Weil Representations of Finite Fields

Tim Tzaneteas

December 2, 2005

1 Introduction

These notes present some of the results of a paper by Paul Gérardin [1] concerning the representations of matrix groups over finite fields. If V is a finite-dimensional vector space over the finite field $\mathbb{F}_q$ of order q, there is a natural representation π, of $GL(V)$ in the space, $\mathbb{C}[V]$, of all complex-valued functions on V, where π is given by

$$(\pi(g)f)(x) = f(g^{-1}x)$$

for $g \in GL(V)$, $f \in \mathbb{C}[V]$, $x \in V$. The character of this representation is given by

$$g \mapsto q^{N(V;g)},\ N(V;g) = \dim\ker(g-1)$$

This, however, does not extend to symplectic groups immediately but by considering $V \times V^*$ equipped with a natural alternating non-degenerate bilinear form, we get the representation π by a process that does extend to symplectic groups, since a symplectic vector space E can be viewed as $E_+ \times E_+^*$, where E_+ is a Lagrangian subspace.

This process gives the Weil representation and for general linear groups is described in section 2, while its extension to symplectic groups is described in section 3. Finally, section 4 states some results about the decomposition of these Weil representations into irreducible representations.

2 Weil Representations of General Linear Groups

Let V be a finite dimensional vector space over a finite field $\mathbb{F}_q$, and let V^* be the dual space of V. We write $< y, x >$ for the action of $y \in V^*$ on $x \in V$, and identify V^{**} with V by setting $< x, y >= - < y, x >$.

Definition 1. Let $H(V)$ be the group $V \times V^* \times \mathbb{F}_q$ with the multiplication induced by identifying each $(x, y, z) \in H(V)$ with the matrix.

$$\begin{pmatrix} 1 & y & z \\ & 1 & x \\ & & 1 \end{pmatrix}.$$

$H(V)$ is called the *Heisenberg group* associated to V.

Explicitly, the multiplication rule is:

$$(x, y, z) \cdot (x', y', z') = (x + x', y + y', z + z' + < y, x' >)$$

This shows that V, V^*, and $\mathbb{F}_q$ are embedded as subgroups of $H(V)$. We can use $H(V)$ to induce a bilinear form on $V \times V^*$ using the commutator, since

$$[(x, y, z), (x', y', z')] = (0, 0, < y, x' > - < y', x >)$$

This bilinear form is clearly alternating, but it is also non-degenerate, since if $((x, y), (x', y')) \mapsto 0$, for all x', y', then $< y, x' >=< y', x >$. Setting $y' = 0$, we have $< y, x' >= 0$ for all x' and thus $y = 0$, and similarly, setting $x' = 0$ gives $< y', x >= 0$ for all y' and thus $x = 0$.

The non-degeneracy of this bilinear form implies that the center of $H(V)$ is $\mathbb{F}_q$: Suppose we have $(x, y, z) \in Z$. Then from the multiplication rule we see that $< y, x' >=< y', x >$ for all x', y', i.e. $< y, x' > - < y', x >= 0$, and thus $x = y = 0$, so $h \in \mathbb{F}_q$. The opposite inclusion, $\mathbb{F}_q \subseteq Z$, follows immediately from the multiplication rule. Non-degeneracy also implies that both $V\mathbb{F}_q$ and $V^*\mathbb{F}_q$ are maximal commutative subgroups in $H(V)$.

Before continuing, we need the following general fact about representations.

Lemma 2. *Let H be a finite group with center Z. Suppose there is a character ζ of Z such that for every $h \in H - Z$, there is $h' \in H$ such that the commutator $[h', h] \in Z$ and $\zeta([h', h]) \neq 1$. Then for any representation η of H given by ζ on Z:*

1. *The character of η is supported in Z*
2. *η is irreducible if and only if its degree is $d(\eta) = \sqrt{[H : Z]}$*

3. There is a unique such irreducible η

Proof. Let η be a representation given by ζ on Z. For any $h \in H - Z$, choose h' as in the statement. Then

$$\mathrm{Tr}\eta(h) = \mathrm{Tr}\eta(h'hh'^{-1}) = \mathrm{Tr}\eta([h',h]h) = \mathrm{Tr}(\zeta([h',h])\eta(h)) = \zeta([h',h])\mathrm{Tr}(\eta(h))$$

and this means $\mathrm{Tr}\eta(h) = 0$, which gives (1).

Now η is irreducible if and only if

$$\sum_{h\in H} |\mathrm{Tr}(\eta(h)|^2 = |H|$$

but we have

$$\sum_{h\in H} |\mathrm{Tr}(\eta(h))|^2 = \sum_{z\in Z} |\zeta(z)|^2 d(\eta)^2 = d(\eta)^2 \sum_{z\in Z} |\zeta(z)|^2 = d(\eta)^2|H|$$

and this proves (2).

Now let π be the representation on H induced by ζ. Then for any $z \in Z$ and f in the space of π,

$$\pi(z)(f)(h) = f(hz) = f(zh) = \zeta(z)f(h)$$

This means $\pi(z) = \zeta(z) \cdot 1$, and thus every irreducible component of π is given by ζ on Z, which gives existence. To see uniqueness, suppose we had both η and η', then

$$< \chi_\eta, \chi_{\eta'} >= |H|^{-1} \sum_{h\in H} \overline{\mathrm{Tr}(\eta(h))}\mathrm{Tr}(\eta'(h)) = |H|^{-1} d(\eta)d(\eta') \sum_{z\in Z} \overline{\zeta(z)}\zeta(z) = 1$$

and this proves (3). □

Proposition 3. *Let ζ be a non-trivial character of the center Z of $H(V)$. Then there exists a unique irreducible representation η_ζ of $H(V)$ that is given by ζ on Z. Its degree is $|V|$ and its character's support is Z.*

Proof. Since the center of $H(V)$ is $\mathbb{F}_q$, we can view ζ as a character on $\mathbb{F}_q$. Since ζ is non-trivial and the bilinear form on $V \times V^*$ is non-degenerate, for any $(x,y) \in V \times V^*$, we can find (x',y') such that $\zeta(< y, x' > + < x, y' >) \neq 1$. This means that for any $h \in H(V) - Z$, there is h' such that $\zeta([h',h]) \neq 1$ and we obviously have $[h',h]$ in the center Z. The proposition then follows as a result of the previous lemma, noting that $\sqrt{[H(V) : Z]} = \sqrt{|V \times V^*|} = |V|$. □

Given a non-trivial character ζ on $\mathbb{F}_q$, let $1 \cdot \zeta$ be the character on $V^*\mathbb{F}_q$ given by $1 \cdot \zeta(yz) = \zeta(z)$. Let π be the representation induced by $1 \cdot \zeta$ on $H(V)$.

Now we can embed $\mathbb{C}[V]$ in the standard space of π because every $h \in H(V)$ can be written uniquely as the product kx with $k \in V^*\mathbb{F}_q$, $x \in V$ (in fact, $(x, y, z) = (0, y, z) \cdot (x, 0, 0)$), and thus any $f \in \mathbb{C}[V]$ can be viewed as being in $\mathbb{C}[H(V)]$ by setting $f(h) = \zeta(h)f(x)$.

$\mathbb{C}[V]$ is invariant under π, and thus we get a representation η in the space $\mathbb{C}[V]$ by restricting π. Since we have $(x, 0, 0) \cdot (x_0, y_0, z_0) = (0, y_0, z_0 - < y_0, x + x_0 >) \cdot (x + x_0, 0, 0)$, η is given explicitly by

$$(\eta(x_0, y_0, z_0)f)(x) = \zeta(z_0)\zeta(< x + x_0, y_0 >)f(x + x_0)$$

Setting $x_0 = y_0 = 0$, we see that η is given by ζ on Z and since its degree is $\dim(\mathbb{C}[V]) = |V|$, we see that in fact $\eta = \eta_\zeta$.

Let $G(V)$ be the subgroup of $GL(V \times V^*)$ that leaves invariant the bilinear form induced on $V \times V^*$ by $H(V)$. For any $g \in GL(V)$, we can find $g^* \in GL(V^*)$ such that $< g^*y, gx >=< y, x >$ for all x, y (in fact, $g^*y = yg^{-1}$). Then we can see that $G(V) = \{(g, g^*)|g \in GL(V)\}$ and since $(gg')^* = g^*g'^*$, we have that $G(V) \cong GL(V)$. This means that a representation of $G(V)$ is also a representation of $GL(V)$. $G(V)$ acts on $H(V)$ via $g \cdot (x, y, z) \mapsto (gx, g^*y, z)$. Finally, we let $GH(V)$ be the semi-direct product of $G(V)$ and $H(V)$ and prove the main theorem of this section.

Theorem 4. *There exists a unique representation W on $G(V)$, called the Weil representation of $G(V)$, such that:*

1. *for any irreducible representation η of $H(V)$ that is non-trivial on its center Z, there is a representation ρ of $GH(V)$ in the space of η such that on $H(V)$, ρ is η and the restriction of ρ to $G(V)$ is W.*

2. *the character of W takes positive values*

Proof. Uniqueness follows from both (1) and (2).

For existence, let a character ζ on Z be given. Consider the character $1 \cdot 1 \cdot \zeta$ of $G(V)V^*\mathbb{F}_q$. Consider the representation induced by $1 \cdot 1 \cdot \zeta$ on

$GH(V)$. Similar to the method above, we can restrict this representation to the representation ρ in the space $\mathbb{C}[V]$ given by

$$(\rho(g_0, x_0, y_0, z_0)f)(x) = \zeta(z_0)\zeta(< g_0^{-1}(x + x_0), y_0 >)f(g_0^{-1}(x + x_0))$$

Restricted to $H(V)$ (i.e. $g_0 = 1$), $\rho = \eta_\zeta$, and restricted to $G(V)$ (i.e. $x_0 = y_0 = z_0 = 0$), ρ acts as $(\rho(g)f)(x) = f(g^{-1}x)$ and thus is independent of ζ. This means we can take W to be the restriction of ρ to $G(V)$.

Now let $\{e_v \in \mathbb{C}[V] | v \in V\}$, where e_v is the function that sends $v \mapsto 1$ and everything else to 0, be a basis of $\mathbb{C}[V]$. Then $(W(g)e_v)(x) = e_v(g^{-1}x) = e_{gv}(x)$, i.e. $W(g)e_v = e_{gv}$. Therefore, under this basis, $W(g)$ is a permutation of the identity matrix, and thus its trace is positive, and this proves (2). □

Corollary 5. *For the Weil representation* W*, and any* $g \in G(V)$*,* $\mathrm{Tr}W(g) = q^{N(V;g)}$*, where* $N(V; g) = \frac{1}{2} \dim \ker(g - 1)$

Proof. From the proof of the theorem, we see that the trace of $W(g)$ is equal to the number of $v \in V$ such that $e_{gv} = e_v$, i.e. it is equal to the order of the kernel of $g - 1$ as an element $GL(V)$, whose dimension is half of the kernel of $g - 1$ as an element of $GL(V \times V^*)$. And the corollary follows from the fact that this kernel is vector space over the finite field $\mathbb{F}_q$. □

3 Weil Representations of Symplectic Groups

We now turn to finite dimensional vector spaces, E, over $\mathbb{F}_q$ with q odd, equipped with a non-degenerate alternating bilinear form j (which implies that the dimension of E is even). Let $i : E \to E^*$ be the map defined as $< i(w), w' >= \frac{1}{2}j(w, w')$. We define the *Heisenberg group*, $H(E, j)$, of (E, j) to be the set $E \times \mathbb{F}_q$ equipped with the multiplication induced by viewing an element $(w, z) \in E \times \mathbb{F}_q$ as the matrix

$$(w, z) = \begin{pmatrix} 1 & i(w) & z \\ & 1 & w \\ & & 1 \end{pmatrix}$$

Explicitly, the multiplication rule is

$$(w, z) \cdot (w', z') = (w + w', z + z' + \frac{1}{2}j(w, w'))$$

As before we have $\mathbb{F}_q$ embedded in $H(E, j)$ as a subgroup, but E itself is not. The non-degeneracy of j, however, again implies that the center of $H(E, j)$ is $\mathbb{F}_q$.

We also define the group of the symplectic form j, $S(E, j)$, to be the set of all $g \in GL(E)$ such that $j(gw, gw') = j(w, w')$ for all $w, w' \in E$. $S(E, j)$ acts on $H(E, j)$ via $g \cdot (w, z) \mapsto (gw, z)$. We now let $SH(E, j)$ be the semi-direct product of these two groups and prove the main theorem of this section.

Theorem 6. *Let ζ be any non-trivial character of the center Z of $H(E, j)$, and let η_ζ be the irreducible representation of $H(E, j)$ given by ζ on Z. Then there exists a unique representation W_ζ of $S(E, j)$, called the* Weil representation of $S(E, j)$ associated to ζ, *such that*

1. *There exists a representation of $SH(E, j)$ that is given by η_ζ on $H(E, j)$ and by W_ζ on $S(E, j)$.*

2. *For any two nontrivial characters ζ and ζ', the Weil representations W_ζ and $W_{\zeta'}$ are the same if and only if ζ and ζ' are conjugate by a non-zero square of $\mathbb{F}_q$, i.e. $\zeta'(z) = \zeta(t^z)$ for some $t \in \mathbb{F}_q^\times$ and for all $z \in \mathbb{F}_q$.*

Proof. Decompose E as $E = E_+ \oplus E_-$, where E_+ and E_- are Lagrangian subspaces. Consider the subgroup of $S(E, j)$, P, defined to be those $g \in S(E, j)$ such that $g(E_+) = E_+$. Define a character χ on P by

$$s \mapsto (\det{}_{E_+} s)^{(q-1)/2}$$

Now consider the the character $\chi \cdot 1 \cdot \zeta$ of PE_+Z, a subgroup of $SH(E, j)$. This acts as

$$\chi \cdot 1 \cdot \zeta(sxz) = \chi(s)\zeta(z)$$

Now let π be the the representation of $PH(E, j)$ induced by $\chi \cdot 1 \cdot \zeta$. Using the methods of the previous section, we could realize π in the space $\mathbb{C}[E_-]$. This representation is given by ζ on Z and has degree $|E_-| = \sqrt{[H(E, j) : Z]}$. This means, by Lemma (2), that the restriction π to $H(E, j)$ is in fact the same as η_ζ. Now the restriction, π_+, of π to P is a representation that extends η_ζ, and it can be shown that since P is a parabolic subgroup of $S(E, j)$ that π_+ can be extended to a representation of $S(E, j)$ that also extends η_ζ and this representation will be W_ζ. This proves (1).

For (2), consider the automorphism of $SH(E, j)$ that maps $(g, w, z) \mapsto (g, tw, t^2 z)$, for $t \in \mathbb{F}_q^\times$. This also maps a character ζ on Z to the character $t\zeta$

on Z defined by $(t\zeta)(z) = \zeta(t^{-2}z)$, and maps $\eta_\zeta \mapsto \eta_{t\zeta}$. And this means that it maps the representation η_ζ to $\eta_{t\zeta}$. But the map is trivial on $S(E,j)$, and since it preserves (1) in the statement of the theorem, we must have that W_ζ is the same as $W_{t\zeta}$.

To show the converse, if ζ and ζ' are not conjugate by a non-zero square, they are conjugate by a non-zero non-square, and then one can explicitly show in this case that the Weil representations are distinct, and this shows (2). □

As with Corollary 5 in the previous section, one can prove the following similar proposition about the character of the Weil representations W_ζ.

Corollary 7. *For the Weil representation W_ζ, and any $s \in S(E,j)$, $|\mathrm{Tr}W_\zeta(s)| = q^{N(E;s)}$, where $N(V;g) = \frac{1}{2}\dim\ker(s-1)$*

4 Characters of Weil Representations

The Weil representation is not an irreducible representation, but its decomposition into irreducible representations is given by the following results which are stated here but not proved.

Theorem 8. *Let V, $G(V)$, and W be as in section 2, and set $n = \dim V$. Then W splits into $q-2$ irreducible representations of degree $\frac{q^n-1}{q-1}$ (corresponding to the $q-2$ nontrivial characters of the center of $G(V)$), one class, if $n > 1$, of degree $\frac{q^n-1}{q-1}$ that is trivial on the center, and twice the trivial representation.*

Theorem 9. *Let E, j, $S(E,j)$, W_ζ be as in section 3, and set $2l = \dim E$. Then each W_ζ splits into two irreducible representations, one of degree $\frac{q^l+1}{2}$ and the other of degree $\frac{q^l-1}{2}$.*

References

[1] Gérardin , Paul, “Weil Representations Associated to Finite Fields.” Journal of Algebra 46 (1977) pp. 54 - 101.