Advances in Group Theory and Applications
© 2017 AGTA - www.advgrouptheory.com/journal
3 (2017), pp. 75–96
ISSN: 2499-1287
DOI: 10.4399/97888255036926

Groups from Class 2 Algebras and the Weil Character *

Christakis A. Pallikaros — Harold N. Ward

(*Received Sep. 21, 2016; Accepted May 5, 2017 — Communicated by F. de Giovanni*)

Abstract

We investigate the behaviour of the Weil character of the symplectic group on restriction to subgroups arising from commutative nilpotent algebras of class 2. We give explicit descriptions of the decomposition of the Weil character when restricted to the unipotent radical of the stabilizer of a maximal totally isotropic subspace and to its centralizer. Moreover, we show how these decompositions can be used to obtain alternative proofs for certain results concerning quadratic forms or Gauss sums.

Mathematics Subject Classification (2010): 20C15, 11F27

Keywords: Weil representations; symplectic group; quadratic form

1 Introduction

Because of their significant properties, Weil representations play an important role in the study of the representation theory of classical groups. The characters of Weil representations have been computed by various authors; see for example [1], [5], [6], [11]. We will be making use of some explicit results concerning the Weil characters of the symplectic group as these are obtained in [14] via the 'theta form'

* The authors are grateful to the referee for carefully reading the paper and making helpful suggestions. They are also grateful to Nataliya Ivanova for her assistance in preparing the manuscript for publication

(see also [11]). The approach in [14] is to follow the treatment for the Weil representation given in [13].

One of the aims of the present work is to follow up in the direction of some of the investigations in [9] and [10] concerning the restriction of the Weil characters of symplectic and unitary groups to certain subgroups, in particular to certain self-centralizing subgroups, with the question of multiplicity freeness. We remark here that the study of the behaviour of element centralizers in Weil representations already began in [4]. Our second aim is to make use of the explicit decompositions of the restricted Weil character we obtain in order to provide links with certain results in related areas such as quadratic forms over finite fields or Gauss sums. Perhaps it could be interesting to investigate further whether the study of such decompositions in this direction can actually lead to useful applications.

At this point we introduce some notation. Fix q a power of an odd prime and consider the Weil representation and its character ω for $Sp(2n, q)$, regarded as a matrix group on $V = GF(q)^{2n}$ defined via the symplectic form φ having matrix

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

The subgroup G of $Sp(2n, q)$ to be considered is $G = \langle -I \rangle \times B$, where B is the set of matrices

$$g_Q = \begin{bmatrix} I & 0 \\ Q & I \end{bmatrix},$$

with Q a symmetric matrix. So B is the unipotent radical of the stabilizer in $Sp(2n, q)$ of a maximal totally isotropic subspace of V, and G, which is the centralizer of B in $Sp(2n, q)$, is a maximal Abelian subgroup of $Sp(2n, q)$. Also note that the matrices $g_Q - I$ with $g_Q \in B$ belong to a nilpotent subalgebra of the full matrix algebra of $2n \times 2n$ matrices over $GF(q)$ of class 2 (compare with the discussion in [9]).

The restriction $\omega|G$ is known to be multiplicity free. In Sections 5 and 6 we give the details of an elementary self-contained proof of Theorem 6 in which we describe explicitly the irreducible characters of G (respectively, B) appearing in the decomposition of $\omega|G$ (respectively, $\omega|B$). Corresponding decompositions for the restriction of the Weil character to the centralizer of a regular unipotent element were studied in [10]. In Section 9 we give a quick proof of the fact that a subgroup H of G with a multiplicity free restriction $\omega|H$ satisfies $|H| \geqslant 2q^n$ and show that this bound is actually attained. Moreover, we give a construction of such a subgroup H with $|H| = 2q^n$

and $\omega|H$ multiplicity free.

In Sections 7, 8 and 9 we give some connections of the explicit decompositions for $\omega|B$ and $\omega|G$ with certain results in related areas. In Section 7 we use the expression for the decomposition $\omega|B$ in order to obtain alternative derivations for the number of solutions of the equation $Q(x) = \alpha$ with $\alpha \in GF(q)$, $x \in GF(q)^n$ and Q a quadratic form of $GF(q)^n$. It is interesting that the expressions we obtain for rank$Q$ even or odd are uniform, which perhaps is not obvious in traditional derivations. In Section 8 we use part of the decomposition $\omega|G$ in order to obtain a q-binomial identity. Finally, in Section 9 we show how specializing the expression for $\omega|B$ further to elements of the subgroup H described above provides a link with the Davenport-Hasse theorem on lifted Gauss sums.

The decompositions in Theorem 6 corroborate results in the preprint by Gurevich and Howe [3] (which appeared after we finished our manuscript), especially those in Section 2.

2 Preliminaries

We consider the Weil representation and its character ω for $Sp(2n, q)$, where q is a power of an odd prime, as a matrix group on $V = GF(q)^{2n}$ (with right action). We refer the reader to [1] for the construction of the Weil representation of various linear groups by means of representations of Heisenberg groups. That paper also presents the computation of the character of the Weil representations. On the other hand, the paper [13] produces the Weil representation through a natural action of a symplectic group on a twisted group algebra. The underlying group of that algebra is the additive group of the vector space on which the symplectic group is defined. In the present paper we will be following the notation about ω in [13], [14] and use some explicit results in [14] about its values. Note that in [5, Proposition 2] it is already shown that for $g \in Sp(2n, q)$ we have

$$|\omega(g)|^2 = q^{\dim V_g},$$

where $V_g = \{v \in V : vg = v\}$.

The symplectic form φ has matrix

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

Writing members of V as pairs (x, y), with $x, y \in GF(q)^n$, one has

$$\varphi((x_1, y_1), (x_2, y_2)) = x_1 y_2^T - y_1 x_2^T,$$

the superscript T standing for transpose.

The subgroup G of $Sp(2n, q)$ to be considered is $G = \langle -I \rangle \times B$, where B is the set of matrices

$$g_Q = \begin{bmatrix} I & 0 \\ Q & I \end{bmatrix}.$$

Such a matrix is in $Sp(2n, q)$ just when $Q^T = Q$; that is, Q is symmetric ("Q" emphasizes the associated quadratic form $Q(v) = vQv^T$ on $GF(q)^n$). Let $\mathbf{S}_n$ be the space of $n \times n$ symmetric matrices over $GF(q)$. There are $q^{n(n+1)/2}$ such matrices.

We will be restricting the Weil character ω to various subgroups of $Sp(2n, q)$. We call a subgroup H of $Sp(2n, q)$ *Weil-free* if the irreducible constituents of $\omega|H$ appear with multiplicity 1. The following theorem follows from results in [2], but we present a proof done in the spirit of [9].

Theorem 1 G *is Weil-free.*

Proof — We use the *orbit criterion*: an Abelian subgroup H of $Sp(2n, q)$ is Weil-free exactly when the number of orbits of H on V is q^n (see [9]). To count the orbits of G, recall that

$$(\#\text{ orbits}) = |G|^{-1} \sum_{v \in V} |G_v|,$$

G_v the stabilizer of v. Notice that the matrices

$$-g_Q = \begin{bmatrix} -I & 0 \\ -Q & -I \end{bmatrix}$$

in $-B$ fix only 0. Since

$$(x, y)^{g_Q} = (x, y) \begin{bmatrix} I & 0 \\ Q & I \end{bmatrix} = (x + yQ, y),$$

$v = (x, y)$ is fixed exactly when $yQ = 0$. We look at three cases:

$v = (0, 0)$: then $|G_{(0,0)}| = |G| = 2q^{n(n+1)/2}$.

$v = (x, 0), x \neq 0$: all members of B fix v and $|G_{(x,0)}| = q^{n(n+1)/2}$. There are $q^n - 1$ such v.

$v = (x, y), y \neq 0$: v is fixed by the elements g_Q with $yQ = 0$. We can set up such Q by thinking of it as a quadratic form with y in the radical. Write $GF(q)^n = \langle y \rangle \oplus W$. Then Q can be given by taking a form on W and extending it by 0 on $\langle y \rangle$. That gives $|G_{(x,y)}| = q^{n(n-1)/2}$, the number of choices for the form on W. There are $q^n(q^n - 1)$ of these v.

Thus for $\sum_{v \in V} |G_v|$ we get

$$\begin{aligned}\sum_{v \in V} |G_v| &= 2q^{n(n+1)/2} + (q^n - 1) \times q^{n(n+1)/2} \\ &\quad + q^n(q^n - 1) \times q^{n(n-1)/2} \\ &= q^{n(n+1)/2}\{2 + q^n - 1 + q^n - 1\} = q^n \times 2q^{n(n+1)/2}.\end{aligned}$$

So $|G|^{-1} \sum_{v \in V} |G_v| = q^n$, as needed. □

3 Irreducible characters of G

To describe the characters of G, let ψ be the *canonical additive character* of $GF(q)$, as used in [13] (the terminology is that of [7, p.190]):

$$\psi(\alpha) = e^{(2\pi i/p)\mathrm{tr}(\alpha)},$$

where tr is the trace function $GF(q) \to GF(p)$, p the prime dividing q. Each linear character of the additive group of $GF(q)$ is given by $\alpha \to \psi(\beta\alpha)$, $\beta \in GF(q)$ [7, Theorem 5.7] (this is equivalent to the nondegeneracy of the trace form $(\alpha, \beta) \to \mathrm{tr}(\alpha\beta)$). In what follows, χ is the quadratic character on $GF(q)^{\#}$ (the nonzero elements) and $\delta = \chi(-1)$. In [13], ρ was defined as

$$\sum_{\alpha \in GF(q)} \psi(\alpha^2);$$

we also have

$$\rho = \sum_{\beta \neq 0} \chi(\beta)\psi(\beta), \tag{1}$$

a Gaussian sum [7, Chapter 5, Section 2]; $\rho^2 = \delta q$. If $Q \in \mathbf{S}_n$, diagonalize Q and let

$$\Delta(Q) = \chi(\text{product of nonzero diagonal entries of } Q).$$

That is, if we write $GF(q)^n$ as $\mathrm{rad}(Q) \oplus W$, $\Delta(Q)$ is $\chi(\det(Q|W))$; $Q|W$ is the *nonsingular part* of Q. If Q has even rank $2k$, we call Q *hyperbolic* or *elliptic* according as $Q|W$ is hyperbolic or elliptic. If $Q|W$ is hyperbolic, then W is the orthogonal sum of hyperbolic planes, and $\det Q|W = (-1)^k$. Thus $\Delta(Q) = \delta^k$. If $Q|W$ is elliptic, then $\Delta(Q) = -\delta^k$.

Lemma 2 *The irreducible characters of* B *are the functions* λ_S *given by*

$$\lambda_S\left(g_Q\right) = \psi(\mathrm{Tr}(SQ)),$$

where $S \in \mathbf{S}_n$ *and* Tr *is the matrix trace. Each* λ_S *extends to two irreducible characters* $\lambda_S^{\pm}$ *of* G *by the formula*

$$\begin{aligned} \lambda_S^{\pm}\left(g_Q\right) &= \psi(\mathrm{Tr}(SQ)) \\ \lambda_S^{\pm}\left(-g_Q\right) &= \pm\psi(\mathrm{Tr}(SQ)), \end{aligned} \tag{2}$$

with the signs in the last equation matching on the two sides.

Proof — That this formula does give all the linear characters of B follows from the fact that the trace form $(S, Q) \to \mathrm{Tr}(SQ)$ on $\mathbf{S}_n$ is nondegenerate. That, in turn, can be seen as follows: suppose that $\mathrm{Tr}(SQ) = 0$ for all $Q \in \mathbf{S}_n$. Take a basis for $GF(q)^n$ that makes S diagonal. Suppose that ζ is a nonzero diagonal entry of S. Choose Q to have 1 at that position and 0 elsewhere. Then $\mathrm{Tr}(SQ) = \zeta$; so $\zeta = 0$ after all. Thus $S = 0$. So these characters λ_S are all distinct; and since there is the correct number of them, they give all the characters of B. Then for the characters of G, we use the direct product decomposition $G = \langle -I \rangle \times B$ to write them as claimed. □

4 Values of ω on G

For the values of ω, we use results from [14]. A member $-g_Q$ of $-B$ has $-g_Q - 1$ invertible, with diagonal entries -2, and [14, Section 6.5] gives

$$\omega\left(-g_Q\right) = \delta^n \chi(\det(-g_Q - 1)) = \delta^n \chi((-2)^{2n}) = \delta^n. \tag{3}$$

As for g_Q, [14, Theorem 6.7] implies that

$$\omega(g) = q^n \rho^{-\dim V^{g-1}} \chi(\det \Theta_g).$$

Here Θ_g is given in [14, Definition 3.3]: it is the form defined on V^{g-1} by

$$\Theta_g(u^{g-1}, v^{g-1}) = \varphi(u^{g-1}, v).$$

We have $(x,y)^{g-1} = (yQ, 0)$. So

$$\begin{aligned} \Theta_g((x_1,y_1)^{g-1},(x_2,y_2)^{g-1}) &= \varphi((x_1,y_1)^{g-1},(x_2,y_2)) \\ &= \varphi((y_1Q,0),(x_2,y_2)) \\ &= y_1 Q y_2^T. \end{aligned}$$

It follows that $\chi(\det \Theta_g) = \Delta(Q)$. Thus

Proposition 3 *The values of ω on G are given by*

$$\omega\left(g_Q\right) = q^n \rho^{-\operatorname{rank} Q} \Delta(Q) \tag{4}$$

$$\omega\left(-g_Q\right) = \delta^n. \tag{5}$$

If $Q = 0$, $\Delta(Q)$ is defined to be 1.

5 Character multiplicities in $\omega|G$

The multiplicity (which is 0 or 1) of a linear character λ in $\omega|G$ is

$$|G|^{-1} \sum_{g \in G} \omega(g) \overline{\lambda(g)}.$$

With $\lambda = \lambda_S^{\pm}$, we get

$$\sum_{g \in G} \omega(g) \overline{\lambda_S^{\pm}(g)} = \sum_{Q \in S_n} q^n \rho^{-\operatorname{rank} Q} \Delta(Q) \psi(-\operatorname{Tr}(SQ)) \pm \sum_{Q \in S_n} \delta^n \psi(-\operatorname{Tr}(SQ))$$

(again, the sign on the right matches the sign in $\lambda_S^{\pm}$). The second summation is 0 if $S \neq 0$, and $\delta^n q^{n(n+1)/2}$ if $S = 0$.

For further computations, we need some standard group-order formulas. They are taken from [12].

$$\begin{array}{ll}
\text{Group} & \text{Order} \\
GL(l,q) & q^{l(l-1)/2}\prod_{i=1}^{l}(q^i-1) \\
O^+(2k,q) & 2q^{k(k-1)}(q^k-1)\prod_{i=1}^{k-1}(q^{2i}-1) \\
O^-(2k,q) & 2q^{k(k-1)}(q^k+1)\prod_{i=1}^{k-1}(q^{2i}-1) \\
O(2k+1,q) & 2q^{k^2}\prod_{i=1}^{k}(q^{2i}-1) \\
Sp(2k,q) & q^{k^2}\prod_{i=1}^{k}(q^{2i}-1).
\end{array} \tag{6}$$

We also need the q-binomial coefficient $\begin{bmatrix} n \\ r \end{bmatrix}_q$ that gives the number of r-dimensional subspaces of $GF(q)^n$. By duality, $\begin{bmatrix} n \\ r \end{bmatrix}_q = \begin{bmatrix} n \\ n-r \end{bmatrix}_q$.

5.1 $S = 0$

When $S = 0$,

$$(\omega, \lambda_0^{\pm})_G = \frac{1}{2q^{n(n-1)/2}} \sum_{Q \in \mathbf{S}_n} \rho^{-\operatorname{rank} Q} \Delta(Q) \pm \frac{\delta^n}{2},$$

since $|G| = 2q^{n(n+1)/2}$. We conclude that the first term must be $1/2$:

$$\sum_{Q \in \mathbf{S}_n} \rho^{-\operatorname{rank} Q} \Delta(Q) = q^{n(n-1)/2}. \tag{7}$$

We shall elaborate on this in Section 8. Thus we have

Proposition 4 *The multiplicity of $\lambda_0^{\pm}$ in ω is*

$$(\omega, \lambda_0^{\pm})_G = \frac{1 \pm \delta^n}{2}.$$

5.2 $S \neq 0$

Here

$$\sum_{g \in G} \omega(g) \overline{\lambda_S^{\pm}(g)} = \sum_{Q \in \mathbf{S}_n} q^n \rho^{-\operatorname{rank} Q} \Delta(Q) \psi(-\operatorname{Tr}(SQ)).$$

It follows that λ_S^+ and λ_S^- appear with the same multiplicity in $\omega|G$. Now note that

$$\mathrm{Tr}(M^T SMQ) = \mathrm{Tr}(SMQM^T).$$

So with M nonsingular, $\lambda_S^\pm$ and $\lambda_{M^TSM}^\pm$ also have the same multiplicity in $\omega|G$. Suppose that $\mathrm{rank} S = r$. The number of members of $\mathbf{S}_n$ congruent to S (that is, of the form $M^T SM$) is

$$\begin{bmatrix} n \\ n-r \end{bmatrix}_q \times \frac{|GL(r,q)|}{|O(S)|} = \begin{bmatrix} n \\ r \end{bmatrix}_q \times \frac{|GL(r,q)|}{|O(S)|},$$

where $O(S)$ is the orthogonal group for S. We want to show that if $r > 1$, then this number is more than $(q^n - 1)/2$. That will imply that the only $S \neq 0$ that can appear in the characters in $\omega|G$ are the ones of rank 1; there are $q^n - 1$ of these [8, Theorem 13.2.47]. Again we separate by parity.

- $r = 2k$: Then

$$|O(S)| \leqslant \left|O^-(2k,q)\right| = 2q^{k(k-1)}(q^k+1)\prod_{i=1}^{k-1}(q^{2i}-1),$$

  from (6). So

$$\begin{aligned}
\begin{bmatrix} n \\ r \end{bmatrix}_q \times \frac{|GL(r,q)|}{|O(S)|} &\geqslant \begin{bmatrix} n \\ 2k \end{bmatrix}_q \times \frac{|GL(2k,q)|}{|O^-(2k,q)|} \\
&= \frac{\prod\limits_{j=n-2k+1}^{n}(q^j-1)}{\prod\limits_{j=1}^{2k}(q^j-1)} \times \frac{q^{k(2k-1)}\prod\limits_{j=1}^{2k}(q^j-1)}{2q^{k(k-1)}(q^k+1)\prod\limits_{i=1}^{k-1}(q^{2i}-1)} \\
&= \frac{\prod\limits_{j=n-2k+1}^{n}(q^j-1)}{2(q^k+1)\prod\limits_{i=1}^{k-1}(q^{2i}-1)} \times q^{k^2} \\
&\geqslant \frac{\prod\limits_{j=n-2k+1}^{n}(q^j-1)}{2(q^k+1)\prod\limits_{i=1}^{k-1}q^{2i}} \times q^{k^2} = \frac{\prod\limits_{j=n-2k+1}^{n}(q^j-1)}{2(q^k+1)} \times q^k.
\end{aligned}$$

Since $n-1 \geqslant n-2k+1$, from $k \geqslant 1$, and $n-2k+1 \geqslant 1$, the product

$$\prod_{j=n-2k+1}^{n-1} (q^j - 1)$$

is nonempty and its smallest factor is at least 2.

Thus

$$\prod_{j=n-2k+1}^{n-1} (q^j - 1) > 1 + \frac{1}{q^k}.$$

We conclude that

$$\begin{bmatrix} n \\ r \end{bmatrix}_q \times \frac{|GL(r,q)|}{|O(S)|} \geqslant \frac{\prod\limits_{j=n-2k+1}^{n} (q^j - 1)}{2(q^k+1)} \times q^k > \frac{q^n - 1}{2}.$$

- $r{=}2k{+}1$: This time, again with the appropriate formula from (6) filled in,

$$\begin{aligned}
\begin{bmatrix} n \\ r \end{bmatrix}_q \times \frac{|GL(r,q)|}{|O(S)|} &= \frac{\prod\limits_{j=n-2k}^{n} (q^j - 1)}{\prod\limits_{j=1}^{2k+1} (q^j - 1)} \times \frac{q^{k(2k+1)} \prod\limits_{j=1}^{2k+1} (q^j - 1)}{2q^{k^2} \prod\limits_{j=1}^{k} (q^{2j} - 1)} \\
&= \frac{\prod\limits_{j=n-2k}^{n} (q^j - 1)}{2 \prod\limits_{j=1}^{k} (q^{2j} - 1)} \times q^{k^2+k} \geqslant \frac{\prod\limits_{j=n-2k}^{n} (q^j - 1)}{2 \prod\limits_{j=1}^{k} q^{2j}} \times q^{k^2+k} \\
&= \frac{\prod\limits_{j=n-2k}^{n} (q^j - 1)}{2} > \frac{q^n - 1}{2},
\end{aligned}$$

as long as $k > 0$.

In the following result we sum up the discussion of this subsection.

Proposition 5 *Let $S \neq 0$. The multiplicity of $\lambda_S^{\pm}$ in ω is*

$$(\omega, \lambda_S^{\pm})_G = \begin{cases} \frac{1}{2q^{n(n-1)/2}} \sum\limits_{Q \in S_n} \rho^{-\operatorname{rank} Q} \Delta(Q) \psi(-\operatorname{Tr}(SQ)) & \textit{if } \operatorname{rank} S = 1 \\ 0 & \textit{otherwise.} \end{cases}$$

6 The decomposition of $\omega|G$

Collecting the results of the preceding section gives

$$\begin{aligned}
\omega|G &= \frac{1+\delta^n}{2}\lambda_0^+ + \frac{1-\delta^n}{2}\lambda_0^- \\
&+ \sum_{\operatorname{rank} S=1}\left(\frac{1}{2q^{n(n-1)/2}}\sum_{Q\in \mathbf{S}_n}\rho^{-\operatorname{rank} Q}\Delta(Q)\psi(-\operatorname{Tr}(SQ))\right)(\lambda_S^+ + \lambda_S^-).
\end{aligned}$$

We still need to determine which congruence class of symmetric matrices S of rank 1 actually appears in the decomposition. (There are two such classes, corresponding to $\Delta(S) = 1$ and $\Delta(S) = -1$. Each class has $(q^n-1)/2$ members.) To do so, we examine the characters on a small subgroup of G.

Let M be the $n \times n$ symmetric matrix with $M_{11} = 1$ and all other entries 0; $\Delta(M) = 1$. Let H be the subgroup consisting of the matrices

$$h_\alpha = \begin{bmatrix} I & 0 \\ \alpha M & I \end{bmatrix}, \quad \alpha \in GF(q).$$

Then $\omega(h_\alpha) = q^n$ if $\alpha = 0$, and $\omega(h_\alpha) = q^n\rho^{-1}\chi(\alpha)$ if $\alpha \neq 0$, by (4). Moreover, $\lambda_{\beta M}^{\pm}(h_\alpha) = \psi(\alpha\beta)$, for $\beta \neq 0$. It follows that

$$\begin{aligned}
(\omega, \lambda_{\beta M}^{\pm})_H &= q^{-1}\left\{q^n + \sum_{\alpha\neq 0} q^n\rho^{-1}\chi(\alpha)\psi(-\alpha\beta)\right\} \\
&= q^{n-1}\left\{1 + \delta\rho^{-1}\chi(\beta)\sum_{\alpha\neq 0}\chi(-\beta\alpha)\psi(-\beta\alpha)\right\} \\
&= q^{n-1}(1+\chi(\beta)\delta),
\end{aligned}$$

by (1). So $\lambda_{\beta M}^{\pm}$ appears in $\omega|H$ just when $\chi(\beta) = \delta$. This implies the following:

Theorem 6

$$\omega|G = \frac{1+\delta^n}{2}\lambda_0^+ + \frac{1-\delta^n}{2}\lambda_0^- + \sum_{\substack{\operatorname{rank} S=1 \\ \Delta(S)=\delta}}(\lambda_S^+ + \lambda_S^-). \tag{8}$$

In particular,

$$\omega|B = \lambda_0 + 2 \sum_{\substack{\text{rank}S=1 \\ \Delta(S)=\delta}} \lambda_S. \tag{9}$$

The Weil character is the sum of two irreducible characters, ω_+, of degree $(q^n+1)/2$, and ω_-, of degree $(q^n-1)/2$. Their values at $-I$ are $\omega_\pm(-I) = \pm\delta^n(q^n \pm 1)/2$ (see [14, Section 6]), the signs all matching. Observing the eigenvalues of $-I$ in the corresponding representations, we can write that

$$\begin{aligned} \omega_+|G &= \frac{1+\delta^n}{2}\lambda_0^+ + \frac{1-\delta^n}{2}\lambda_0^- + \sum_{\substack{\text{rank}S=1 \\ \Delta(S)=\delta}} \lambda_S^{\delta^n} \\ \omega_-|G &= \sum_{\substack{\text{rank}S=1 \\ \Delta(S)=\delta}} \lambda_S^{-\delta^n}. \end{aligned}$$

As an immediate consequence we get that both $\omega_+|B$ and $\omega_-|B$ are multiplicity free.

7 Computations with the $\omega|B$ decomposition

In this section we use the expression for the decomposition $\omega|B$ in order to obtain alternative derivations for the number of solutions of the equation $Q(x) = \alpha$ with $\alpha \in GF(q)$, $x \in GF(q)^n$ for the quadratic form Q on $GF(q)^n$. For this we first confirm, using a different approach, the above decomposition.

7.1 Confirmation of the $\omega|B$ decomposition

Recall that

$$g_Q = \begin{bmatrix} I & 0 \\ Q & I \end{bmatrix}.$$

By (4), $\omega(g_Q) = q^n\rho^{-\text{rank}Q}\Delta(Q)$. Let $\text{rank}Q = r$. Then (9) gives

$$\omega(g_Q) = q^n\rho^{-r}\Delta(Q) = 1 + 2 \sum_{\substack{\text{rank}S=1 \\ \Delta(S)=\delta}} \psi(\text{Tr}(SQ)). \tag{10}$$

If $x \in GF(q)^n$, $x \neq 0$, then $x^T x$ is a rank 1 symmetric matrix. Two such products $x^T x$ and $y^T y$ are equal just when $y = \pm x$. For $x = (\xi_1, \ldots, \xi_n)$, the diagonal entries of $x^T x$ are the ξ_i^2. Thus since at least one is nonzero, $\Delta(x^T x) = 1$. So all symmetric $n \times n$ rank 1 matrices can be written as $x^T x$ ($x \neq 0$) or $\nu x^T x$, where ν is a fixed nonsquare in $GF(q)$ (as mentioned above, there are $(q^n - 1)/2$ matrices of each type). We can rewrite (10) as follows:

$$\begin{aligned} \omega(g_Q) &= q^n \rho^{-r} \Delta(Q) \\ &= \sum_x \left\{ \frac{1+\delta}{2} \psi(\mathrm{Tr}(x^T x Q)) + \frac{1-\delta}{2} \psi(\mathrm{Tr}(\nu x^T x Q)) \right\}. \end{aligned} \tag{11}$$

The factors $(1 \pm \delta)/2$ pick out the S with $\Delta(S) = \delta$ and adjust for the fact that each S appears twice; the 1 on the right in (10) comes from $x = 0$ (recall also that we have set $\Delta(0) = 1$).

Now

$$\mathrm{Tr}(x^T x Q) = \mathrm{Tr}(x Q x^T) = \mathrm{Tr}(Q(x)) = Q(x),$$

so the preceding formula becomes

$$q^n \rho^{-r} \Delta(Q) = \sum_x \left\{ \frac{1+\delta}{2} \psi(Q(x)) + \frac{1-\delta}{2} \psi(\nu Q(x)) \right\}. \tag{12}$$

Let σ denote the sum. To evaluate σ we need the number of times $Q(x) = \alpha$ for $\alpha \in GF(q)$. These counts for nonzero α depend only on whether α is a square or not, since $Q(\beta x) = \beta^2 Q(x)$. Let 0 be taken on Z times (including $Q(0) = 0$); a given nonzero square S times; and a given nonsquare N times. Then

$$Z + (S + N)(q - 1)/2 = q^n.$$

We also need the character sums

$$\sum_{\alpha \neq 0 \text{ square}} \psi(\alpha) = \frac{\rho - 1}{2} \quad \text{and} \quad \sum_{\alpha \text{ nonsquare}} \psi(\alpha) = \frac{-\rho - 1}{2}, \tag{13}$$

which follow from

$$\sum_{\alpha \neq 0} \psi(\alpha) = -1, \quad \sum_{\alpha \neq 0 \text{ square}} \psi(\alpha) - \sum_{\alpha \text{ nonsquare}} \psi(\alpha) = \rho.$$

Collecting terms in σ according to whether $Q(x)$ is zero, a nonzero square or a nonsquare we get

$$\begin{aligned}\sigma &= Z\left\{\frac{1+\delta}{2}+\frac{1-\delta}{2}\right\}+S\left\{\frac{1+\delta}{2}\frac{\rho-1}{2}+\frac{1-\delta}{2}\frac{-\rho-1}{2}\right\}\\ &\quad +N\left\{\frac{1+\delta}{2}\frac{-\rho-1}{2}+\frac{1-\delta}{2}\frac{\rho-1}{2}\right\}\\ &= Z-\frac{S+N}{2}+\delta\rho\frac{S-N}{2}.\end{aligned}$$

Then put $Z = q^n - (S+N)(q-1)/2$ to obtain

$$\sigma = q^n - \frac{q(S+N)}{2} + \delta\rho\frac{S-N}{2}. \tag{14}$$

Now we need S and N. If Q_0 is the nonsingular part of Q, the counts for Q are those for Q_0 multiplied by q^{n-r}. Here are these numbers for Q, obtained from [7, Theorems 6.26 and 6.27] for Q_0:

$$\begin{array}{cc} \multicolumn{2}{c}{r \text{ even}} \\ S & N \\ q^{n-1}-\delta^{r/2}\Delta(Q)q^{n-r/2-1} & q^{n-1}-\delta^{r/2}\Delta(Q)q^{n-r/2-1}=S \\ \\ \multicolumn{2}{c}{r \text{ odd}} \\ S & N \\ q^{n-1}+\delta^{(r-1)/2}q^{n-(r+1)/2}\Delta(Q) & q^{n-1}-\delta^{(r-1)/2}q^{n-(r+1)/2}\Delta(Q) \end{array} \tag{15}$$

Substituting into (14), we obtain simplifications corresponding to the parity of r.

- r even: then $S = N$ and

$$\begin{aligned}\sigma &= q^n - \frac{q}{2}(2q^{n-1} - 2\delta^{r/2}\Delta(Q)q^{n-r/2-1})\\ &= \delta^{r/2}\Delta(Q)q^{n-r/2}.\end{aligned}$$

  Since $q^{r/2} = \delta^{r/2}\rho^r$, this is correctly $q^n\rho^{-r}\Delta(Q)$.

- r odd: then

$$\begin{aligned}\sigma &= q^n - \frac{q}{2}2q^{n-1} + \delta^{(r-1)/2}q^{n-(r+1)/2}\Delta(Q)\delta\rho \\ &= \delta^{(r+1)/2}q^n q^{-(r+1)/2}\rho\Delta(Q) \\ &= \delta^{(r+1)/2}q^n\delta^{(r+1)/2}\rho^{-r-1}\rho\Delta(Q) \\ &= q^n\rho^{-r}\Delta(Q),\end{aligned}$$

again correct.

7.2 The S, N formulas

In point of fact, the formulas for S and N follow from those for $\omega|B$. Combining (10) and (12) gives

$$q^n\rho^{-r}\Delta(Q) = q^n - \frac{q(S+N)}{2} + \delta\rho\frac{S-N}{2}. \tag{16}$$

For a needed second equation, let Q' be Q scaled by a nonsquare and let S' and N' be the number of solutions of the equation $Q'(x) = \alpha$ for α a nonzero square and α a nonsquare respectively (with x in $GF(q)^n$). Then $S' = N$ and $N' = S$, and $\Delta(Q') = (-1)^r\Delta(Q)$. Formula (16) for Q' reads

$$q^n\rho^{-r}(-1)^r\Delta(Q) = q^n - \frac{q(S+N)}{2} + \delta\rho\frac{N-S}{2}. \tag{17}$$

Solving (16) and (17) for S and N produces

$$\begin{aligned}S &= q^{n-1} - \frac{1+(-1)^r}{2}q^{n-1}\rho^{-r}\Delta(Q) + \frac{1-(-1)^r}{2}q^n\rho^{-r-1}\delta\Delta(Q) \\ N &= q^{n-1} - \frac{1+(-1)^r}{2}q^{n-1}\rho^{-r}\Delta(Q) - \frac{1-(-1)^r}{2}q^n\rho^{-r-1}\delta\Delta(Q),\end{aligned}$$

and then

$$\begin{aligned}Z &= q^n - (S+N)\frac{q-1}{2} \\ &= q^{n-1} + \frac{1+(-1)^r}{2}q^{n-1}(q-1)\rho^{-r}\Delta(Q).\end{aligned}$$

These are uniform expressions (perhaps not obvious in traditional derivations!) which give (15) on taking r even or odd.

Incidentally, when $\delta = -1$ or q is not a square, ρ is not rational. In that case, the formulas follow from equating coefficients in (16) for the quadratic field $\mathbb{Q}(\rho) = \mathbb{Q} + \mathbb{Q}\rho$ and again solving for S and N.

8 A q-binomial identity

Recall equation (7):

$$\sum_{Q \in \mathcal{S}_n} \rho^{-\operatorname{rank} Q} \Delta(Q) = q^{n(n-1)/2}.$$

If $\operatorname{rank} Q$ is odd, then with ν a nonsquare in $GF(q)$, $\Delta(\nu Q) = -\Delta(Q)$, and the terms for Q and νQ in the sum cancel. Thus since $\rho^{-2k} = \delta^k q^{-k}$,

$$\begin{aligned} q^{n(n-1)/2} &= \sum_{Q \in \mathcal{S}_n} \rho^{-\operatorname{rank} Q} \Delta(Q) \\ &= \sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{\substack{Q \in \mathcal{S}_n \\ \operatorname{rank} Q = 2k}} \delta^k q^{-k} \Delta(Q). \end{aligned} \tag{18}$$

Let $\operatorname{rank} Q = 2k$. As pointed out in Section 3, if Q is hyperbolic, then $\Delta(Q) = \delta^k$; and if Q is elliptic, then $\Delta(Q) = -\delta^k$.

Now we can give a specific formula for

$$\sum_{\substack{Q \in \mathcal{S}_n \\ \operatorname{rank} Q = 2k}} \delta^k q^{-k} \Delta(Q).$$

The number of terms with Q hyperbolic is

$$\begin{bmatrix} n \\ 2k \end{bmatrix}_q \times \frac{|GL(2k, q)|}{|O^+(2k, q)|},$$

and the number with Q elliptic is

$$\begin{bmatrix} n \\ 2k \end{bmatrix}_q \times \frac{|GL(2k, q)|}{|O^-(2k, q)|}.$$

Thus

$$\sum_{\substack{Q\in \mathbf{S}_n\\ \operatorname{rank} Q=2k}} \delta^k q^{-k}\Delta(Q) =$$

$$\delta^k q^{-k}\begin{bmatrix} n\\ 2k\end{bmatrix}_q \times |GL(2k,q)| \times \delta^k\left(\frac{1}{|O^+(2k,q)|}-\frac{1}{|O^-(2k,q)|}\right);$$

the second δ^k is the factor needed for $\Delta(Q)$. By (6),

$$\frac{1}{|O^+(2k,q)|}-\frac{1}{|O^-(2k,q)|}=\frac{1}{q^{k(k-1)}\prod_{i=1}^{k}(q^{2i}-1)}$$

(note the addition of one more factor in the product). So, again by (6),

$$\begin{aligned}\sum_{k=0}^{\lfloor n/2\rfloor}\sum_{\substack{Q\in \mathbf{S}_n\\ \operatorname{rank} Q=2k}} \delta^k q^{-k}\Delta(Q) &= \sum_{k=0}^{\lfloor n/2\rfloor}\delta^k q^{-k}\begin{bmatrix} n\\ 2k\end{bmatrix}_q \times \delta^k\frac{q^{k(2k-1)}\prod_{i=1}^{2k}(q^i-1)}{q^{k(k-1)}\prod_{i=1}^{k}(q^{2i}-1)}\\ &= \sum_{k=0}^{\lfloor n/2\rfloor}\begin{bmatrix} n\\ 2k\end{bmatrix}_q q^{k^2-k}\prod_{i=0}^{k-1}(q^{2i+1}-1).\end{aligned}$$

Thus from (18),

$$q^{n(n-1)/2}=\sum_{k=0}^{\lfloor n/2\rfloor}\begin{bmatrix} n\\ 2k\end{bmatrix}_q q^{k^2-k}\prod_{i=0}^{k-1}(q^{2i+1}-1).$$

We may see why this identity holds by counting the number of skew-symmetric $n\times n$ matrices over $GF(q)$. The number of skew-symmetric $n\times n$ matrices of rank $2k$ is

$$\begin{aligned}\begin{bmatrix} n\\ 2k\end{bmatrix}_q \times \frac{|GL(2k,q)|}{|Sp(2k,q)|} &= \begin{bmatrix} n\\ 2k\end{bmatrix}_q \frac{q^{k(2k-1)}\prod_{i=1}^{2k}(q^i-1)}{q^{k^2}\prod_{i=1}^{k}(q^{2i}-1)}\\ &= \begin{bmatrix} n\\ 2k\end{bmatrix}_q q^{k^2-k}\prod_{i=0}^{k-1}(q^{2i+1}-1)\end{aligned}$$

(see [8, Theorem 13.2.48]), and that is to be summed from $k = 0$

to $\lfloor n/2 \rfloor$ (giving 1 at $k = 0$). But the total number of skew-symmetric $n \times n$ matrices is simply $q^{n(n-1)/2}$.

9 Minimum Weil-free subgroups of G

Suppose that H is a subgroup of G. If $\omega|H$ is also Weil-free, then $|H| \geqslant q^n$. It cannot be that $|H| = q^n$, because then $\omega|H$ would just be the sum of all q^n linear characters of H. But that sum is q^n at I and 0 at $h \neq I$, whereas $\omega(h) \neq 0$, by (4). Thus $|H| \geqslant 2q^n$. We shall show that there are Weil-free subgroups of order $2q^n$. If $|H| = 2q^n$, then

$$H = \langle -I \rangle \times (H \cap B)$$

(for this last point observe first that the assumption q is odd ensures that $-I$ is the unique element of order 2 in G, so $-I \in H$ as H has even order).

Adapting the orbit count in the proof of Theorem 1, we find that $2q^n \times$(number of orbits) of such an H is

$$2q^n + (q^n - 1)q^n + \sum_x \sum_{y \neq 0} \left| H_{(x,y)} \right| \geqslant$$

$$2q^n + (q^n - 1)q^n + q^n(q^n - 1) = 2q^{2n}.$$

So if H is to be Weil-free, each $H_{(x,y)}$ with $y \neq 0$ must be just $\{I\}$. Again as in the proof of Theorem 1, this means that if $g_Q \in H$, with $Q \neq 0$, then Q must have full rank n. So what would work is an n-dimensional subspace W of $\mathbf{S}_n$ whose nonzero members are all nonsingular. Then $H \cap B$ would be $\{g_Q | Q \in W\}$.

To construct W, realize $GF(q)^n$ as $GF(q^n)$ and let tr be the trace function $GF(q^n) \to GF(q)$. Then for $\alpha \in GF(q^n)$, the function Q_α given by $Q_\alpha(\zeta) = \mathrm{tr}(\alpha\zeta^2)$ is a quadratic form on $GF(q^n)$. The corresponding bilinear form is $B_\alpha(\xi, \eta) = \mathrm{tr}(\alpha\xi\eta)$. This is nondegenerate when $\alpha \neq 0$, making Q_α nonsingular then. Now let

$$W = \{Q_\alpha | \alpha \in GF(q^n)\}.$$

The rest of this section is devoted to an evaluation concerning subgroup H.

Formula (12) for Q_a reads

$$q^n \rho^{-n} \Delta(Q_\alpha) = \sum_{\zeta \in GF(q^n)} \left\{ \frac{1+\delta}{2} \psi(Q_\alpha(\zeta)) + \frac{1-\delta}{2} \psi(\nu Q_\alpha(\zeta)) \right\}.$$

Because $\nu \in GF(q)$ and $\rho^2 = \delta q$, this becomes

$$\delta^n \rho^n \Delta(Q_\alpha) = \sum_{\zeta \in GF(q^n)} \left\{ \frac{1+\delta}{2} \psi(\mathrm{tr}(\alpha\zeta^2)) + \frac{1-\delta}{2} \psi(\mathrm{tr}(\nu\alpha\zeta^2)) \right\}. \quad (19)$$

One has to be careful with the matrix interpretation. Let $\zeta_1, \ldots, \zeta_n$ be a $GF(q)$-basis of $GF(q^n)$. Then the matrix for B_α is $\left[\mathrm{tr}(\alpha\zeta_i\zeta_j)\right]$ which can be written as the product

$$ABC$$

where

$$A = \begin{bmatrix} \zeta_1 & \zeta_1^q & \ldots & \zeta_1^{q^{n-1}} \\ \zeta_2 & \zeta_2^q & \ldots & \zeta_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ \zeta_n & \zeta_n^q & \ldots & \zeta_n^{q^{n-1}} \end{bmatrix}, \quad B = \begin{bmatrix} \alpha & 0 & \ldots & 0 \\ 0 & \alpha^q & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \alpha^{q^{n-1}} \end{bmatrix}$$

and

$$C = \begin{bmatrix} \zeta_1 & \zeta_2 & \ldots & \zeta_n \\ \zeta_1^q & \zeta_2^q & \ldots & \zeta_n^q \\ \vdots & \vdots & \ldots & \vdots \\ \zeta_1^{q^{n-1}} & \zeta_2^{q^{n-1}} & \ldots & \zeta_n^{q^{n-1}} \end{bmatrix},$$

giving an expression for $\left[\mathrm{tr}(\alpha\zeta_i\zeta_j)\right]$ in the form

$$D \times \mathrm{diag}(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}) \times D^T.$$

Taking determinants gives

$$\det\left[\mathrm{tr}(\alpha\zeta_i\zeta_j)\right] = (\det D)^2 \prod_{i=0}^{n-1} \alpha^{q^i} = (\det D)^2 N(\alpha),$$

in which $(\det D)^2$ is the discriminant of the extension $GF(q^n)/GF(q)$

and $\prod_{i=0}^{n-1} \alpha^{q^i}$ is the norm $N(\alpha)$ of α. Then

$$\Delta(Q_a) = \chi((\det D)^2)\chi(N(\alpha)).$$

Applying the automorphism $\xi \to \xi^q$ to D cycles its columns; so $(\det D)^q = (-1)^{n-1} \det D$, the sign being that of an n-cycle. Thus $\chi((\det D)^2) = (-1)^{n-1}$: $(\det D)^2$ is a square in $GF(q)$ only when its square-root $\det D$ is in $GF(q)$. For $\chi(N(\alpha))$ we have

$$\chi(N(\alpha)) = N(\alpha)^{\frac{q-1}{2}} = \left(\alpha^{\frac{q^n-1}{q-1}}\right)^{\frac{q-1}{2}} = \alpha^{\frac{q^n-1}{2}} = X(\alpha),$$

where $X(\alpha)$ is the quadratic character of α for the field $GF(q^n)$ (we can determine any $\chi(z)$ by reading it in $GF(q)$). All together,

$$\Delta(Q_\alpha) = (-1)^{n-1}X(\alpha).$$

For the right side of (19), we have that $\sum_\zeta \psi(\mathrm{tr}(\beta\zeta^2)) = X(\beta)P$, where P is the "ρ" for $GF(q^n)$, by the formulas in (13) for $GF(q^n)$. Moreover, since ν is a nonsquare in $GF(q)$, $X(\nu) = (-1)^n$. Therefore (19) becomes

$$\begin{aligned} \delta^n\rho^n(-1)^{n-1}X(\alpha) &= \left\{\frac{1+\delta}{2}X(\alpha)P + \frac{1-\delta}{2}(-1)^n X(\alpha)P\right\} \\ &= X(\alpha)P\left\{\frac{1+(-1)^n}{2} + \delta\frac{1-(-1)^n}{2}\right\}, \end{aligned}$$

or

$$\delta^n\rho^n(-1)^{n-1} = P\left\{\frac{1+(-1)^n}{2} + \delta\frac{1-(-1)^n}{2}\right\}.$$

This simplifies to

$$P = (-1)^{n-1}\rho^n,$$

on sorting by the parity of n. That is a particular instance of the Davenport-Hasse theorem on lifted Gauss sums [7, Theorem 5.14].

REFERENCES

[1] P. Gérardin: "Weil representations associated to finite fields", *J. Algebra* 46 (1977), 54–101.

[2] R. Guralnick – K. Magaard – J. Saxl – P.H. Tiep: "Cross characteristic representations of symplectic and unitary groups", *J. Algebra* 257 (2002), 291–347.

[3] S. Gurevich – R. Howe: "Small representations of finite classical groups", *arXiv:1609.01276v1* (2016).

[4] G. Heide – A.E. Zalesski: "Passman's problem on adjoint representations", in Groups, Rings and Algebras, *Contemp. Math.*, Providence (2006), 163–176.

[5] R. Howe: "On the character of Weil's representation", *Trans. Amer. Math. Soc.* 177 (1973), 287–298.

[6] I.M. Isaacs: "Characters of solvable and symplectic groups", *Amer. J. Math.* 95 (1973), 594–635.

[7] R. Lidl – H. Niederreiter: "Finite Fields", *Cambridge University Press*, (1997).

[8] G.L. Mullen – D. Panario, editors: "Handbook of Finite Fields", *CRC Press*, Boca Raton (2013).

[9] C.A. Pallikaros – H.N. Ward: "Commutative nilpotent closed algebras and Weil representations", *Comm. Algebra* 43 (2015), 4839–4859.

[10] C.A. Pallikaros – A.E. Zalesski: "Weil representations and some nonreductive dual pairs in symplectic and unitary groups", *Comm. Algebra* 39 (2011), 2156–2178.

[11] T. Thomas: "The character of the Weil representation", *J. Lond. Math. Soc. (2)*, 77 (2008), 221–239.

[12] D.E. Taylor: "The Geometry of the Classical Groups", *Heldermann Verlag*, Berlin (1992).

[13] H.N. Ward: "Representations of symplectic groups", *J. Algebra* 20 (1972), 182–195.

[14] H.N. Ward: "Matrices for the Weil representation", *arXiv:1705.09138* (2017).

Christakis A. Pallikaros
Department of Mathematics and Statistics
University of Cyprus
PO Box 20537, 1678 Nicosia, Cyprus
e-mail: pallikar@ucy.ac.cy

Harold N. Ward
Department of Mathematics
University of Virginia
Charlottesville, VA 22904, USA
e-mail: hnw@virginia.edu