ON 2-TRANSITIVE SETS OF EQUIANGULAR LINES

ULRICH DEMPWOLFF and WILLIAM M. KANTOR

(Received 1 April 2022; accepted 3 June 2022; first published online 22 August 2022)

Abstract

We determine all finite sets of equiangular lines spanning finite-dimensional complex unitary spaces for which the action on the lines of the set-stabiliser in the unitary group is 2-transitive with a regular normal subgroup.

2020 Mathematics subject classification: primary 52C35; secondary 05C25, 20B25, 81P15.

Keywords and phrases: 2-transitive, equiangular lines.

1. Introduction

A set \( \mathcal{L} \) of equiangular lines in a complex unitary vector space \( V \) is a set of 1-spaces that generates \( V \) such that the angle between any two members of \( \mathcal{L} \) is constant. This is a notion that has arisen in various contexts, from combinatorics \([14, 18]\) to quantum state tomography \([16]\). As in \([11]\), this paper is concerned with sets of equiangular lines exhibiting a significant amount of symmetry.

Two sets of lines are equivalent if there is a unitary transformation sending one set to the other. The unitary automorphism group \( \text{Aut}(\mathcal{L}) \) of \( \mathcal{L} \) is the set of unitary transformations sending \( \mathcal{L} \) to itself; the automorphism group \( \text{Aut} \mathcal{L} \) of \( \mathcal{L} \) is the group of permutations of \( \mathcal{L} \) induced by \( \text{Aut}(\mathcal{L}) \). The purpose of this note is to deal with a type of 2-transitive action of \( \text{Aut} \mathcal{L} \) not considered in \([11]\).

THEOREM 1.1. Let \( \mathcal{L} \) be a 2-transitive set of equiangular lines in the complex unitary space \( V \) and such that the automorphism group of \( \mathcal{L} \) has a regular normal subgroup. Let \( |\mathcal{L}| = n \), \( \dim V = d \) and \( 1 < d < n - 1 \). Then one of the following occurs:

(i) \( n = 4 \) and \( d = 2 \);
(ii) \( n = 64 \) and \( d = 8 \) or 56;
(iii) \( n = 2^{2m} \) and \( d = 2^{m-1}(2^m - 1) \) or \( 2^{m-1}(2^m + 1) \) for \( m \geq 2 \); or
(iv) \( n = p^{2m} \) and \( d = p^m(p^m - 1)/2 \) or \( p^m(p^m + 1)/2 \) for a prime \( p > 2 \) and \( m \geq 1 \).

For each pair \( (n, d) \) in (i)–(iv), there is a unique such set \( \mathcal{L} \) up to equivalence.
We are assuming that Aut$L$ is finite and 2-transitive. Such a group has either a nonabelian quasi-simple socle (the so-called quasi-simple type) or it possesses a normal, regular subgroup (the so-called affine type). This note deals with the affine type. The quasi-simple type occurs in [11]. The case $n = d^2$ is completely settled in [22] producing (i), (ii) (and the case $n = 3^2 = d^2$ of (iv)), while the corresponding question over the reals is implicitly dealt with in [18] (producing (iii)). The assumption $1 < d < n − 1$ excludes degenerate examples (see [11]).

The proof of the theorem uses the classification of the finite 2-transitive groups (a consequence of the classification of the finite simple groups), together with mostly standard group theory and representation theory. We start with general observations concerning a 2-transitive line set $L$ in a complex unitary space $V$. In Section 2.3, we show that Aut($L$) = $Z$($U$(V))$G$, where $G$ is a finite group 2-transitive on $L$, and then that $V$ is an irreducible $G$-module. The set-stabiliser $H = G_\ell$ of $\ell \in L$ has a linear character $\lambda$ such that, if $W$ is the module that affords the induced character $\lambda^G$, then $W = V \oplus V'$ for a second irreducible $G$-module $V'$ (Proposition 2.6(d)), which explains why 2-transitive line sets occur in pairs in the theorem. (See [11, page 3] for another explanation of this fact using Naimark complements.) Then we specialise to the case where Aut $L$ has a 2-transitive subgroup with a regular normal subgroup.

Section 2 contains group-theoretic background and Section 3 describes the examples in Theorem 1.1(iii) and (iv), while Section 4 contains the proof of the theorem. In the theorem, Aut($L$) and Aut $L$ are as described in the following remark.

**Remark 1.2.** For $L$ in Theorem 1.1, Aut($L$) = $GZ$, $Z = Z(U(V))$ where $G = E \rtimes S$ with a $p$-group $E$ and $H = G_\ell$, $\ell \in L$, is $Z(G) \times S$, where $Z(G) = E \cap Z$. In Section 4, we prove that the following statements hold for the various cases in the theorem:

(i) $E = Q_8$, $|S| = 3$ and $Z(G) = Z(E)$ has order 2;
(ii) $E$ is the central product of an extraspecial group of order $2^7$ with a cyclic group of order 4, $S \cong G_2(2)' \cong \text{PSU}(3, 3)$ and $Z(G) = Z(E)$ has order 4;
(iii) $E$ is elementary abelian of order $2^{2m+1}$, $S \cong \text{Sp}(2m, 2)$ and $Z(G) = E \cap Z$ has order 2; and
(iv) $E$ is extraspecial of order $p^{2m+1}$ and exponent $p$, $S \cong \text{Sp}(2m, p)$ and $Z(G) = Z(E)$ has order $p$.

2. **Group theoretic background**

Many facts of this section are basic and covered in the books of Aschbacher [1] and Huppert and Blackburn [10]. Our notation will follow the conventions of these references. We also need the classification of the 2-transitive finite groups. The groups of affine type are listed, for instance, in Liebeck [15, Appendix 1].

**Lemma 2.1.** Let $G$ be a finite 2-transitive permutation group and $V \leq G$ an elementary abelian regular normal subgroup of order $p'$ for a prime $p$. Identify $G$ with a group of affine transformations $x \mapsto x^g + c$ of $V = \mathbb{F}_p^d$, where $g \in G_0$ and $0, c \in V$. Then $G$ is a
semidirect product \( V \rtimes G_0 \) with \( G_0 \leq \text{GL}(V) \), and one of the following occurs:

(i) \( G_0 \leq \text{GL}(1, p') \);
(ii) \( G_0 \simeq \text{SL}(s, q), q^s = p', s > 2 \);
(iii) \( G_0 \simeq \text{Sp}(s, q), q^s = p' \);
(iv) \( G_0 \simeq G_2(q)^t, q^6 = 2^t \), where \( G_2(q) < \text{Sp}(6, q) \leq \text{Sp}(t, 2) \);
(v) \( G_0 \) is \( A_6 \simeq \text{Sp}(4, 2)' \) or \( A_7, p' = 16 \);
(vi) \( G_0 \simeq \text{SL}(2, 3) \) with \( t = 2 \) and \( p' = 5^2, 7^2, 11^2 \) or \( 23^2 \);
(vii) \( G_0 \simeq \text{SL}(2, 5) \) with \( t = 2 \) and \( p' = 9^2, 11^2, 19^2, 29^2 \) or \( 59^2 \);
(viii) \( p' = 3^4 \) and \( G_0 \) has a normal extraspecial subgroup \( Q \) of order \( 2^{1+4} \) such that
\( G_0 = Q \rtimes S \) with \( S \leq O^-(4, 2) \simeq S_5 \) and \(|S|\) divisible by 5;
(ix) \( G_0' \) is \( \text{SL}(2, 13), p' = 3^6 \).

2.1. Some indecomposable modules. Let \( U \) be an elementary abelian \( p \)-group (written additively) and \( S \leq \text{Aut}(U) \), that is, we consider \( U \) as a faithful \( \mathbb{F}_pS \)-module. We say that \( U \) is indecomposable if \( U \) is not the direct sum of two proper \( S \)-submodules. We are interested in modules with the following property.

HYPOTHESIS (I). \( U \) has a trivial \( S \)-submodule \( U_0 \neq 0 \), \( S \) acts transitively on the nontrivial elements of \( V = U/U_0 \) and the proper submodules of \( U \) lie in \( U_0 \). The possible pairs \((S, V)\) are listed in Lemma 2.1 (\( S \) taking the role of \( G_0 \)). The module \( U \) is an indecomposable module which extends a trivial module by \( V \).

**Lemma 2.2.** Let \( U \) be an indecomposable \( \mathbb{F}_pS \)-module satisfying (I) with \( \dim U_0 = 1 \). Then \( p = 2 \) and

(a) \( S \) has a normal subgroup \( S_0 \) and one of the following occurs:

1. \( \dim V = 2m, m > 1, S_0 \simeq \text{Sp}(2a, 2^b)' \), \( m = ab \), or \( S_0 \simeq G_2(2^b)' \), \( m = 3b \); or
2. \( \dim V = 3, S = S_0 = \text{SL}(3, 2) \).

(b) The module \( U \) exists in case (a) and is unique as an \( S_0 \)-module.

(c) Let \( S \simeq \text{Sp}(2a, 2^b)' \), \( m = ab \), or \( S \simeq G_2(2^b)' \), \( m = 3b \). Then \( S \) has an embedding into a group \( S^* \simeq \text{Sp}(2m, 2) \) and \( U \) is the restriction of the unique \( \mathbb{F}_2S^* \)-module (satisfying (I)) to \( S \).

Before we start the proof, we recall a few basic facts about group representations and cohomology. Let \( G \) be a finite group and \( V \) be an \( n \)-dimensional \( FG \)-module associated with the matrix representation \( D : G \rightarrow \text{GL}(n, F) \). Define the map \( D^* : G \rightarrow \text{GL}(n, F) \) by \( D^*(g) := D(g^{-1})' \). With respect to \( D^* \), the space \( V \) becomes a \( G \)-module, the dual module \( V^* \) of \( V \).

We describe the connection of the existence of indecomposable modules with cohomology of degree 1 and follow Aschbacher [1, Section 17]. Let \( G \) be a finite group and \( V \) a finite dimensional, faithful \( \mathbb{F}_pG \)-module. A mapping \( \delta : G \rightarrow V \) is called a derivation or 1-cocycle if \( \delta(xy) = \delta(x)v + \delta(y) \) for all \( x, y \in G \). If \( v \in V \), then \( \delta_v \), defined by \( \delta_v(x) = v - vx \) is also a derivation. Such derivations are called inner derivations or 1-coboundaries. The set \( Z^1(G, V) \) of derivations and the set \( B^1(G, V) \) of inner
derivations become elementary abelian $p$-groups with respect to pointwise addition. The factor group

$$H^1(G, V) = Z^1(G, V)/B^1(G, V)$$

is the first cohomology group of $G$ with respect to $V$.

Suppose, $V$ is a simple $G$-module. By Schur’s lemma, $K = \text{End}_{\mathbb{F}_p}(V)$ is a finite field, say $\mathbb{F}_p$. We consider the following property.

other names, such as ‘Heisenberg groups’, ‘Weyl–Heisenberg groups’ and ‘generalised Pauli groups’). We consider the following property.

We turn to Hypothesis (I) ($S$ taking the role of $G$). By [1, (17.12)], we have the following assertions:

(i) there exists an $\mathbb{F}_p S$-module with property (I) if and only if $H^1(S, V^*) \neq 0$; and

(ii) every $\mathbb{F}_p S$-module with property (I) is a quotient of a uniquely determined $\mathbb{F}_p S$-module $W$ with property (I) such that $\dim C_W(S) = \dim H^1(S, V^*)$.

If $V^*$ is simple then the module $W$ in (ii) is even a $KS$-module, where now $K = \text{End}_{\mathbb{F}_p}(V)$.

So if $U$ satisfies (I) and $\dim U_0 = 1$, then there exists a hyperplane $W_0$ of $C_W(S)$ such that $U \cong W/W_0$. If $\dim \mathbb{F}_p H^1(S, V^*) = 1$, then the multiplicative group of $K$ acts transitively on the hyperplanes of $C_W(S)$, that is, $U \cong W/W_1$ for any hyperplane $W_1$ of $C_W(S)$.

**PROOF OF LEMMA 2.2.** Assume the existence of a module $U$ as desired. Then $S$ has no normal subgroup $N \neq 1$ with $(|N|, p) = 1$ and $C_V(N) = 0$ as otherwise, by [1, (24.6)], $U = [U, N] \oplus U_0$ is a $G$-decomposition. This excludes case (1) of Lemma 2.1 and forces $p = 2$ (since $Z(S)$ contains an involution $z$ with $C_V(z) = 0$ if $p > 2$).

So we have to consider cases (2)–(5) of Lemma 2.1 for $S$. Assume $\dim \mathbb{F}_{2^b} V = 2^t$. In cases (2)–(4), we have $S_0 \leq S$ with $S_0 \cong \text{SL}(a, 2^b)$, $ab = t$, $a > 2$, $\text{Sp}(2a, 2^b)$, $2ab = t$, and $G_2(2^b)'$, $3b = t$, and $V$ is the defining $\mathbb{F}_{2^b} S_0$-module. In case (2), we get assertion (a,2) by [12]. In cases (3) and (4), $H^1(S_0, V^*)$ has dimension 1 over $\mathbb{F}_{2^b}$ by [12]. It follows that a module with property (I) and $\dim U_0 = 1$ exists and is unique up to isomorphism. We get assertions (a) and (b) once we exclude case (5). So assume $S \cong A_7$, $U$ is a 5-dimensional $\mathbb{F}_2 S$-module, $U/U_0$ is simple and $\dim U_0 = 1$ for $U_0 \subseteq C_U(S)$. There are 16 hyperplanes in $U$ that intersect $U_0$ trivially. A permutation representation of $S$ of degree $\leq 16$ has degree 1, 7 or 15. Hence, $U_0$ has an $S$-invariant complement in $U$ and $U$ is decomposable. This excludes case (5).

For (c), note that $S \cong \text{Sp}(2a, 2^b)$, $ab = m$, is a subgroup of $S^* = \text{Sp}(2m, 2) \cong O(2m + 1, 2)$ [9, Hilfssatz 1] and so is $S \cong G_2(2^b)'$, $3b = m$ [15, page 513]. The indecomposable $S^*$-module $U$ is the $O(2m + 1, 2)$-module [17, pages 55, 143]. As $S$ acts transitively on $V = U/U_0$, we see that $U$ is indecomposable as an $S$-module. \qed

### 2.2. On representations of extraspecial groups.

A finite, nonabelian $p$-group $E$ ($p$ a prime) is **extraspecial** if $Z(E) = E' = \Phi(E)$ has order $p$ (these groups have many other names, such as ‘Heisenberg groups’, ‘Weyl–Heisenberg groups’ and ‘generalised Pauli groups’). We consider the following property.
HYPOTHESIS (E). Let $p$ be a prime and $m \geq 1$ an integer. If $p > 2$, then $E$ is an extraspecial group of order $p^{1+2m}$ and exponent $p$ and if $p = 2$, then $E$ is the central product of an extraspecial group of order $2^{1+2m}$ with a cyclic group of order 4.

Assume Hypothesis (E) and let $A = \{ \alpha \in \text{Aut}(E) \mid \alpha_{Z(E)} = 1_{Z(E)} \}$ be the centraliser of $Z(E)$ in the automorphism group. Then (see [7, 21]),

$$A/\text{Inn}(E) \cong \text{Sp}(2m, p).$$

(2.1)

Denote by $\zeta_k = \exp(2\pi i/k)$ a primitive $k$th root of unity. Assertions (a) and (b) of the next Lemma are [1, (34.9)] and [10, Satz V.16.14], whereas the last assertion follows from [21, Theorem 1].

**Lemma 2.3.** Assume Hypothesis (E) and let $U$ be a $p^m$-dimensional complex space. Set $Z(E) = \langle z \rangle$.

(a) In the case $p = 2$, there exist precisely two faithful, irreducible representations $D_j : E \to \text{GL}(U)$, $j = 1, 3$, and $D_j(z) = \zeta_4^j \cdot 1_U$. Every faithful, irreducible representation of $E$ is of this form.

(b) In the case $p > 2$, there exist precisely $p - 1$ faithful, irreducible representations $D_j : E \to \text{GL}(U)$, $1 \leq j \leq p - 1$, and $D_j(z) = \zeta_p^j \cdot 1_U$. Every faithful, irreducible representation of $E$ is of this form.

For each $j$, there is an automorphism $\gamma_j$ of $E$ such that $D_j$ can be defined by $D_j(e) = D_1(e\gamma_j)$ for all $e \in E$, so $D_j(E) = D_1(E)$.

2.3. Basic properties of 2-transitive line sets. In this subsection, $L$ denotes a 2-transitive set of $n$ equiangular lines in a complex unitary space $V$ of dimension $d < n$. Let $K$ be the kernel of the permutation action of $\text{Aut}(L)$ on $L$, which clearly contains $Z := Z(U(V))$.

**Lemma 2.4.** We have $K = Z$.

**Proof.** Let $g \in K$. Let $m$ be the minimal number of nonzero $a_i$ in a dependency relation $\sum_i a_i v_i = 0$, $\langle v_i \rangle \in L$. Apply $g$ to obtain another dependency relation $\sum_i k_i a_i v_i = 0$ with the same $m$ nonzero $k_i a_i$; these relations must be multiples of one another by minimality. Thus, restricting to nonzero $a_i$ produces constant $k_i$.

Any two different members $\langle v_i \rangle, \langle v_j \rangle$ of $L$ occur with nonzero coefficients in such a relation. Then $g$ acts on all members of $L$ with the same scalar, and so is a scalar transformation since $L$ spans $V$. □

**Lemma 2.5.** There is a finite group $G$ such that $\text{Aut}(L) = GZ$.

**Proof.** By [1, (33.9)], $D = \text{Aut}(L')$ is finite. Let $G \leq \text{Aut}(L)$ be a finite group such that $D \leq G$ and $GZ/Z$ has maximal order in $\text{Aut } L = \text{Aut}(L)/Z$. Suppose $GZ < \text{Aut}(L)$. Pick $h \in \text{Aut}(L) - GZ$. Then $h^m \in Z$ for some integer $m$, so there is $z \in Z$ such that $h^m = z^{-m}$. Since $[G, hz] \subseteq D \leq G$, we get $|\langle G, hz \rangle| < \infty$ and $GZ/Z < \langle G, h \rangle Z/Z = \langle G, hz \rangle /Z$, a contradiction. □
PROPOSITION 2.6. Let $G$ be as in Lemma 2.5 and let $H = G_1$, $\ell \in L$, be the stabiliser of a line. Let $\lambda$ be the linear character of $H$ afforded by $\ell$. Then:

(a) $V$ is simple and a constituent of the module $W$ which affords $\lambda^G$;
(b) $W = V \oplus V'$ with a simple module $V'$ inequivalent to $V$;
(c) $V$ and $V'$ as $H$-modules afford $\lambda$ with multiplicity 1; and
(d) there is a set $L'$ of $n$ lines of $V'$ on which $G$ acts 2-transitively if $d < n - 1$.

PROOF. By 2-transitivity, $G = H \cup HtH$ for $t \in G - H$. Assume that $V = V_1 \oplus \cdots \oplus V_r$ for simple $G$-modules $V_i$. Let $\chi_i$ be the character of $V_i$.

Let $\ell = \langle v \rangle$. If $v = v_1 + \cdots + v_r$ with $v_i \in V_i$, then each $v_i \neq 0$ since $\langle L \rangle = V$. As $\lambda(h)v = \lambda(h)v_1 + \cdots + \lambda(h)v_r$ for $h \in H$, $\lambda$ is a constituent of $\langle \chi_i \rangle_H$. By Frobenius Reciprocity, each $\chi_i$ is a constituent of $\lambda^G$.

We claim that $\lambda^G = \psi_1 + \psi_2$ for distinct irreducible characters $\psi_i$ of $G$. For, by Mackey’s theorem [10, Satz V.16.9], $(\lambda^G)_H = ((\lambda^{1,1})_{H\cap H'})^H + ((\lambda^{1,1})_{H\cap H'})^H$. By Frobenius Reciprocity, $(\lambda^G, \lambda^G) = (\lambda, (\lambda^G)_H) = 1 + (\lambda, ((\lambda^{1,1})_{H\cap H'})^H) = (\lambda, ((\lambda^{1,1})_{H\cap H'})^H) = 1$. Hence, $(\lambda^G, \lambda^G) = 1$ or 2. If $\lambda^G$ is irreducible, then each $\chi_i = \lambda^G$, so $d = r\lambda^G(1) = r|\lambda| \geq n$. This contradiction proves the claim. By Frobenius Reciprocity, $(\lambda, (\psi_i)_H) = 1$ for $i = 1, 2$. Then (a)–(c) follow if $r = 1$.

We now assume $r > 1$. Each $\chi_i$ is in $\{\psi_1, \psi_2\}$. If $\{\chi_1, \chi_2\} = \{\psi_1, \psi_2\}$, then we would have $d \geq \chi_1(1) + \chi_2(1) = \lambda^G(1) = |L|$, which is not the case.

Since $\psi_1 \neq \psi_2$, we are left with the possibility $\chi_1 = \chi_2 \in \{\psi_1, \psi_2\}$, say $\chi_1 = \psi_1$. Let $\phi: V_1 \to V_2$ be a $G$-isomorphism. Since $\lambda$ has multiplicity 1 in $\psi_1$, the morphism $\phi$ sends the unique submodule of $(V_1)_H$ affording $\lambda$ to the unique submodule of $(V_2)_H$ affording $\lambda$. Thus, $v_1\phi = av_2$ with $a \in \mathbb{C}^\times$. Then

$$\langle v_1g + v_2g \mid g \in G \rangle = \langle v_1g + a^{-1}v_1\phi g \mid g \in G \rangle = V_1(1 + a^{-1})\phi,$$

showing $\langle L \rangle \subseteq V_1(1 + a^{-1})\phi \oplus V_3 \oplus \cdots \oplus V_r$. This contradicts the fact that $L$ spans $V$.

For (d), note that by (c), $V'$ contains an $H$-invariant 1-space $\ell'$. Then $\ell'G$ is a 2-transitive line set of size $n$ since $\dim V' = n - d > 1$ and since $H$ is maximal in $G$.

REMARK 2.7. $\lambda$ is a nontrivial character for $1 < d < n - 1$ (since $((1_H)_G, 1_G) = 1$ by Frobenius Reciprocity).

3. Examples of 2-transitive line sets

In this section, we describe the examples listed in Theorem 1.1. See [8, 22] for Theorem 1.1(i) and (ii).

EXAMPLE 3.1 (for Theorem 1.1(iii)). Let $m > 1$ and let $E = \mathbb{F}_{2^m+1}$. Then $E$ is an $O(2m+1, 2)$-space with radical $R$ [17, pages 55, 143]. Then $S := O(2m+1, 2) \simeq \text{Sp}(2m, 2) = \text{Sp}(E/R)$ is transitive on the $d := 2^{m-1}(2^m - 1)$ hyperplanes of $E$ of type $O^+(2m, 2)$ and on the $2^{m-1}(2^m + 1)$ hyperplanes of type $O^+(2m, 2)$ [17, page 139]. Label the standard basis elements of $V = \mathbb{C}^d$ as $v_M$ with $M$ ranging over the first of these sets of hyperplanes. Let $S$ act on this basis as it does on these hyperplanes. This action is
2-transitive (as observed implicitly for line sets in [18] and first observed in [5]), so the only irreducible $S$-submodules of $V$ are $\langle \bar{v} \rangle$ and $\bar{v}^\perp$, where $\bar{v} := \sum_M v_M$.

Each such $M$ is the kernel of a unique character $\lambda_M : E \rightarrow \{\pm 1\}$. Let $e \in E$ act on $V$ by $v_M e := \lambda_M(e)v_M$ for each basis vector $v_M$. If $1 \neq r \in R$, then $\lambda_M(r) = -1$ since $r \notin M$, so $r$ acts as $-1$ on $V$. If $e \in E$ and $h \in S$, then $(\bar{v}e)h = \bar{v}h \cdot h^{-1}eh = \bar{ve}h$, so $S$ acts on $\langle \bar{v} \rangle E$, a set of 1-spaces of $V$. Since $S$ is irreducible on $\bar{v}^\perp$, the set $\langle \bar{v} \rangle E = \langle \bar{v} \rangle ES$ spans $V$ and $\langle \bar{v} \rangle$ is the only 1-space fixed by $S$. In particular, $\langle \bar{v} \rangle$ affords the unique involutory linear character $\lambda$ of $H = R \rtimes S$ whose kernel is $S$. Clearly, $(E/R) \rtimes S$ acts 2-transitively on the $n = 2^m$ cosets of $S$. These are the $d$-dimensional examples in Theorem 1.1(iii). The $2^{m-1}(2^m + 1)$ hyperplanes of type $O^+(2m, 2)$ produce similarly the $(n - d)$-dimensional examples.

Example 3.2 (For Theorem 1.1(iv)). Let $p > 2$ be a prime, $m$ a positive integer and $E$ an extraspecial group of order $p^{1+2m}$ and exponent $p$. Using Lemma 2.3, we consider $E$ as a subgroup of $U(W)$, $W$ a complex unitary space of dimension $p^m$. By [2], the normaliser of $E$ in $U(W)$ contains a subgroup $G = E \rtimes S$, $G/E \simeq \text{Sp}(2m, p)$ inducing $\text{Sp}(2m, p)$ on $E/Z(E)$, with $ES$ acting 2-transitively on the $n = p^{2m}$ cosets of $H = Z(E) \rtimes S$. Moreover, $Z(S) = \langle e \rangle$ has order 2, and $W = W_+ \perp W_-$ for the eigenspaces $W_+$ and $W_-$ of $e$ (with $\dim W_+ = (p^m - e)/2$ for $e \in \{\pm 1\}$, $p^m \equiv e (\text{mod } 4)$); these are irreducible $S$-modules (Weil modules) [2, 6].

Let $U$ be one of these eigenspaces, say of dimension $d$. As $G/E \simeq S$, we can consider $U$ as a $G$-module. Define $V := W \otimes U^* \subset W \otimes W^*$ ($U^*$ dual to $U$). If $\chi$ is the character of $S$ on $U$, then $\bar{\chi} \bar{\chi}$ is the character of $S$ on $U \otimes U^*$. Trivially, $(\bar{\chi} \bar{\chi}, 1_S) = (\chi, \chi) = 1$, so there is a unique 1-space $\langle v_0 \rangle$ in $U \otimes U^*$ (and hence in $V$) fixed pointwise by $S$ (and it is the only 1-space fixed by the group $S$). In particular, $\langle v_0 \rangle$ affords a nontrivial linear character $\lambda$ of $H$ with kernel $S$. Since $E$ is irreducible on $W$ while $S$ is irreducible on $U^*$, the set $\langle v_0 \rangle ES$ spans $V$. These are the examples in Theorem 1.1(iv).

Lemma 3.3. Let $p$ be a prime, $m \geq 1$ an integer and $G = ES$ as in Example 3.1 if $p = 2$ and as in Example 3.2 if $p > 2$. Let $\mathcal{L}$ be a line set of size $n = p^{2m}$ in a complex unitary space $V$ with $1 < \dim V < n - 1$ such that $G \leq \text{Aut}(\mathcal{L})$ induces a 2-transitive action on $\mathcal{L}$. Then $\mathcal{L}$ is equivalent to a line set of Example 3.1 or 3.2.

Moreover, if $\lambda$ is a linear character of $Z(G) \rtimes S$, ker $\lambda = S$, then every constituent of the module associated with $\lambda^G$ contains a $G$-invariant line set satisfying the assumptions of this lemma.

Proof. For $i = 1, 2$, let $\mathcal{L}_i \subseteq V_i$ be line sets in complex unitary spaces and let $G_i = E_i \rtimes S_i \leq U(V_i)$, $S_i \simeq \text{Sp}(2m, p)$ be isomorphic groups as in the examples with a 2-transitive action on $\mathcal{L}_i$. Let $\ell_i \in \mathcal{L}_i$ and $H_i = (G_i)_{\ell_i}$. We assume that one of the line sets belongs to an example and, arguing by symmetry, we can also assume $1 < \dim V_i \leq n/2$, $i = 1, 2$.

Claim. $\mathcal{L}_1$ is equivalent to $\mathcal{L}_2$. By Proposition 2.6 and Remark 2.7, the representation $\lambda_i$ of $H_i$ on $\ell_i$ is a nontrivial linear character of $H_i$. We have $H_i = Z_i \times S_i$, $Z_i = Z(G_i)$. Let $\alpha : G_1 \rightarrow G_2$ be an isomorphism.
Case $p > 2$. The group $S_i$ is a representative of the unique class of complements of $E_i$ in $G_i$ (note that $S = C_G(Z(S))$ and $Z(S)$ is a Sylow 2-subgroup of $E \rtimes Z(S) \leq G$). So we can assume $H_2 = H_1 \alpha$, $S_2 = S_1 \alpha$. We also can assume $S_i = \ker \lambda_i$ by Lemma 4.1 below. By Lemma 2.3, there exists an automorphism $\gamma$ of $G_1$ such that $\lambda_1(z) = \lambda_2(z \gamma \circ \alpha)$ for $z \in Z$. So replacing, if necessary, $\alpha$ by $\gamma \circ \alpha$, we may assume that $\lambda_1(z) = \lambda_2(z \alpha)$ holds. Define a representation $D : G_1 \to \text{GL}(V_2)$ by

$$vD(g) = v(g \alpha), \quad v \in V_2, \ g \in G_1.$$ 

Let $W$ be the module associated with the induced character $\lambda_1^{G_1}$. By Proposition 2.6, both $G_1$-modules are isomorphic to the same irreducible submodule of $W$, that is, $V_1 \cong V_2$. Hence, there exists a $G_1$-morphism $\phi : V_1 \to V_2$ with $\ell_1 \pi = \ell_2$ ($\lambda_1$ has multiplicity 1 in $V_1$ and $V_2$). The claim holds for $p > 2$.

Case $p = 2$. Assume first $m > 2$. Then $S_2$ and $S_1 \alpha$ are complements of $E_2$ in $G_2$. By [1, (17.7)], there exists $\beta \in \text{Aut}(G_2)$ with $S_2 = (S_1 \alpha) \beta$. So replacing $\alpha$, if necessary, by $\alpha \circ \beta$, we can assume $H_1 \alpha = H_2$ and $S_1 \alpha = S_2$. Note that $H$ has precisely one nontrivial linear character. Now arguing as in the case $p > 2$, we see that $\mathcal{L}_1$ and $\mathcal{L}_2$ are equivalent. In the case $m = 2$, replace $S_i$ by $S_i'$, then the argument from case $m > 2$ carries over and shows the equivalence of $\mathcal{L}_1$ and $\mathcal{L}_2$. The first assertion of the lemma holds and the second follows from the preceding discussion. $\square$

4. Proof of Theorem 1.1 and automorphism groups

In this section, $p$ is a prime and $\mathcal{L}$ denotes a set of $n = p^t$ equiangular lines in a complex unitary space $V$ of dimension $d$ with $1 < d < n - 1$. By the assumptions of Theorem 1.1 and the results of Section 2.3, there exists a finite group $G \leq \text{Aut}(\mathcal{L})$ with a 2-transitive action on $\mathcal{L}$. Set $Z = Z(G)$. Then $G/Z$ has a regular normal subgroup and $V$ is a simple $G$-module. We assume $n \neq 4$. As for $n = 4$, the results in [22] imply assertion (i) of Theorem 1.1. It suffices to assume that no proper subgroup of $G/Z$ has a 2-transitive action on $\mathcal{L}$ and that no subgroup of $\text{Aut}(\mathcal{L})$, which covers the quotient $GZ/Z$, has order $< |G|$. We set $H = G_\ell$, $\ell \in \mathcal{L}$. Then the character/representation $\lambda : H \to \text{U}(\ell)$ of $H$ on $\ell$ is nontrivial by Remark 2.7. Observe that there is some flexibility in the choice of $G$: generators of $G$ can be adjusted by scalars. We show that $G$ can be chosen such that $G \leq \tilde{G}$ where $\tilde{G}$ is a group which is used to construct a line set in Examples 3.1 and 3.2.

**Lemma 4.1.** We may assume $G = E \rtimes S$, $H = Z \times S$, where $S$ is the kernel of the action of $H$ on $\ell$. Moreover, $Z \leq E$ and one of the following occurs:

(a) $p = 2$, $E$ is an elementary abelian 2-group, $|Z| = 2$ and $E$ as an $S$-module satisfies Hypothesis (I); or
(b) $t = 2m$, $E$ satisfies Hypothesis (E) and $E/Z(E)$ is a simple $S$-module.
PROOF. Let $M$ be the pre-image of the regular, normal subgroup of $G/Z$. Since $M/Z$ is abelian, we have $M = E \times Z_{p'}$ with a Sylow $p$-subgroup $E$ of $M$ and $Z_{p'}$ is the largest subgroup of $Z$ with an order coprime to $p$. Let $L$ be the kernel of $\lambda$.

We may assume that $E = M$, $Z \leq E$ and $S = L$ is a complement of $Z$ in $H$. Clearly, $Z \leq H \cap M$ and $L \cap Z = 1$. As $H/L$ is cyclic, we can choose $c \in H$ such that $H = \langle c, L \rangle$. Pick $\omega \in \mathbb{C}$ of norm 1 such that $S = \langle \omega c, L \rangle$ has a trivial action on $L$. Then $\tilde{G} = ES$ is 2-transitive on $L$. Moreover, $S \cap E \leq S \cap (\tilde{G} \cap E) \leq S \cap Z(U(V)) = 1$. Since $Z \supseteq Z \cap E = Z(\tilde{G}) \cap E = Z(\tilde{G})$ and $G/Z \cong \tilde{G}/Z(\tilde{G})$, we get $|\tilde{G}| \leq |G|$. So we may assume $G = \tilde{G}$ and $H = (E \cap Z) \times S$. In particular, $Z \leq E$.

Assume first that $E$ is abelian. Set $\Omega = \langle e \in E \mid |e| = p \rangle$. This group is a characteristic elementary abelian subgroup of $E$. If $\Omega \leq Z$, then $E$ is cyclic, and $S \neq 1$ is a $p'$-group (isomorphic to a subgroup of $\text{Aut}(E)$ of order $p - 1$). By Remark 2.7, $Z \neq 1$. This contradicts [1, (23.3)] (on automorphism groups of cyclic groups).

So $E = \Omega Z$ and, by the minimal choice of $G$, we obtain $E = \Omega$. If $Z$ has an $S$-invariant complement $E_0$ in $E$, then by induction, $G = E_0 S$ contradicting $Z \neq 1$. So $1 < Z < E$ is the unique composition series of $E$ as an $S$-module and assertion (a) follows as $Z$ is cyclic.

Assume now that $E$ is nonabelian. If $N$ were a characteristic, normal, abelian subgroup of $E$ of rank $\geq 2$, then $1 < NZ/Z \leq E/Z$ would be an $S$-invariant series. By our minimal choice $N = E$, this is absurd. So $E$ is of symplectic type and therefore, by [1, (23.9)], $E = C \circ E_1$ where $E$ is extraspecial or $r = 1$ and $C$ is cyclic or $p = 2$ or $C$ is a generalised quaternion group, a dihedral group or a semidihedral group of order $\geq 16$.

Suppose $p > 2$. By [1, (23.11)], $E$ is extraspecial of exponent $p$. So assertion (b) follows for $p > 2$.

Suppose finally $p = 2$. A standard reduction (see for instance [19, Lemma 5.12]) shows that $E$ contains a characteristic subgroup $F$ such that $F$ is extraspecial of order $2^{1+2m}$ or satisfies hypothesis (E). By our choice of $G$, we have $E = F$ as $t = 2m > 2$. If $E$ is extraspecial, then $S$ cannot act transitively on the nontrivial elements of $E/Z(E)$ as there are cosets modulo $Z(E)$ of elements of order 4 as well as cosets of elements of order 2. So assertion (b) holds for $p = 2$.

By Lemma 4.1, we distinguish the cases $E$ abelian ($p = 2$), $E$ nonabelian, $p > 2$, and $E$ nonabelian, $p = 2$. Then Lemmas 4.2 and 4.3 complete the proof of Theorem 1.1. The proof of Lemma 4.2 is very similar to the proof of Lemma 3.3.

**Lemma 4.2.** The following assertions hold.

(a) If $E$ be abelian, then Theorem 1.1(iii) holds.
(b) If $E$ be nonabelian and $p > 2$, then Theorem 1.1(iv) holds.

**Proof.** If $E$ is abelian, Lemma 2.2 applies. Case (a.2) of this lemma does not occur. Let $G = E \rtimes S$, $S \cong SL(3, 2)$, $Z = C_E(S)$ and $E/Z$ be the natural $S$-module. A simple $E$-module in $V$ affords a nontrivial character $\chi$ of $E$ and its kernel $E_\chi$ is a hyperplane intersecting $Z$ trivially. There are precisely 8 such hyperplanes. The group $S$ acts transitively on these hyperplanes (otherwise, as the smallest degree of a nontrivial
permutation representation of \( S \) is 7, \( S \) would fix one of these hyperplanes and \( E \) would not be an indecomposable \( S \)-module. Hence, \( \dim V \geq 8 = n \), a contradiction.

So there exists an embedding \( \iota : G \to \tilde{G} \), \( \tilde{G} = \tilde{E} \rtimes \tilde{S} \), \( \tilde{S} \cong \text{Sp}(2m, p) \) with \( \tilde{E} = E_t \), \( St \leq \tilde{S} \). This follows from (c) of Lemma 2.2 if \( p = 2 \) and for \( p > 2 \), it is clear by (2.1). The linear character \( \tilde{\lambda} \) of \( H_t \) defined by

\[
\tilde{\lambda}(hu) = \lambda(h), \quad h \in H, \tag{4.1}
\]

has a unique extension to \( \tilde{H} = Z_t \times \tilde{S} \) such that \( \ker \tilde{\lambda} = \tilde{S} \). Let \( \tilde{W} \) be the module associated with the induced character \( (\tilde{\lambda})^{\tilde{G}} \). By Proposition 2.6 and Lemma 3.3, we have a decomposition into simple \( \tilde{G} \)-modules \( \tilde{W} = \tilde{V} \oplus \tilde{V}' \) and both modules contain \( \tilde{G} \)-invariant line sets. We turn \( \tilde{W} \) into a \( G \)-module by

\[
\tilde{w} \cdot g = \tilde{w}(gt), \quad \tilde{w} \in \tilde{W}, \quad g \in G.
\]

By Mackey’s theorem [10, Satz V.16.9] and (4.1),

\[
((\tilde{\lambda})^{\tilde{G}})_G = ((\tilde{\lambda})_{H \cap G})^G = (\lambda_H)^G.
\]

So \( \tilde{W} \) as a \( G \)-module affords \( \lambda^G \). Then by Proposition 2.6, \( V \) is isomorphic to \( \tilde{V} \) or \( \tilde{V}' \). Say \( V \cong \tilde{V} \). An isomorphism \( \phi : V \to \tilde{V} \) maps the line set \( L \) onto \( \tilde{L} \phi \) such that \( \ell \phi \) and \( \ell \phi \) both afford as \( H \)-spaces the character \( \lambda \). However, \( \tilde{V} \) contains a \( \tilde{G} \)-invariant line set containing a line affording \( \tilde{\lambda} \). Thus, by (4.1) and Proposition 2.6, \( L \phi \) is this \( \tilde{G} \)-invariant line set. Using Lemma 3.3 again completes the proof. \( \square \)

**Lemma 4.3.** Let \( E \) be nonabelian and \( p = 2 \). Then (i) or (ii) of Theorem 1.1 hold.

**Proof.** By Proposition 2.6, we may assume \( d = \dim V \leq n/2 = 2^{2m-1} \). As \( E \) satisfies Hypothesis (E), \( S \) is isomorphic to a subgroup of \( \text{Sp}(2m, 2) \) (see (2.1)). By Lemma 2.1 and by the minimal choice of \( G \), we have \( H/Z(H) \cong \text{SL}(2, 2^m) \) or \( \cong \text{G}_2(2^b) \) and \( b = m/3 \). Let \( V = V_1 \oplus \cdots \oplus V_r \), a decomposition into irreducible \( E \)-modules. Clearly, all \( V_i \) are faithful \( E \)-modules, in particular, \( d = 2^m \ell \). A generator of \( Z \) induces the same scalar on each \( V_i \) as the eigenspaces of this generator are \( G \)-invariant. Lemma 2.3 shows that all \( V_i \)'s are pairwise isomorphic. If \( \ell = 1 \), then \( n = 2^{2m} = d^2 \) and an application of the main result of [22] proves the assertion of the lemma.

So assume \( \ell > 1 \). Denote by \( D \) the representation of \( G \) afforded by \( V \) and apply [10, Satz V.17.5]. Then \( D(g) = P_1(g) \otimes P_2(g) \) where the \( P_i \) terms are irreducible projective representations of \( G \) and \( P_2 \) is also a projective representation of \( S \cong G/E \) of degree \( \ell \). Denote by \( m_S \) the minimal degree of a nontrivial projective representation of \( S \). By [10, Satz V.24.3], \( m_S \) is the minimal degree of a nontrivial, irreducible representation of the universal covering group of \( S \). We have \( m_S = 2^m - 1 \) for \( S \cong \text{SL}(2, 2^m), m > 3 \) [20, Table 3], [13], \( m_S = 2^m - 2^b \) for \( S \cong \text{G}_2(2^b) \), \( m = 3b, b \neq 2 \) [20, Table 3], [13], \( m_S = 2 \) for \( S \cong \text{SL}(2, 4), m = 2 \) [4], and \( m_S = 12 \) for \( S \cong \text{G}_2(4), m = 12 \) [4]. Since \( m_S 2^m \leq d \leq 2^{2m-1} \), only the last two cases may occur.

For \( S \cong \text{G}_2(4) \), degree 12 is the only degree of a nontrivial, irreducible, projective representation of degree \( \leq 64 \). By Proposition 2.6, there exists an irreducible
\( G \)-module \( V' \) such that \( \dim V' = 2^{12} - d = 64 \cdot 52 \) and 52 is the degree of an irreducible, projective representation of \( S \), a contradiction.

Assume finally \( m = 2 \). It follows from [7, Theorem 4] that there exists a group \( G = E \rtimes S \), \( S \simeq \text{SL}(2, 4) \), and this group is unique up to isomorphism. Using GAP or Magma, one can compute characters of \( G \). For \( H = Z(E) \rtimes S \), there exist precisely two linear characters of \( H \) with kernel \( S \). For any such character \( \lambda \), the induced character \( \lambda^G \) is irreducible, which rules out this possibility too. \( \square \)

### 4.1. Automorphism groups.

**Proof of Remark 1.2.** For cases (i) and (ii), we refer to [8, 22]. For the remaining two cases, we have, by Theorem 1.1, a finite subgroup \( G = E \rtimes S \leq \text{Aut}(\mathcal{L}) \), with \( |E/(E \cap Z)| = p^{2m}, Z = Z(U(V)) \) and \( S \simeq \text{Sp}(2m, p) \). The assertions follow in cases (iii) and (iv) if \( E/(E \cap Z) \) is normal in \( \text{Aut} \mathcal{L} \), that is, if \( \text{Aut} \mathcal{L} \) has a regular, abelian normal subgroup. Suppose \( \text{Aut} \mathcal{L} \) has a nonabelian simple socle. Then, by the classification of the 2-transitive groups (see [3]), \( \text{Aut} \mathcal{L} \) is at least triply transitive. In that case, the application of Proposition 2.6 (to a point stabiliser) forces \( \dim V = d = n - 1 \), a contradiction. \( \square \)

**References**

[1] M. Aschbacher, *Finite Group Theory*, 2nd edn (Cambridge University Press, Cambridge 2000).

[2] B. Bolt, T. G. Room and G. E. Wall, ‘On the Clifford collineation, transform and similarity groups I, II’, *J. Aust. Math. Soc.* 2 (1961), 60–79, 80–96.

[3] P. J. Cameron, ‘Primitive permutation groups and finite simple groups’, *Bull. Lond. Math. Soc.* 13 (1981), 1–22.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson and J. G. Thackray, *Atlas of Finite Groups* (Oxford University Press, Eynsham 1985).

[5] L. E. Dickson, ‘The groups of Steiner in problems of contact (second paper)’, *Trans. Amer. Math. Soc.* 3 (1902), 377–382.

[6] P. Gérardin, ‘Weil representations associated to finite fields’, *J. Algebra* 46 (1977), 54–101.

[7] R. L. Griess Jr, ‘Automorphisms of extra special groups and nonvanishing degree 2 cohomology’, *Pacific J. Math.* 48 (1973), 403–422.

[8] S. G. Hoggar, ‘64 lines from a quaternionic polytope’, *Geom. Dedicata* 69 (1998), 287–289.

[9] B. Huppert, ‘Singer–Zyken in klassischen Gruppen’, *Mat. Z.* 117 (1970), 141–150.

[10] B. Huppert and N. Blackburn, *Endliche Gruppen I* (Springer, Berlin, 1967), *Finite Groups II, III* (Springer, Berlin, 1982).

[11] J. W. Iverson and D. G. Mixon, ‘Doubly transitive lines II: almost simple symmetries’, Preprint, 2019, arXiv:1905.06859.

[12] W. Jones and B. Parshall, ‘On the 1-cohomology of finite groups of Lie type’, *Proc. Conf. Finite Groups (Utah 1975)* (eds. W. R. Scott and F. Gross) (Academic Press, New York, 1976), 313–328.

[13] V. Landazuri and G. M. Seitz, ‘On the minimal degrees of projective representations of the finite Chevalley groups’, *J. Algebra* 32 (1974), 418–443.

[14] P. E. H. Lemmens and J. J. Seidel, ‘Equiangular lines’, *J. Algebra* 24 (1973), 494–512.

[15] M. W. Liebeck, ‘The affine permutation groups of rank three’, *Proc. Lond. Math. Soc. (3)* 54 (1987), 477–516.

[16] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, ‘Symmetric informationally complete quantum measurements’, *J. Math. Phys.* 45 (2004), 2171–2180.

[17] D. E. Taylor, *The Geometry of the Classical Groups* (Heldermann, Berlin, 1992).
[18] D. E. Taylor, ‘Two-graphs and doubly transitive groups’, *J. Combin. Theory Ser. A* 61 (1992), 113–122.
[19] J. Thompson, ‘Nonsolvable finite groups all of whose local subgroups are solvable’, *Bull. Amer. Math. Soc. (N.S.)* 74 (1968), 383–437.
[20] P. H. Tiep and A. E. Zaleskii, ‘Some aspects of finite linear groups: a survey’, *J. Math. Sci. (N.Y.)* 100 (2000), 1893–1914.
[21] D. Winter, ‘The automorphism group of an extraspecial $p$-group’, *Rocky Mountain J. Math.* 2 (1972), 159–168.
[22] H. Zhu, ‘Super-symmetric informationally complete measurements’, *Ann. Physics* 362 (2015), 311–326.

ULRICH DEMPWOLFF, Department of Mathematics, University of Kaiserslautern, Kaiserslautern 67653, Germany
e-mail: dempwolff@mathematik.uni-kl.de

WILLIAM M. KANTOR, Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
e-mail: kantor@uoregon.edu