Canad. Math. Bull. Vol. **42** (1), 1999 pp. 125–128

Modular Vector Invariants of Cyclic Permutation Representations

Larry Smith

Abstract. Vector invariants of finite groups (see the introduction for an explanation of the terminology) have often been used to illustrate the difficulties of invariant theory in the modular case: see, *e.g.*, [1], [2], [4], [7], [11] and [12]. It is therefore all the more surprising that the *unpleasant* properties of these invariants may be derived from two unexpected, and remarkable, *nice* properties: namely for vector permutation invariants of the cyclic group Z/p of prime order in characteristic p the image of the transfer homomorphism $\mathrm{Tr}^{\mathrm{Z}/p}\colon \mathrm{F}[V] \to \mathrm{F}[V]^{\mathrm{Z}/p}$ is a prime ideal, and the quotient algebra $\mathrm{F}[V]^{\mathrm{Z}/p}/\operatorname{Im}(\mathrm{Tr}^{\mathrm{Z}/p})$ is a polynomial algebra on the top Chern classes of the action.

To begin we fix some notations and terminology, beginning with the simplest case. Let F be a field of characteristic 2 and $\tau\colon \mathrm{Z}/2 \hookrightarrow \mathrm{GL}(2,\mathrm{F})$ the tautological representation of $\mathrm{Z}/2$ over F, *i.e.*, the nontrivial element of $\tau(\mathrm{Z}/2)$ is the permutation matrix $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$. For a positive integer m let $\tau_m\colon \mathrm{Z}/2 \hookrightarrow \mathrm{GL}(2m,\mathrm{F})$ be the m-fold direct sum $\underbrace{\tau \oplus \cdots \oplus \tau}_{m}$. We are interested in the ring $\mathrm{F}[V]^{\mathrm{Z}/2}$ of $\mathrm{Z}/2$-invariant[1] polynomial functions on the vector space $V = \mathrm{F}^{2m}$.

The rings of vector invariants $\mathrm{F}[V]^{\mathrm{Z}/2}$ have been studied by many authors, and the difficulty of computation, and unpleasant properties, of these rings used to illustrate the complexity of invariant theory in the modular case: see, *e.g.*, [1], [2], [4], [7], [11] and [12] (particularly Section 4). For example, if

$$\mathrm{Tr}^{\mathrm{Z}/2}\colon \mathrm{F}[V] \to \mathrm{F}[V]^{\mathrm{Z}/2}$$

is the transfer homomorphism, then it is known [5], [3], and [12, Section 4, Example 1], that $\mathrm{Tr}^{\mathrm{Z}/2}$ is not surjective (as it would be if F had odd characteristic or characteristic 0), and that the Krull dimension of the quotient ring[2] is at least m. For $m > 3$ these rings are not Cohen-Macaulay nor are they generated by linear and quadratic forms, again as they would be if the characteristic of the F were not 2. There are analagous results for permutation representations of cyclic groups of prime order p in characteristic p.

The following theorems are therefore all the more surprising, since they show that the *unpleasant* properties of these rings of invariants are consequences of two unexpected *pleasant* properties that somehow have gone unnoticed: at least I know of no reference for them,

[1]For a general reference on invariant theory we refer to [11], and for a survey of some recent developments see [12].

[2]In general, see, *e.g.*, [11, Section 2.4], if $\rho\colon G \hookrightarrow \mathrm{GL}(n,\mathrm{K})$ is a representation of a finite group G over the field K, then the transfer homomorphism $\mathrm{Tr}^G\colon \mathrm{K}[V] \to \mathrm{K}[V]^G$ is a $\mathrm{K}[V]^G$-module homomorphism, and hence $\operatorname{Im}(\mathrm{Tr}^G) \subseteq \mathrm{K}[V]^G$ is an ideal.

Received by the editors June 11, 1997.
AMS subject classification: 13A50.
Keywords: polynomial invariants of finite groups.

published or otherwise. This manuscript arose in the course of computing some examples to illustrate the spectral sequence introduced in [13] for the study of the homological codimension of modular rings of invariants. However, the results discovered are so surprising, pretty, and simple that it seems useful to write them up independently of the technical manuscript [13].

I am grateful to M. D. Neusel for a number of useful conversations and tutorials, as well as access to [7], and to the members of the Laboratoire de Mathématiques Émil Picard de l'Université Paul Sabatier de Toulouse for their hospitality.

Theorem 1 *Let* F *be a field of characteristic* 2 *and* $\tau_m \colon \mathrm{Z}/2 \hookrightarrow \mathrm{GL}(2m, \mathrm{F})$ *the representation of* $\mathrm{Z}/2$ *implemented by the permutation matrix*

$$\begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{bmatrix} \in \mathrm{GL}(2m, \mathrm{F}).$$

Let $x_1, \dots, x_m, y_1, \dots, y_m$ *be the standard basis for the dual vector space* V^* *of* $V = \mathrm{F}^{2m}$. *Then*

(i) $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$ *is a prime ideal of height m in* $\mathrm{F}[V]^{\mathrm{Z}/2}$, *and*
(ii) $\mathrm{F}[V]^{\mathrm{Z}/2}/\,\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2}) \cong \mathrm{F}[q_1, \dots, q_m]$ *is a polynomial algebra on the quadratic forms* $q_i = x_i y_i$, $i = 1, \dots, m$.

Proof We begin by describing $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2}) \subset \mathrm{F}[V]^{\mathrm{Z}/2}$. To this end introduce the $\mathrm{Z}/2$-invariant linear forms

$$\ell_i = x_i + y_i, \quad i = 1, \dots, m.$$

The $2m$ $\mathrm{Z}/2$-invariant polynomials $\ell_1, \dots, \ell_m, q_1, \dots, q_m$ are a system of parameters for $\mathrm{F}[V]^{\mathrm{Z}/2}$ and a regular sequence[3] in $\mathrm{F}[V]$. Hence $\mathrm{F}[V]$ is a free module over the polynomial subalgebra $\mathrm{F}[\ell_1, \dots, \ell_m, q_1, \dots, q_m] \subset \mathrm{F}[V]$. A basis for $\mathrm{F}[V]$ as $\mathrm{F}[\ell_1, \dots, \ell_m, q_1, \dots, q_m]$-module consists of the monomials[4] $\{x^E \mid E = (e_1, \dots, e_m), e_i = 0 \text{ or } 1 \text{ for } i = 1, \dots, m\}$, *i.e.*, all the monomial divisors of $x_1 \cdot x_2 \cdots x_m$. Therefore $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$ is the ideal in $\mathrm{F}[V]^{\mathrm{Z}/2}$ generated by the binomials

$$\mathrm{Tr}^{\mathrm{Z}/2}(x^E) = x^E + y^E : E = (e_1, \dots, e_m), \quad e_i = 0 \text{ or } 1 \text{ for } i = 1, \dots, m.$$

Since τ_m is a permutation representation, $\mathrm{F}[V]^{\mathrm{Z}/2}$ has an F-basis consisting of orbit sums of monomials [11, Lemma 4.2.1]. If $x^A y^B \in \mathrm{F}[V]$ is a monomial, then the orbit sum of its $\mathrm{Z}/2$-orbit is

$$\mathrm{S}(x^A y^B) = \begin{cases} x^A y^B + x^B y^A & \text{if } A \neq B \\ x^C y^C & \text{if } A = C = B, \end{cases}$$

[3] If $m \geq 3$ they are *not* a regular sequence in $\mathrm{F}[V]^{\mathrm{Z}/2}$: see [12, Section 4, Example 3], or in slightly different notation [11, Section 6.7, Example 2].

[4] If $E = (e_1, \dots, e_m)$ is an m tuple of nonnegative integers we write x^E for the monomial $x_1^{e_1} \cdots x_m^{e_m}$.

so there are two types of orbit sums: orbit sums of length 2

$$x^A y^B + x^B y^A, \quad A \neq B$$

and orbit sums of length 1

$$x^C y^C.$$

Let $S \subset \mathrm{F}[V]^{\mathrm{Z}/2}$ be the subalgebra generated by the quadratic forms $q_1, \ldots, q_m$. The elements of S are precisely the F-linear combinations of the orbit sums of length 1. On the otherhand $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$ consists of the F-linear combinations of the orbit sums of length 2. Hence

$$S \cap \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2}) = \{0\}$$

and therefore the map

$$\pi \colon S \hookrightarrow \mathrm{F}[V]^{\mathrm{Z}/2} \to \mathrm{F}[V]^{\mathrm{Z}/2} / \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$$

is monic. However, τ_m being a direct sum of copies of the regular representation of $\mathrm{Z}/2$ implies by an essential result due to M. D. Neusel, [7, Lemma 3.1], (Lemma 4.1 in [8]) that $\mathrm{F}[V]^{\mathrm{Z}/2}$ is generated as an algebra by $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$ and top orbit Chern classes. The orbits of $\mathrm{Z}/2$ acting on $\{x_1, \ldots, x_m, y_1, \ldots, y_m\}$ are $\{x_i, y_i\}$ for $i = 1, \ldots, m$, and the corresponding top orbit Chern classes are the quadratic forms $q_1, \ldots, q_m$, so π is also epic. Therefore π induces an isomorphism

$$\mathrm{F}[q_1, \ldots, q_m] \to \mathrm{F}[V]^{\mathrm{Z}/2} / \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$$

which proves (ii).

By definititon $\ker(\pi) = \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$. The quotient ring $\mathrm{F}[V]^{\mathrm{Z}/2} / \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2})$ being a polynomial algebra over a field is an integral domain and hence $\ker(\pi)$ must be a prime ideal. Since $\mathrm{F}[q_1, \ldots, q_m]$ has Krull dimension m and $\mathrm{F}[V]^{\mathrm{Z}/2}$ has Krull dimension $2m$ it follows that the prime ideal $\ker(\pi) = \mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/2}) \subset \mathrm{F}[V]^{\mathrm{Z}/2}$ must have height m, proving (i). ■

This result is used in [13] to show that $\mathrm{hom} - \mathrm{codim}(\mathrm{F}[V]^{\mathrm{Z}/2}) = \min\{2m, m+2\}$.

There is an analagous result for the m-fold regular representation of Z/p over a field F of characteristic p when p is an odd prime. The proof, apart from the need to encumber the notations with indices, is the same as for the case $p = 2$. The key points are:

(i) The orbit of a monomial has either 1 or p elements.
(ii) Orbit sums of monomials are an F-basis for the ring of invariants.
(iii) The orbit sums of monomials with orbit size p are an F-basis for $\mathrm{Im}(\mathrm{Tr}^{\mathrm{Z}/p})$.

The theorem may be formulated as follows.

Theorem 2 *Let $p \in \mathrm{N}$ be a prime integer,* F *be a field of characteristic p and $\tau_m \colon \mathrm{Z}/p \hookrightarrow \mathrm{GL}(mp, \mathrm{F})$ the m-fold direct sum of the regular representation of Z/p over* F. *Then*

https://doi.org/10.4153/CMB-1999-014-5 Published online by Cambridge University Press

(i) $\operatorname{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ *is a prime ideal of height*[5] $m(p-1)$ *in* $\mathbb{F}[V]^{\mathbb{Z}/p}$*, and*
(ii) $\mathbb{F}[V]^{\mathbb{Z}/p} / \operatorname{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \cong \mathbb{F}[c_p(X_1), \ldots, c_p(X_m)]$ *is a polynomial algebra on the top orbit Chern classes* $c_p(X_1), \ldots, c_p(X_m)$ *of the* m *orbits* $X_1, \ldots, X_m$ *of* $\mathbb{Z}/p$ *on the dual standard basis for* V^**.* ■

The results presented here can be, and have been, generalized to other permutation representations by M. D. Neusel [8], and R. J. Shank and D. L. Wehlau [10].

References

[1] M.-J. Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p*. C. R. Acad. Sci. Paris Sér. A **264**(1967), 653–656.
[2] G. Ellingsrud and T. Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*. Compositio Math. **41**(1980), 233–244.
[3] M. Feshbach, *p-Subgroups of Compact Lie Groups and Torsion of Infinite Height in $H^*(BG; \mathbb{F}_p)$*. Michigan Math. J. **29**(1982), 299–306.
[4] R. M. Fossum and P. A. Griffith, *Complete Local Factorial Rings which are not Cohen-Macaulay in Characteristic p*. Ann. Sci. École Norm. Sup. Sér. 4 **8**(1975), 189–200.
[5] K. Kuhnigk, *Transfer in Invariantenringen*. Diplomarbeit, Univ. Göttingen, to appear.
[6] M. D. Neusel, *Invariants of some Abelian p-Groups in Characteristic p*. Proc. Amer. Math. Soc., to appear.
[7] ———, *Mme. Bertin's* $\mathbb{Z}/4$ *Revisited*. Preprint Number 1, Uni. Magdeburg, 1997.
[8] ———, *The Transfer in the Invariant Theory of Modular Permutation Representations (Mme. Bertin's* $\mathbb{Z}/4$ *Revisited, revised version)*. Preprint, AG-Invariantentheorie (Friedland, Germany), 1997.
[9] D. Richman, *Vector Invariants of Finite Groups in Characteristic p*. Adv. Math **81**(1990), 30–65.
[10] R. J. Shank and D. L. Wehlau, *The Transfer in Modular Invariant Theory*. Preprint.
[11] L. Smith, *Polynomial Invariants of Finite Groups*. A. K. Peters, Waltham, MA (second corrected printing), 1997.
[12] ———, *Polynomial Invariants of Finite Groups, A Survey of Recent Developments*. Bull. Amer. Math. Soc. **34**(1997), 211–250.
[13] ———, *Invariant Theory and the Koszul Complex*. Preprint, AG-Invariantentheorie, 1997, to appear in J. Math. Kyoto Univ.

[5] $m(p-1) = \operatorname{codim}_{\mathbb{F}}(V^{\mathbb{Z}/p} \subset V)$.