreducible under $N$, $\{vn : n \in N\}$ spans $U$, and hence $G_v$ stabilises $U$. Therefore

$$|G : G_v| = |G : G_U| \cdot |G_U : G_v|.$$ 

As $G$ is $\frac{1}{2}$-transitive this is independent of $v \in U^2$, and hence $G_U$ is $\frac{1}{2}$-transitive on $U^2$, as in (iii).

Finally, (iv) follows by the minimality of $G$. 

By [14, Theorem A], $O_r(G_0)$ is cyclic for each odd prime $r$, and hence is central by Lemma 2.3(ii). Consequently $F(G_0) = ZE$ where $E = O_2(G_0)$. Moreover [14, Theorem A] also shows that $\Phi(E)$ is cyclic, hence contained in $Z$, and $|E/\Phi(E)| \leq 2^3$.

Now let $F^*(G_0) = ZER_1 \cdots R_k$, a commuting product with each $R_i$ quasisimple (possibly $k = 0$).

**Lemma 2.4** We have $k \geq 1$.

**Proof.** Suppose $k = 0$, and write $N = F^*(G_0) = ZE$. Since $V \downarrow G$ is primitive, every characteristic abelian subgroup of $E$ is cyclic, so $E$ is a 2-group of symplectic type. By a result of Philip Hall ([2, 23.9]), we have $E = E_1 \circ F$ where $E_1$ is either 1 or extraspecial, and $F$ is cyclic, dihedral, semidihedral or generalised quaternion; in the latter three cases, $|F| \geq 16$. Since $N = F^*(G_0)$ we have $C_{G_0}(N) \leq N$ and $G_0/C_{G_0}(N) \leq \text{Aut}(N)$. Hence $\text{Aut}(N)$ must be insoluble, and it follows that $|E_1/\Phi(E_1)| \geq 2^4$.

Now $E$ has a characteristic subgroup $E_0 = E_1 \circ L$, where $L = C_4$ if 4 divides $|F|$ and $L = 1$ otherwise. Then $E_0 \triangleleft G$. Let $U$ be an irreducible $KE_0$-submodule of $V$. By Lemma 2.3, $E_0$ is faithful on $U$ and $G_U$ is $\frac{1}{2}$-transitive on $U^2$. Write $H = (G_U)^U$.

Assume that $H$ is soluble. As $H$ is $\frac{1}{2}$-transitive on $U$, it is therefore given by [14, Theorem B], which implies that one of the following holds:

(a) $H$ is a Frobenius complement;
(b) $H \leq \Gamma L_1(q^u)$, where $|U| = q^u$;  
(c) $H \leq GL_2(q^u)$ with $|U| = q^{2u}$, and $H$ consists of all monomial matrices of determinant $\pm 1$;  
(d) $|U| = p^2$ with $p \in \{3, 5, 7, 11, 17\}$, or $|U| = 3^4$.

In all cases except the last one in (d), it follows (using Proposition 2.1(i) for (a)) that $|E_0/\Phi(E_0)| \leq 2^n$, which is a contradiction. In the exceptional case $|U| = 3^4$ and $|E_0/\Phi(E_0)| = 2^n$. But in this case any 3'-subgroup of Aut($N$) is soluble, and hence $G_0$ is soluble, again a contradiction.

Hence $H$ is insoluble. As $H$ is not a Frobenius complement by Proposition 2.1(ii), it is not semiregular on $U^t$, and so Lemma 2.3(iv) implies that $U = V$. Hence $E_0$ is irreducible on $V$ and so $F$ is cyclic and $N = ZE = ZE_0$. We have $|E_0/\Phi(E_0)| \leq 2^n$ by [14, Theorem A], and hence $|E_0/\Phi(E_0)| = 2^{2m}$ with $m = 2, 3$ or 4.

**Case** $m = 4$. Suppose first that $m = 4$, so $E_1 = 2^{1+8}$ and dim $V = 16$. By [14, Lemmas 2.6, 2.10] we have $E_1 = E_0$, so that $|Z|_2 = 2$ and $G_0 \leq ZO_9(2)$ $(\epsilon = \pm)$. Also [14, Lemma 2.4] gives $(p^2 - 1)_2 \geq 2^4$, hence $p \geq 7$, and the proof of [14, Lemma 2.12] gives $|G/N| \geq q^8/2^9$. Since $G/N \leq O_9(2)$, it follows that $q = 7$. Hence $G/N$ is an insoluble 7'-subgroup of $O_9(2)$ of order greater than $7^8/2^9$. Using [5], we see that such a subgroup is contained in one of the following subgroups of $O_9(2)$:

$$2^6 O_7(2), 2^{1+8} (S_3 \times S_5) (\epsilon = -)$$

$$S_3 \times O_6(2), 2^6 (S_6 \times 2), 2^6 (S_5 \times S_3), (S_5 \times S_3).2 (\epsilon = +)$$

We now consider elements of order 3 in $G$. These are elements $t_k$ lying in subgroups $O_7(2)^k$ of $O_9(2)$ for $1 \leq k \leq 4$ and acting on the 16-dimensional space $V$ as a tensor product of $k$ diagonal matrices $(\omega, \omega^{-1})$ with an identity matrix of dimension $2^{4-k}$, where $\omega \in K^*$ is a primitive cube root of 1; there are also scalar multiples $\omega t_k$ if $Z$ contains $\omega I$. We compute the action of $t_k$ on $V$ and also the class of the image of $t_k$ in $O_9(2)$ in Atlas notation, as follows:

<table>
<thead>
<tr>
<th>$k$</th>
<th>action of $t_k$ on $V$</th>
<th>Atlas notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$(\omega^8, \omega^{-1})$</td>
<td>$3A (\epsilon = -), 3A (\epsilon = +)$</td>
</tr>
<tr>
<td>2</td>
<td>$(\omega^8, \omega^4, \omega^{-1})$</td>
<td>$3B (\epsilon = -), 3E (\epsilon = +)$</td>
</tr>
<tr>
<td>3</td>
<td>$(\omega^4, \omega^6, \omega^{-1})$</td>
<td>$3C (\epsilon = -), 3D (\epsilon = +)$</td>
</tr>
<tr>
<td>4</td>
<td>$(\omega^5, \omega^{-1})$</td>
<td>$-(\epsilon = -), 3BC (\epsilon = +)$</td>
</tr>
</tbody>
</table>

Hence every element of order 3 in $G$ has fixed point space on $V$ of dimension at most 8. Considering the above subgroups of $O_9(2)$, we compute that the total number of elements of order 3 in $G$ is less than $2^{20}$. If $G$ contains an element of order 3 fixing a nonzero vector in $V$, then as $G$ is $2$-transitive, every nonzero vector is fixed by some element of $G$ of order 3. Hence $V$ is the union of the subspaces $C_V(t)$ over $t \in G$ of order 3, so that

$$|V| \leq \sum_{t \in G, |t|=3} |C_V(t)|.$$  

(3)

This yields $7^{16} < 2^{20} \cdot 7^8$, which is false.

It follows that $G$ contains no element of order 3 fixing a nonzero vector. So every element of order 3 in $G/N$ is conjugate to $t_1$.

We now complete the argument by considering involutions in $G$. Now $G$ certainly contains involutions which fix nonzero vectors, so arguing as above we have

$$|V| \leq \sum_{t \in G, |t|=2} |C_V(t)|.$$  

(4)

The group $G/N$ is an insoluble 7'-subgroup of $O_9(2)$, all of whose elements of order 3 are conjugates of $t_1$. Using Magma [4], we compute that there are 206 such subgroups if $\epsilon = +$, and 59 if $\epsilon = -$. For each of these possibilities for $G/N$ we compute the list of involutions of $G$ and their fixed point space dimensions. All possibilities contradict (4). For example, when $\epsilon = -$ the largest possibility for $G$ has 188 involutions with fixed space of dimension 12; 74886 with dimension 8; and 188 with dimension 4. Hence (4) gives

$$7^{16} \leq 188 \cdot (7^{12} + 7^4) + 74886 \cdot 7^8,$$
which is false. This completes the proof for \( m = 4 \).

**Case** \( m = 3 \). Now suppose \( m = 3 \), so that \( \dim V = 8 \). This case is handled along similar lines to the previous one. By [14, Lemma 2.9], either \(|Z|_2 = 2 \) and \( G_0/N \leq O_6^-(2) \), or \( 4 \) divides \(|Z|\) and \( G \) contains a field automorphism of order 2 (so that \( q \) is a square), and \( G_0/N \leq Sp_6(2) \). As \( G_0 \) is insoluble, its order is divisible by 2 and 3, so \( p \geq 5 \). Also each non-central involution in \( G_0 \) fixes a nonzero vector.

Assume now that 7 divides \(|G|\). If 7 divides \(|G/G_0|\) then \( q \geq 5^7 \) and we easily obtain a contradiction using (4); so 7 divides \(|G_0|\). Elements of order 7 in \( G_0 \) act on \( V \) as \( (1^2, \omega, \omega^2, \ldots, \omega^6) \) where \( \omega \) is a 7th root of 1 in the algebraic closure of \( F_q \) (since they are rational in \( O_6^+(2) \)). In particular they fix nonzero vectors, so \( \frac{1}{2} \)-transitivity implies \[ |V| \leq \sum_{t \in G:|t|=7} |C_V(t)|. \] (5)

The number of elements of order 7 in \( Sp_6(2) \) is 207360, and hence the number in \( G_0 \) is at most \((q - 1,7) \cdot 2^6 \cdot 207360\). Each fixes at most \( q^2 \) vectors, so (5) gives \[ q^8 \leq (q - 1,7) \cdot 2^6 \cdot 207360 \cdot q^2, \] which implies that \( q \leq 13 \). Hence \( q = 5, 11 \) or 13 (not 7 as \( G_0 \) is a \( p \)-group). As \( q \) is prime, by the first observation in this case, we have \(|Z|_2 = 2\) and \( G/N \leq O_6^-(2) \). But then the number of elements of order 7 in \( G \) is at most \( 2^6 \cdot 5760 \), so (5) forces \( q = 5 \). So \( G/N \) is an insoluble \( 5 \)-subgroup of \( O_6^+(2) \), and now we use Magma to see that such a group \( G \) is not \( \frac{1}{2} \)-transitive on the nonzero vectors of \( V = V_8(5) \).

Therefore 7 does not divide \(|G|\). It follows that \( G_0/N \) is contained in one of the following subgroups of \( Sp_6(2) \):

\[ O_6^-(2), S_6 \times S_3, 2^4 \cdot S_6. \]

As \( G_0 \) is insoluble and a \( p \)-group, we have \( p \geq 7 \). We now consider elements of order 3 in \( G \). These are conjugate to elements \( t_k \) (\( 1 \leq k \leq 3 \)) lying in subgroups \( (O_2^-(2))^k \) of \( Sp_6(2) \), and acting on \( V \) as follows:

\[ t_1 : (\omega^{(4)}, \omega^{-1}(4)), \]
\[ t_2 : (1^4, \omega^{(2)}, \omega^{-1}(2)), \]
\[ t_3 : (1^2, \omega^{(3)}, \omega^{-1}(3)). \]

Suppose \( G \) has an element of order 3 which fixes nonzero vectors in \( V \), so that (3) holds. We argue as in the previous case that \( q \) is not a cube, so 3 does not divide \(|G/G_0|\). In \( O_6^-(2) \), the numbers of elements conjugate to \( t_1, t_2, t_3 \) are 240, 480, 80 respectively. Hence, if \( G_0/N \leq O_6^-(2) \) then (3) gives \[ q^8 \leq 2^4 \cdot 480q^4 + 2^6 \cdot 80q^2 + 2^4 \cdot 240q^4 + 2^5 \cdot 480q^2 + 2^7 \cdot 80q^3 \] where the last three terms are only present if 3 divides \(|Z|\). This gives \( q = 7 \). Similarly \( q = 7 \) is the only possibility if \( G_0/N \) is contained in \( S_6 \times S_3 \) or \( 2^4 \cdot S_6 \). But now we compute using Magma that such groups \( G \) are not \( \frac{1}{2} \)-transitive on the nonzero vectors of \( V = V_8(7) \).

Thus all elements of order 3 in \( G \) are fixed point free on \( V^r \), and hence \( G_0/N \) is an insoluble \( 7 \)-subgroup of \( Sp_6(2) \), all of whose elements of order 3 are conjugate to \( t_1 \). We compute that there are 10 such subgroups, and for each of them, (4) implies that \( q = 7 \) is the only possibility: for example, the largest possible \( G_0 \) has 60 (resp. 3526, 60) involutions with fixed point spaces on \( V \) of dimension 6 (resp. 4, 2), so (4) yields

\[ q^8 \leq 60q^6 + 3526q^4 + 60q^2, \]

hence \( q = 7 \). Finally, we compute that none of the possible subgroups \( G \) is \( \frac{1}{2} \)-transitive on the nonzero vectors of \( V = V_8(7) \).

**Case** \( m = 2 \). Now suppose \( m = 2 \), so that \( \dim V = 4 \). Then \( G_0/N \) is an insoluble subgroup of \( Sp_4(2) \), so is isomorphic to \( S_6, A_6, S_5 \) or \( A_5 \).
Assume that $G_0/N$ is $A_6$ or $S_6$. Then 4 divides $|Z|$ (so divides $q - 1$). Elements of $G_0$ of order 3 are conjugate to $t_k$ ($k = 1, 2$) lying in $S_{p_2}(2)^c$; and $t_1$ acts on $V$ as $(\omega^2, \omega^{-1}(2))$, $t_2$ as $(1^2, \omega, \omega^{-1})$. By assumption $G_0$ contains elements in both classes, so (3) yields

$$q^4 \leq 2^4 \cdot 40q^2 + 2 \cdot 2^4 \cdot 40q + 2 \cdot 2^2 \cdot 40q^2,$$

where the last two terms are present only if 3 divides $|Z|$ (hence also $q - 1$). Since 4 divides $q - 1$, we conclude that $q = 13$ or 17 in this case.

Now assume $G_0/N$ is $A_5$ or $S_5$. As $G$ is a $p'$-group, $p \geq 7$. We compute that $G_0$ has at most 230 involutions, so (4) gives $q^4 \leq 230q^2$, whence $q \leq 13$.

Thus in all cases, we have $q = 7, 11, 13$ or 17. We now compute that none of the possibilities for $G$ is $1/2$-transitive on the nonzero vectors of $V = V_q(q)$. This completes the proof of the lemma.

\section*{Lemma 2.5}

Either $|E/\Phi(E)| \leq 2^2$, or $|E/\Phi(E)| = 2^4$ and $p = 3$.

\textbf{Proof.} The result is trivial if $E \leq Z$, so suppose this is not the case. Let $N = ZE \triangleleft G$, and let $U$ be an irreducible $KN$-submodule of $V$. By Lemma 2.3, $N$ is faithful on $U$ and $G_U$ is $1/2$-transitive on $U^2$. Write $H = (G_U)^U$.

Assume first that $H$ is insoluble. Now $H$ is not semiregular on $U^2$ (as it is not a Frobenius complement by Proposition 2.1, having $N \cong N^U$ as a normal subgroup), so Lemma 2.3(iv) implies that $U = V$. But then $N = ZE$ is irreducible on $V$, which forces $k = 0$, contrary to Lemma 2.4.

Hence $H$ is soluble. As it is $1/2$-transitive on $U^2$, it is therefore given by [14, Theorem B]; the list is given under (a)-(d) in the proof of Lemma 2.4. In all cases except the last one in (d), it follows that $|E/\Phi(E)| \leq 2^2$; in the exceptional case $|U| = 3^4$ and $|E/\Phi(E)| = 2^4$. Hence the conclusion of the lemma holds.

\section*{Lemma 2.6}

If $R_i \triangleleft G$, then $R_i = SL_2(5)$ and $V / R_i = U^l$, a direct sum of $l$ copies of an irreducible $KR_i$-submodule $U$ of dimension 2.

\textbf{Proof.} Suppose $R := R_i \triangleleft G$. By Lemma 2.3, $V / R = U^l$ with $U$ irreducible and $(G_U)^U$ $1/2$-transitive. If $(R, \dim U) = (SL_2(5), 2)$ then the conclusion holds, so suppose this is not the case. If $R^U$ is semiregular then $R$ is a Frobenius complement, so $R \cong SL_2(5)$; but then $\dim V$ must be 2 by Proposition 2.2(i), which we have assumed not to be the case. Therefore $R^U$ is not semiregular, and so $U = V$ by Lemma 2.3(iv). In particular $F^*(G_0) = ZR$.

At this point we wish to apply [11, Theorem 2.2]: this states that, with specified exceptions, any $p'$-subgroup of $GL_4(p)$ that has a normal irreducible quasisimple subgroup, has a regular orbit on vectors. In order to apply this, we need to establish that our quasisimple normal subgroup $R$ of $G$ acts irreducibly on $V$, regarded as an $F_pR$-module. To see this, we go back to the proof of Lemma 2.3, letting $N := R \triangleleft G$. Taking $U'$ to be an irreducible $F_pR$-submodule of $V$, that proof shows that $R$ is faithful on $U'$, and that $G_{U'}$ is $1/2$-transitive on $U'$. Hence by the minimality of $G$, either $U' = V$ (which is the conclusion we want), or $G_{U'}^U$ is semiregular or as in (ii) or (iii) of Theorem 1. In the semiregular case, Proposition 2.1 implies that $R = SL_2(5)$ and $U'$ is a 2-dimensional $R$-module over some extension $K$ of $F_p$, and this holds in (ii) and (iii) of Theorem 1 as well. However this can only happen if $\dim_K V = 2$, contradicting our assumption that $(R, \dim U) \neq (SL_2(5), 2)$. Hence $U' = V$, as desired.

Now we apply [11, Theorem 2.2] which determines all the possibilities for $G$ not having a regular orbit on $V$; these are

1. the case with $R = A_c$ ($c < p$) and $V$ the deleted permutation module of dimension $c - 1$, and

2. the cases listed in Table 2 (note that in column 4 of row 14 of the table, $G_{18}$ and $G_9$ denote groups of orders 18 and 9).

\textbf{Case (1)} In this case $G = Z_0H$ where $Z_0$ is a group of scalars and $H = A_c$ or $S_c$, and $V = \{v_1, \ldots, v_c\} \in F^p : \sum v_i = 0$. If $v_1 = (1, -1, 0, \ldots, 0)$ and $v_2 = (1, 1, -2, 0, \ldots, 0)$, one
Lemma 2.7 We have $k = 1$.

Proof. Suppose $k > 1$. Assume first that $R_i ⋼ G$ for all $i$. Then $N := R_1 R_2 ⋼ G$; moreover $N$ is not a Frobenius complement by Proposition 2.1, so is not semiregular on $V^*$, and hence Lemma 2.3(iv) shows that $N$ is irreducible on $V$. Now Lemma 2.6 implies that

$$N = R_1 R_2 = SL_2(5) \otimes SL_2(5) \leq G \leq \Gamma L_4(q).$$

Let $V = U \otimes W$ be a tensor decomposition preserved by $N$, with $\dim U = \dim W = 2$. If $q \neq p$ or $p^2$ with $p \leq 61$, and also $q \neq 7^4$, then Proposition 2.2 shows that the group induced by $G/Z$ on $1$-spaces of $U$ has a regular orbit, and the same for $W$. Pick $\langle u \rangle$ and $\langle w \rangle$ in such orbits ($u \in U, w \in W$). Then $G_{w \otimes w} \leq Z$ and so $G_{w \otimes w} = 1$. Hence $G$ has a regular orbit on $V^*$, a contradiction. And if $q = p$, $p^2$ or $7^4$, then

$$G \leq Z \cdot (SL_2(5) \otimes SL_2(5)), a = Z \cdot R_1 R_2, a \leq \Gamma L_4(q),$$

where $a$ divides $4$. Here $G_0 = Z \cdot R_1 R_2$. Let $u_1, u_2$ be a basis of $U$ and $w_1, w_2$ a basis of $W$. Writing matrices relative to these bases, define $R_i^T = \{ A^T : A \in R_i \}$. Then by [8, Lemma 4.3], for the vector $v = u_1 \otimes w_1 + u_2 \otimes w_2$ we have

$$(G_0)_v = \{ B \otimes B^{-T} : B \in R_1 \cap R_2^T \}.$$  \hfill (6)

There is only one conjugacy class of subgroups $SL_2(5)$ in $GL_2(q)$, so we can choose bases $u_i, w_i$ such that $R_1 = R_2^T$; then for the corresponding vector $v$ the order of $(G_0)_v$ is divisible by $60$. On

<table>
<thead>
<tr>
<th>$G/Z$</th>
<th>$n$</th>
<th>$q$</th>
<th>$G_v \leq$</th>
<th>$m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_5$</td>
<td>3</td>
<td>11</td>
<td>$C_2$</td>
<td>3</td>
</tr>
<tr>
<td>$S_4$</td>
<td>4</td>
<td>7</td>
<td>$C_2$</td>
<td>3</td>
</tr>
<tr>
<td>$S_6$</td>
<td>5</td>
<td>7</td>
<td>$C_2$</td>
<td>5</td>
</tr>
<tr>
<td>$A_6,2$</td>
<td>4</td>
<td>7</td>
<td>$C_3$</td>
<td>2</td>
</tr>
<tr>
<td>$A_6$</td>
<td>3</td>
<td>19,31</td>
<td>$C_2, C_2$</td>
<td>5,3</td>
</tr>
<tr>
<td>$A_7$</td>
<td>4</td>
<td>11</td>
<td>$C_3$</td>
<td>7</td>
</tr>
<tr>
<td>$L_2(7)$</td>
<td>3</td>
<td>11</td>
<td>$C_2$</td>
<td>3</td>
</tr>
<tr>
<td>$L_2(7),2$</td>
<td>3</td>
<td>25</td>
<td>$C_2$</td>
<td>3</td>
</tr>
<tr>
<td>$L_3(3),2$</td>
<td>7</td>
<td>5</td>
<td>$C_2$</td>
<td>7</td>
</tr>
<tr>
<td>$L_3(3),2$</td>
<td>6</td>
<td>5</td>
<td>$S_3$</td>
<td>4</td>
</tr>
<tr>
<td>$U_4(2)$</td>
<td>4</td>
<td>7</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>$U_4(2)$</td>
<td>5</td>
<td>7,13,19</td>
<td>$S_4, V_4, C_2$</td>
<td>5,5,5</td>
</tr>
<tr>
<td>$U_4(2),2$</td>
<td>6</td>
<td>7,11,13</td>
<td>$D_{12}, V_4, C_2$</td>
<td>5,5,5</td>
</tr>
<tr>
<td>$U_4(2)$</td>
<td>4</td>
<td>13,19,31,37</td>
<td>$G_{18}, G_9, C_3, C_2$</td>
<td>4,2,2,3</td>
</tr>
<tr>
<td>$U_4(3),2$</td>
<td>6</td>
<td>13,19,31,37</td>
<td>$W(B_3), S_3 \times C_2, V_4, C_2$</td>
<td>5,5,5,5</td>
</tr>
<tr>
<td>$U_5(2)$</td>
<td>10</td>
<td>7</td>
<td>$V_4$</td>
<td>3</td>
</tr>
<tr>
<td>$S_p(2)$</td>
<td>7</td>
<td>11,13,17,19</td>
<td>$C_3, V_4, C_2, C_2$</td>
<td>7,7,7,7</td>
</tr>
<tr>
<td>$Ω_{2}^{+}(2)$</td>
<td>8</td>
<td>11,13,17,19,23</td>
<td>$W(B_3), S_4, S_3, V_4, C_2$</td>
<td>7,7,7,7,7</td>
</tr>
<tr>
<td>$J_2$</td>
<td>6</td>
<td>11</td>
<td>$S_3$</td>
<td>4</td>
</tr>
</tbody>
</table>
the other hand there are bases for which $R_i \cap R_i^T$ has order dividing 20, giving a vector stabilizer in $G$ of order coprime to 3. This contradicts $\frac{1}{2}$-transitivity.

Thus not all the $R_i$ are normal subgroups of $G$. Relabelling, we may therefore take it that $G$ permutes $l$ factors $R_1, \ldots, R_l$ transitively by conjugation, where $l > 1$. Let $N = R_1 \cdots R_l$. Lemma 2.3(iv) implies that $N$ is irreducible on $V$, so that $k = l$ and $F^*(G_0) = Z N$. Now [1, (3.16), (3.17)] implies that $N$ preserves a tensor decomposition $V = V_1 \otimes \cdots \otimes V_l$ with $\dim V_i$ independent of $i, N \leq \otimes GL(V_i)$ and $G \leq N_{\text{TL}}(\otimes GL(V_i)) = (GL(V_1) \circ \cdots \circ GL(V_k)).S_l.(\sigma)$ with $\sigma$ a field automorphism acting on all factors.

Let $G_1$ be the kernel of the natural map from $G$ to $S_k$, so that $G_1 = G \cap B$ where $B = (GL(V_1) \circ \cdots \circ GL(V_k)).(\sigma)$. There is a map $\phi : G_1 \rightarrow PLY(V_1)$ which has image normalizing the simple irreducible group $T := R_1/Z(R_1)$.

Just as in the second paragraph of the proof of Lemma 2.6, $N$ acts irreducibly on $V$, regarded as an $F_p$-$N$-module. It follows that $R_i$ acts irreducibly on $V_1$, regarded as an $F_p R_i$-module: for if $W_1$ is a proper nonzero $F_p R_i$-submodule of $V_1$, then by the transitivity of $G$ on the $R_i$, there is a proper nonzero $F_p R_i$-submodule $W_i$ of $V_i$ for each $i$, and then $W_1 \otimes \cdots \otimes W_l$ is an $F_p$-$N$-submodule of $V$, contradicting the $F_p$-$N$-irreducibility of $V$.

As in the proof of Lemma 2.6, this means that we can apply [11, Theorem 2.2] to the action of $G_1 \sigma$ on $V_1$. This shows that one of the following holds:

(a) $G_1 \phi$ has a regular orbit on the 1-spaces of $V_1$;

(b) $T$ and $V_1$ are among the exceptions indicated in (1) and (2) of the proof of Lemma 2.6;

(c) $(T, \dim V_1) = (A_5, 2)$.

Assume first that (a) holds and (c) does not. So $G_1 \phi$ has a regular orbit on 1-spaces in $V_1$. Let $\langle \langle v \rangle \rangle$ be a 1-space in such an orbit. Write also $v$ for the corresponding vector in the other $V_1$, and let $H$ be the stabiliser $(G_1)_{\langle \langle v \rangle \rangle}$. Then $H$ fixes the 1-space $\langle \langle v \rangle \rangle$ and so by the choice of $v$, we have $H \leq Z$, the group of scalars in $G$. Hence in fact $H = 1$. It follows that $G_{\otimes \cdots \otimes \sigma}$ has order dividing $k!$. Also, assuming $R_i \neq SL_2(r)$, there is an involution $r_i \in R_i \setminus Z$ fixing a nonzero vector $u_i \in V_i$, and hence we see that $G_{\otimes \cdots \otimes \sigma}$ has order divisible by $2^k$. However $2^k$ does not divide $k!$, so this is impossible. For $R_i \cong SL_2(r)$ we have $\dim V_i > 2$ (as we are assuming (c) does not hold), and use a similar argument with an element of order 3 fixing a vector (which can be seen to exist from the character table of $SL_2(r)$ in [7]).

Now consider case (b), where $T, V_i$ are as in (1) or (2) of the proof of Lemma 2.6. For $T, V_i$ as in Table 2 (apart from $U_4(2)$ in dimension 4), let $v, u \in V_1$ be as in the last paragraph of the proof of Lemma 2.6, and let $C$ be the group in the fourth column of Table 2 and $m$ the integer in the fifth. Then $(G_1)_{\otimes \cdots \otimes \sigma}$ is isomorphic to a subgroup of $C^{2k}$, so that $G_{\otimes \cdots \otimes \sigma}$ has order dividing $|C|^{2k}$. On the other hand $(G_1)_{\otimes \cdots \otimes \sigma}$ has order divisible by $m^k$. Since $G$ is $\frac{1}{2}$-transitive, this implies that $m^k$ divides $|C|^{2k}$, which is not the case.

The remaining cases in (b) are: $T = A_c (c < p), V_i$ the deleted permutation module; and $T = U_4(2), V_l = V_4(7)$. In the latter case $T$ has two orbits on 1-spaces in $V_l$ with stabilizers of orders 72 and 648; so as above $G$ has a vector stabiliser of order dividing $72^k$ and another of order divisible by $648^{k-1}$, a contradiction. Now suppose $T = A_c (c < p)$ and $V_i$ is the deleted permutation module, which we represent as $(x_1, \ldots, x_r) \in F_p^r : \sum x_i = 0$. By Bertrand's Postulate (see [9]) we can choose a prime $r$ such that $\frac{p}{2} < r < c$. Let $v_1, v_2$ be the following vectors in $V_1$:

$$v_1 = (1^r, -r, 0^{r-1}), \quad v_2 = (1^{r-1}, 1-r, 0^{r-2}).$$

Then $G_{\otimes \cdots \otimes \sigma}$ has order divisible by $r^k$, while $G_{\otimes \cdots \otimes \sigma}$ has order dividing $m^k r!$, where $m = (r-1)!/(c-r)!$ (note that $1-r \neq 1$ in $F_p$, since $p > c$). Hence $r^k$ divides $r!$. Thus not all the $R_i$ act irreducibly on $V$.

Finally consider case (c). Here $\dim V_1 = 2$ and $R_i \equiv SL_2(5)$; this case requires a special argument. Since $R_i$ is $F_p$-irreducible on $V_1$, we must have $q = p$ or $p^2$, and hence $G \leq Z : (SL_2(5) \circ \cdots \circ SL_2(5)).S_k.(\sigma)$ with $\sigma$ of order 1 or 2. Write $s = \lfloor \frac{2}{5} \rfloor$. As in the argument after (6), there is a vector $v \in V_1 \otimes V_2$ whose stabilizer in $SL_2(5) \otimes SL_2(5)$ contains a diagonal copy of $SL_2(5)$. Tensoring $v$ with the corresponding vectors in $V_3 \otimes V_4, \ldots, V_{2s-1} \otimes V_{2s}$ (and a further vector in $V_s$ if $k$ is odd), we see that there is a vector in $V$ with stabilizer in $G$ of order divisible by 60$^s$. On the other hand there is a 1-space $\langle w \rangle$ in $V_1$ with stabilizer in $SL_2(5)/Z(SL_2(5))$ of
groups are the Mathieu groups $M_22$; or a $3$-transitive subgroup of $AGL_2(q)$ for a discussion of sharply $4$-transitive groups.

Let $X$ be a minimal counterexample. In conclusion (ii) or (iii) of Theorem 1. This is our final contradiction to the assumption that $X$ is not 5-transitive. This gives the proposition for $q = 3, 5, 7$. Hence $G/Z$ is a Frobenius complement (so $W$ is a Frobenius group). Proposition 2.1 shows that $|G| = 11, 19, 29 or 169 and $W$ is irreducible on $V$ with stabilizer of order dividing 2 or 3. The latter can only hold if $q = 2$, 3 or 5. Then $G/Z$ is a Frobenius group. A Magma computation shows that no 4-point stabilizer has orbits of size 3 and 16, so that $G/Z$ is a 5-transitive group. Such groups are classified in [14, Theorem B]. From this it follows that one of the following holds:

(a) $G/W$ is a Frobenius complement (so $E$ is a generalised quaternion);
(b) relative to some basis of $W$ we have $G/W = S_0(q)$, the group of monomial $2 \times 2$ matrices of determinant $\pm 1$;
(c) $|W| = p^2$ with $p \in \{7, 11, 17\}$.

In case (c), $q = p$; also $p \neq 7, 17$ as $SL_2(5) \not\leq GL_2(p)$ for these values. Hence $V = U \otimes W = V_4(p)$ with $p = 11$, and a Magma computation shows that there is no such $1/2$-transitive group $G$ in this case.

In case (a), $G/W \leq Z \cdot SL_2(3) < GL_2(q)$; and in (b), $G/W = Z \cdot 2^2 < Z \cdot SL_2(3, 2) < GL_2(q)$. In either case it follows that $V = U \otimes W$ and $G \leq Z \cdot (SL_2(5) \otimes (SL_2(3), 2)) < GL_2(q) \otimes GL_2(q) < GL_4(q)$. Write $G = GZ/Z$, so that $G \leq A_5 \times S_4$.

We saw in the proof of Proposition 2.2 that at least $q - 62$ of the elements of $P_1(U)$ lie in regular orbits of $A_5$. Similarly, at least $q - 32$ elements of $P_1(W)$ lie in regular orbits of $S_4$. Hence if $q > 61$ then, picking $\langle u \rangle \in P_1(U)$ and $\langle w \rangle \in P_1(W)$ in regular orbits, we see that $u \otimes w$ lies in a regular orbit of $G$ on $V^5$. This is a contradiction, since $G$ is a 5-transitive but not semiregular. Hence $q \leq 61$. Now a Magma computation shows that no $1/2$-transitive groups arise in cases (a) and (b) as well.

Thus we finally have $F^*(G_0) = ZR_1$ with $R_1 = SL_2(5)$ and $V \downarrow R_1 = U^1$, dim$U = 2$. Here $G/Z$ is $A_5$ or $S_5$, so $l = 1$. Now Proposition 2.2(iii) shows that $q = 11, 19, 29 or 169$ and $G$ is as in conclusion (ii) or (iii) of Theorem 1. This is our final contradiction to the assumption that $G$ is a minimal counterexample.

This completes the proof of Theorem 1.

3 Proof of Proposition 4

Let $k \geq 2$ and suppose that $X$ is a $(k + \frac{1}{2})$-transitive permutation group of degree $n$. Assume that $X$ is not $k$-transitive. We refer to [10, §2] for the list of 2-transitive groups, and to [6, §7.6] for a discussion of sharply $k$-transitive groups.

The proposition is trivial if $X$ is $A_n$ or $S_n$, so assume this is not the case. Then $k \leq 5$, as there are no 6-transitive groups apart from $A_n$ and $S_n$. Apart from $A_n$ and $S_n$, the only 5-transitive groups are the Mathieu groups $M_{12}$ and $M_{24}$, and the only 4-transitive, not 5-transitive, groups are $M_{11}$ and $M_{23}$. The groups $M_{11}$ and $M_{12}$ are sharply 4- and 5-transitive respectively; and in $M_{23}$, a 4-point stabilizer has orbits of size 3 and 16, so that $M_{23}$ is not $4\frac{1}{2}$-transitive and also $M_{24}$ is not $5\frac{1}{2}$-transitive. This gives the proposition for $k = 4$ or 5.

Next let $k = 3$. Then $X$ is a 3-transitive but not 4-transitive group, hence is one of the following: $AGL_2(q)$ (degree $2^d$) or $2^d.A_7$ (degree $2^d$) or $M_{11}$ (degree 12); $M_{22}$ or $M_{22.2}$ (degree 22); or a 3-transitive subgroup of $PGL_2(q)$ (degree $q + 1$). The affine groups here are not $3\frac{1}{2}$-transitive, as a 3-point stabilizer fixes a further point. Neither are $M_{11}, M_{22}$ or $M_{22.2}$ as 3-point
stabilizers have orbits of size 3, 6, or 3, 16. Finally, suppose that $X$ is a 3-transitive subgroup of $P^T L_2(q)$. There are two possible sharply 3-transitive groups here, namely $PGL_2(q)$ and a group $M(q^3) := L_2(q^3) : 2$ with $q = q^3$ and $q$ odd, which is an extension of $L_2(q^3)$ by a product of a diagonal and a field automorphism. Assuming that $X$ is not one of these, it must be the case that a 3-point stabilizer $X_{αβγ} = ⟨φ⟩$, where $φ$ is a field automorphism. Since $X$ is $3^2$-transitive, $⟨φ⟩$ acts semiregularly on the remaining $q - 2$ points, so any nontrivial power of $φ$ must fix exactly 3 points. It follows that $q = p^2$ with $p$ prime, and $φ$ has order $p$, which is the example in conclusion (iii) of Proposition 4.

Now suppose that $k = 2$. Consider first the case where $X$ is almost simple, and let $T = soc(X)$. When $T$ is not $L_2(q)$, $Sz(q)$ or $G_2(q)$, the arguments in [10, §3] show that a 2-point stabilizer $X_{αβ}$ has orbits of unequal sizes on the remaining points, contradicting $2^3_2$-transitivity. The groups with socle $L_2(q)$ are in conclusion (iv) of Proposition 4. If $T = G_2(q)$ (of degree $q^3 + 1$), then $X_{αβ}$ has order $(q - 1)f$, where $f = \mid X : T \mid$ is odd, and $X_{αβ}$ is generated by an element $x$ of order $q - 1$ and a field automorphism of odd order $f$. This group has a unique involution $x^{q-1}/2$ which fixes $q + 1$ points. It follows that some nontrivial orbits of $X_{αβ}$ have odd size and some have even size, contrary to $2^3_2$-transitivity. Now consider $T = Sz(q)$, of degree $q^2 + 1$. If $X = T$ then it is a Zassenhaus group, and is in (iv) of the proposition. Otherwise, $X = ⟨T, φ⟩$ where $φ$ is a field automorphism of odd order $f$, say, and $φ$ fixes $q^3 + 1$ points, where $q = q^3$. For suitable $α, β$ we have $X_{αβ} = ⟨x, φ⟩$, where $x$ has order $q - 1$, and $⟨x⟩$ has $q + 1$ orbits of size $q - 1$. Now $φ$ fixes points in some of these orbits, so by $2^3_2$-transitivity it must fix a point in each of them. But $[fix(φ)] = q^3 + 1 < q + 1$, which is a contradiction.

Finally, suppose $X$ is affine (with $k = 2$). Write $X = T(V)X_0 ≤ AGL(V)$, where $n = \mid V \mid$, $T(V)$ is the translation subgroup, and $X_0 ≤ GL(V)$. We refer to [10, §2(B)] for the list of possibilities for the transitive linear group $X_0$. If $X_0 ≤ SL_d(q)$ ($n = q^d, d ≥ 2$), $Sp_{2d}(q')$ ($n = q^d),$ or $G_2(q')$ ($n = q^d$), the arguments in [10, §4] show that for some $v ∈ V^2$, $X_0v$ has nontrivial orbits of unequal sizes. In cases (6-8) of [10, §2(B)], we have $X_0 ≤ L_2(q), L_2(3), 2^1+4$ or $SL_2(13)$, and $n ∈ \{3^4, 3^6, 5^2, 7^4, 11^2, 19^2, 23^2, 29^2, 59^2\}$; in each case $n - 2$ is coprime to the order of a 2-point stabilizer $X_{0v}$, so it follows by $2^3_2$-transitivity that $X_{0v} = 1$. In other words, $X$ must be sharply 2-transitive, as in conclusion (ii) of the proposition.

It remains to deal with the case where $X ≤ A := AΓL_1(q)$ ($n = q$). Here $A_{01}$ consists of field automorphisms, so if we pick $v ∈ F_q$ such that $v$ lies in no proper subfield of $F_q$, then $A_{01v} = 1$. Hence by $2^3_2$-transitivity, all 3-point stabilizers in $X$ are trivial – that is, $X$ is a Zassenhaus group. It is well known that the non-sharply 2-transitive Zassenhaus groups in the 1-dimensional affine case are just $AΓL_1(2^p)$ with $p$ prime, as in (iv) of the proposition. This is easy to see: we have $X_{01} = ⟨φ⟩$, where $φ$ is a field automorphism, and this acts semiregularly on $F_q \setminus \{0, 1\}$; hence, as argued at the end of the $k = 3$ case above, $q = 2^p$ with $p$ prime and $X = AΓL_1(2^p)$, as required.

This completes the proof of Proposition 4.

References


Martin W. Liebeck, Dept. of Mathematics, Imperial College, London SW7 2BZ, UK, email: m.liebeck@imperial.ac.uk

Cheryl E. Praeger, School of Mathematics and Statistics, University of Western Australia, Western Australia 6009, email: praeger@maths.uwa.edu.au

Jan Saxl, DPMMS, CMS, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK, email: saxl@dpmms.cam.ac.uk