The Sylow 2-Subgroups of the Finite Classical Groups

ROGER CARTER AND PAUL FONG*

Department of Mathematics, The University, Newcastle-upon-Tyne, England
University of California, Berkeley, California

Communicated by Graham Higman
Received January 16, 1964

INTRODUCTION

Let $G$ be a finite classical group over a finite field of characteristic $p$ (the term will be made precise below). The Sylow $l$-subgroups of $G$, where $l$ is a prime number, have been given by Weir [7] in the case $l \neq 2, l \neq p$; and by Chevalley [2], and Ree [6] in the case $l = p$. In the latter case the normalizers of the Sylow $p$-subgroups were obtained as well. It is our purpose in this paper to settle the remaining case $l = 2, p \neq 2$, which is perhaps the most interesting in view of the importance of the prime 2 for the simple group associated to $G$. For the purposes of this paper a classical group over $GF(q), q = p^n$, will be any one of the following groups:

I. The general linear group $GL_n(q)$, order

$$q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1).$$

II. The symplectic group $Sp_{2n}(q)$, order

$$q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1).$$

III. The unitary group $U_n(q)$, order

$$q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i).$$

IV. The proper orthogonal group $O_{2n+1}^+(q)$, order

$$q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1).$$

* The work of the second author was partially supported by National Science Foundation Grant GP-1610.
V. The orthogonal group $O_{2n}(\eta, q), \eta = \pm 1$, order

$$2q^{n(n-1)}(q^n - \eta) \prod_{i=1}^{n} (q^{2i} - 1).$$

(The reason for the choice of $O_{2n+1}(q)$ rather than $O_{2n+1}(q)$ in IV will be apparent in the proofs.) A general description of these groups can be found in Artin [1] and Dickson [3].

The determination of the Sylow 2-subgroups and their normalizers will proceed in three stages (the orthogonal cases differing slightly, however): (i) degree 2, (ii) degree $2^r$, (iii) degree $n$. In (i) these subgroups can be computed directly. Once these are known, the construction given by the wreath product will give the corresponding subgroups in degree $2^r$. It is an immediate consequence of the definition of the wreath product $G \wr H$ of two finite groups $G$ and $H$ that if $G$ is a (irreducible) linear group of matrices, then $G \wr H$ is also a (irreducible) linear group. Moreover, if $G$ is a group of symplectic, unitary, or orthogonal matrices, then $G \wr H$ is respectively symplectic, unitary, or orthogonal. The final stage (iii) will follow easily from the results of (ii).

I. Sylow 2-Subgroups of $GL_n(q), Sp_{2n}(q), \text{ and } U_n(q)$

For I, II, or III, let $w_r$ be the exact power of 2 in the order of the corresponding group of dimension $2^r, r \geq 1$. If $r \geq 2$, then $w_r/w_{r-1}$ is the power of 2 in

$$\prod_{i=0}^{2^r-1} (q^{2^r-2i} - 1) \quad \text{in I}$$

$$\prod_{i=0}^{2^{r-1}-1} (q^{2^r-2i} - 1) \quad \text{in II}$$

$$(q^{2^r-2i} - 1)(q^{2^r-2i-1} + 1) \quad \text{in III.}$$

(1)

In I write $w_r/w_{r-1} = 2^{f(q, r)}$; in II write $w_r/w_{r-1} = 2^{g(q, r)}$. If $\nu$ is the exponential valuation of the integers with respect to 2, normalized by the condition $\nu(2) = 1$, then in III

$$\frac{w_r}{w_{r-1}} = 2^{2^{r-2\nu(q-1)} + 1} 2^{g(q, r)}.$$
since \(v(q^{m} + 1) = v(q + 1)\) whenever \(m\) is odd. It follows from the definition of \(f(q, r)\), \(g(q, r)\), and from (1) that

\[
\begin{align*}
f(q, r) &= \frac{1}{2} (2^r - 2^{r-1}) v(q - 1) + f(q^2, r - 1) \quad (r \geq 3) \\
g(q, r) &= \frac{1}{2} (2^{r-1} - 2^{r-2}) v(q^2 - 1) + g(q^2, r - 1) \quad (r \geq 3)
\end{align*}
\]

and hence

\[
\begin{align*}
f(q, r) &= v(q^{2^r} - 1) + \sum_{i=0}^{r-2} 2^{r-2-i} v(q^{2^i} - 1) \quad (r \geq 2) \\
g(q, r) &= v(q^{2^r} - 1) + \sum_{i=1}^{r-2} 2^{r-2-i} v(q^{2^i} - 1) \quad (r \geq 2) \quad (2)
\end{align*}
\]

(An empty sum will of course be zero.) By (2) we have

\[
f(q, r + 1) - 2f(q, r) = v(q^{2^{r+1}} - 1) - 2v(q^{2^r} - 1) + v(q^{2^{r-1}} - 1).
\]

Since

\[
v(q^{2^{r+1}} - 1) = v(q^{2^r} + 1) + v(q^{2^r} - 1) = 1 + v(q^{2^r} - 1),
\]

and

\[
v(q^{2^{r-1}} - 1) = v(q^{2^r} - 1) - v(q^{2^{r-1}} + 1) = v(q^{2^r} - 1) - 1,
\]

it follows that \(f(q, r + 1) = 2f(q, r)\). Similarly \(g(q, r + 1) = 2g(q, r)\). If we define

\[
\begin{align*}
F(r) &= f(q, r + 1), \\
G(r) &= g(q, r + 1)
\end{align*}
\]

then for \(r \geq 1\), we have

\[
F(r + 1) = 2F(r), \quad G(r + 1) = 2G(r). \quad (3)
\]

It now follows that

\[
\omega_r = \begin{cases} 
2^{F(r)-1} & \text{in I} \\
2^{G(r)-1} & \text{in II} \\
2^{r-1}v(q+1)2^{G(r)-1} & \text{in III.}
\end{cases} \quad (4)
\]

Indeed,

\[
\begin{align*}
F(1) &= v(q^4 - 1) + v(q - 1) = 1 + v(q^2 - 1) + v(q - 1), \\
G(1) &= v(q^4 - 1) = 1 + v(q^2 - 1),
\end{align*}
\]

and these are the correct values in (4) when \(r = 1\). Assuming (4) holds for \(1, 2, \ldots, r - 1\), we have in I,

\[
\omega_r = \omega_{r-1} 2^{F(r-1)} = 2^{2^{F(r-1)-1}} = 2^{F(r)-1}.
\]
in II
\[ w_r = w_{r-1} 2^{G(r-1)} \]
in III
\[ w_r = w_{r-1} 2^{G(r-1)} \]

Thus (4) holds for all \( r \geq 1 \).

Let \( T_i = Z_2 \times Z_2 \times \cdots \times Z_2 \) be the wreath product of \( Z_2 \) \( i \) times (\( Z_n \) in general is the cyclic group of order \( n \)). If \( W \) is a Sylow 2-subgroup of \( GL_2(q) \), \( Sp_2(q) \), or \( U_2(q) \), then \( W_r = W \wr T_{r-1} \) is certainly a 2-subgroup of the corresponding group in dimension \( 2^r \) (we define \( W_1 = W \)). But an induction argument shows that \( W_r \) is even a Sylow 2-subgroup. Indeed, this is true by definition for \( r = 1 \), and if we assume it so for \( 1, 2, \cdots, r-1 \), then \( W_r \) has order \( 2^r \), by (4). We have thus proved

**Lemma 1.** Let \( W \) be a Sylow 2-subgroup of \( GL_2(q) \), \( Sp_2(q) \), or \( U_2(q) \). The \( W_r = W \wr T_{r-1} \) is a Sylow 2-subgroup of \( GL_{2^r}(q) \), \( Sp_{2^r}(q) \), or \( U_{2^r}(q) \) respectively.

We determine \( W \) in each of the above cases. It will be useful not only to present \( W \) as a definite group of \( 2 \times 2 \) matrices, but to compute as well a lower bound for the number of distinct right translates \( a \times 2 \times 2 \) matrix \( A \), not \( (0 \ 0) \), can have under the action of right multiplication by the matrices of \( W \).

I. \( GL_2(q) \) has order \( q(q^2 - 1)(q - 1) \). If \( q \equiv 1 \pmod{4} \) let \( 2^s \) be the exact power of 2 dividing \( q - 1 \) (written \( 2^s | q - 1 \)). Then \( W \) has order \( 2^{2s+1} \). Let \( \epsilon \) be a primitive \( 2^s \)-th root of unity in \( GF(q) \). The matrices

\[
\begin{pmatrix}
\epsilon & 0 \\
0 & 1
\end{pmatrix}, \quad
\begin{pmatrix}
1 & 0 \\
0 & \epsilon
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & \epsilon
\end{pmatrix}
\]

generate a group of order \( 2^{2s+1} \), and hence \( W \simeq Z_{2^s} \times Z_2 \). A matrix \( A \) not \( (0 \ 0) \) has at least \( 2^{s+1} \) distinct right translates under \( W \); moreover, if \( A \) has no columns of zeros, then \( A \) has at least \( 2^{2s} > 2^{s+1} \) distinct right translates. If \( q \equiv 3 \pmod{4} \) and \( 2^s \nmid q + 1 \), then \( W \) has order \( 2^{s+2} \). Let \( \epsilon \) be a primitive \( 2^{s+1} \)-st root of unity in \( GF(q^2) \).

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & \epsilon + \epsilon^q \end{pmatrix}
\]

is a matrix in \( GL_2(q) \) of order \( 2^{s+1} \), since \( P^{-1}XP = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \), where \( P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \). The matrix \( Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \) transforms \( X \) onto \( X^{-1}X^2 \). The product \( YX \) has order 2; \( W \) is thus a so-called semidihedral group. A matrix \( A \) not \( (0 \ 0) \) has at least \( 2^{s+1} \) distinct right translates under \( W \). Indeed, \( PAP^{-1} \) has \( 2^{s+1} \) distinct
right translates already under the cyclic subgroup generated by \((\sigma_0 \tau_0)\). Note that in both cases the Sylow 2-subgroups of \(PGL_2(q)\) are dihedral.

II. \(Sp_2(q)\) has order \(q(q^2 - 1)\). It is well-known that \(Sp_2(q) \cong SL_2(q)\) and that \(W\) is a generalized quaternion group [4]. If \(q \equiv 1 \pmod{4}\) and \(2^e \mid q - 1\), then \(W\) has order \(2^{e+1}\). Let \(\epsilon\) be a primitive \(2^e\)-th root of unity in \(GF(q)\); the matrices \((\sigma_0 \tau_0)\), \((-\sigma_0 \tau_0)\) generate a group isomorphic to \(W\). A matrix \(A\) not \((\sigma_0 \tau_0)\) has at least \(2^e\) distinct right translates under \(W\). If \(q \equiv 3 \pmod{4}\) and \(2^e \mid q - 1\), then \(W\) has order \(2^{e+1}\). The matrices \(X^2, Y\) discussed in I above generate a group in \(SL_2(q)\) isomorphic to \(W\), so that the number of distinct right translates of \(A\) not \((\sigma_0 \tau_0)\) is at least \(2^e\).

III. \(U_2(q)\) has order \(q(q - 1)(q^2 - 1)\). If \(q = 3 \pmod{4}\), and \(2^e \mid q - 1\), then \(W\) has order \(2^{e+1}\). Let \(\epsilon\) be a primitive \(2^e\)-th root of unity in \(GF(q^2)\). The matrices \((\sigma_0 \tau_0), (\sigma_1 \tau_0), (\sigma_0 \tau_1)\) generate in \(U_2(q)\) a subgroup of order \(2^{e+1}\), and hence \(W \cong Z_2 \times Z_2\). The number of right translates of \(A\) not \((\sigma_0 \tau_0)\) in this case is not less than \(2^{e+1}\), and is not less than \(2^{2e}\) if \(A\) has no columns of zeros. If \(q \equiv 1 \pmod{4}\) and \(2^e \mid q - 1\), then \(W\) has order \(2^{e+2}\). Let \(\epsilon\) be a primitive \(2^e\)-th root of unity in \(GF(q^2)\). Then \(\epsilon^2 = -\epsilon\). Set \(\gamma = (\epsilon + \epsilon^{-1})/2, \delta = (\epsilon - \epsilon^{-1})/2\), so that \(\gamma^2 = -\gamma, \delta^2 = -\delta, \gamma^2 = -\delta^2\). Since \(\gamma^2\) is in \(GF(q)\), we can find nonzero elements \(\rho, \beta\) in \(GF(q)\) with \(\alpha^2 + \beta^2 = \gamma^2\) [3, p. 46]. The matrices \(X = (\frac{\alpha + \beta}{\beta}, -\frac{\alpha - \beta}{\beta}), Y = (\frac{1}{\alpha}, -\frac{1}{\alpha})\) are in \(U_2(q)\). The eigenvalues of \(X\) are \(\epsilon, -\epsilon^{-1}\), so \(X\) has order \(2^{e+1}\). Moreover, \(Y^2 = X^2, Y^{-1}XY = X^{-1}X^2\). Hence \(W = \{X, Y\}\) is semidihedral. The group \(\{X^2, Y\}\) is a subgroup of \(W\) of order \(2^{e+1}\) whose matrices all have the form \((-\frac{\alpha}{\beta}, \frac{\alpha}{\beta}, \frac{\alpha}{\beta}, \frac{\alpha}{\beta})\) with \(a^2 + b^2 = 1\). Let \(A = (\frac{a}{b}, \frac{b}{a}, \frac{b}{a}, \frac{b}{a})\). Then

\[
\begin{pmatrix}
  a_1 & a_2 \\
  a_3 & a_4
\end{pmatrix}
\begin{pmatrix}
  a & b \\
  -b & a
\end{pmatrix}
= 
\begin{pmatrix}
  a_1 & a_2 \\
  a_3 & a_4
\end{pmatrix}
\begin{pmatrix}
  a & b \\
  -b & a
\end{pmatrix}
\]

is equivalent to four homogeneous equations in the \(a_i\) with matrix

\[
\begin{pmatrix}
  a - 1 & -b^a & 0 & 0 \\
  b & a^b - 1 & 0 & 0 \\
  0 & 0 & a - 1 & -b^a \\
  0 & 0 & b & a^b - 1
\end{pmatrix}
\]

Since the \(a_i\) are not all zero, the determinant \([\det(a - 1)(a^b - 1) - b^a q]\) must be zero, or equivalently \(a + a^b = 2\). If \(\omega\) and \(\omega'\) are the eigenvalues of \((-\frac{\alpha}{\beta}, \frac{\alpha}{\beta})\), then \(\omega\) and \(\omega'\) are the roots of the equation \(t^2 - 2t + 1 = 0\), which implies \(\omega = \omega' = 1\). Since the order of \((-\frac{\alpha}{\beta}, \frac{\alpha}{\beta})\) is prime to \(p\), this means that \((-\frac{\alpha}{\beta}, \frac{\alpha}{\beta})\) is the identity matrix. Thus at least \(2^{e+1}\) distinct right translates of \(A\) arise.
Consider now the $n$-dimensional case. In I or III write
\[ n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t}, \]
in II write
\[ 2n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t}, \]
where $r_1 < r_2 < \cdots < r_t$. If $W_r$ is a Sylow 2-subgroup of the corresponding group in dimension $2^r$, then

\[ S = W_{r_1} \times W_{r_2} \times \cdots \times W_{r_t}, \]
is clearly a 2-subgroup of the corresponding group in dimension $n$. Here $W_0$ in I is the Sylow 2-subgroup of the multiplicative group of $GF(q)$, $W_0$ in III is the Sylow 2-subgroup of the group of $(q+1)$-st roots of unity in $GF(q^2)$. In order to prove that $S$ is actually a Sylow 2-subgroup, we are reduced by induction to proving $w_{r_i}$ is the exact power of 2 dividing
\[ (q^n - 1) (q^{n-1} - 1) \cdots (q^{n+1} - 1) \]
in I (5) holds for $r_i = 0, 1$. For $r_i \geq 2$, the exponent of 2 in
\[ v(q^n - 1) = v(q^{2^r} - 1); \]
in II $v(q^{2^n} - 1) = v(q^{2^{r_1}} - 1)$. The proof of the assertions contained in (5) is as follows: In I (5) holds for $r_i = 0, 1$. For $r_i \geq 2$, the exponent of 2 in (5) is
\[ v(q^n - 1) + \sum_{i=0}^{r_i-2} 2^{r_i-2-i} v(q^{2^i} - 1), \]
which agrees with the value of $w_{r_i}$ in (2). In II (5) holds for $r_i = 1$. For $r_i \geq 2$ the exponent of 2 in (5) is
\[ v(q^{2^n} - 1) + \sum_{i=1}^{r_i-2} 2^{r_i-2-i} v(q^{2^i} - 1), \]
which is the desired one. In III for \( r_1 = 0, \omega_0 = 2^{r(q-1)} \), while the power of 2 in (5) is \( 2^{r(q^2+1)} = 2^{r(q-1)} \) since \( n \) is odd. For \( r_1 \geq 1 \), the exponent of 2 in (5) is \( 2^{r-1}\varphi(q-1) + G(r_1) - 1 \). This verifies (5) in this case. Hence we have proved

**Theorem 1.** Let \( S \) be a Sylow 2-subgroup of \( GL_n(q) \), \( Sp_{2n}(q) \), or \( \mathbb{U}(q) \), and let \( 2^{r_1} - 2^{r_2} + \cdots + 2^{r_t}, r_1 < r_2 < \cdots < r_t \), be the 2-adic expansion of the dimension of the underlying space. Then \( S \cong W_{r_1} \times W_{r_2} \times \cdots \times W_{r_t} \), where \( W_r \) is a Sylow 2-subgroup of \( GL_{2r}(q) \), \( Sp_{2r}(q) \), or \( \mathbb{U}_{2r}(q) \) respectively.

**II. Sylow 2-Subgroups of \( O_{2n+1}^\pm(q) \) and \( O_{2n}(\eta, q) \)**

Consider first the case \( O_{2n}^\pm(q) \). Let \( W \) be a Sylow 2-subgroup of \( O_{2n}(\eta, q) \), where \( q \equiv \eta \pmod{4} \), and \( \mathfrak{W} \) its faithful representation in \( O_{2n}(q) \). Since the group \( O_{2n}(\eta, q) \) is dihedral (this is true whether \( \eta = 1 \) or \( \eta = -1 \) (Artin [1], p. 131)), \( W \) is dihedral. The representation \( \mathfrak{W} = \mathfrak{W} \oplus \det \mathfrak{W} \) embeds \( W \) in \( O_{2n}(q) \), and a consideration of the orders shows that \( \mathfrak{W}(W) \) is a Sylow 2-subgroup of \( O_{2n}(q) \). If \( q = 0 \pmod{4} \) and \( 2^{t} \| q - 1 \), then \( \mathfrak{W}(W) \) may be taken as the group generated by \((1_{n}, 1_{n}), (1_{n}, -1_{n})\) where \( \epsilon \) is a primitive \( 2^n \)-th root of unity. This follows from the fact that the underlying quadratic form may be taken as \( x_1^2 + y_2^2 \) (I, p. 144). In this case, \( W \) has order \( 2^{2^{n+1}} \) and the number of distinct right translates of \( A \) not \((0,0)^\circ \) by \( \mathfrak{W}(W) \) is at least \( 2^n \). If \( q = 1 \pmod{4} \) and \( 2^{t} \| q + 1 \), then \( W \) has order \( 2^{2^{n+1}} \). The underlying quadratic form in this case may be taken as \( x_1^2 - x_2^2 \). The matrices of the form \((a, b, -b, a)\), where \( a^2 - b^2 = 1 \), form a subgroup of order \( q - 1 \) in \( O_{2n}(-1, q) \) (3, p. 46). In particular, we may assume that \( \mathfrak{W}(W) \) contains a subgroup of order \( 2^n \) whose matrices have this form. If

\[
A = \begin{pmatrix}
a_1 & a_2 \\
a_3 & a_4
\end{pmatrix},
\]

then

\[
\begin{pmatrix}
a_1 & a_2 \\
a_3 & a_4
\end{pmatrix} \begin{pmatrix}
a & b \\
-b & a
\end{pmatrix} = \begin{pmatrix}
a_1 & a_2 \\
a_3 & a_4
\end{pmatrix}
\]

can occur if and only if \((a, b, -b, a)\) is the identity matrix. Thus \( A \) has at least \( 2^n \) distinct right translates under \( \mathfrak{W}(W) \).

A comparison of the orders of \( O_{2n+1}^\pm(q) \) and \( Sp_{2n}(q) \), \( n \geq 1 \), shows that their 2-power parts are the same. If we define \( W_r = W \uparrow T_{r-1}, r \geq 1 \), setting \( W_1 = W \), then the order of \( W_r \) is that of a Sylow 2-subgroup of \( O_{2r+1}^\pm(q) \).

In order to embed \( W_r \) in \( O_{2r+1}^\pm(q) \), we need
LEMMA 2. Let \( W \) be a Sylow 2-subgroup of \( O^*_3(q) \), \( \mathfrak{W} \) the faithful irreducible representation of \( W \) discussed above. Let \( W_r = W \cap T_{r-1} \). Then the faithful irreducible representation \( \mathfrak{W}_r \) of \( W_r \) associated to the representation \( \mathfrak{W} \) of \( W \) embeds \( W_r \) as a Sylow 2-subgroup in \( O^*_q(\eta, q) \) with \( q^{2r-1} \equiv \eta \) (mod 4).

Proof. For \( r = 1 \) there is nothing to prove. Assume the lemma has been proved for 1, 2, ..., \( r-1 \). That \( \mathfrak{W}_r \) is a faithful irreducible representation of \( W_r \) in \( O^*_q(\pm 1, q) \) follows from the fact on wreath products mentioned in the introduction. The orders involved imply, moreover, that \( \mathfrak{W}_r \) embeds \( W_r \) in \( O^*_q(\eta, q) \) with \( q^{2r-1} \equiv \eta \) (mod 4). This proves the lemma. As \( \det \mathfrak{W}_r \supseteq \mathfrak{W}_r \) embeds \( W_r \) in \( O^*_q(\eta, q) \), we have

**Corollary.** \( W_r \) is a Sylow 2-subgroup of \( O^*_2(q) \).

Consider now the general case \( O^*_n(q) \). If

\[
2n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_l}, \quad r_1 < r_2 < \cdots < r_l,
\]

is the 2-adic expansion of \( 2n \), then \( S = W_{r_1} \times W_{r_2} \times \cdots \times W_{r_l} \) is a 2-group whose order is that of a Sylow 2-subgroup of \( O^*_n(q) \). Moreover, \( S \) can be embedded by a faithful representation \( \mathfrak{S} = \mathfrak{W}_{r_1} \oplus \mathfrak{W}_{r_2} \oplus \cdots \oplus \mathfrak{W}_{r_l} \) in \( O^*_n(\eta, q) \) with \( q^{n-1} \equiv \eta \) (mod 4). The orders involved show that \( S \) is a Sylow 2-subgroup of \( O^*_n(\eta, q) \). The representation \( \det \mathfrak{S} \supseteq \mathfrak{S} \) embeds \( S \) in \( O^*_n(q) \). Thus we have proved

**Theorem 2.** Let \( S \) be a Sylow 2-subgroup of \( O^*_n(q) \) and let

\[
2n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_l}, \quad r_1 < r_2 < \cdots < r_l.
\]

Then \( S \cong W_{r_1} \times W_{r_2} \times \cdots \times W_{r_l} \), where \( W_r \) is a Sylow 2-subgroup of \( O^*_n(q) \).

Consider, finally, \( V \). If \( q^n = \eta \) (mod 4), then we have already seen that a Sylow 2-subgroup of \( O^*_n(\eta, q) \) is isomorphic to one of \( O^*_n(q) \). Suppose then that \( q^n \equiv -\eta \) (mod 4). For \( n = 1 \), \( O^*_2(\eta, q) \) has order \( 4g \), where \( g \) is odd. A Sylow 2-subgroup \( T \) of \( O^*_2(\eta, q) \) is then abelian of type \( Z_2 \times Z_2 \). For \( n \geq 2 \), we note that a Sylow 2-subgroup \( S_0 \) of \( O^*_{\eta-1}(q) \) can be embedded as a Sylow 2-subgroup in \( O^*_2(\eta, q) \) with \( q^{\eta-1} \equiv \eta \) (mod 4). Let \( V \) be the underlying space of \( O^*_{\eta-2}(\eta, q) \) and \( P \) the underlying plane for \( O^*_2(\eta', q) \), where \( \eta' \) is chosen so that \( P \perp V \) is an underlying space for \( O^*_2(\eta, q) \). Indeed, \( \eta' = \eta \) if \( q \equiv 1 \) (mod 4); \( \eta' = 1 \) if \( q \equiv -1 \) (mod 4). Then \( T \times S_0 \) is a Sylow 2-subgroup for \( O^*_n(\eta, q) \). We have therefore proved
THEOREM 3. Let $S$ be a Sylow 2-subgroup of $O_{2n}(\eta, q)$.

(i) If $q^n \equiv \eta \pmod{4}$, then $S$ is isomorphic to a Sylow 2-subgroup of $O_{2n+1}(q)$.

(ii) If $q^n \equiv -\eta \pmod{4}$, then $S \cong Z_2 \times Z_2 \times S_0$, where $S_0$ is a Sylow 2-subgroup of $O_{2n-1}^+(q)$.

III. NORMALIZERS OF THE SYLOW 2-SUBGROUPS

LEMMA 3. Let $G$ be any one of the groups $GL_2(q)$, $Sp_2(q)$, $U_2(q)$, $O_3^+(q)$, or $O_4(q, q)$, and let $Z(G)$ be the center of $G$. If $W$ is a Sylow 2-subgroup of $G$ and $N(W)$ its normalizer in $G$, then

\[ (N(W): WZ(G)) = \begin{cases} 1 & \text{if } G \neq Sp_2(q) \\
3 & \text{if } G = Sp_2(q) \end{cases} \quad \text{with} \quad q \equiv \pm 3 \pmod{8} \]

Proof. The groups $O_2(q, q)$ are dihedral, so that their Sylow 2-subgroups are self-normalizing. In all the other cases $G/Z(G)$ has dihedral Sylow 2-subgroups $D$. If $D$ has order 8 or more, than any automorphism of $D$ has order a power of 2. Thus in those cases where ($D : 1$) $\geq$ 8, and this will be the case as long as $G \neq Sp_2(q)$ with $q \equiv 3 \pmod{8}$, $N(W) \cong C(W) W$. But it is easily computed that $C(W) W = WZ(G)$ in these cases. For $G = Sp_2(q)$ with $q = \pm 3 \pmod{8}$, $W$ is a quaternion group, and $N(W)$ is known to be the extension of $W$ by an automorphism of order 3 [4].

We shall require the following result of P. Hall's:

LEMMA 4. Let $S_n$ be the symmetric group on $n$ symbols. Then the Sylow 2-subgroups of $S_n$ are self-normalizing.

Proof. Let

\[ n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t}, \]

where $r_1 < r_2 < \cdots < r_t$. If $T_r$ is $Z_2 \times Z_2 \times \cdots \times Z_2$ $r$ times, then it is known that $T = T_{r_1} \times \cdots \times T_{r_t}$ is a Sylow 2-subgroup of $S_n$ (5, pp. 81-82). Note that $T$ has $i$ transitive components of degrees $2^{r_1}$, $2^{r_2}$, $\cdots$, $2^{r_t}$. Let $x$ be an element of $S_n$ normalizing $T$. If $i$, $j$ are symbols in the same transitive component, the $iy = j$ for some $y$ in $T$.

\[ (ix) (x^{-1}yx) = jx, \quad x^{-1}yx \in T. \]

Thus $ix$, $jx$ are in the same transitive component. But different components have distinct number of elements. Thus $x$ leaves each component fixed.
It is therefore sufficient to show that $T_r$ is self-normalizing in $S_{2^r}$, and this we do by induction $T_r$ is the semidirect product of $M = T_{r-1} \times T_{r-1}$, by $Z_2$. Let $H$ be the stabilizer of a symbol in $T_r$. Then $H$ is a subgroup of $M$, and $M$ is generated by all the stabilizers in $T_r$. If $x$ is an element normalizing $T_r$, then $x$ permutes the stabilizers among themselves, so that $x$ normalizes $M$. Now $M$ has two transitive components, each of degree $2^{r-1}$. As above we can show that $x$ either leaves the components fixed or interchanges them. The normalizer $N(T_r)$ then has a normal subgroup of index 2 leaving both components of $M$ fixed. By induction this subgroup is $M$ itself, and hence $N(T_r) = T_r$. This completes the proof.

Let $G$ be any one of the groups $GL_2(q), Sp_2(q), U_2(q)$, or $O_2(\eta, q)$ with $q^{2r-1} = \eta (\text{mod } 4), r \geq 1$. We have seen in Lemmas 1 and 2 that if $W_r$ is a Sylow 2-subgroup of $G$, then we may consider the elements of $W_r$ as $2^{r-1} \times 2^{r-1}$ monomial matrices of type $T_{r-1}$, each coefficient not $(0, 0)$ being a $2 \times 2$ matrix in a fixed presentation of $W_1 = W$. (By a monomial matrix of type $T_{r-1}$, we mean that the associated permutation matrix is in $T_{r-1}$.)

**Lemma 5.** Let $G, W_r$ be as above. If $A$ is a matrix of $G$ normalizing $W_r$, then $A$, when considered as a $2^{r-1} \times 2^{r-1}$ matrix of $2 \times 2$ blocks, is monomial of type $T_{r-1}$.

**Proof.** Consider the set of all row vectors $(x_1, \ldots, x_{2^{r-1}})$ with $2^{r-1}$ components $x_i$, each $x_i$ being an arbitrary $2 \times 2$ matrix over $GF(q)$ (over $GF(2)$ in case $G = U_2(q)$). Say that two such vectors $(x_1, \ldots, x_{2^{r-1}})$ and $(\beta_1, \ldots, \beta_{2^{r-1}})$ are equivalent if there is a matrix $M$ in $W_r$ such that

$$(x_1, \ldots, x_{2^{r-1}}) \cdot M = (\beta_1, \ldots, \beta_{2^{r-1}}).$$

In other words, $(\beta_1, \ldots, \beta_{2^{r-1}})$ can be obtained from $(x_1, \ldots, x_{2^{r-1}})$ by first permuting the components by a permutation of type $T_{r-1}$, and then multiplying these components on the right by arbitrary elements of $W_r$. Consider in particular the rows of $A$. Since $A$ normalizes $W_r$, every vector equivalent to a row $\nu$ of $A$ is obtained from some row $\nu'$ of $A$ by multiplying each component of $\nu'$ on the left by a fixed element of $W_r$. Let $\nu$ be a fixed row of $A$ and $m$ the number of components of $\nu$ not $(0, 0)$. $m > 0$ since $A$ is nonsingular. We show $m = 1$.

Since $T_{r-1}$ is transitive, there is a vector equivalent to $\nu$ in which a prescribed component is not $(0, 0)$. There are therefore at least $2^{r-1}/m$ vectors equivalent to $\nu$, no two of which have the nonzero components in the same position. How many distinct vectors are there equivalent to $\nu$? To any given arrangement of the nonzero components, there are at least $(b)^m$ distinct vectors equivalent to $\nu$, where $b$ is a lower bound for the number of right translates a $2 \times 2$ matrix not $(0, 0)$ can have under $W_r$. But this has been computed in
sections I and II. Indeed, define \( s \) as follows: if \( q \equiv 1 \pmod{4} \), let \( 2^s \parallel q - 1 \); if \( q = 1 \pmod{4} \), let \( 2^s \parallel q - 1 \). Then

\[
\begin{array}{ccc}
q \pmod{4} & (W : 1) & b \\
\hline
1 & 1 & 2^{2s-1} 2^{s+1} \\
1 & -1 & 2^{2s+1} 2^{s-1} \\
\hline
2 & 1 & 2^{s+1} 2^{s} \\
2 & -1 & 2^{s-1} 2^{s} \\
\hline
3 & 1 & 2^{2s-1} 2^{s+1} \\
3 & -1 & 2^{2s+1} 2^{s-1} \\
\hline
5 & 1 & 2^{s+1} 2^{s} \\
5 & -1 & 2^{s-1} 2^{s} \\
\end{array}
\]

The number of distinct vectors obtainable by scalar multiplication on the left from the rows of \( A \) is at most \( 2^{r-1}(W : 1) \). Hence

\[
\frac{2^{r-1}}{m}(b)^m \leq 2^{r-1}(W : 1),
\]

or

\[
(b)^m \leq m(W : 1).
\]  

(6)

If \( (W : 1) = 2^{s+1}, b = 2^{s+1} \), then (6) becomes \( 2^{s(m-1)} : m-2 \leq m \), which implies \( m = 1 \). Similarly, if \( (W : 1) = 2^{s+1}, b = 2^s \), then \( m = 1 \). If \( (W : 1) = 2^{s-1}, b = 2^{s+1} \), then (6) becomes \( 2^{s(m-2)+m-1} \leq m \), which implies \( m = 1 \) or 2. Moreover, if \( m = 2 \), the equality must hold in (6). By earlier remarks, this implies that the two nonzero components of \( v \) both contain a column of zeroa. But for this row scalar multiplication on the left by elements of \( W \) yield at most \( 2^{2s} \) distinct vectors. Hence the strict inequality would hold in (6), which is impossible. Thus \( m = 1 \).

The matrix \( A \) is therefore monomial when considered as a matrix of \( 2 \times 2 \) blocks. The associated permutation normalizes \( T_{r-1} \), so that by Lemma 4, \( A \) is monomial of type \( T_{r-1} \). This proves the lemma. It should be remarked that if \( G \) is symplectic, unitary, or orthogonal, then the \( 2 \times 2 \) nonzero blocks in \( A \) are respectively symplectic, unitary, or orthogonal. In the orthogonal case, these \( 2 \times 2 \) blocks are in \( O_2(1, q) \) if \( q \equiv 1 \pmod{4} \), in \( O_2(-1, q) \) if \( q = -1 \pmod{4} \).
Lemma 6. Let $G$ be any one of the groups $GL_2(q)$, $Sp_2(q)$, $U_2(q)$, or $O_2(\eta, q)$ with $q^{2z-1} \equiv \gamma \pmod{4}$, and let $Z(G)$ be the center of $G$. If $W_r$ is a Sylow 2-subgroup of $G$ and $N(W_r)$ its normalizer in $G$, then

$$(N(W_r) : W_rZ(G)) = \begin{cases} 1 & \text{if } G \neq Sp_2(q) \text{ with } q \equiv \pm 3 \pmod{8} \\ 3 & \text{if } G = Sp_2(q) \text{ with } q \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. If $A$ normalizes $W_r$, then by Lemma 5 $A$ is monomial of type $T_{r-1}$ when $A$ is considered as a $2^{r-1} \times 2^{r-1}$ matrix of $2 \times 2$ blocks. It follows easily from inspection that the nonzero blocks of $A$ are either all in $W_r$ or in the same coset of $W$ in $N(W)$, where $N(W)$ is the normalizer of $W$ in the corresponding group of degree 2. The lemma then follows from Lemma 3.

Theorem 4. Let $G$ be any one of the groups $GL_v(q)$, $Sp_2(q)$, or $U_2(q)$, and let

$$
2^n = 2^r_1 + 2^r_2 + \cdots + 2^r_t,
$$

where $r_1 < r_2 < \cdots < r_t$, be the 2-adic expansion of the dimension of the underlying space. If $N(S)$ is the normalizer of a Sylow 2-subgroup $S$ of $G$ in $G$, then

I. $N(S) \cong S \times Z_{k_1} \times Z_{k_2} \times \cdots \times Z_{k_t}$, where $Z_{k_i}$ occurs $t$ times; $k_i$ is given by the condition $q \equiv \pm 1 \pmod{8}$.

II. $(N(S) : S) = \begin{cases} 1 & \text{if } q \equiv \pm 1 \pmod{8} \\ 3 & \text{if } q \equiv \pm 3 \pmod{8}. \end{cases}$

III. $N(S) \cong S \times Z_{k_1} \times Z_{k_2} \times \cdots \times Z_{k_t}$, where $Z_{k_i}$ occurs $t$ times; $k_i$ is given by the condition $q \equiv \pm 1 \pmod{8}$.

Proof. In each of the above cases $S$ is embedded in $G$ by a direct sum of nonequivalent irreducible representations. If $A$ is a matrix of $G$ normalizing $S$, then Schur's lemma implies that $A$ itself breaks up into a direct sum of matrices corresponding to the irreducible constituents involved. The theorem then follows from Lemma 6. (Note that in II a description of $N(S)$ can be easily obtained from the results of Lemmas 3 and 5.)

Theorem 5. Let $G$ be any one of the groups $O_{2n+1}(q)$, $O_{2n}(\eta, q)$. Then the Sylow 2-subgroups of $G$ are self-normalizing.

Proof. Consider first the case $G = O_{2n+1}(q)$. If

$$2n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_t},$$

where $r_1 < r_2 < \cdots < r_t$, then a Sylow 2-subgroup $S$ of $G$ is embedded in $G$ by the direct sum $\lambda \oplus \mathbb{W}_{r_1} \oplus \cdots \oplus \mathbb{W}_{r_t}$ of irreducible representations, where $\lambda$ is a nontrivial character assuming only the values $\pm 1$, and $\mathbb{W}_r$ is a representation in $O_2(\eta, q)$ with $q^{2r-1} \equiv \eta (\pmod{4})$. As in Theorem 4 it follows that $N(S) = S$. Suppose then that $G = O_{2n}(\eta, q)$. If $q^n \equiv \eta (\pmod{4})$, then
this case is included in the discussion of $O_{2n+1}^+(q)$. We may assume then that $q^n = -\eta \pmod{4}$. By Theorem 2, $S \simeq Z_2 \times Z_2 \times S_0$, where $S_0$ is a Sylow 2-subgroup of $O_{2n-2}(\eta', q)$ with $q^{n-1} = \eta' \pmod{4}$. Moreover, $S$ is embedded into $G$ by the direct sum of a 2-dimensional representation $\mathbb{3}$ of $Z_2 \times Z_2$ in $O_2(q''', q)$ with $q'' = -\eta''' \pmod{4}$ and the natural representation of $S_0$ in $O_{2n-2}(\eta', q)$. $\mathbb{3}$ decomposes into two non-equivalent linear representations. As before we can conclude that $N(S) = S$.

REFERENCES