RANK 3 SUBGROUPS OF ORTHOGONAL GROUPS

BY
BETTY SALZBERG STARK

1. Introduction

The projective commutator subgroup of an orthogonal group over a finite field K of odd characteristic, $P\Omega_n(K)$ (where $n \geq 5$), is known to be a rank 3 permutation group on the one-dimensional singular subspaces of the underlying vector space [6]. In this paper, we prove the following theorem:

MAIN THEOREM. *Let $H < P\Omega_n(K)$, $5 \leq n \leq 7$, K a finite field of odd characteristic. Suppose H is a rank 3 permutation group on the one-dimensional singular subspaces of the underlying n-dimensional orthogonal space. Then $H = P\Omega_n(K)$.*

This result is analogous to a result of Higman and McLaughlin on rank 3 subgroups of symplectic and unitary groups for dimensions $4 \leq n \leq 8$ [3], later improved to include dimensions $n > 8$ by Perin [4]. Unfortunately, we were not able to apply Perin's method in this paper. However, we do prove some lemmas in Sections 3, 4, and 6 which hold for all dimensions $n \geq 5$, and which may be of independent interest. In addition, we make some remarks in Section 8, explaining why the question in the main theorem does not make sense for smaller dimensions.

2. Siegel elations

Let $B(x, y)$ be the nondegenerate symmetric bilinear form defining the orthogonal space. If $B(x, x) = 0$ and x is not zero, we say x is *singular*. If all of the vectors of some nonzero subspace are singular or zero we say the subspace is singular. The set of all vectors y such that $B(x, y) = 0$ for all x in some subset S of vectors is called $S^{\perp}$ ("S perp"). With these notations, we can define a Siegel transformation $\rho(x, u)$ in $\Omega_n(K)$, and its image in $P\Omega_n(K)$, the Siegel elation $r(x, u)$. (A Siegel elation is an elation on the hyperplane $x^{\perp}$.)

A Siegel transformation, $\rho(x, u)$, (where x is singular, and $B(x, u) = 0$) sends vectors v in $x^{\perp}$ to $v + B(v, u)x$. Tamagawa [6] shows that such a transformation can be extended in only one way to an element (also called $\rho(x, u)$) of the orthogonal group. Precisely, if y is a singular vector such that $B(x, y) = 1$ and $B(u, y) = 0$ (such a vector y can always be found), then $\rho(x, u)$ sends y to $y - u - Q(u)x$ (where $2Q(u) = B(u, u)$).

We define a *point* to be a one-dimensional subspace and a *line* to be a 2-dimensional subspace.

Received April 24, 1974.

The set of all $\rho(x, ku)$, $k \in K$, x and u fixed ($\rho(x, 0)$ is the identity), and u not in the subspace spanned by x, is a group $\Sigma\langle x, u\rangle$ isomorphic to the additive group of K, since $\rho(x, u)\rho(x, v) = \rho(x, u + v)$. We showed in [5] that if u is singular, $\Sigma\langle x, u\rangle$ is determined by the line $\langle x, u\rangle$ spanned by x and u. (We use $\langle x\rangle$ to mean subspace spanned by x.) Further, such a group is conjugate in $\Omega_n(K)$ to a root group for long roots in the Chevalley group B_n or D_n. (Root groups are the canonical generators of Chevalley groups [2].) Accordingly, if u is singular, we call $\Sigma\langle x, u\rangle$ a group of root type 1. If u is not singular, $\Sigma\langle x, u\rangle$ corresponds to a root group (in the Chevalley group B_n) for short roots, and we call it a group of root type 2. We shall speak of Siegel elations and transformations of type 1 or 2 with u singular or nonsingular respectively.

3. Rank 3 subgroups of $P\Omega_n(K)$ with projective root 1 groups

Let us define the image of a group of root type 1 in $P\Omega_n(K)$ to be a projective root 1 group. The set of all Siegel elations of type 1 generates $P\Omega_n(K)$ whenever the index of the space is ≥ 2 (the index of the space is the dimension of the largest totally singular subspace; for $n > 5$ the index is always ≥ 2). [1]. We now show:

LEMMA 1. *Suppose G is a rank 3 subgroup of $P\Omega_n(K)$, $n \geq 5$, which contains a projective root 1 group. Then $G = P\Omega_n(K)$.*

Proof. First, if G is rank 3 on singular points, this means the stabilizer of one such point P is transitive on the set of points perpendicular to P. Thus G is transitive on singular lines. But for $\tau \in 0_n(K)$, $\tau\rho(x, u)\tau^{-1} = \rho(\tau(x), \tau(u))$. Thus by conjugation τ sends $\Sigma\langle x, u\rangle$ to $\Sigma\langle \tau(x), \tau(u)\rangle$. Now suppose the image of such a τ is in G. The transitivity of G on singular lines thus implies the transitivity of G on projective root 1 groups. (We recall there is a one-to-one correspondence between groups of root type 1 and singular lines.) Thus we get all Siegel elations of type 1, and $G = P\Omega_n(K)$.

4. One Siegel elation of type 1

In this section, we prove the following lemma, which is immediate from Lemma 1 in the case K is a prime field, but is otherwise nontrivial:

LEMMA 2. *Suppose G is a rank 3 subgroup of $P\Omega_n(K)$, $n \geq 5$, which contains one Siegel elation of type 1. Then $G = P\Omega_n(K)$.*

Proof. We begin with $n = 5$. Suppose G is rank 3 subgroup of $P\Omega_5(K)$ and G contains a Siegel elation of type 1. Then it contains a Siegel elation of type 1 for each singular line in the space, since G is transitive on singular lines. Then G is isomorphic to a subgroup of $PSp_4(K)$ since $PSp_4(K) \cong P\Omega_5(K)$. (These are the Chevalley groups C_2 and B_2.) The Siegel elations of type 1 correspond to root groups for long roots which correspond to elations in $PSp_4(K)$. To have a Siegel elation of type 1 for each singular line is to have one element out of each member of the conjugacy class of root groups for long roots. This corresponds to having what Higman and McLaughlin call a P, $P^{\perp}$ elation for each nonzero point P in the 4-dimensional symplectic space. We may then quote Theorem 1 of Higman and McLaughlin's paper [3] to see that $G \cong PSp_4(K) \cong P\Omega_5(K)$.

Next we argue by induction, as in Higman and McLaughlin's proof of Theorem 1. Suppose G is a rank 3 subgroup of $P\Omega_n(K)$. Then if U is a linear variety corresponding to an $n-1$ dimensional subspace U' of V, and $V = U' \perp P$, where P is a nonsingular point, $G_P \mid U$ contains a Siegel elation of type 1 for each singular line in U. Thus, by the induction hypothesis, $G_P \mid U \cong P\Omega_{n-1}(K)$. Now we look at a Siegel elation τ in $G_P \mid U$. Then τ is the restriction of $\tau \perp \sigma$ in G_P, where τ acts on U and σ acts on P. But $\tau \perp \sigma$ has a preimage γ in $\Omega_n(K)$. We claim that γ is in fact a Siegel transformation. To see this, we first note that the natural homomorphism of the p-Sylow subgroup of $\Omega_{n-1}(K)$ onto the p-Sylow of $P\Omega_{n-1}(K)$ is actually an isomorphism. Thus $\gamma \mid U'$ is a Siegel transformation. In particular $\gamma \mid U'$ has determinant 1. But if $P = \langle w \rangle$, then $\gamma(w) = \pm w$ since γ is orthogonal. Thus, since elements of $\Omega_n(K)$ have determinant 1, $\gamma(w) = w$. Thus γ is a Siegel transformation on V. Since this holds for all Siegel elations of $G_P \mid U$, we see G contains a projective root one group and $G = P\Omega_n(K)$.

5. Basis notation

When we talk about elements in a subgroup G of $P\Omega_n(K)$, we will want to refer to matrix representations of elements in $\Omega_n(K)$ which correspond to these elements of G in the sense of being preimages under the natural homomorphism $\Omega_n(K) \to P\Omega_n(K)$. For this purpose, we set up a standard basis notation for n-dimensional orthogonal space. The vector space V can be decomposed as follows:

$$V = \langle x_1, x_{-1} \rangle \perp \langle x_2, x_{-2} \rangle \perp \cdots \perp \langle x_k, x_{-k} \rangle \perp W$$

where $B(x_i, x_{-i}) = 1$, W is anisotropic of dimension 0, 1, or 2, and all other products are zero. Since K is finite of odd characteristic such a basis can always be found [1]. In particular $B(x_i, x_i) = 0$, or x_i is *singular*. We order the basis $x_1, x_2, x_3, \ldots, x_k, W, x_{-k}, \ldots, x_{-1}$. With respect to this ordering, the matrix for B is

$$J_n = \begin{pmatrix} & & & & & & 1 \\ & & & & & \iddots & \\ & & & & 1 & & \\ & & & B(W) & & & \\ & & 1 & & & & \\ & \iddots & & & & & \\ 1 & & & & & & \end{pmatrix}$$

A matrix A represents an element of the n-dimensional orthogonal group with respect to B, if $AJ_nA^t = J_n$.

6. One Siegel elation of type 2.

In this section we prove the following:

LEMMA 3. *Suppose G is a rank 3 subgroup of $P\Omega_n(K)$, $n \geq 5$, which contains a Siegel elation of type 2. Then $G = P\Omega_n(K)$.*

Proof. We look at a matrix representation of the preimage in $\Omega_n(K)$ of an element of $G_{\langle x_1\rangle,\langle x_2\rangle}$ (the stabilizer of two singular points which are perpendicular to each other) in the standard basis.

$$\left(\begin{array}{cc|c|cc} a & 0 & * & * & * \\ 0 & b & * & * & * \\ \hline 0 & 0 & A & * & * \\ \hline 0 & 0 & 0 & b^{-1} & 0 \\ 0 & 0 & 0 & 0 & a^{-1} \end{array}\right).$$

Let the preimage of $G_{\langle x_1\rangle,\langle x_2\rangle}$ be called M. Let H be the subgroup of M with $a = b = 1$. But H is the preimage of some subgroup H_0 of $G_{\langle x_1\rangle,\langle x_2\rangle}$ and the index of H_0 in $G_{\langle x_1\rangle,\langle x_2\rangle}$ divides $(q-1)^2$ ($|K| = q$).

We now show H_0 is transitive on the singular points which are perpendicular to x_1, but not to x_2. To do this, we show that

$$|G_{\langle x_1\rangle,\langle x_2\rangle} : G_{\langle x_1\rangle,\langle x_2\rangle,\langle x_{-2}\rangle}| = q^{n-3},$$

the number of singular points perpendicular to x_1, but not to x_2. Since $((q-1)^2, q^{n-3}) = 1$, this implies $|H_0 : H_{0\langle x_{-2}\rangle}| = q^{n-3}$. We illustrate:

$$\begin{tikzcd} & G_{\langle x_1\rangle,\langle x_2\rangle} \arrow[dl, dash, "q^{n-3}"'] \arrow[dr, dash, "x\ (\text{divides } (q-1)^2)"] & \\ G_{\langle x_1\rangle,\langle x_2\rangle,\langle x_{-2}\rangle} \arrow[dr, dash] & & H_0 \arrow[dl, dash, "q^{n-3}"] \\ & H_{0\langle x_{-2}\rangle} & \end{tikzcd}$$

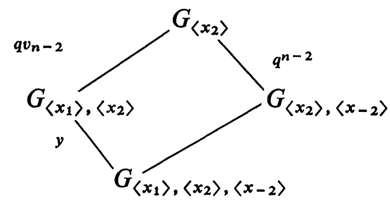
Let $y = |G_{\langle x_1\rangle,\langle x_2\rangle} : G_{\langle x_1\rangle,\langle x_2\rangle,\langle x_{-2}\rangle}|$. To show $y = q^{n-3}$, we use a similar index argument. First we remark that in all cases, if $v_n =$ the number of singular points in the n dimensional orthogonal space, then $(v_n, q) = 1$ [1]. The number of singular points perpendicular to $\langle x_2\rangle$ but not equal to $\langle x_2\rangle$ is qv_{n-2}. Thus, since G is rank 3,

$$|G_{\langle x_2\rangle} : G_{\langle x_1\rangle,\langle x_2\rangle}| = qv_{n-2}.$$

The number of singular points not perpendicular to $\langle x_2\rangle$ is q^{n-2}. Thus

$$|G_{\langle x_2\rangle} : G_{\langle x_2\rangle,\langle x_{-2}\rangle}| = q^{n-2}.$$

This implies $q^{n-3} \mid y$. But q^{n-3} is exactly the number of points perpendicular to $\langle x_1 \rangle$ but not to $\langle x_2 \rangle$, so $y = q^{n-3}$. We illustrate:



Now suppose we have a Siegel elation of type 2, which, without loss of generality, we may call $r(x_1, x_2 + \alpha x_{-2})$ for some $\alpha \in K^*$. We now conjugate $r(x_1, x_2 + \alpha x_{-2})$ by some τ in H_0 which takes $\langle x_{-2} \rangle$ to $\langle x_{-2} + w - x_2 \rangle$, where w is some nonsingular vector perpendicular to x_2, x_1, x_{-1}, and x_{-2}. A preimage of τ in H fixes the vectors x_1, x_2 and sends x_{-2} to $x_{-2} + w - x_2$. Thus $\tau r(x_1, x_2 + \alpha x_{-2})\tau^{-1}$ is $r(x_1, x_2 + \alpha(x_{-2} + w - x_2))$. We multiply

$$r(x_1, x_2 + \alpha x_{-2}) r(x_1, -x_2 - \alpha x_{-2} - \alpha w + \alpha w_2) = r(x_1, -\alpha w + \alpha x_2).$$

(We recall $\rho(x, u)\rho(x, v) = \rho(x, u + v)$ and since we are in a finite field, $\rho(x, u)^k = \rho(x, -u)$, for $k = p - 1$, char $K = p$.)

Also by conjugating $r(x_1, x_2 + \alpha x_{-2})$ by σ in H_0 which sends $\langle x_{-2} \rangle$ to $\langle x_{-2} - w - x_2 \rangle$, and multiplying as above, we get $r(x_1, \alpha w + \alpha x_2)$ in G. The product

$$r(x_1, \alpha w + \alpha x_2) r(x_1, -\alpha w + \alpha x_2) = r(x_1, 2\alpha x_2),$$

which is a Siegel elation of type 1.

7. The subgroup of G fixing one point; the proof of the theorem

Let us look at the preimage M in $\Omega_n(K)$ of the stabilizer of a singular point, $G_{\langle x_1 \rangle}$. Since G is a rank 3 subgroup, $q^{n-2} \mid |G_{\langle x_1 \rangle}|$. Hence $q^{n-2} \mid |M|$. The elements of M can be represented in our standard bases as

$$\begin{pmatrix} a & \xi' & z' \\ 0 & A' & \eta' \\ 0 & 0 & a^{-1} \end{pmatrix}.$$

Let N be the subgroup of M with $a = 1$. Since $(M\colon N, q) = 1$, then $q^{n-2} \mid |N|$. There is a homomorphism h from N to $0_{n-2}(K)$ where elements of N are represented as

$$\begin{pmatrix} 1 & \xi & z \\ 0 & A & \eta \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$h\colon \begin{pmatrix} 1 & \xi & z \\ 0 & A & \eta \\ 0 & 0 & 1 \end{pmatrix} \to A.$$

We also know that $AJ_{n-2}A^t = J_{n-2}$, $\xi J_{n-2}\xi^t + 2z = 0$, and $AJ_{n-2}\xi^t + \eta = 0$. With this information, we see that any nonidentity element of the kernel is the Siegel transformation $\rho(x_1, \eta)$. But $A \in 0_{n-2}$, and for $n = 5, 6, 7$, $q^{n-2} \nmid |0_{n-2}|$. This proves the theorem.

8. Small dimensions

If the index of the space is smaller than 2, we cannot have the traditional rank 3 representation, where G is transitive on singular points and the stabilizer of a point P is transitive on the set of singular points perpendicular to P.

In dimension $n = 2$, there are at most two singular points. For dimensions 3 and 4, index 1, no two singular points are perpendicular to each other and Lemma 2 of Tamagawa [6] shows that $P\Omega_n(K)$ is doubly transitive on singular points.

For dimension $n = 4$, index 2, Witt's theorem implies that $PO_4(K)$ is a rank 3 permutation group. However, $P\Omega_4(K)$ is not rank 3. The Siegel elations of type 1 generate $P\Omega_4(K)$, and have two orbits of singular lines, namely

$$\{\langle x_{-1}, x_{-2}\rangle, \langle x_1 + kx_{-2}, x_2 - kx_{-1}\rangle, k \in F\}$$

and

$$\{\langle x_{-1}, x_2\rangle, \langle x_1 + kx_2, x_{-2} - kx_{-1}\rangle, k \in F\}.$$

References

1. E. Artin, *Geometric algebra*, Interscience, New York, 1964.
2. R. Carter, *Simple groups of Lie type*, Interscience, New York, 1972.
3. D. G. Higman and J. E. McLaughlin, *Rank 3 subgroups of finite symplectic and unitary groups*, J. Reine. Angew. Math., vol. 218 (1965), pp. 174–189.
4. D. Perin, *On collineation groups of finite projective spaces*, Math. Zeitschr., vol. 126 (1972), pp. 135–142.
5. B. S. Stark, *Some subgroups of $\Omega(V)$ generated by groups of root type* 1, Illinois J. Math., vol. 17 (1973), pp. 584–607.
6. T. Tamagawa, *On the structure of the orthogonal groups*, Amer. J. Math., vol. 80, (1958) pp. 191–197.

Northeastern University
Boston, Massachusetts