On the Doubly Transitive Permutation Representations $\mathrm{Sp}(2m, \mathbb{F}_2)$.

Peter Sin,
University of Florida
Supported by NSF grant DMS0071060

Presented at University of South Alabama, 11th November, 2004

0. Introduction

Group actions

Let G be a group acting on a set S. The action is *transitive* if S is a single orbit. The action is *doubly transitive* if any ordered pair of distinct elements of S can be sent to any other by some element of G. Equivalently, G acts doubly transitively if the stabilizer of an element of S acts transitively on the other elements.

Let R be any commutative ring. Let $R[S]$ be the free R-module with basis S. The G-action makes $R[S]$ into a module for the group algebra RG.

Lemma. *If G acts transitively on S, then $\mathrm{End}_{RG}R[S]$ is a free R-module with basis given be the orbit sums of the stabilizer of an element.*

Corollary. *If R is a field of characteristic zero and G acts double transitively, then $R[S]$ is the direct sum of the trivial module with a simple module.*

When the field has positive characteristic dividing $|G|$, the situation may be much more complicated. In fact, as we shall see, the structure of $R[S]$ can be very complicated and interesting. For example, the composition length of $R[S]$ is unbounded.

In this talk, we will explore the mod 2 permutation modules of a famous class of doubly transitive group actions, first considered in the 19th century by Steiner, Jordan and Riemann.

1. Quadratic forms over the field of two elements

- V , vector space of dimension $2n$ over $\mathbb{F}_2$ (Assume $n \geq 2$)
- $S^2(V^*)$, the vector space of all quadratic forms on V
- $\wedge^2(V)^* \cong \wedge^2(V^*)$, and the space of all alternating bilinear forms on V.

By definition, a quadratic form has an associated bilinear form

$$\theta(q)(v,u) = q(v+u) - q(v) - q(u) \tag{1}$$

and this formula defines the *polarization* homomorphism from $S^2(V^*)$ to $\wedge^2(V^*)$. The quadratic forms with zero polarization can be identified with V^* and we have a short exact sequence of $\mathrm{GL}(V)$-modules

$$0 \longrightarrow V^* \longrightarrow S^2(V^*) \xrightarrow{\theta} \wedge^2(V^*) \longrightarrow 0. \tag{2}$$

Equivalence of forms in a symplectic space

Fix a nonsingular alternating form b on V Let $\mathrm{Sp}(V)$ be the group preserving b.
Every element of $V^* = \ker\theta$ can be written as $b(-,x)^2$ for some $x \in V$. So if q is any quadratic form polarizing to b, then

$$\theta^{-1}(b) = \{q + b(-,x)^2 \mid x \in V\}. \tag{3}$$

Now the group $\mathrm{GL}(V)$ acts on $S^2(V^*)$ by

$$(gq)(v) = q(g^{-1}v)$$

Two quadratic forms in the same orbit are called *equivalent*.

If two forms q and $q' \in \theta^{-1}(b)$ are equivalent, the conjugating element of $\mathrm{GL}(V)$ must belong to $\mathrm{Sp}(V)$, so the $\mathrm{Sp}(V)$-orbits in $\theta^{-1}(b)$ are in bijection with equivalence classes of forms. The stabilizer in $\mathrm{Sp}(V)$ (or $\mathrm{GL}(V)$) of q is the orthogonal group $\mathrm{O}(V, q)$.
The map

$$V \to \theta^{-1}(b), \quad v \mapsto q + b(-, v) \tag{4}$$

is an isomorphism of $\mathrm{O}(V, q)$-sets.

By Witt's Lemma $\mathrm{O}(V, q)$ has two orbits on $V \setminus \{0\}$ consisting of isotropic and anisotropic vectors, so it has two orbits on $\theta^{-1}(b) \setminus \{q\}$.

Let $e_1, \ldots, e_n, f_1, \ldots, f_n$ be a symplectic basis for V with respect to b and let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be the dual basis for V^*. Thus,

$$b(e_i, f_j) = x_i(e_j) = y_i(f_j) = \delta_{i,j}, \quad b(e_i, e_j) = b(f_i, f_j) = 0. \tag{5}$$

The quadratic forms $q^+ = \sum_{i=1}^n x_i y_i$ and $q^- = x_1^2 + y_1^2 + \sum_{i=1}^n x_i y_i$ are inequivalent since they have Witt index n and $n - 1$ respectively. Therefore, the two orbits of $\mathrm{O}(V, q)$ on $\theta^{-1}(b) \setminus \{q\}$ are determined by the Witt index.

Let $\mathcal{Q}^+$ be the set forms of maximal index in $\theta^{-1}(b)$ and $\mathcal{Q}^-$ the set of minimal index.
We have proved:

Theorem. $\mathrm{Sp}(V)$ *acts doubly transitively on the sets* $\mathcal{Q}^+$ *and* $\mathcal{Q}^-$.

Remark. The first proof of the double transitivity of the $\mathrm{Sp}(V)$-action on the forms of maximal index appeared in Jordan's *Traité des Substitutions, p. 236*.

Remark. An easy computation shows that the isotropic vectors of q correspond in (4)to forms of the same Witt index as q.

2. The permutation modules $k[\mathcal{Q}^+]$ and $k[\mathcal{Q}^-]$

We now want to study the submodule structure of $k[\mathcal{Q}^+]$ and $k[\mathcal{Q}^-]$, where k is an algebraically closed field of characteristic 2. By this, we mean we would like to describe the simple composition factors and their multiplicities and in addition we would like to have some information about how the composition factors fit together.

Composition factors

We can get a rough idea about the composition factors as follows. The module $\theta^{-1}(\mathbb{F}_2 b)$ (see(2)) is the union of V^* and the nontrivial coset $\theta^{-1}(b) = \mathcal{Q}^+ \cup \mathcal{Q}^-$. These two cosets are isomorphic $\langle g\rangle$-sets for any element $g \in \mathrm{Sp}(V)$ of odd order. Therefore, in the Grothendieck group of $k\mathrm{Sp}(V)$-modules,

$$k[\mathcal{Q}^+] + k[\mathcal{Q}^-] = k[V^*] \cong \wedge(V_k^*),$$

where $V_k = V \otimes k$.

Thus, $k[\mathcal{Q}^+]$ and $k[\mathcal{Q}^-]$ each have roughly half of the composition factors of $\wedge(V_k^*)$. This already shows that the number of composition factors tends to ∞ as $n \to \infty$.

The exterior algebra

The exterior powers $\wedge^r(V_k^*)$ are fundamental modules and have been studied in detail by several authors (e.g. [1], [2], [4] and [6]). They are modules for the algebraic group $\mathrm{Sp}(V_k)$. It is known [4, Appendix A] that as modules for the algebraic group $\mathrm{Sp}(V_k)$, the exterior powers have filtrations by Weyl modules and also good filtrations (by duals of Weyl modules). Weyl modules are certain reductions of simple modules for the corresponding complex semisimple Lie algebra, in this case $\mathfrak{s}p(2n)$. Hence, the dimensions and characters are given by Weyl's Character Formula.

3. Structure of $k[\mathcal{Q}^{\pm}]$

Our aim is to describe the submodule structure of $k[\mathcal{Q}^{\pm}]$, taking as our model the above description of the structure of $\wedge(V^*)$. Of course we must be careful since $k[\mathcal{Q}^{\pm}]$ are not modules for the algebraic group $\mathrm{Sp}(V_k)$.
Here is the plan:

- Cut $\wedge(V_k^*)$ into two pieces.
- Introduce coordinates so that we can have a notion of "polynomial degree" in order to define filtrations.
- Prove that the graded modules of $k[\mathcal{Q}^{\pm}]$ with respect to the above fitrations are isomorphic to the two pieces into which we have cut $\wedge(V_k^*)$
- Prove that the graded pieces have an action of the algebraic group $\mathrm{Sp}(V_k)$ and have *either* good or Weyl filtrations.

The exterior algebra and the spin module

We will describe here how we cut the exterior algebra in two. Consider b as an element of degree two in $\wedge(V_k^*)$. In characteristic two we have $b^2 = 0$. So the map δ given by multiplication by b makes $\wedge(V_k^*)$ into a complex. It is best for us to keep the standard grading on $\wedge(V_k^*)$ so δ has degree two. Obviously, the complex decomposes into a direct sum $\wedge(V_k^*) = \wedge(V_k^*)^{even} \bigoplus \wedge(V_k^*)^{odd}$. The symplectic group $\mathrm{Sp}(V_k)$ which preserves b acts on this complex, hence also on its homology groups.

Proposition. $H^i(\wedge(V_k^*), \delta) = 0$ *unless* $i = n$ *, in which case it affords an irreducible representation of* $\mathrm{Sp}(V_k)$ *of dimension* 2^n*.*

3.1. Filtrations and graded modules

Next, certain filtrations on the modules $k[\mathcal{Q}^{\pm}]$ come from the fact that $\mathcal{Q}^{+}$ and $\mathcal{Q}^{-}$ are the $\mathbb{F}_2$-rational points of quadrics in some affine space. We consider the associated graded modules A^{+} and A^{-}.

Theorem. *We have isomorphisms of graded* $k\mathrm{Sp}(V)$*-modules* $\mathrm{gr}(A^{+}) \cong \mathrm{Coker}\delta$ *and* $\mathrm{gr}(A^{-}) \cong \mathrm{Im}\delta$

Next we study the image and kernel of δ as modules for the algebraic group $\mathrm{Sp}(V_k)$.

Proposition. *(i)* $\wedge^r(V_k^*)/\mathrm{Im}\delta \cap \wedge^r(V_k^*)$ *has a good filtration for* $0 \leq r \leq n$ *and a Weyl filtration for* $n+1 \leq r \leq 2n$.

(ii) $\wedge^r(V_k^*)/\mathrm{Ker}\delta \cap \wedge^r(V_k^*)$ *has a good filtration for* $0 \leq r \leq n-1$ *and a Weyl filtration for* $n \leq r \leq 2n$.

Proof. Use the general fact [7, II.4.17] that in a short exact sequence

$$0 \to W' \to W \to W'' \to 0 \tag{6}$$

of rational modules for a reductive algebraic group, if W' and W have good filtrations then so does W'', together with the dual statement that if W'' and W have Weyl filtrations then so does W'. Then use Proposition and induction. $\square$

Back
Full Screen
Close
Quit

4. Module structure for orthogonal groups

Lemma. *Assume $n \geq 3$. Let $L(n)$ be the last fundamental module. Then $H^1(\mathrm{Sp}(V_k), L(n)) = 0$.*

Proposition. *Each Weyl module $V(i)$ ($i = 1,\ldots,n$) of the algebraic group $\mathrm{Sp}(V_k)$ satisfies the following properties. The restrictions of its composition factors to the subgroup $\mathrm{O}(V, f)$ remain simple and distinct as modules for this subgroup. Furthermore, the lattice of submodules remains the same. That is, the groups $\mathrm{Sp}(V_k)$, $\mathrm{O}(V, f)$ leave invariant the same subspaces of each $V(i)$.*

5. Examples

$\wedge(V)$:

$$1 \oplus 6 \oplus (1 \oplus 14) \oplus \begin{array}{c} 6 \\ | \\ 8 \\ | \\ 6 \end{array} \oplus (14 \oplus 1) \oplus 6 \oplus 1$$

Cokerδ :

$$1 \oplus 6 \oplus 14 \oplus \begin{array}{c} 6 \\ \Big| \\ 8 \end{array} \oplus 1$$

Figure 1:

$k[\mathcal{Q}^+]$:

$$\begin{array}{ccc} & 1 & \\ & | & \\ & 6 & \\ / & & \backslash \\ 8 & & 14 \\ \backslash & & / \\ & 6 & \\ & | & \\ & 1 & \end{array}$$

$k[\mathcal{Q}^-]$:

$$\begin{array}{c} 1 \\ | \\ 6 \\ | \\ 14 \\ | \\ 6 \\ | \\ 1 \end{array}$$

Figure 2: Submodule structures for $\mathrm{Sp}(6,2)$.

Introduction
Quadratic forms . . .
The permutation . . .
Structure of $k[\mathcal{Q}^{\pm}]$
Module structure . . .
Examples
Theta . . .
Back
Full Screen
Close
Quit

$n = 4:$

$$1 \oplus 8 \oplus \begin{array}{c} 1 \\ | \\ 26 \end{array} \oplus 48 \oplus \begin{array}{ccc} & 26 & \\ / & & \backslash \\ 1 & & 16 \end{array} \oplus 8 \oplus 1$$

$n = 5:$

$$1 \oplus 10 \oplus 44 \oplus \begin{array}{c} 10 \\ | \\ 100 \end{array} \oplus \begin{array}{c} 1 \\ | \\ 164 \\ | \\ 1 \end{array} \oplus \begin{array}{ccc} & 100 & \\ / & & \backslash \\ 10 & & 32 \end{array} \oplus 44 \oplus 10 \oplus 1$$

Figure 3: Submodule structure of $\mathrm{gr}(k[\mathcal{Q}^+])$ for $n = 4,\ 5$.

6. Theta Characteristics of curves

Let C be a smooth projective complex algebraic curve.
A *divisor* on C is a finite integral combination $\sum_p n_p p$ of points of C. The *degree* of this divisor is $\sum_p n_p$. If f is a rational function its divisor is defined to be

$$(f) = (\text{sum of zeroes}) - (\text{sum of poles}),$$

everything counted with multiplicities. The degree of (f) is zero for every rational function. Two divisors are *linearly equivalent* if they differ by the divisor of a rational function. The linear equivalence classes form a group $\mathrm{Cl}(C)$. This group is isomorphic to the group of isomorphism classes of line bundles on C.
The *Jacobian*, $J(C)$ may be identified with $\mathrm{Cl}^0(C)$, the subgroup of divisor classes of degree zero. It is an abelian variety of (complex) dimension g, the genus of C.

Some important divisors include:

- the trivial divisor, of degree zero, corresponding to the structure sheaf $\mathcal{O}$
- the canonical divisor K (which by Riemann-Roch has degree $2g-2$). This corresponds to the sheaf of regular differentials (aka holomorphic or abelian differentials). We have $h^0(C,K)=g$.
- J_2, the group of points of order 2 in $J(C)$, i.e line bundles L such that $L \otimes L = \mathcal{O}$. We have $|J_2| = 2^{2g}$.
- the *theta characteristics*, divisors L such that $2L = K$. Note that J_2 acts regularly on the set of these, so there are also 2^{2g} of them. L is called even or odd according to the parity of $h^0(C,L)$.

On J_2 we have the *Weil paring*, a symplectic form over $\mathbb{F}_2$. For each theta characteristic L define the map $q_L : J_2 \longrightarrow \mathbb{F}_2$ by

$$q_L(\eta) = h^0(C, L \otimes \eta) - h^0(C, L).$$

The *Riemann-Mumford relation* says that q_L is a quadratic form with the Weil pairing as its associated bilinear form. The group $\mathrm{Sp}(2g, 2)$ acts as the "global monodromy". Thus, the sets $\mathcal{Q}^{\pm}$ turn out to be the same as the sets of odd and even theta characteristics.

Example. [12] Let C be a non-hyperelliptic curve of genus g=3. Then C is embedded (using a basis of sections of the canonical sheaf) a quartic in $\mathbb{P}^2$, because 2g-2=4 and g=3=2+1. The (hyperplanes=) lines of $\mathbb{P}^2 = \mathbb{P}H^0(C, K)$ are in bijection with the regular differentials on C. It is a famous classical fact that there are 28 bitangents, lines which are tangent at two points. If ℓ is tangent at x and y, and corresponds to the differential ϕ, then $(\phi) = 2x + 2y$. so $x + y$ is a theta characteristic. These 28 are the odd ones.

References

[1] A. M. Adamovich, Analogues of spaces of primitive forms over a field of positive characteristic, *Moscow Univ. Math. Bull.* **39** No. 1 (1984) 53–56.

[2] A. M. Adamovich, The submodule structure of Weyl modules for symplectic groups with fundamental highest weights, *Moscow Univ. Math. Bull.* **41** No 2 (1986) 6–9.

[3] J. Dieudonne, "La Géométrie des groupes classiques" (3rd ed.) Springer Verlag, Berlin, 1971.

[4] S. Donkin, On tilting modules and invariants for Algebraic Groups, in "Finite Dimensional Algebras and related topics" (V.Dlab and L.L.Scott, Eds.) Kluwer Academic Publishers, (1994) 59–77.

[5] M. Dowd, P. Sin, Representations of algebraic groups in characteristic 2, *Comm. Algebra* **24** (1996) 2597–2696.

[6] R. Gow, Construction of $p-1$ irreducible modules with fundamental highest weight for the symplectic group in characteristic p, *J. London Math. Soc.* **58** (1998) 619–632.

[7] J. C. Jantzen, "Representations of Algebraic Groups" Academic Press, London, 1987.

[8] C. Jordan, "Traité des Substitutions et des équations algébriques" Gauthier-Villars, Paris, 1870.

[9] I. Kaplansky, "Linear Algebra and Geometry" Allyn and Bacon, Boston, 1969.

[10] F. J. MacWilliams, N. J. A. Sloane, "The theory of error-correcting codes" I, II, North-Holland Mathematical Library, Vol. 16. North-Holland, Amsterdam (1977).

[11] B. Mortimer, The modular permutation representations of the known doubly transitive groups, *Proc. London Math.Soc.* **41** (1980) 1–20

[12] D. Mumford, Curves and their Jacobians, University of Michigan Press, Ann Arbor (1975).