THE PRIMITIVE RANK 3 EXTENSION OF THE POINTWISE STABILIZER OF $PSp(2m, q)$

BY

ARTHUR YANUSHKA

Introduction

Let G be a finite transitive group of permutations of a finite set X. The *rank* of G is by definition the number of orbits of the stabilizer of a point. The transitive group G is *primitive* if the stabilizer of a point is a maximal subgroup of G. Let H be a finite transitive group of permutations of a finite set Y. Then (G, X) is a *primitive rank* 3 *extension* of (H, Y) if G is a primitive rank 3 permutation group on X and if there is an orbit D of G_a, the pointwise stabilizer of $a \in X$ such that $(G_a, D) \cong (H, Y)$ as permutation groups. Several sporadic simple groups have been discovered as rank 3 extensions of certain known groups.

In this paper we consider a rank 3 extension problem related to the projective symplectic group $PSp(2m, q)$. This group is primitive of rank 3 when considered as a group of permutations of the points of a projective space P of dimension $2m - 1$ over the field of q elements. Indeed for $v \in P$, the group $PSp(2m, q)_v$ has 3 orbits on P, namely $\{v\}$, the set of all points of P unequal to v which are perpendicular to v, which we denote $\Delta(v)$, and the set of all points of P which are not perpendicular to v. We show that the only primitive rank 3 extension of $PSp(2m, q)_v$ on $\Delta(v)$ is the natural one of $PSp(2m, q)$ on P. A precise statement is the following.

THEOREM A. *Let G be a finite transitive group of permutations of a finite set X. Let P be a projective space of dimension $2m - 1$ over the field of q elements. For $v \in P$ let $\Delta(v)$ denote the set of all elements of P which are unequal to v and perpendicular to v. Suppose (G, X) is a primitive rank 3 extension of*

$$(PSp(2m, q)_v, \Delta(v)).$$

Then $X \cong P$ and $G \cong PSp(2m, q)$.

A key step in the proof of this theorem is the determination of the structure of a certain subgroup of G_a for $a \in X$. The identification of this subgroup of G_a depends on the following result about q' subgroups of $Sp(2m, q)$.

THEOREM B. *Let W be a subgroup of $Sp(2m, q)$ for some positive integer $m \geq 2$ and for some prime power q. Suppose $|W|_{q'} = |Sp(2m, q)|_{q'}$. Then:*

(i) *For $m = 2$ and $q = 2$, either $W = Sp(4, 2)$ or $Sp(4, 2)'$.*
(ii) *For $m = 2$ and $q = 3$, either $W = Sp(4, 3)$ or $|Sp(4, 3): W| = 3^3$.*
(iii) *For $m = 2$ and $q > 3$ and for $m > 3$, the group $W = Sp(2m, q)$.*

Received July 26, 1974.

We derived Theorem B independently of the work of G. Seitz [11]. In fact Theorem B is an immediate corollary of a theorem of Seitz on flag-transitive subgroups of Chevalley groups because the group W which satisfies the hypothesis of Theorem B is flag-transitive. Our method of proof differs from Seitz's and involves the determination of the possible structure of W_v for a vector v. We include a proof of Theorem B in this paper since it follows easily from the lemmas needed for the proof of Theorem A. The method of proof of Theorem B generalizes to prove similar statements about q' subgroups for the other Chevalley groups.

1. The proof of Theorem B

The purpose of this section is to prove Theorem B. The proof is by induction on m. Let $W \leq Sp(2m, q)$ such that

$$|W|_{q'} = |Sp(2m, q)|_{q'}.$$

A key step in the proof is the determination of the structure of W_v, the subgroup of W which fixes the vector v. The proof of the theorem involves matrix computation and consists of a sequence of lemmas, some of which will be used in the proof of Theorem A.

LEMMA 1.1. *Let W be a subgroup of $SL(2, q)$. Suppose $|W|_{q'} = |SL(2, q)|_{q'}$. Then:*

(i) *If $q = 2$, either $W = SL(2, 2)$ or W is cyclic of order* 3.
(ii) *If $q = 3$, either $W = SL(2, 3)$ or W/Z is dihedral of order* 4, *where Z denotes the center of $SL(2, q)$.*
(iii) *If $q = 5$, either $W = SL(2, 5)$ or W/Z is the alternating group of degree* 4.
(iv) *If $q = 7$, either $W = SL(2, 7)$ or W/Z is the symmetric group of degree* 4.
(v) *If $q = 11$, either $W = SL(2, 11)$ or W/Z is the alternating group of degree* 5.
(vi) *If $q \notin \{2, 3, 5, 7, 11\}$, the group $W = SL(2, q)$.*

Proof. The lemma follows from an examination of Dickson's complete list of nontrivial subgroups of $PSL(2, q)$. See [8].

Remark. Since $SL(2, q) \cong Sp(2, q)$, Lemma 1.1 gives a list of the q' subgroups of $Sp(2, q)$.

For the prime power q let F denote the Galois field of q elements. Let V_{2m} denote a $2m$-dimensional vector space over F with ordered basis

$$\{e_1, e_2, \ldots, e_m, e_{-m}, \ldots, e_{-2}, e_{-1}\}$$

Let V_{2m}^* denote the set of nonzero points of V_{2m}. Let f be an alternating form defined by $f(e_i, e_{-i}) = 1 = -f(e_{-i}, e_i)$; all other products are zero. Then the matrix J of the form f with respect to the given basis is

$$J = \begin{vmatrix} & 0_m \\ -0_m & \end{vmatrix} \quad \text{where} \quad 0_m = \begin{vmatrix} & & & & 1 \\ & & & 1 & \\ & & \cdot^{\cdot^{\cdot}} & & \\ & 1 & & & \\ 1 & & & & \end{vmatrix}.$$

Note that a blank in a matrix indicates that the entry is zero. By definition the symplectic group

$$Sp(2m, q) = \{A \in GL(2m, q): AJA' = J\},$$

where A' denotes the transpose of A and $GL(2m, q)$ denotes the general linear group of matrices of size $2m$ over F. Denote $Sp(2m, q)$ simply as S. Let S_i denote $S_{\langle e_i \rangle}$, the subgroup of S which fixes the vector $\langle e_i \rangle$. Then

$$S_1 = \left\{ \begin{vmatrix} a & r & d \\ & C & a^{-1}CJr' \\ & & a^{-1} \end{vmatrix} : a, d \in F, r \in V_{2(m-1)}, C \in Sp(2(m-1), q) \right\}.$$

The group S is primitive of rank 3 in its action on the 1-dimensional subspaces of V_{2m}. Indeed for a subspace $\langle v \rangle$, S_v has nontrivial orbits

$$\{\langle w \rangle : f(v, w) = 0, w \neq v\},$$

which we denote $\Delta(v)$ and $\{\langle w \rangle : f(v, w) \neq 0\}$.

Notation. Let $m \geq 2$. Let $M(a, B, d, C)$ denote the matrix

$$\begin{vmatrix} a & B & d \\ & C & a^{-1}CJB' \\ & & a^{-1} \end{vmatrix}$$

where $a, d \in F$ and $a \neq 0$; $B \in V_{2(m-1)}$; $C \in Sp(2(m-1), q)$.

We have the following rule for multiplication:

$$M(a, B, d, C) \cdot M(e, F, h, G) = M(ae, aF + BG, ah + e^{-1}BGJF' + de^{-1}, CG).$$

Note that if $g = M(a, B, d, C)$, then $g^{-1} = M(a^{-1}, -a^{-1}BC^{-1}, -d, C^{-1})$.

Notation. Let N denote $\{M(a, B, d, I): a, d \in F; B \in V_{2(m-1)}\}$. Let U denote $\{M(a, 0, d, I): a, d \in F\}$. Let T denote $\{M(1, 0, d, I): d \in F\}$. Let Q denote $\{M(a, 0, 0, I): a \in F\}$.

Then N, U, T, and Q are subgroups of S_1. The group T consists of the symplectic transvections with center e_1 and $\langle T^s : s \in S \rangle = S$. Clearly $Q \leq U \leq N$ and $N \leq S_1$.

Define a natural map $\sigma\colon Sp(2m, q)_{\langle e_1\rangle} \to Sp(2(m-1), q)$ by

$$M(a, B, d, C) \to C.$$

Then σ is an epimorphism with kernel N.

In order to prove Theorem B, we must determine the structure of $W_1 = W \cap S_1$. We do this by first finding the structure of $W_1 \cap N$ and then W_1.

LEMMA 1.2. *Let X be a subgroup of S_1 such that $Q \leq X \cap N$.*

(i) *If $X \cap N \leq U$, then either $X \cap N = U$ or $X \cap N = Q$.*

(ii) *If $X \cap N \nleq U$ and if $\sigma(XN)$ is transitive on $V^*_{2(m-1)}$, then $X \cap N = N$ if $(m, q) \neq (2, 2)$. If $(m, q) = (2, 2)$, then either $X \cap N = N$ or*

$$|N: X \cap N| = 2.$$

Proof. (i) The group U is a Frobenius group with kernel T and complement Q. The group Q is a maximal subgroup of U.

(ii) Let $B \in \sigma(XN)$. Let x_B be a preimage or inverse image of B in X. Then $x_B = M(a, C, d, B)$ for some a, C, d. which depend on B. If $w \in X \cap N$, then $x_B^{-1}wx_B \in X \cap N$ for all $B \in \sigma(XN)$ because $X \cap N \trianglelefteq X$. Since $X \cap N \nleq U$, there is an element $w = M(A, R, D, I) \in X \cap N$ with $R \neq 0$. Let $y = w \cdot M(A^{-1}, 0, 0, I)$. Then $y = M(1, R, AD, I) \in X \cap N$. So

$$x_B^{-1}yx_B = M(1, a^{-1}RB, a^{-2}AD + 2a^{-2}RBJC', I) \in X \cap N$$

where a, C, d depend on $B \in \sigma(XN)$. To eliminate partially this dependence, compute for $g \in F^*$,

$$z = M(a, 0, 0, I)x_B^{-1}yx_BM(a^{-1}g, 0, 0, I). \tag{1}$$

Then

$$z = M(g, RB, g^{-1}(AD + 2RBJC'), I) \in X \cap N$$

for all $B \in \sigma(XN)$ and $g \in F^*$. Since $R \neq 0$ and $\sigma(XN)$ is transitive on $V^*_{2(m-1)}$, the element RB runs through $V^*_{2(m-1)}$ as B runs through $\sigma(XN)$. Now

$$M(1, -R, d, I) \cdot M(g, R, b, I) = M(g, 0, b + g^{-1}d, I) \in X \cap N$$

for some $b, d \in F$. So $M(a, C, b, I) \in X \cap N$ for all $a \in F^*$, for all $C \in V_{2(m-1)}$ and for some $b \in F$ where b depends on a and C.

Now we claim that b can be chosen arbitrarily for $(m, q) \neq (2, 2)$. Indeed there is a $y = M(-1, R, b, I) \in X \cap N$ with $b \neq 0$. Otherwise $M(-1, R, b, I)$ has $b = 0$ always. For $R = (10\ldots0)$ and $r = (0\ldots01)$,

$$M(-1, R, 0, I) \cdot M(-1, r, 0, I) = M(1, R - r, 1, I),$$

a contradiction. If q is odd, then $y^2 = M(1, 0, -2b, I) \in T$ and $y^2 \neq 1$.

If q is even, then $y = M(1, R, b, I)$ with $b \neq 0$. If $R \neq 0$, then recompute z of (1) to find $z = M(g, RB, g^{-1}b, I) \in X \cap N$. Then

$$zy = M(g, gR + RB, (g + g^{-1})b + RBJR', I) \in X \cap N.$$

If $q \neq 2$, pick $g \in F^*$ such that $g \neq g^{-1}$, then pick $B \in \sigma(XN)$ such that $RB = gR$. So $zx = M(g, 0, (g + g^{-1})b, I) \in X \cap N$ with $(g + g^{-1})b \neq 0$. If $q = 2$, then $z = M(1, RB, 1, I)$ for all $B \in \sigma(XN)$. For $R = (10\ldots0)$ and $r = (010\ldots0)$, if $m \geq 3$, then $RJr' = 0$ and

$$M(1, R, 1, I) \cdot M(1, r, 1, I) = M(1, R + r, 0, I).$$

Then

$$M(1, R + r, 0, I) \cdot M(1, R + r, 1, I) = M(1, 0, 1, I) \in X \cap N.$$

So in all cases except $(m, q) = (2, 2)$, there is $y = M(g, 0, b. I) \in X \cap N$ with $b \neq 0$. By (i), $\langle Q, y\rangle = U \leq X \cap N$. Then

$$M(1, 0, B, I) \cdot M(a, C, b, I) = M(a, C, b + Ba^{-1}, I) \in X \cap N$$

where b depends on a and C and where a, B, C are arbitrary. So

$$M(a, C, B, I) \in X \cap N$$

for all $a, B \in F$ and all $C \in V_{2(m-1)}$. Thus $X \cap N = N$ if $(m, q) \neq (2, 2)$. If $(m, q) = (2, 2)$, then either $X \cap N = N$ or

$$X \cap N = \{I, M(1, r, 1, I) \colon r \in V_2^*\}.$$

This completes the proof of Lemma 1.2.

LEMMA 1.3. *Let X be a subgroup of S_1 such that $Q \leq X \cap N \leq U$. Let $B \in \sigma(XN)$ and let $x_B = M(a, r, d, B)$ be a preimage of B which lies in X, where a, r, d depend on B.*

(i) *If $q \neq 2$, then $r = 0$ and $x_B = M(a, 0, d, B)$. If $Q = X \cap N$ and if $q > 3$, then $d = 0$ and $x_B = M(a, 0, 0, B)$.*

(ii) *If $q = 3$, assume $\sigma(XN) = Sp(2(m-1), 3)$. If $Q = X \cap N$ and if $m \geq 3$, then $d = 0$ and $x_B = M(a, 0, 0, B)$.*

(iii) *If $q = 2$, assume $\sigma(XN) = Sp(2(m-1), 2)$. Then there is $n \in N$ such that for all $B \in \sigma(X)$, $x^n = M(1, 0, d, B)$. If $X \cap N = I$ and if $m \geq 4$, then there is $n \in N$ such that $x^n = M(1, 0, 0, B)$.*

Proof. (i) Fix $B \in \sigma(XN)$. Let $x_B = M(a, r, d, B)$ be a fixed preimage of B which lies in X, where a, r, d depend on B. Let $x_{B^{-1}} = M(A, R, D, B^{-1})$ be a fixed preimage of B^{-1} which lies in X, where A, R, D depend on B^{-1}. Since $Q \leq X \cap N$, the element $M(g, 0, 0, I) \in X$ for all $g \in F^*$. So

$$\begin{aligned} &x_B M(g, 0, 0, I)x_{B^{-1}} \\ &\quad = M(agA, agR + rB^{-1}, agD + A^{-1}rB^{-1}JR' + dg^{-1}A^{-1}, I) \in X \cap N. \end{aligned}$$

Since $X \cap N \leq U$, it follows that $agR + rB^{-1} = 0$ for all $g \in F^*$. For $q \neq 2$ it follows that $R = 0$ and so $x_B = M(a, 0, d, B)$.

Now assume $X \cap N = Q$. Then for all $g \in F^*$,

$$x_B M(g, 0, 0, I)x_{B^{-1}} = M(agA, 0, agD + dg^{-1}A^{-1}, I) \in Q.$$

So $agD + dg^{-1}A^{-1} = 0$ for all $g \in F^*$. For $q \neq 3$ it follows that $D = 0$ and so $x_B = M(a, 0, 0, B)$.

(ii) Let $B \in \sigma(XN)$. Since $X \cap N = Q$, let $x_B = M(1, 0, d, B)$ be a preimage of B which lies in X where d depends on B. Suppose $y_B = M(1, 0, D, B)$ is another preimage of B which lies in X. Then

$$y_B^{-1}x_B = M(1, 0, d - D, I) \in X \cap N = Q.$$

So $d = D$ and d is uniquely determined by B when the (1, 1) entry of the matrix x_B is chosen to be 1. In this case denote the unique d by d_B. Then $x_B = M(1, 0, d_B, B)$. For $C \in \sigma(XN)$, let

$$x_C = M(1, 0, d_C, C) \quad \text{and} \quad x_{BC} = M(1, 0, d_{BC}, BC).$$

Then

$$x_{BC}^{-1}x_Bx_C = M(1, 0, d_B + d_C - d_{BC}, I) \in X \cap N = Q.$$

So $d_{BC} = d_B + d_C$. By assumption $\sigma(XN) = Sp(2(m - 1), 3)$. Thus the rule $B \to d_B$ defines a homomorphism δ from $Sp(2(m - 1), 3)$ into F a group of order 3. If $m > 2$, then $PSp(2(m - 1), 3)$ is a simple group. Since $\ker \delta \trianglelefteq Sp(2(m - 1), 3)$, it follows that $\delta \equiv 0$ if $m > 2$. So $x_B = M(1, 0, 0, B)$ if $m > 2$. If $m = 2$, then $\ker \delta = Sp(2, 3)$ or a Sylow 2 subgroup of $Sp(2, 3)$.

(iii) For $q = 2$ and for $B \in \sigma(XN) = Sp(2(m - 1), 2)$, let $x_B = M(1, r, d, B)$ be a preimage of B in X where r and d depend on B. Let $y_B = M(1, R, D, B)$ be another preimage of B in X. Then

$$y_B^{-1}x_B = M(1, r + R, d + RJr' + D, I) \in X \cap N \leq U.$$

So $r + R = 0$ and r is uniquely determined by B. Denote the unique r by r_B. Then $x_B = M(1, r_B, d, B)$. For $C \in \sigma(XN)$, let

$$x_C = M(1, r_C, e, C) \quad \text{and} \quad x_{BC} = M(1, r_{BC}, f, BC).$$

Then

$$\begin{aligned} &x_{BC}^{-1}x_Bx_C \\ &\quad = M(1, r_C + r_BC + r_{BC}, e + r_BCJr_C' + d + r_{BC}Jr_C' + r_{BC}C^{-1}Jr_B' + f, I) \\ &\qquad \in X \cap N. \end{aligned}$$

So $r_{BC} = r_C + r_BC$. Thus the rule $B \to r_B$ defines a derivation r from $Sp(2(m - 1), 2)$ into $V_{2(m-1)}$. We claim that r is an inner derivation. If r is inner, then there is $R \in V_{2(m-1)}$ such that

$$r_B = R + RB \quad \text{for all } B \in Sp(2(m - 1), 2).$$

Set $n = M(1, R, 0, I)$. Then $n \in N$ and $x_B^n = M(1, 0, d + RBJR', B)$. If in addition $X \cap N = I$, then $x_B^n = M(1, 0, d_B, B)$ where d_B is uniquely determined by B. The rule $B \to d_B$ defines a homomorphism δ from $Sp(2(m - 1), 2)$ into F, a group of order 2. If $m \geq 4$, then $Sp(2(m - 1), 2)$ is a simple group and so $\ker \delta = Sp(2(m - 1), 2)$. If $m = 3$, then $\ker \delta = Sp(4, 2)$ or $Sp(4, 2)'$. If $m = 2$, then $\ker \delta = Sp(2, 2)$ or $Sp(2, 2)'$. If $m \geq 4$, then $x_B^n = M(1, 0, 0, B)$.

It remains to show that r is inner. If $m = 2$, then r is inner because the F-dimension of the first cohomology group of $SL(2, 2)$ with coefficients in V_2 is zero by a theorem of D. Higman [4]. If $m > 2$, then the F-dimension of the first cohomology group of $Sp(2(m-1), 2)$ with coefficients in $V_{2(m-1)}$ is one by a theorem of H. Pollatsek [10]. In fact there is an outer derivation $u: Sp(2(m-1), 2) \to V_{2(m-1)}$ with the property that if T is a symplectic non-orthogonal transvection with center x, then $u(T) = x$.

For $m > 2$ assume that r is outer. There is an inner derivation i such that $ir = u$. Since i is inner, there is $R \in V_{2(m-1)}$ such that $i(B) = RB + B$ for all $B \in Sp(2(m-1), 2)$. Let $n = M(1, R, 0, I)$. Then X^n satisfies the same hypotheses as X and $x_B^n = M(1, u_B, d, B)$. So without loss of generality, assume $n = I$ and $r = u$.

Let B be the transvection with center e_2 and C be the transvection with center e_{-2}. Then $r_B = e_2$ and $r_C = e_{-2}$. Note

$$B = \begin{vmatrix} 1 & & 1 \\ & I & \\ & & 1 \end{vmatrix} \quad \text{and} \quad C = \begin{vmatrix} 1 & & \\ & I & \\ 1 & & 1 \end{vmatrix}.$$

Then $r_{BC} = e_2 + e_{-2} = r_{CB}$ and $r_{CB} + r_{BC}CB = e_2$. But

$$\begin{aligned} x_{BC}x_{CB} &= M(1, r_{BC}, d, BC) \cdot M(1, r_{CB}, e, CB) \\ &= M(1, r_{CB} + r_{BC}CB, e + r_{BC}CBJr'_{CB} + d, I) \in X \cap N. \end{aligned}$$

Since $X \cap N \leq U$, it follows that $r_{CB} + r_{BC}CB = 0$, a contradiction. So r is not outer and this finishes the proof of the lemma.

LEMMA 1.4. *Let X be a subgroup of S_1 such that $XN = S_1$ and $Q \leq X \cap N$. If $(m, q) \neq (2, 2)$, then X is one of the following three subgroups:*

(i) $\{M(a, 0, d_B, B): a, d_B \in F; B \in Sp(2(m-1), q)\}$ *where d_B is determined by B and $d_B = 0$ if $(m, q) \neq (3, 2), (2, 3)$,*

(ii) $\{M(a, 0, d, B): a, d \in F, B \in Sp(2(m-1), q)\}$, *or*

(iii) S_1.

If $(m, q) = (2, 2)$, then X is one of the following four subgroups:

(i) $\{M(1, 0, d_B, B): d_B \in F, B \in Sp(2, 2)\}$,

(ii) $\{M(1, 0, d, B): d \in F, B \in Sp(2, 2)\}$,

(iii) $\{M(1, r, d_{B,r}, B): d_{B,r} \in F, r \in V_2, B \in Sp(2, 2)\}$ *where $d_{B,r}$ is uniquely determined by B and r, or*

(iv) S_1.

Proof. Assume $(m, q) \neq (2, 2)$. Note $\sigma(XN) = Sp(2(m-1), q)$. By Lemma 1.2, either $X \cap N = Q$, U, or N. If $X \cap N = Q$, then for $B \in Sp(2(m-1), q)$, a preimage in X has the form $X_B = M(a, 0, d_B, B)$ where a and d_B depend on B and where $d_B = 0$ if $(m, q) \neq (3, 2), (2, 3)$ by Lemma 1.3.

Then

$$\langle x_B, Q\colon B \in Sp(2(m-1), q)\rangle$$
$$= \{M(a, 0, d_B, B)\colon a, d_B \in F;\ B \in Sp(2(m-1), q)\}$$

is a subgroup of X of order $(q-1)|Sp(2(m-1), q)| = |X|$. So X is of type (i) if $X \cap N = Q$.

If $X \cap N = U$, then $x_B = M(a, 0, d, B)$ where a, d depend on B by Lemma 1.3. Let $n = M(a^{-1}, 0, -d, I) \in U \leq X$. Then $x_B n = M(1, 0, 0, B) \in X$ and

$$\langle M(1, 0, 0, B), U\colon B \in Sp(2(m-1), q)\rangle$$
$$= \{M(a, 0, d, B)\colon a, d \in F;\ B \in Sp(2(m-1), q)\}$$

is a subgroup of X of order $(q-1)q|Sp(2(m-1), q)| = |X|$. So X is of type (ii) if $X \cap N = U$.

If $X \cap N = N$, then $X_B = M(a, r, d, B)$ where a, r, d depend on B. Let $n = M(a^{-1}, -a^{-1}r, -d, I) \in N \leq X$. Then $x_B n = M(1, 0, 0, B) \in X$ and

$$\langle M(1, 0, 0, B), N\colon B \in Sp(2(m-1), q)\rangle = S_1.$$

If $X \cap N = N$, then $X = S_1$.

Now assume $(m, q) = (2, 2)$. By Lemma 1.2, either

$$X \cap N = I,\ U,\ \{M(1, r, 1, I), I\colon r \in V_2^*\} \quad \text{or} \quad N.$$

If $X \cap N = I$, then X is conjugate to a subgroup of type (i) by Lemma 1.3 (iii). If $X \cap N = U$, then X is of type (ii). If

$$X \cap N = \{M(1, r, 1, I), I\colon r \in V_2^*\},$$

let $x_B = M(1, r, d, B)$ and $y_B = M(1, r, e, B)$ be preimages in X of $B \in Sp(2, 2)$. Then

$$x_B y_B^{-1} = M(1, 0, d + e, I) \in X \cap N.$$

So $d = e$ and d is uniquely determined by $r \in V_2$ and $B \in Sp(2, 2)$. Let $x_B = M(1, r, d, B)$. If $r \neq 0$, then

$$n = M(1, r, 1, B) \in X \quad \text{and} \quad x_B n = M(1, 0, 1 + d, B) \in X.$$

Then

$$\langle M(1, 0, d, B), X \cap N\colon B \in Sp(2, 2)\rangle$$
$$= \{M(1, r, d_{r,B}, B)\colon r \in V_2,\ B \in Sp(2, 2)\}$$

where $d_{r,B}$ is uniquely determined by r and B. This group is a subgroup of X of order $2^2|Sp(2, 2)| = |X|$ and X is of type (iii). If $X \cap N = N$, then $X = S_1$ and 1.4 holds.

LEMMA 1.5. *Let W be a subgroup of S such that W is transitive on V_{2m}^* and $\sigma(W_1N) = Sp(2(m-1), q)$. Then*

$$W_1 \not\leq \{M(a, 0, d, B)\colon a, d \in F;\ B \in Sp(2(m-1), q)\}.$$

Proof. Suppose not. Suppose

$$W_1 \leq \{M(a, 0, d, B)\colon a, d \in F;\ B \in Sp(2(m-1), q)\}.$$

Let $(a\ b\ c)' \in V_{2m}^*$ where $a, c \in F$, $c \neq 0$; $b \in V_{2(m-1)}$. Since W is transitive on V_{2m}^*, there is $w \in W$ such that $w(e_1) = (a\ b\ c)'$. Let

$$w = \begin{vmatrix} a & d & g \\ b & E & h \\ c & f & i \end{vmatrix},$$

where $g, i \in F$; $d', f', h \in V_{2(m-1)}$ and where g, i, d, f, h, E depend on a, b, c. We claim that $h = zb$ for some $z \in F$.

Indeed let $K \in \sigma(W_1N)$ such that $K(b) = b$. Then

$$M(1, 0, 0, K^{-1})wM(1, 0, 0, K) = \begin{vmatrix} a & dK & g \\ b & K^{-1}EK & K^{-1}h \\ c & fK & i \end{vmatrix}.$$

So $w^{-1}M(1, 0, 0, K^{-1})wM(1, 0, 0, K) \in W_1$ and this element equals $M(l, 0, m, R)$ for some $l, m \in F$; $R \in Sp(2(m-1), q)$. Then

$$M(1, 0, 0, K^{-1})wM(1, 0, 0, K) = wM(l, 0, m, R)$$

$$= \begin{vmatrix} al & dR & am + gl^{-1} \\ bl & ER & bm + hl^{-1} \\ cl & fR & cm + il^{-1} \end{vmatrix}.$$

So $l = 1$, $m = 0$ since $c \neq 0$ and $K^{-1}h = h$. If $K \in \sigma(W_1N) = Sp(2(m-1), q)$ such that $K(b) = b$, then $K(h) = h$. So $\{b, h\}$ is a linearly dependent set of vectors of $V_{2(m-1)}$ since $Sp(2(m-1), q)$ is primitive in its action on the lines of $V_{2(m-1)}$. So there is $z \in F$ such that $h = zb$.

Since w is a symplectic transformation, $wJw' = J$. Then

$$\text{(2)} \qquad w = \begin{vmatrix} a & (az - g)b'JE & g \\ b & E & zb \\ c & (cz - i)b'JE & i \end{vmatrix}$$

where $ai - cg = 1$ and $E \in Sp(2(m-1), q)$ for some g, z, i, E which depend on a, b, c.

Let $u \in W$ such that $u(e_1) = (a\ b\ c)$ where $a, c \in F$, $c \neq 0$ and $b \in V_{2(m-1)}^*$. Then

$$u = \begin{vmatrix} a & (az - g)b'JE & g \\ b & E & zb \\ c & (cz - i)b'JE & i \end{vmatrix}$$

for some g, z, i, E which depend on a, b, c. Let $v \in W$ such that $v(e_1) = (-z\ 0\ 1)'$ where z is determined by u. Then by (2),

$$v = \begin{vmatrix} -z & & k \\ & H & \\ 1 & & l \end{vmatrix}$$

for some $k, l \in F$; $H \in Sp(2(m-1), q)$ which depend on $-z, 0, 1$. Now

$$uv = \begin{vmatrix} g - az & (az - g)b'JEH & ak + gl \\ & EH & -b \\ i - cz & (cz - i)b'JEH & ck + il \end{vmatrix} \in W$$

where $b \neq 0$. But $(uv)(e_1) = (g - az \quad 0 \quad i - cz)'$. If $i - cz = 0$, then

$$uv \in W_1 \leq \{M(a, 0, d, B)\}.$$

So $(az - g)b'JEH = 0$. Since $E, H \in Sp(2(m-1), q)$ and $b \neq 0$, it follows that $az - g = 0$ and $(uv)(e_1) = (0\ 0\ 0)$, a contradiction. So $i - cz \neq 0$ and $(uv)(e_1) = (g - az \quad 0 \quad i - cz)$. By (2),

$$uv = \begin{vmatrix} g - az & & n \\ & M & \\ i - cz & & r \end{vmatrix}$$

for some M, n, r. This contradiction completes the proof.

Notation. For a natural number i, let $v_i = (q^i - 1)/(q - 1)$.

LEMMA 1.6. *Let W be a subgroup of S such that $|W|_{q'} = |S|_{q'}$. Then W is transitive on V^*_{2m},*

$$|\sigma(W_1N)|_{q'} = |Sp(2(m-1), q)|_{q'} \quad \textit{and} \quad |W_1 \cap N|_{q'} = q - 1.$$

Proof. Note $|W: W_1| \leq v_{2m}$. Now compute $|\sigma(W_1N)|_{q'}$.

$$\begin{aligned} |\sigma(W_1N)|_{q'} &= |W_1|_{q'} \cdot |W_1 \cap N|_{q'}^{-1} \\ &\geq |W|_{q'} \cdot v_{2m}^{-1} \cdot |N|_{q'}^{-1} \\ &= |Sp(2(m-1), q)|_{q'}, \end{aligned}$$

since $|W|_{q'} = |S|_{q'}$. So $|\sigma(W_1N)|_{q'} = |Sp(2(m-1), q)|_{q'}$, $|W_1 \cap N|_{q'} = |N|_{q'}$ and $|W: W_1| = v_{2m}$. To see that $|W: W_{e_1}| = q^{2m} - 1$, use the natural map $\sigma_1: S_{e_1} \to Sp(2(m-1), q)$ defined by the rule $M(1, r, d, B) \to B$. So 1.6 holds.

We can now begin the proof of Theorem B, which proceeds by induction on m.

LEMMA 1.7. *Let W be a subgroup of $Sp(4, q)$. Suppose $|W|_{q'} = |Sp(4, q)|_{q'}$.*

Then:

(i) *For $q \neq 2, 3$, the group $W = Sp(4, q)$.*
(ii) *For $q = 3$, either $W = Sp(4, 3)$ or $|Sp(4, 3): W| = 3^3$.*
(iii) *For $q = 2$, either $W = Sp(4, 2)$ or $Sp(4, 2)'$.*

Proof. (i) By Lemma 1.6, W is transitive on V_4^*,

$$|\sigma(W_1N)|_{q'} = |Sp(2, q)|_{q'} \quad \text{and} \quad |W_1 \cap N|_{q'} = q - 1.$$

Since N is solvable, the q'-Hall subgroup of $W_1 \cap N$ is conjugate to Q by an element n of N. Clearly W^n is transitive on V_4^* and $|\sigma(W_1^nN)|_{q'} = |Sp(2, q)|_{q'}$. So without loss of generality, assume $W_1 \cap N \geq Q$. By Lemma 1.1, $W_1N = S_1$ with possible exceptions if $q \in \{2, 3, 5, 7, 11\}$. By Lemmas 1.5 and 1.4, $W_1 = S_1$ if $q \neq 2, 3$. Since $|W: W_1| = v_4$, it follows that $W = S$. To complete the proof of (i), we must show that the possibility that $\sigma(W_1N)$ is a proper subgroup of $Sp(2, q)$ does not occur for $q \in \{3, 5, 7, 11\}$.

Indeed suppose $\sigma(W_1N) < Sp(2, q)$ for $q \in \{3, 5, 7, 11\}$. We claim that $\sigma(W_1N)$ is transitive on V_2^*. Indeed let $E = \sigma(W_1N)$. By hypothesis $|E| = q^2 - 1$. So E contains Z, the center of $Sp(2, q)$. Now

$$|E_1| \mid (|Sp(2, q)_1|, |E|) = q - 1.$$

Since $q \in \{3, 5, 7, 11\}$, it follows that $|E_1| = 2$ or $q - 1$. If $|E_1| = 2$, then

$$|E: E_1| = (q^2 - 1)/2 \mid |Sp(2, q): Sp(2, q)_1| = q + 1,$$

which does not occur for $q \in \{5, 7, 11\}$. So $|E_1| = q - 1$ and E_1 is conjugate to the subgroup

$$\left\{\begin{vmatrix} x & \\ & x^{-1} \end{vmatrix} : x \in F^*\right\}$$

of 2×2 diagonal matrices. Thus $|E: E_{e_1}| = q^2 - 1$ and $\sigma(W_1N)$ is transitive on V_2^*. If $W_1 \cap N \not\leq U$, then $W_1 \cap N = N$ for $q \in \{3, 5, 7, 11\}$ by Lemma 1.2 (ii). So $W_1 \geq T$ and since W is transitive on V_4^*, it follows that $W = Sp(4, q)$ and $\sigma(W_1N) = Sp(2, q)$, a contradiction. So $W_1 \cap N \leq U$. If $W_1 \cap N = U$, then $W_1 \geq T$, which leads to a contradiction. So $W_1 \cap N = Q$.

For $B \in \sigma(W_1N)$, let $w_B = M(a, r, d, B)$ be a preimage of B which lies in W_1, where a, r, d depend on B. If $q \in \{5, 7, 11\}$, then $r = 0$ and $d = 0$ by Lemma 1.3 (i). Then

$$W_1 = \{M(a, 0, 0, B): a \in F^*, B \in \sigma(W_1N)\}.$$

If $q = 3$, then $w_B = M(a, 0, d, B)$ where a, d depend on $B \in \sigma(W_1N)$. Since $W_1 \cap N = Q$, we can choose $a = 1$ and then d is uniquely determined by B. In this case denote the unique d by d_B. From the proof of Lemma 1.3 (ii), it follows that the rule $B \rightarrow d_B$ defines a homomorphism from $\sigma(W_1N)$ which has order 8 into F which has order 3. So $d_B = 0$ for all $B \in \sigma(W_1N)$ and

$$W_1 = \{M(a, 0, 0, B): a \in F^*, B \in \sigma(W_1N)\}.$$

If $q \in \{3, 5, 7, 11\}$, then $|Sp(4, q): W| = q^4$. But $Sp(4, q)$ has no subgroup of index q^4 by a theorem of H. Mitchell [9]. This is a contradiction.

(ii) Suppose $q = 3$ and $\sigma(W_1N) = Sp(2, 3)$. So $W_1N = S_1$. By Lemma 1.4 either $W_1 = S_1$ in which case $W = S$ since W is transitive or

$$W_1 = \{M(a, 0, d, B): a, d \in F, B \in Sp(2, 3)\}$$

in which case a contradiction results by Lemma 1.5 or

$$W_1 = \{M(a, 0, d_B, B): a, d_B \in F; B \in Sp(2, 3); \ker d = Sp(2, 3) \text{ or } Sp(2, 3)'\}.$$

If $\ker d = Sp(2, 3)$, then a contradiction results by Lemma 1.5. So $\ker d = Sp(2, 3)'$ and $|Sp(4, 3): W| = 3^3$. Note $Sp(4, 3)$ has a subgroup of index 3^3 by a theorem of H. Mitchell [9].

(iii) Suppose $q = 2$ and $\sigma(W_1N) = Sp(2, 2)$. So $W_1N = S_1$. Apply Lemma 1.4. If $W_1 = S_1$, then $W = S$. If

$$W_1 = \{M(1, r, d_{r,B}, B): d_{r,B} \in F, r \in V_2, B \in Sp(2, 2)\},$$

then $|S: W| = 2$. Since $Sp(4, 2)$ is the symmetric group of degree 6, it follows that W is the alternating group of degree 6. If

$$W_1 = \{M(a, 0, d, B): a, d \in F, B \in Sp(2, 2)\},$$

then $W_1 \geq T$ and so $W = S$, a contradiction. If

$$W_1 = \{M(a, 0, d_B, B): a, d_B \in F; B \in Sp(2, 2); \ \ker d = Sp(2, 2) \text{ or } Sp(2, 2)'\}$$

then $|S: W| = 2^4$. But the symmetric group of degree 6 has no subgroup of index 2^4 by a theorem in B. Huppert [8].

Now suppose $\sigma(W_1N) < Sp(2, 2)$. Then $\sigma(W_1N)$ is transitive on V_2^*. If $W_1 \cap N \not\leq U$, then by Lemma 1.2 either $W_1 \cap N = N$ in which case $W_1 \geq T$ and so $W = S$, a contradiction or $|N: W_1 \cap N| = 2$ in which case $|W_1| = 2^2 \cdot 3$ and $|S: W| = 2^2$. But the symmetric group of degree 6 has no subgroup of index 2^2 [8]. If $W_1 \cap N \leq U$, then either $W_1 \cap N = U = T$ in which case $W_1 \geq T$ and $W = S$, a contradiction or $W_1 \cap N = I$ in which case $|W_1| = 3$ and $|S: W| = 2^4$. But the symmetric group of degree 6 has no subgroup of index 2^4. This completes the proof of 1.7.

LEMMA 1.8. *Let W be a subgroup of $Sp(2m, q)$ where $m > 2$. Suppose $|W|_{q'} = |Sp(2m, q)|_{q'}$. Suppose Theorem* B *holds for $2 \leq m_1 < m$. Then $W = Sp(2m, q)$.*

Proof. By Lemma 1.6, W is transitive on V_{2m}^*,

$$|\sigma(W_1N)|_{q'} = |Sp(2(m-1), q)|_{q'} \quad \text{and} \quad |W_1 \cap N|_{q'} = q - 1.$$

Since N is solvable, we may assume without loss of generality that the q'-Hall subgroup of $W_1 \cap N$ is Q. By the induction assumption,

$$\sigma(W_1N) = Sp(2(m-1), q) \quad \text{if } (m, q) \notin \{(3, 2), (3, 3)\}.$$

So $W_1N = Sp(2m, q)_1$ if $(m, q) \notin \{(3, 2), (3, 3)\}$. By Lemmas 1.4 and 1.5, we have $W_1 = Sp(2m, q)_1$. Because $|W: W_1| = v_{2m}$, it follows that $W = Sp(2m, q)$.

Suppose $(m, q) = (3, 3)$ and $\sigma(W_1N) = Sp(4, 3)$. Then $W = Sp(6, 3)$ by Lemmas 1.4 and 1.5. Suppose $|Sp(4, 3): \sigma(W_1N)| = 3^3$. From the proof of Lemma 1.7 (ii) we know that $\sigma(W_1N)$ is transitive on V_4^*. If $W_1 \cap N \nleq U$ then by Lemma 1.2 (ii), $W_1 \cap N = N$, $W_1 \geq T$ and so $W = Sp(6, 3)$, a contradiction. If $W_1 \cap N = U \geq T$, then $W = Sp(6, 3)$, a contradiction. So

$$W_1 \cap N = Q.$$

For $B \in \sigma(W_1N)$ let $x_B = M(a, r, d, B)$ be a preimage of B which lies in W_1. By Lemma 1.3 (i), $r = 0$. From the proof of Lemma 1.3 (ii) it follows that d is uniquely determined by B when $a = 1$ so that the rule $B \to d_B$ defines a homomorphism d from $\sigma(W_1N)$ into F, a group of order 3. If $\ker d \neq \sigma(W_1N)$, then $|\sigma(W_1N): \ker d| = 3$ and $|Sp(4, 3): \ker d| = 3^4$. But $Sp(4, 3)$ has no subgroup of index 3^4 by a result in B. Huppert [8]. So $\ker d = \sigma(W_1N)$ and $x_B = M(1, 0, 0, B)$. Since $W_1 \cap N = Q$, it follows that

$$W_1 = \{M(a, 0, 0, B): a \in F^*, B \in \sigma(W_1N)\}.$$

We wish to apply Lemma 1.5 to W to derive a contradiction. Its proof holds for $\sigma(W_1N) < Sp(4, 3)$, if for all $v \in V_4^*$ with $v \neq e_1$, there is $K \in \sigma(W_1N)_{e_1}$ such that $K(v) \neq v$. Indeed this condition is satisfied because

$$\sigma(W_1N)_{e_1} = \{M(1, 0, d_B, B).\ d_B \in F, B \in Sp(2, 3)\},$$

where $\ker d$ is a Sylow 2 subgroup of $Sp(2, 3)$.

Suppose $(m, q) = (3, 2)$ and $\sigma(W_1N) = Sp(4, 2)$ or $Sp(4, 2)'$. Then $W_1N = S_1$ or $|S_1: W_1N| = 2$. If $W_1 \cap N \nleq U$, then by Lemma 1.2 (ii), $W_1 \cap N = N$, $W_1 \geq T$ and $W = S$. If $W_1 \cap N = U$, then $W = S$, a contradiction. So $W_1 \cap N = I$ and $|W_1| = |Sp(4, 2)|$ or $|Sp(4, 2)'|$. Then $|Sp(6, 2): W| = 2^5$ or 2^6. But $Sp(6, 2)$ has no subgroups with these indices by a theorem of J. Frame [3]. This contradiction completes the proof of Lemma 1.8 and of Theorem B.

2. Facts about rank 3 groups

Assume (G, X) is a primitive rank 3 permutation group. For $a \in X$ denote the G_a orbits by $\{a\}$, $D(a)$ of length k and $C(a)$ of length l. For $b \in D(a)$ let $\lambda = |D(a) \cap D(b)|$. For $b \in C(a)$ let $\mu = |D(a) \cap D(b)|$. We now collect the necessary facts about rank 3 groups.

LEMMA 2.1. *Let G be a primitive rank 3 group of even order. Then:*

(i) $\mu l = k(k - \lambda - 1)$.

(ii) $0 < \mu < k$.

(iii) *Let $D = (\lambda - \mu)^2 + 4(k - \mu)$. Then D is a square.*

(iv) *$a \in D(b)$ iff $b \in D(a)$.*

(v) *$D(a)$ and $C(a)$ are each self-paired orbits of G_a.*

(vi) *If $b \in D(a)$, then there is $g \in G$ such that $g(a) = b$ and $g(b) = a$.*

Proof. See [5], [12].

Denote $a \cup D(a)$ simply as $a^{\perp}$. For $a \neq b$ define the "line" $R(ab)$ by

$$R(ab) = \bigcap\{z^{\perp}: a, b \in z^{\perp}\}.$$

Call $R(ab)$ *totally singular* (resp. *hyperbolic*) if $b \in D(a)$ (resp. $b \in C(a)$).

LEMMA 2.2. *Let G be a primitive rank 3 group of even order. Then:*

(i) *G is transitive on totally singular (resp. hyperbolic) lines.*

(ii) *If $b \in D(a)$ and if $x \in R(ab) - \{a\}$, then $R(ax) = R(ab)$.*

(iii) *If $b \in D(a)$, then $x \in R(ab)$ iff $a^{\perp} \cap x^{\perp} = a^{\perp} \cap b^{\perp}$.*

(iv) *If $b \in D(a)$, then $G_{R(ab)}$, the global stabilizer of $R(ab)$, is 2 transitive on the points of $R(ab)$ unless $R(ab) = \{a, b\}$.*

(v) *If $\mu > \lambda + 1$, then $G_{R(xy)}$ is 2 transitive on the points of $R(xy)$ unless $R(xy) = \{x, y\}$.*

Proof. See [5].

Denote the pointwise stabilizer in G of $a^{\perp}$ simply as $T(a)$.

LEMMA 2.3. *Let G be a primitive rank 3 group of even order. Then:*

(i) $\bigcap\{T(x): x \in D(a)\} = 1$.

(ii) *If $\mu > \lambda + 1$, then $|T(a)|$ divides $(|R(af)| - 1)$ for $f \in C(a)$.*

Proof. See [5], [6].

3. The proof of Theorem A for $m = 2$

For the rest of the paper, we assume that $(G. X)$ is a primitive rank 3 extension of $(PSp(2m, q)_v, \Delta(v))$ for $m \geq 2$ and $v \in P$, the projective space formed from V_{2m}. Denote $PSp(2m, q)$ simply as S and for a basis element $e_r \in P$ denote $PSp(2m, q)_{e_r}$ simply as S_r. Fix $a \in X$. Let $i: D(a) \to \Delta(e_1)$ be the bijection and $j: G_a \to S_1$ be the isomorphism which establish the permutation isomorphism of $(G_a, D(a))$ and $(S_1, \Delta(e_1))$. That is, for all $x \in D(a)$ and for all $g \in G_a$,

$$i(g(x)) = (j(g))(i(x)).$$

Since S_1 is not faithful on $\Delta(e_1)$, it follows that G_a is not faithful on $D(a)$ and so $T(a) \neq 1$. Now

$$k = |D(a)| = q(q^{2m-2} - 1)/(q - 1).$$

For $r \in \mathrm{N}$, the set of natural numbers, let v_r denote $(q^r - 1)/(q - 1)$. Then $k = qv_{2m-2}$.

The purpose of the next two sections is to prove Theorem A. First we determine the parameters λ, μ, and l of G and then we identify the subgroup G_{abf} for $b \in D(a)$, $f \in C(a) \cap D(b)$ by Theorem B. Then we show that the number of points of an abstract "line" $R(xy)$ is $q + 1$. From these results we can conclude that X is a projective space and that G is a group of symplectic collineations. The details of the proof differ somewhat according as $m = 2$ or $m > 2$.

The rest of Section 3 considers the case $m = 2$ while Section 4 considers the case $m > 2$.

Now assume $m = 2$. Then $S = PSp(4, q)$.

LEMMA 3.1. *The group* S_1 *is a transitive rank* 3 *group on* $\Delta(e_1)$ *with subdegrees* 1, $q - 1$, *and* q^2.

Proof. Since $e_2 \in \Delta(e_1)$, the group $S_{2,1}$ equals

$$\left\{ \left| \begin{matrix} a & & c & d \\ & b & e & a^{-1}bc \\ & & b^{-1} & \\ & & & a^{-1} \end{matrix} \right| Z\colon a, b, c, d, e \in F \right\}.$$

The group $S_{2,1}$ on $\Delta(e_1)$ has orbits

$$\{e_1\}, \quad \{(a, b, 0, 0)\colon a, b \in F^*\}, \quad \text{and} \quad \{(c, e, b^{-1}, 0)\colon b, c, e \in F\}.$$

So 3.1 holds.

We wish to determine the intersection numbers λ and μ of the rank 3 group G. For $b \in D(a)$ and for $c \in D(a) \cap D(b)$, it follows that $c^{G_{ab}} \subseteq D(a) \cap D(b)$ and that $D(a) \cap D(b)$ is a union of nontrivial G_{ab} orbits on $D(a)$. So

$$\lambda \in \{0, q - 1, q^2, q^2 + q - 1\}$$

from Lemma 3.1. In this section let b, c be the fixed elements of $D(a)$ such that $i(b) = e_2$ and $i(c) = e_{-2}$.

LEMMA 3.2. $\lambda \neq 0$.

Proof. Suppose $\lambda = 0$. Now

$$|G_{ba}\colon G_{bac}| = |S_{2,1}\colon S_{2,1,-2}| = q^2$$

by Lemma 2.1. Then

$$\begin{aligned} |G_{bc}\colon G_{bca}| &= |G_b\colon G_{ba}| \cdot |G_{ba}\colon G_{bac}| \cdot |G_b\colon G_{bc}|^{-1} \\ &= kq^2/l \\ &= \mu q^2/(k - 1), \end{aligned}$$

since by Lemma 2.1, $\mu l = k(k - \lambda - 1) = k(k - 1)$. Since $k - 1 = q^2 + q - 1$ and $\mu q^2/(k - 1) \in \mathbf{N}$, it follows that $(k - 1) \mid \mu$. But $\mu \leq k - 1$ because G is primitive. So $\mu = k - 1$. Then

$$D = (\lambda - \mu)^2 + 4(k - \mu) = (k - 1)^2 + 4 = x^2$$

for some $x \in \mathbf{N}$. Then $4 = (x - (k - 1))(x + (k - 1))$ implies $k = 5/2$ or 1, a contradiction. So $\lambda \neq 0$ and 3.2 holds.

LEMMA 3.3. $\lambda = q - 1$ *and* $\mu l = kq^2$.

Proof. If $\lambda = q^2 + q - 1 = k - 1$, then $\mu = 0$ because

$$\mu l = k(k - \lambda - 1)$$

and thus G is imprimitive, a contradiction.

Suppose $\lambda = q^2$. So $D(a) \cap D(b)$ equals the G_{ab} orbit of length q^2. Define a subgroup R of G_a by

$$R = \bigcap \{G_{abx}\colon x \text{ lies in the } G_{ab} \text{ orbit of length } q^2\}.$$

Then

$$j(R) = \bigcap \{S_{1,2,v}\colon v \text{ lies in the } S_{1,2} \text{ orbit of length } q^2\}.$$

It follows from matrix computation that

$$j(R) = \left\{ \begin{vmatrix} 1 & & & d \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{vmatrix} Z\colon d \in F \right\},$$

where Z is the center. Note $j(R)$ fixes $\Delta(e_1)$ pointwise.

Since the G_{ab} orbit of length q^2 lies in $D(b)$, the pointwise stabilizer in G_b of the $D(b)$ orbit is a subgroup of R; that is $T(b) \leq R$. Let $t \in T(b)$. Then $j(t) \in j(R)$ and $j(t)$ fixes $\Delta(e_1)$ pointwise. So t fixes $D(a)$ pointwise and $t \in T(a)$. Thus $T(b) \leq T(a)$. Since G is transitive on X, there is $h \in G$ such that $h(b) = a$. Then $T(b)^h = T(a)$ and so $T(b) = T(a)$. For $x \in D(a)$, there is $g \in G_a$ such that $g(b) = x$. So $T(a) = T(b)^g = T(x)$ and

$$T(a) = \bigcap \{T(x)\colon x \in D(a)\}.$$

By Lemma 2.3 (i). $\bigcap \{T(x)\colon x \in D(a)\} = 1$. So $T(a) = 1$. But by hypothesis $T(a) \neq 1$, a contradiction. So $\lambda \neq q^2$ and $\lambda = q - 1$. So 3.3 is proved.

LEMMA 3.4. (i) *For $y \in D(x)$, the "line" $R(xy) = x^\perp \cap y^\perp$ and $|R(xy)| = q + 1$.*

(ii) *For $x \in D(a)$, $i(R(ax)) = \langle e_1, i(x)\rangle$ where $\langle e_1, i(x)\rangle$ denotes the projective line determined by e_1 and $i(x)$.*

Proof. (i) Clearly $R(ab) \subseteq a^\perp \cap b^\perp$, where $a^\perp \cap b^\perp$ is the union of $\{a, b\}$ and the orbit of G_{ab} of length $q - 1$. So $i(a^\perp \cap b^\perp)$ is the union of $\{e_1, e_2\}$ and the orbit of S_{12} of length $q - 1$ and

$$i(a^\perp \cap b^\perp) = \langle e_1, e_2\rangle.$$

Let $u \in a^\perp \cap b^\perp - \{a\}$. Then $a^\perp \cap u^\perp$ is the union of $\{a, u\}$ and the orbit of G_{au} of length $q - 1$. So

$$i(a^\perp \cap u^\perp) = \langle e_1, i(u)\rangle = \langle e_1, e_2\rangle = i(a^\perp \cap b^\perp)$$

since $i(u) \in \langle e_1, e_2\rangle - \{e_1\}$. So $a^\perp \cap u^\perp = a^\perp \cap b^\perp$ which implies $u \in R(ab)$. So $a^\perp \cap b^\perp \subseteq R(ab)$ and $a^\perp \cap b^\perp = R(ab)$. Since G is a transitive group of rank 3, G is transitive on totally singular lines. It follows that for $y \in D(x)$, the line $R(xy) = x^{\perp} \cap y^{\perp}$.

(ii) For $x \in D(a)$, the line $R(ax) = a^{\perp} \cap x^{\perp}$ and $i(R(ax))$ is the union of $\{e_1, i(x)\}$ and the orbit of $S_{1,i(x)}$ of length $q - 1$. Thus $i(R(ax)) = \langle e_1, i(x)\rangle$. This completes the proof.

We wish to determine the parameter μ. Since $C \in D(a) \cap C(b)$,

$$\begin{aligned}|G_{bc}: G_{bca}| &= |G_b: G_{ba}| \cdot |G_{ba}: G_{bac}| \cdot |G_b: G_{bc}|^{-1}\\ &= kq^2/l\\ &= \mu q^2/(k - \lambda - 1)\\ &= \mu.\end{aligned}$$

Now

$$j(G_{abc}) = S_{1,2,-2} = \left\{\left|\begin{matrix} x & & & z \\ & y & & \\ & & y^{-1} & \\ & & & x^{-1}\end{matrix}\right| Z: x, y, z \in F\right\},$$

a group of order $\varepsilon^{-1}(q - 1)^2 q$, which has index q^2 in $j(G_{ab}) = S_{1,2}$ where $\varepsilon = (2, q - 1)$. Let

$$Q = \left\{\left|\begin{matrix} x & & & \\ & y & & \\ & & y^{-1} & \\ & & & x^{-1}\end{matrix}\right| Z: x, y \in F\right\}.$$

Then Q is a q'-Hall subgroup of the solvable group $S_{1,2}$.

Since G is rank 3 of even order, by Lemma 2.1 the D orbit of G_a is self-paired and there is $g \in G$ such that $g(a) = b$ and $g(b) = a$. Then

$$\mu = |G_{bc}: G_{bca}| = |G_{ag(c)}: G_{ag(c)b}|.$$

The q'-Hall subgroup of $G_{abg(c)}$ is conjugate to $j^{-1}(Q)$ by an element $h \in G_{ab}$. Let $f = hg(c)$. Then $f \in C(a) \cap D(b)$. Now $\mu = |G_{af}: G_{abf}|$ where G_{abf} is conjugate to G_{abc}. Also

$$|G_{abf}| = \varepsilon^{-1}(q - 1)^2 q, \; |G_{ab}: G_{abf}| = q^2 \quad \text{and} \quad G_{abf} \geq j^{-1}(Q).$$

We will determine the value of μ by determining the possible structure of $j(G_{abf})$ in $S_{1,2}$. Denote $j(G_{abf})$ simply as K.

LEMMA 3.5. *The group K is one of the following three groups:*

(i)
$$\left\{\left|\begin{matrix} x & & & z \\ & y & & \\ & & y^{-1} & \\ & & & x^{-1}\end{matrix}\right| Z\right\},$$

(ii) $$\left\{\begin{vmatrix} x & & z & \\ & y & & x^{-1}yz \\ & & y^{-1} & \\ & & & x^{-1} \end{vmatrix} Z\right\}$$

(iii) $$\left\{\begin{vmatrix} x & & & \\ & y & z & \\ & & y^{-1} & \\ & & & x^{-1} \end{vmatrix} Z\right\}.$$

where x, y, $z \in F$.

Proof. Let $h \in K - Q$. Then $h \in S_{1,2} - Q$. Let

$$h = \begin{vmatrix} x & & m & t \\ & y & n & x^{-1}ym \\ & & y^{-1} & \\ & & & x^{-1} \end{vmatrix} Z$$

where at least one of m, n, t is nonzero. Since $K > Q$, we may assume without loss of generality that $x = y = 1$. If not, consider

$$h_1 = \begin{vmatrix} x^{-1} & & & \\ & y^{-1} & & \\ & & y & \\ & & & x \end{vmatrix} Z \cdot h.$$

Then h has at least $\varepsilon^{-1}(q - 1)$ Q—conjugates since for u, $v \in F^*$,

$$\begin{vmatrix} u & & & \\ & v & & \\ & & v^{-1} & \\ & & & u^{-1} \end{vmatrix} \cdot h \cdot \begin{vmatrix} u^{-1} & & & \\ & v^{-1} & & \\ & & v & \\ & & & u \end{vmatrix} Z = \begin{vmatrix} 1 & & uvm & u^2t \\ & 1 & v^2n & uvm \\ & & 1 & \\ & & & 1 \end{vmatrix} Z.$$

Now $\langle Q, h\rangle \supseteq \{Q, sh^r: r, s \in Q\}$, a set of order at least

$$\varepsilon^{-1}(q - 1)^2 + \varepsilon^{-2}(q - 1)^2(q - 1) > |K|/2.$$

So $\langle Q, h\rangle = K$ and exactly one of m, n, t is nonzero. This implies 3.5.

LEMMA 3.6. *The group K is not equal to $S_{1,2,-2}$.*

Proof. Suppose $K = S_{1,2,-2}$. Then $G_{abf} = G_{abc}$ and $T(a) \leq G_{abc} \leq G_f$ where $f \in C(a)$. For $x \in C(a)$ there is $g \in G_a$ such that $g(f) = x$. Then

$$T(a) \leq G_f^g = G_x \quad \text{and} \quad T(a) \leq \bigcap \{G_x: x \in C(a)\}.$$

But by definition $T(a) = \bigcap \{G_x: x \in a \cup D(a)\}$. So

$$T(a) = \bigcap \{G_x: x \in X\} = 1.$$

This contradiction proves the lemma.

LEMMA 3.7. (i) *For* $x \in D(a) \cap D(b)$,

$$G_{af} \cap G_{a,R(ax)} = G_{axf}.$$

(ii) $G_{af} \not\leq G_{a,R(ab)}$.
(iii) $\mu = q + 1$ *and* $l = q^3$.
(iv) *Case* (ii) *of Lemma* 3.5 *does not occur.*

Proof. (i) Clearly $G_{axf} \leq G_{af} \cap G_{a,R(ax)}$. Let

$$g \in G_{af} \cap G_{a,R(ax)}.$$

Then $g(x) \in R(ax) \cap D(f)$. If $g(x) \neq x$, then

$$a \in R(ax) = R(xg(x)) \subseteq f^{\perp},$$

a contradiction. So $g(x) = x$ and $x \in G_{axf}$.

(ii) If $G_{af} \leq G_{a,R(ab)}$, then $G_{af} = G_{af} \cap G_{a,R(ab)} = G_{abf}$ and

$$\mu = |G_{af}: G_{abf}| = 1.$$

Then

$$D = (q-2)^2 + 4(q^2 + q - 1) = 5q^2$$

is a square, a contradiction. So $G_{af} \not\leq G_{a,R(ab)}$ and there is $g \in G_{af} - G_{a,R(ab)}$ such that $g \notin G_{abf}$.

(iii) $\mu = |G_{af}: G_{afb}| = |b^{G_{af}}|$. We compute the possible values for μ from the action of G_{abf} on $\{R(ax): x \in D(a)\}$. Now

$$b^{G_{af}} = \{b\} \cup \bigcup \{x^{G_{abf}}: \text{there is } g \in G_{af} \text{ with } g(b) = x\}.$$

For $x \in D(a) \cap D(f)$, by (i), $G_{afx} = G_{afR(ax)}$ and so $G_{abfx} = G_{abfR(ax)}$. Then

$$|x^{G_{abf}}| = |G_{abf}: G_{abfx}| = |G_{abf}: G_{abfR(ax)}| = |R(ax)^{G_{abf}}|.$$

By Lemma 3.4 (ii), for $x \in D(a)$, $i(R(ax)) = \langle e_1, i(x)\rangle$. So the action of G_{abf} on $\{R(ax): x \in D(a)\}$ can be computed from the action of $j(G_{abf}) = K$ on $\{\langle e_1, e_2\rangle, \langle e_1, (0\ u\ 1\ 0)'\rangle: u \in F\}$.

In case (ii) of Lemma 3.5, on the above set K has orbits of lengths 1, 1, $(q-1)/2$, $(q-1)/2$ if q is odd and of lengths 1, 1, $q-1$ if q is even. Notice that K fixes $\langle e_1, e_{-2}\rangle$ but does not fix e_{-2}. By (i) $c \notin D(a) \cap D(f)$. Since $b \in D(a) \cap D(f)$, there does not exist $g \in G_{af}$ such that $g(b) = c$. Since there does exist $g \in G_{af} - G_{afb}$ by (ii), $g(b)$ lies in an orbit of length $(q-1)/2$ if q is odd or of length $q-1$ if q is even. So $\mu = (q+1)/2$ or q if q is odd and $\mu = q$ if q is even in case (ii).

If $\mu = (q+1)/2$, then

$$\begin{aligned} D &= (q - 1 - (q+1)/2)^2 + 4(q^2 + q - (q+1)/2) \\ &= (17q^2 + 2q + 1)/4 \\ &= x^2 \end{aligned}$$

for some $x \in \mathbf{N}$. So $q(17q + 2) = (2x - 1)(2x + 1)$. Since $(2x - 1, 2x + 1) = 1$ and q is a prime power, either $q \mid (2x - 1)$ or $q \mid (2x + 1)$. If there is $t \in \mathbf{N}$ such that $qt = 2x - 1$, then

$$17q + 2 = t(qt + 2) \quad \text{and} \quad (17 - t^2)q = 2(t - 1) \geq 0.$$

So $t \in \{1, 2, 3, 4\}$ and a contradiction results in each case. If there is $t \in \mathbf{N}$ such that $qt = 2x + 1$, then

$$17q + 2 = (qt - 2)t \quad \text{and} \quad (t^2 - 17)q = 2(t + 1) \geq (t^2 - 17)3$$

because q is odd. So $53 \geq t(3t - 2)$ and $t \in \{1, 2, 3, 4\}$. For these values of t, $2(t + 1) > 0$ while $(t^2 - 17)q < 0$, a contradiction. So $\mu \neq (q + 1)/2$.

If $\mu = q$, then

$$D = (q - 1 - q)^2 + 4(q^2 + q - q) = 1 + 4q^2 = x^2$$

for some $x \in \mathbf{N}$. Then $1 = (x - 2q)(x + 2q)$, which implies $4q = 2$, a contradiction. So $\mu \neq q$ and case (ii) does not occur.

So case (iii) of Lemma 3.5 must occur. On

$$\{\langle e_1, e_2\rangle, \langle e_1, (0\ u\ 1\ 0)\rangle' : u \in F\},$$

the group K has orbits of lengths 1 and q. Since there is $g \in G_{af} - G_{abf}$, the parameter $\mu = q + 1$. Since $\mu l = q^3(q + 1)$, the parameter $l = q^3$. This completes the proof of 3.7.

LEMMA 3.8. *If $q \neq 2, 3$, then*

$$j(G_{af}) = \left\{ \left| \begin{matrix} x & & \\ & B & \\ & & x^{-1} \end{matrix} \right| Z : x \in F, B \in SL(2, q) \right\}.$$

Proof. Define M a subgroup of G_a by

$$M = \bigcap \{G_{a, R(ax)} : x \in D(a)\}.$$

By Lemma 3.5 (i), $G_{af} \cap M = G_{abf} \cap M$. Since $i(R(ax)) = \langle e_1, i(x)\rangle$ for $x \in D(a)$,

$$\begin{aligned} j(M) &= \bigcap \{S_{1, \langle e_1, v\rangle} : v \in \Delta(e_1)\} \\ &= \{M(x, r, y, I)Z : x, y \in F; r \in V_2\} \\ &= N. \end{aligned}$$

Define a map $\sigma: S_1 \to SL(2, q)$ by $M(x, r, y, B)Z \to B$. Then σ is an epimorphism with kernel N.

Now since $\mu = q + 1$ and $K = j(G_{abf})$,

$$|\sigma(j(G_{af})N)| = |j(G_{af}) : K| \cdot |K| \cdot |K \cap N|^{-1} = |SL(2, q)|.$$

So $j(G_{af})N = S_1$ and $G_{af} \cap N = Q$. Apply Lemma 1.4 to see that 3.8 holds.

Let (G, X) be a primitive rank 3 group of even order. Associate to G a block design A' whose points are the elements of X and whose blocks are the symbols $b^\perp$, one for each $b \in X$. A point c and a block $b^\perp$ are defined to be *incident* if $c \in \{b\} \cup D(b) = b^\perp$. In A', two blocks $a^\perp$ and $b^\perp$ have $\lambda + 2$ points in common if $b \in D(a)$ and μ points in common if $b \notin a^\perp$. The group G is faithfully represented as a group of collineations of A' when the action of $g \in G$ on the points and blocks is defined by

$$a \to g(a), \qquad a^\perp \to (g(a))^\perp.$$

The correspondence $a \leftrightarrow a^\perp$ defines a polarity δ of A' and the collineations induced by G commute with δ.

LEMMA 3.9. *For $y \in C(x)$, $|R(xy)| = q + 1$.*

Proof. Let $|R(xy)| = h + 1$. Since $\mu = \lambda + 2$, the design A' is a symmetric design. In a symmetric design,

$$2 \leq |R(xy)| \leq (n - (\lambda + 2))/(k + 1 - (\lambda + 2)) = q + 1$$

by a theorem in P. Dembowski [1]. So $h \leq q$. By Lemma 2.3 (ii), $|T(a)| \mid h$. Since $T(a) \neq 1$, $h > 1$. If $q = 2$ (resp. 3), then $h = 2$ (resp. 3).

Assume $q > 3$. Since G is primitive and $\mu = \lambda + 2$, the group $G_{R(ab)}$ is 2-transitive on the points of $R(ab)$ by Lemma 2.2. Since $G_{R(af),a,f} = G_{af}$, it follows that $|G_{R(af),a}\colon G_{af}| = h$. Let $g \in G_{a,R(af)} - G_{af}$. Then $g \in G_a - G_{af}$. Let

$$j(g) = M(x, r, y, B)Z$$

where either $r \neq 0$ or $y \neq 0$. By Lemma 3.8, $M(1, 0, 0, B^{-1})Z \in j(G_{af})$ and so

$$j(g) \cdot M(1, 0, 0, B^{-1})Z = M(x, rB^{-1}, y, I)Z \in j(G_{a,R(af)}) \cap N.$$

Now $j(G_{a,R(af)})N = S_1$ and $j(G_{a,R(af)}) \cap N \geq Q$. If $r \neq \bar{0}$ then from Lemma 1.4, $j(G_{a,R(af)}) = S_1 = j(G_a)$ so

$$h = |G_{a,R(af)}\colon G_{af}| = |G_a\colon G_{af}| = l = q^3,$$

a contradiction as $h \leq q$. So $r = \bar{0}$ and $y \neq 0$. From Lemma 1.4,

$$j(G_{a,R(af)}) = \{M(x, 0, y, B)Z\colon x, y \in F, B \in SL(2, q)\}.$$

So $|G_{a,R(af)}\colon G_{af}| = q = h$, as claimed.

LEMMA 3.10. (i) *The design A' is isomorphic to the system of points and hyperplanes of a projective space of dimension* 3 *over F.*

(ii) $G \cong PSp(4, q)$.

Proof. (i) The design A' is a symmetric design in which lines carry $q + 1$ points by Lemmas 3.4 and 3.9. By a theorem of P. Dembowski and A. Wagner [2], it follows that A' is isomorphic to the system of points and hyperplanes of a projective space P over F. The dimension is 3 because $|b^\perp| = qv_2 + 1 = v_3$.

(ii) The group G acts on $A' \cong P$ and G leaves the polarity $b \leftrightarrow b^{\perp}$ invariant for $b \in X$. So G is a subgroup of the automorphism group of A', which is isomorphic to the group of symplectic collineations of P. The nontrivial elements of $T(b)$ fix the hyperplane $b^{\perp}$ pointwise and fix no point outside this hyperplane. So these elements are symplectic elations. For each $b \in X \cong P$, the group G contains a symplectic elation with center x. By a theorem of D. Higman and J. McLaughlin [7], it follows that there is a subgroup H of G such that $H \cong PSp(4, q)$. Since $|G| = v_4|G_a| = v_4|S_1| = |PSp(4, q)|$, it follows that $G \cong PSp(4, q)$. Thus 3.10 holds and Theorem A is proved for $m = 2$.

4. The proof of Theorem A for $m > 2$

In this section we assume that $m > 2$.

LEMMA 4.1. *The group S_1 is a transitive rank 4 group on $\Delta(e_1)$ with subdegrees* $1, q - 1, q^2v_{2m-4}$, *and* q^{2m-2}.

Proof. Since $e_2 \in \Delta(e_1)$, the group

$$S_{1,2} = \{M(a, r, d, B)Z\colon a, d \in F;\ r \in V_{2(m-1)};\ B \in Sp(2(m - 1), q)_{e_2}\}$$

where $V_{2m} = \langle e_1, e_{-1}\rangle \perp V_{2(m-1)}$. The group $S_{1,2}$ on $\Delta(e_1)$ has orbits

$$\{e_2\},\quad \langle e_1, e_2\rangle - \{e_1, e_2\},\quad \{(xyv00)'\colon x, y \in F,\ v \in V_{2(m-2)}{}^*\}$$

and

$$\{(xyv10)'\colon x, y \in F,\ v \in V_{2(m-2)}\}$$

of respective lengths $1, q - 1, q^2v_{2m-4}$ and q^{2m-2}, as desired.

We wish to determine the intersection numbers λ and μ of the rank 3 group G. For $b \in D(a)$ and for $c \in D(a) \cap D(b)$, it follows that $c^{G_{ab}} \subseteq D(a) \cap D(b)$ and that $D(a) \cap D(b)$ is a union of nontrivial G_{ab} orbits on $D(a)$. In this section let b, c be the fixed elements of $D(a)$ such that $i(b) = e_2$ and $i(c) = e_{-2}$.

LEMMA 4.2. $\lambda \neq 0$.

Proof. The proof is similar to that of Lemma 3.2.

LEMMA 4.3. (i) *The G_{ab} orbit of length q^{2m-2} is not contained in $D(a) \cap D(b)$.*

(ii) $\lambda = q - 1, q^2v_{2m-4}$, *or* $q^2v_{2m-4} + q - 1$.

Proof. (i) Suppose this orbit of length q^{2m-2} is contained in $D(a) \cap D(b)$. We will derive a contradiction with an argument similar to that contained in Lemma 3.3. Define a subgroup R of G_a by

$$R = \bigcap \{G_{abx}\colon x \text{ lies in the } G_{ab} \text{ orbit of length } q^{2m-2}\}.$$

It follows from matrix computation that

$$j(R) = \{M(1, 0, d, I)Z\colon d \in F\}$$

and so $j(R)$ fixes $\Delta(e_1)$ pointwise. Since the G_{ab} orbit of length q^{2m-2} lies in $D(b)$, the group $T(b) \leq R$ which implies $T(b) = T(a)$. Then $T(a) = 1$, a contradiction.

(ii) Since $D(a) \cap D(b)$ is a union of the nontrivial G_{ab} orbits, by (i) and Lemma 4.2 it follows that $\lambda = q - 1$, $q^2 v_{2m-4}$ or $q^2 v_{2m-4} + q - 1$, as claimed.

LEMMA 4.4. (i) *If* $\lambda = q - 1$, *then*

$$|G_{bc}\colon G_{bca}| = tq^{2m-4} \quad \textit{and} \quad \mu = v_{2m-3}t$$

for some $t \in \mathbf{N}$.

(ii) *If* $\lambda = q^2 v_{2m-4}$, *then*

$$|G_{bc}\colon G_{bca}| = q^{2m-2} \quad \textit{and} \quad \mu = q^{2m-2} + q - 1.$$

(iii) *If* $\lambda = q^2 v_{2m-4} + q - 1$, *then* $|G_{bc}\colon G_{bca}| = \mu$.

Proof. By Lemma 4.3 (i), $c \in D(a) \cap C(b)$. Note

$$|G_{ab}\colon G_{abc}| = |S_{1,2}\colon S_{1,2,-2}| = q^{2m-2}.$$

Now

$$\begin{aligned}|G_{bc}\colon G_{bca}| &= |G_b\colon G_{ab}| \cdot |G_{ab}\colon G_{abc}| \cdot |G_b\colon G_{bc}|^{-1} \\ &= kq^{2m-2}/l \\ &= \mu q^{2m-2}/(k - \lambda - 1)\end{aligned}$$

since $k(k - \lambda - 1) = \mu l$.

(i) If $\lambda = q - 1$, then

$$|G_{bc}\colon G_{bca}| = \mu q^{2m-4}/v_{2m-3} \in \mathbf{N}.$$

There is $t \in \mathbf{N}$ such that $\mu = v_{2m-3}t$ because $(v_{2m-3}, q^{2m-4}) = 1$. Then $|G_{bc}\colon G_{bca}| = tq^{2m-4}$.

(ii) If $\lambda = q^2 v_{2m-4}$, then

$$|G_{bc}\colon G_{bca}| = \mu q^{2m-2}/(q^{2m-2} + q - 1) \in \mathbf{N}.$$

There is $t \in \mathbf{N}$ such that

$$\mu = (q^{2m-2} + q - 1)t = ((q - 1)v_{2m-2} + q)t$$

because $(q^{2m-2} + q - 1, q^{2m-2}) = 1$. Since G is primitive,

$$\mu = ((q - 1)v_{2m-2} + q)t < k = qv_{2m-2},$$

which implies $t = 1$.

(iii) If $\lambda = q^2 v_{2m-4} + q - 1$, then $|G_{bc}\colon G_{bca}| = \mu$. This completes the proof of the lemma.

We wish to determine the parameter μ by determining the possible structure of G^g_{abc} for $g \in G$. Now

$$j(G_{abc}) = S_{1,2,-2} = \{M(x, (0r0), z, C)Z: x, z \in F, r \in V_{2(m-2)}$$

and

$$C = M(y, 0, 0, B) \quad \text{where } y \in F^*, B \in Sp(2(m-2), q)\}.$$

Define

$$\tau: S_{1,2} \to Sp(2(m-2), q) \tag{1}$$

by the rule that for $s \in S_{1,2}$, $\tau(s)$ is the matrix of size $2(m-2)$ obtained from s by deleting the rows and the columns of s indexed by ± 1 and ± 2. Then τ is an epimorphism. Let M be ker τ. Then M is a solvable group of order

$$\varepsilon^{-1}(q-1)^2 q^{4m-5}.$$

Let Q be the q'-Hall subgroup of M which consists of diagonal matrices. Note $\tau(S_{1,2,-2}) = Sp(2(m-2), q)$ and $S_{1,2,-2} \cap M \geq Q$.

Since G is rank 3 of even order, the D orbit of G_a is self-paired and there is $g \in G$ such that $g(a) = b$ and $g(b) = a$. Because $j(G_{abc})M = S_{1,2}$, it follows that $j(G_{abg(c)})M \leq S_{1,2}$. Since

$$\tau(j(G_{abg(c)})M) \leq Sp(2(m-2), q)$$

and

$$|j(G_{abg(c)})| = \varepsilon^{-1}(q-1)^2 q^{2m-3}|Sp(2(m-2), q)|,$$

it follows that

$$|j(G_{abg(c)}) \cap M|_{q'} = \varepsilon^{-1}(q-1)^2$$

and

$$|\tau(j(G_{abg(c)})M)|_{q'} = |Sp(2(m-2), q)|_{q'}.$$

The q'-Hall subgroup of $j(G_{abg(c)}) \cap M$ is conjugate to Q by an element $m \in M \leq S_{1,2}$. Let $f \in (j^{-1}(m))(g(c))$. Then $f \in C(a) \cap D(b)$ and G_{abf} is conjugate to G_{abc} by an element of G. Note

$$|G_{bc}: G_{bca}| = |G_{af}: G_{abf}|. \tag{2}$$

We will determine the possible structure of $j(G_{abf})$, a subgroup of $S_{1,2}$ of index q^{2m-2} and of order $\varepsilon^{-1}(q-1)^2 q^{2m-3}|Sp(2(m-2), q)|$ such that $j(G_{abf}) \cap M \geq Q$. Denote $j(G_{abf})$ simply as K.

Now $KM \leq S_{1,2}$ such that $|\tau(KM)|_{q'} = |Sp(2(m-2), q)|_{q'}$. By Theorem B and Lemma 1.1, $KM = S_{1,2}$ if $m \geq 5$, if $m = 4$ and $q \neq 2, 3$ or if $m = 3$ and $q \neq 2, 3, 5, 7, 11$. For $m = 3$ and $q = 5, 7, 11$ assume $KM = S_{1,2}$. We will show that the cases $KM < S_{1,2}$ do not occur later in Lemma 4.13. Assume for $m = 3$, $q \neq 2, 3$ and for $m = 4$, $q \neq 2, 3$. We will discuss these excluded cases later.

Define

$$\sigma: PSp(2m, q)_{\langle e_1\rangle, \langle e_2\rangle} \to Sp(2(m-1), q)_{\langle e_2\rangle} \tag{3}$$

by $M(a, r, d, B)Z \to B$ where $a, d \in F$; $r \in V_{2(m-1)}$ and $B \in Sp(2(m-1), q)_2$ and where $V_{2m} = \langle e_1, e_{-1}\rangle^{\perp} V_{2(m-1)}$. For $s \in S_{1,2}$, $\sigma(s)$ is the matrix of size $2(m-1)$ obtained from s by deleting the rows and the columns of s indexed by ± 1. Note the map σ defined by (3) is a restriction of the map σ of Section 1 to the group $S_{1,2}$.

LEMMA 4.5. *$\sigma(K)$ equals one of the following three subgroups:*
(i) $\{M(y, 0, 0, B)\colon y \in F, B \in Sp(2(m-2), q)\}$,
(ii) $\{M(y, 0, z, B); y, z \in F, B \in Sp(2(m-2), q)\}$,
(iii) $\{M(y, r, z, B)\colon y, z \in F, r \in V_{2(m-2)}, B \in Sp(2(m-2), q)\}$.

Proof. We have $KM = S_{1,2}$ where $K \cap M \geq Q$. So

$$\sigma(K)\sigma(M) = Sp(2(m-1), q)_2$$

and

$$\sigma(K) \cap \sigma(M) \geq \{M(y, 0, 0, I)\colon y \in F^*\}.$$

Now Lemma 1.4 implies the result.

Define

$$v\colon PSp(2m, q)_{\langle e_1\rangle, \langle e_2\rangle} \to Sp(2(m-1), q)_{\langle e_1\rangle} \tag{4}$$

by the rule that for $s \in S_{1,2}$, $v(s)$ is the matrix of size $2(m-1)$ obtained from s by deleting the rows and the columns of s indexed by ± 2. Let N_2 be the subgroup of $S_{1,2}$ defined by

$$N_2 = \{M(x, (0ry), z, I)Z\colon x, y, z \in F, r \in V_{2(m-2)}\}.$$

LEMMA 4.6. *Let Y be a subgroup of $S_{1,2}$ such that $Y \geq Q$ and $\tau(Y)$ is transitive on $V^*_{2(m-2)}$. Then $Y \cap N_2$ is one of the following 6 subgroups:*
(i) N_2,
(ii) $\{M(x, (0r0), z, I)Z\colon x, z \in F, r \in V_{2(m-2)}\}$,
(iii) $\{M(x, (00y), z, I)Z\colon x, y, z \in F\}$,
(iv) $\{M(x, 0, z, I)Z\colon x, z \in F\}$,
(v) $\{M(x, (00y), 0, I)Z\colon x, y \in F\}$,
(vi) $\{M(x, 0, 0, I)Z\colon x \in F^*\}$.

Proof. By Lemma 1.2 if $v(Y \cap N_2) \not\leq U$, then $v(Y \cap N_2) = v(N_2)$ and

$$Y \cap N_2 \supseteq \{M(x, (0rc), z, I)Z\colon x, z, c \in F, r \in V_{2(m-2)}\}$$

where c depends on x, r, z. If $c \neq 0$ for some x, r, z, then for

$$B = M(y^{-1}, 0, 0, I) \in Sp(2(m-1), q),$$

the element $M(1, 0, 0, B)Z \in Y$ and so

$$M(1, 0, 0, B^{-1})M(x, (0rc), z, I)M(1, 0, 0, B)Z$$
$$= M(x, (0rcy), z, I) \in Y \cap N_2$$

where cy is any element of F^*. It follows from matrix computation that $Y \cap N_2 = N_2$. If $c = 0$ for all x, r, c, then $Y \cap N_2$ is of type (ii).

Assume now that $\nu(Y \cap N_2) = U$. So

$$Y \cap N_2 \supseteq \{M(x, (00c), z, I)Z: x, z, c \in F\}$$

where c depends on x, z. If $c \neq 0$ for some x, z, then $Y \cap N_2$ is of type (iii). If $c = 0$ for all x, z, then $Y \cap N_2$ is of type (iv).

If $\nu(Y \cap N_2) = \{M(x, 0, 0, I): x \in F^*\}$, then $Y \cap N_2$ is of type (v) or (vi). This completes the proof of the lemma.

LEMMA 4.7. (i) *In case* (i) *of Lemma* 4.5, $K = S_{1,2,-2}$.
(ii) $K \neq S_{1,2,-2}$.

Proof. In case (i), $|K \cap N_2| = \varepsilon^{-1}(q - 1)q^{2m-3}$ because $\ker \sigma = N_2$ and $\sigma(K) \cong K/K \cap N_2$. Note $\tau(K) = Sp(2(m - 2), q)$. By Lemma 4.6, since $m > 2$,

$$K \cap N_2 = \{M(x, (0r0), z, I)Z: x, z \in F, r \in V_{2(m-2)}\}.$$

For $C \in \sigma(K)$ let $k_C = M(a, (0rz), d, C)Z$ be a pre-image of C which lies in K where a, $(0rz)$, d depend on C. Then

$$k_C \cdot M(a^{-1}, (0\ -a^{-1}r\ 0), -d, I)Z = M(1, (00z), 0, C)Z \in K.$$

We claim that $z = 0$ for all $C \in \sigma(K)$.

Indeed for $C \in \sigma(K)$ let k_C be the pre-image

$$M(1, (00z), 0, C)Z$$

which lies in K and let l_C be the pre-image

$$M(1, (00y), 0, C)Z$$

which lies in K; then

$$k_C l_C^{-1} = M(1, (0, 0, z - y)C^{-1}, 0, I) \in K \cap N_2.$$

So z is uniquely determined by C when $k_C = M(1, (00z), 0, C)Z$. Denote this unique z by z_C.

Since $K \cap N_2 \geq Q$,

$$M(x, 0, 0, I)k_C M(x^{-1}, 0, 0, I)Z = M(1, (0, 0, xz_C), 0, C)Z$$

and so $z_C = 0$ if $q > 2$.

If $q = 2$, then $\sigma(K) = \{M(1, 0, 0, B): B \in Sp(2(m - 2), 2)\}$. Then the map defined by the rule $C \to z_C$ is a homomorphism from

$$\sigma(K) \cong Sp(2(m - 2), 2)$$

into F, a group of order 2. Since $m \geq 5$, $Sp(2(m - 2), 2)$ is simple. Since the kernel is a normal subgroup, it follows that $z_C = 0$.

Now $k_C = M(1, 0, 0, C)Z \in K$ and

$$K \geq \langle M(1, 0, 0, C)\dot{Z}, K \cap N_2 : C \in \sigma(K) \rangle = S_{1,2,-2}.$$

Since $|K| = |S_{1,2,-2}|$, it follows that $K = S_{1,2,-2}$.

(ii) If $K = S_{1,2,-2}$, then the proof of Lemma 3.6 works for $m > 2$ to yield $T(a) = 1$, a contradiction. So 4.7 holds.

LEMMA 4.8. *Case* (ii) *of Lemma* 4.5 *does not occur.*

Proof. Suppose

$$\sigma(K) = \{M(y, 0, z, B) : y, z \in F, B \in Sp(2(m - 2), q)\}.$$

Note $\tau(K) = Sp(2(m - 2), q)$. Then $|K \cap N_2| = \varepsilon^{-1}(q - 1)q^{2m-4}$. If $m > 3$, then $K \cap N_2$ is not equal to any of the six possible subgroups of Lemma 4.6, a contradiction. If $m = 3$, then

$$K \cap N_2 = \{M(x, (00y), z, I)Z : x, y, z \in F\}.$$

For $C \in \sigma(K)$ let $k_C = M(x, (0ry), z, C)Z$ be a pre-image which lies in K where x, $(0ry)$, z are determined by C. Apply v and then Lemma 1.3 to conclude that $r = 0$. So $k_C = M(x, (00y), z, C)Z$ and

$$k_C M(x^{-1}, (00 - x^{-1}y), -z, I)Z = M(1, 0, 0, C)Z \in K.$$

So

$$K = \langle M(1, 0, 0, C)Z, K \cap N_2 : C \in \sigma(K) \rangle$$
$$= \{M(x, (00y), z, C)Z : x, y, z \in F, C \in \sigma(K)\}.$$

Let P be a p-Sylow subgroup of K. Then P is abelian. Let R be a p-Sylow subgroup of $S_{1,2,-2}$. Then $|R'| = \varepsilon^{-1}q^2$. Since G_{abf} is conjugate to G_{abc}, it follows that $j^{-1}(P)$ is conjugate to $j^{-1}(R)$. This contradiction proves the lemma.

LEMMA 4.9. $K = \{M(x, 0, 0, C)Z : x \in F^*, C \in \sigma(K)\}$ *where* $\sigma(K) = \{M(y, r, z, B) : y, z \in F, r \in V_{2(m-2)}, B \in Sp(2(m - 2), q)\}$.

Proof. By Lemmas 4.7 and 4.8, $\sigma(K) = \{M(y, r, z, B)\}$. Then $|K \cap N_2| = \varepsilon^{-1}(q - 1)$. Since $K \geq Q$, it follows that

$$K \cap N_2 = \{M(x, 0, 0, I)Z : x \in F^*\}.$$

For $C \in \sigma(K)$ let $k_C = M(a, r, d, C)Z$ be a pre-image of C which lies in K where a, r, d depend on C. By Lemma 1.3 (i) for $q \neq 2$, $r = 0$ and $d = 0$. So $k_C = M(a, 0, 0, C)Z$ and $M(1, 0, 0, C)Z \in K$. So

$$K = \langle M(1, 0, 0, C)Z, K \cap N_2 : C \in \sigma(K) \rangle$$
$$= \{M(x, 0, 0, C)Z : x \in F^*, C \in \sigma(K)\}.$$

For $q = 2$, let $C = M(1, s, z, B) \in \sigma(K)$ and let

$$k_C = M(1, (0, r, d), f, C)Z$$

be a pre-image in K where $d, f \in F$, $r \in V_{2(m-2)}$ and where r, d, f depend on C. Apply the map ν of (4) and then Lemma 1.3 (iii) to conclude that there is $\nu(n) \in \nu(S_{1,2})$ such that $\nu(k_C)^{\nu(n)} = M(1, 0, 0, B)$. Since $n \in S_{1,2} = j(G_{ab})$, the group $G_{abf}^{j^{-1}(n)}$ satisfies the same conditions as G_{abf} and we may assume without loss of generality that $n = 1$. So

$$k_C = M(1, (00d), 0, C)Z,$$

where d depends on C. We claim that $d = 0$. Indeed since $K \cap N_2 = I$, d is uniquely determined by C. Denote this unique d by d_C. Then the map d defined by the rule $C \to d_C$ is a homomorphism from $\sigma(K) \cong Sp(2(m-1), 2)_1$ into F, a group of order 2. Let $L = \ker d$. Let $N = \{M(1, r, z, I) : z \in F, r \in V_{2(m-2)}\}$. If $N \leq L$, then

$$L/N \leq Sp(2(m-1), 2)_1/N \cong Sp(2(m-2), 2),$$

which is a simple group for $m \geq 5$. So $L = Sp(2(m-1), 2)_1$. If $N \not\leq L$, then $LN = Sp(2(m-1), 2)_1$. Now Lemma 1.4 yields a contradiction. So 4.9 is proved.

LEMMA 4.10. (i) $\lambda = q^2 v_{2m-4} + q - 1 = v_{2m-2} - 2$ *and* $\mu = v_{2m-2}$.
(ii) $j(G_{af}) = \{M(x, 0, 0, B) : x \in F^*, B \in Sp(2(m-1), q)\}$.

Proof. By Lemma 4.9,

$$K = j(G_{abf}) = \{M(x, 0, 0, B) : x \in F^*, B \in Sp(2(m-1), q)_2\}.$$

Define $\sigma : S_1 \to Sp(2(m-1), q)$ by the rule $M(x, r, y, B)Z \to B$. Then

$$\sigma(K) = Sp(2(m-1), q)_2 \leq \sigma(j(G_{af})) \leq \sigma(j(G_a)) = Sp(2(m-1), q).$$

Now $Sp(2(m-1), q)_2$ is a maximal subgroup of $Sp(2(m-1), q)$ because $Sp(2(m-1), q)$ is primitive in its action on the lines of $V^*_{2(m-1)}$. Either $\sigma(j(G_{af})) = Sp(2(m-1), q)_2$ or $\sigma(j(G_{af})) = Sp(2(m-1), q)$.

If $\sigma(j(G_{af})) = Sp(2(m-1), q)_2$, then

$$\begin{aligned} j(G_{af}) &\leq \{M(x, r, y, C)Z : x, y \in F, r \in V_{2(m-1)}, C \in Sp(2(m-1), q)_2\} \\ &= S_{1,\langle 1,2\rangle}. \end{aligned}$$

Now

$$|G_{af} : G_{abf}| = |b^{G_{af}}| = |i(b)^{j(G_{af})}| \leq |e_2^{S_{1,\langle 1,2\rangle}}| = q.$$

Let

$$g = M(x, (yrz), w, C)Z \in j(G_{af})$$

where $x, y, z, w \in F$, $r \in V_{2(m-2)}$ and $C \in Sp(2(m-1), q)_2$. Assume $y \neq 0$ for some $g \in j(G_{af})$. Since $j(G_{af}) \geq K \geq Q$, for all $u \in F^*$,

$$M(u, 0, 0, I)Z \cdot g = M(ux, (uy\ ur\ uz), uw, C)Z \in j(G_{af}).$$

Then $|e_2^{j(G_{af})}| = q$. If $y = 0$ for all $g \in j(G_{qf})$, then

$$j(G_{af}) \leq S_{1,2} \quad \text{and} \quad |e_2^{j(G_{af})}| = 1.$$

So $|G_{af}: G_{abf}| = 1$ or q and $|G_{af}: G_{abf}| = |G_{bc}: G_{bca}|$ by (2). From Lemma 4.4, it follows that

$$\lambda = q^2 v_{2m-4} + q - 1 \quad \text{and} \quad |G_{af}: G_{abf}| = \mu.$$

We claim that the cases $\lambda = q^2 v_{2m-4} + q - 1$, $\mu = 1$ and $\lambda = q^2 v_{2m-4} + q - 1$, $\mu = q$ do not occur. Indeed assume first $\mu = 1$. Then

$$\begin{aligned} D &= (q^2 v_{2m-4} + q)^2 + 4(q v_{2m-2} - 1) \\ &= q^2(v_{2m-3}^2 + (2q^{m-2})^2) \end{aligned}$$

is a square. There is $z \in \mathbf{N}$ such that $v_{2m-3}^2 + (2q^{m-2})^2 = z^2$. Since q is a prime power and v_{2m-3} is odd, $(z, v_{2m-3}) = 1$ and

$$q^{2m-4} = (z - v_{2m-3})/2 \cdot (z + v_{2m-3})/2.$$

So $1 = (z - v_{2m-3})/2$ and $q^{2m-4} = (z + v_{2m-3})/2$. Then $1 + v_{2m-3} = q^{2m-4}$, a contradiction.

Now assume $\mu = q$. Then

$$D = (q^2 v_{2m-4} - 1)^2 + 4(q v_{2m-2} - q) = (q^2 v_{2m-4} + 1)^2 + (2q^{m-1})^2 = z^2$$

for some $z \in \mathbf{N}$. Since q is a prime power and $q^2 v_{2m-4} + 1$ is odd,

$$(z, q^2 v_{2m-4} + 1) = 1$$

and

$$q^{2m-2} = (z - (q^2 v_{2m-4} + 1))/2 \cdot (z + q^2 v_{2m-4} + 1)/2.$$

So $1 = (z - (q^2 v_{2m-4} + 1))/2$ and $q^{2m-2} = (z + q^2 v_{2m-4} + 1)/2$. Then $q^{2m-2} = 2 + q^2 v_{2m-4}$, a contradiction.

Thus $\sigma(j(G_{af})) = Sp(2(m-1), q)$ and $j(G_{af})N = S_1$ where

$$N = \{M(x, r, y, I)Z \colon x, y \in F, r \in V_{2(m-1)}\} = \ker \sigma.$$

Note $j(G_{af}) \geq K \geq \{M(x, 0, 0, I)Z \colon x \in F^*\}$. Apply Lemma 1.4. If $j(G_{af}) = S_1 = j(G_a)$ then $l = 1$ and $\mu = k(k - \lambda - 1)$, which does not occur since G is primitive. If

$$j(G_{af}) = \{M(x, 0, y, B)Z \colon x, y \in F, B \in Sp(2(m-1), q)\},$$

then by Lemma 4.10 (ii), $|G_{af}: G_{abf}| = q v_{2m-2}$ while $|b^{G_{af}}| = |e_2^{j(G_{af})}| = v_{2m-2}$, a contradiction. So

$$j(G_{af}) = \{M(x, 0, 0, B)Z \colon x \in F^*, B \in Sp(2(m-1), q)\}.$$

Then $|G_{af}: G_{abf}| = v_{2m-2} = |e_2^{j(G_{af})}|$. From Lemma 4.4, it follows that

$$\lambda = q^2 v_{2m-4} + q - 1 = v_{2m-2} - 2 \quad \text{and} \quad \mu = v_{2m-2}.$$

This completes the proof of 4.10.

LEMMA 4.11. (i) *For* $y \in C(x)$, $|R(xy)| = q + 1$.
(ii) *For* $y \in D(x)$, $|R(xy)| = q + 1$.

Proof. (i) The proof is similar to that of Lemma 3.9.
(ii) Since A' is a symmetric design,

$$2 \leq |R(ab)| \leq (n - (\lambda + 2))/(k + 1 - (\lambda + 2)) = q + 1.$$

Note $R(ab) - \{a\} \leq D(a) \cap b^{\perp}$. Now $u \in R(ab)$ iff $a^{\perp} \cap u^{\perp} = a^{\perp} \cap b^{\perp}$ iff the union of $\{a, u\}$ and the orbits of G_{au} of lengths $q - 1$ and $q^2 v_{2m-4}$ equals the union of $\{a, b\}$ and the orbits of G_{ab} of lengths $q - 1$ and $q^2 v_{2m-4}$. This occurs iff the union of $\{e_1, i(u)\}$ and the orbits of $S_{1,i(u)}$ of lengths $q - 1$ and $q^2 v_{2m-4}$ equals the union of $\{e_1, e_2\}$ and the orbits of $S_{1,2}$ of lengths $q - 1$ and $q^2 v_{2m-4}$. For $v \in \langle e_1, e_2 \rangle - \{e_1, e_2\}$, it follows from matrix computation that the orbit of $S_{1,v}$ of length $q^2 v_{2m-4}$ equals the orbit of $S_{1,2}$ of length $q^2 v_{2m-4}$ and that the union of $\{e_1, v\}$ and the orbit of $S_{1,v}$ of length $q - 1$ equals the union of $\{e_1, e_2\}$ and the orbit of $S_{1,2}$ of length $q - 1$. So $i^{-1}(v) \in R(ab)$ and $|R(ab)| = q + 1$, as claimed.

LEMMA 4.12. (i) *The design* A' *is isomorphic to the system of points and hyperplanes of a projective space of dimension* $2m - 1$ *over* F.
(ii) $G \cong PSp(2m, q)$.

Proof. The proof is similar to that of Lemma 3.10. The dimension is $2m - 1$ since $|b^{\perp}| = qv_{2m-2} + 1 = v_{2m-1}$. So Theorem A holds for $m \geq 5$; $m = 4$, $q \geq 3$; $m = 3$, $q > 11$.

LEMMA 4.13. *If* $m = 3$ *and* $q = 5, 7,$ *or* 11, *the cases* $KM < S_{1,2}$ *do not occur.*

Proof. If $KM < S_{1,2}$, then $\tau(KM) < SL(2, q)$ of index q and of order $q^2 - 1$. From the proof of Lemma 1.7, it follows that $\tau(KM)$ is transitive on V_2^*. Now

$$\sigma(K) \geq \{M(y, 0, 0, I) \colon y \in F, I \in SL(2, q)\}$$

and $|Sp(4, q)_2 \colon \sigma(KM)| = q$. It follows from Lemmas 1.2 and 1.3 that $\sigma(K)$ equals one of the following three subgroups of $Sp(4, q)_2$:
(i) $\{M(y, 0, 0, B) \colon y \in F^*, B \in \tau(K)\}$,
(ii) $\{M(y, 0, z, B) \colon y, z \in F^*, B \in \tau(K)\}$,
(iii) $\{M(y, r, z, B) \colon y, z \in F^*, r \in V_2, B \in \tau(K)\}$.
In case (i), $|K \cap N_2| = \varepsilon^{-1}(q - 1)q^4 = |N_2|$. Then

$$K = \{M(x, (0rz), w, C)Z \colon x, z, w \in F, r \in V_2, C \in \sigma(K)\}.$$

Let P be a p-Sylow subgroup of K. Then $|P'| = \varepsilon^{-1}q$. Let R be a p-Sylow subgroup of $S_{1,2,-2}$. Then $|R'| = \varepsilon^{-1}q^2$. Since $G_{abf} = j^{-1}(K)$ is conjugate to $G_{abc} = j^{-1}(S_{1,2,-2})$, a contradiction results.

In case (ii), $|K \cap N_2| = \varepsilon^{-1}(q-1)q^3$. By Lemma 4.6,

$$K \cap N_2 = \{M(x, (0r0), z, I)Z: x, z \in F, r \in V_2\}.$$

It follows by a proof similar to that of Lemma 4.7 (i) that

$$K = \{M(x, (0r0), w, C)Z: x, w \in F, r \in V_2, C \in \tau(K)\}.$$

If P is a p-Sylow subgroup of K, then $|P'| = \varepsilon^{-1}q$, a contradiction.

In case (iii), $|K \cap N_2| = \varepsilon^{-1}(q-1)q$. By Lemma 4.6, either

(a) $K \cap N_2 = \{M(x, 0, w, I)Z: x, w \in F\}$, or

(b) $K \cap N_2 = \{M(x, (00w), 0, I)Z: x, w \in F\}$.

In case (a) it follows by Lemma 1.3 (i) that

$$K = \{M(x, 0, w, C)Z: x, w \in F, C \in \sigma(K)\}.$$

If P is a p-Sylow subgroup of K, then $|P'| = \varepsilon^{-1}q$, a contradiction. In case (b) it follows by an argument similar to that in Lemma 4.8 that

$$K = \{M(x, (00w), 0, C)Z: x, w \in F, C \in \sigma(K)\}.$$

If P is a p-Sylow subgroup of K, then $|P'| = \varepsilon^{-1}q$, a contradiction. This finishes the proof of 4.13.

Note Lemma 4.13 implies that Theorem A holds for $m = 3$, $q = 5$, 7, or 11.

LEMMA 4.14. *Theorem* A *holds for the cases* $(m, q) = (3, 2), (4, 2), (3, 3), (4, 3)$.

Proof. (i) Assume $(m, q) = (3, 2)$. By Lemma 4.3 (ii), $\lambda = 1$, 12, or 13. We claim $\lambda = 13$. If $\lambda = 1$, then by Lemma 4.4 $\mu = 7t$ for some $t \in \mathbf{N}$. Since $\mu < k = 30$, $t \in \{1, 2, 3, 4\}$. But for each t the parameter $D = (\lambda - \mu)^2 + 4(k - \mu)$ is not a square. So $\lambda \neq 1$. If $\lambda = 12$, then by Lemma 3.4 $\mu = 17$ and $D = 77$. So $\lambda = 13$.

We claim $\mu = 15$. Now

$$D = (13 - \mu)^2 + 4(30 - \mu) = (\mu - 15)^2 + 2^6$$

is a square and $\mu l = 2^5 \cdot 15$. Let $x = |\mu - 15|$. Then there is $y \in \mathbf{N}$ such that $x^2 + 2^6 = (x + y)^2$. So $2^6 = 2xy + y^2$ and $y = 2z$ for some $z \in \mathbf{N}$. Then $2^4 = (x + z)z$. For some $b \in \{0, 1, 2, 3, 4\}$, $z = 2^b$ and $x = 2^{4-b} - 2^b$. So $\mu = 15 \pm (2^{4-b} - 2^b)$ and $\mu \mid 2^5 \cdot 15$. Since $0 < \mu < k = 30$, it follows that $b = 2$ and $\mu = 15$. So A' is a symmetric design. Now apply Lemmas 4.11 and 4.12 to see that Theorem A holds.

(ii) Assume $(m, q) = (4, 2)$. The argument is similar to that of (i).

(iii) Assume $(m, q) = (3, 3)$. By Lemma 4.3, $\lambda = 2$, 36, or 38. We claim $\lambda = 38$. If $\lambda = 2$, then by Lemma 4.4 $\mu = 13t$ for some $t \in \mathbf{N}$. Then

$$D = (13t - 2)^2 + 4(120 - 13t) = (13t - 4)^2 + 36 \cdot 13 = z^2$$

for some $z \in \mathbf{N}$. Let $x = (z - (13t - 4), z + 13t - 4)$ It follows that $x = 2$ or 6. If $x = 2$, then

$$3^2 \cdot 13 = (z + 4 - 13t)/2 \cdot (z + 13t - 4)/2 = 1 \cdot 107 \text{ or } 9 \cdot 13.$$

In the first case, $13t - 4 = 106$ and in the second case, $13t - 4 = 4$, a contradiction. If $x = 6$, then

$$13 = (z + 4 - 13t)/6 \cdot (z + 13t - 4)/6$$

and $(13t - 4)/3 = 12$, a contradiction. So $\lambda \neq 2$. If $\lambda = 36$, then by Lemma 3.4 $\mu = 83$ and $D = 2{,}357$, a nonsquare. So $\lambda = 38$.

We claim $\mu = 40$. Now

$$D = (38 - \mu)^2 + 4(120 - \mu) = (\mu - 40)^2 + 4 \cdot 3^4$$

is a square and $\mu l = 3^5 \cdot 40$. Let $x = |\mu - 40|$. There is $y \in \mathrm{N}$ such that $x^2 + 4 \cdot 3^4 = (x + y)^2$. So $4 \cdot 3^4 = 2xy + y^2$ and $y = 2z$ for some $z \in \mathrm{N}$. Then $3^4 = (x + z)z$. For some $b \in \{0, 1, 2, 3, 4\}$, $z = 3^b$ and $x = 3^{4-b} - 3^b$. So $\mu = 40 \pm (3^{4-b} - 3^b)$ and $\mu \mid 3^5 \cdot 40$. Since $0 < \mu < k = 120$, it follows that $b = 2$ and $\mu = 40$. So A' is a symmetric design. Apply Lemmas 4.11 and 4.12 to see that Theorem A holds.

(iv) Assume $(m, q) = (4, 3)$. The argument is similar to that of (iii). This completes the proof of the lemma and of Theorem A for $m > 2$.

References

1. P. Dembowski, *Finite geometries*, Springer-Verlag, Berlin, 1968.
2. P. Dembowski and A. Wagner, *Some characterizations of finite projective spaces*, Arch. Math., vol. 11 (1960), pp. 465–469.
3. J. Frame, *The classes and representations of the groups of 27 lines and 28 bitangents*, Ann. Mat. Pura Appl. (4), vol. 32 (1951), pp. 83–119.
4. D. Higman, *Flag-transitive collineation groups of finite projective spaces*, Illinois J. Math., vol. 6 (1962), pp. 434–446.
5. ———, *Finite permutation groups of rank 3*, Math. Zeitschr., vol. 86 (1964), pp. 145–156.
6. ———, *Primitive rank 3 groups with a prime subdegree*, Math. Zeitschr., vol. 91 (1966), pp. 70–86.
7. D. Higman and J. McLaughlin, *Rank 3 subgroups of finite symplectic and unitary groups*, J. Reine Angew. Math., vol. 218 (1965), pp. 174–189.
8. B. Huppert, *Endliche gruppen* I, Springer-Verlag, Berlin, 1967.
9. H. Mitchell, *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc., vol. 15 (1914), pp. 379–396.
10. H. Pollatsek, *First cohomology groups of some linear groups over fields of characteristic 2*, Illinois J. Math., vol. 15 (1971), pp. 393–417.
11. G. Seitz, *Flag-transitive subgroups of Chevalley groups*, Ann. of Math. (2), vol. 97 (1973), pp. 27–56.
12. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

University of Michigan
Ann Arbor, Michigan