INVARIANTS OF THE DIAGONAL C_p-ACTION ON V_3

H.E.A. CAMPBELL, B. FODDEN, AND DAVID L. WEHLAU

ABSTRACT. Let C_p denote the cyclic group of order p where $p \geq 3$ is prime. We denote by V_3 the indecomposable three dimensional representation of C_p over a field $\mathbf{F}$ of characteristic p. We compute a set of generators, in fact a SAGBI basis, for the ring of invariants $\mathbf{F}[V_3 \oplus V_3]^{C_p}$. Our main result confirms the conjecture of SHANK[15], for this example, that all modular rings of invariants of C_p are generated by rational invariants, norms and transfers.

1. INTRODUCTION

Let C_m denote the cyclic group of order m. Let $\mathbf{F}$ be a field of characteristic $p \geq 3$.

Let $\rho : C_p \to \mathrm{GL}(W)$ be a representation of C_p defined over $\mathbf{F}$. The action of C_p on W induces an action on W^* which extends naturally to an action by algebra automorphisms on $\mathbf{F}[W]$, the symmetric algebra of W^*. Specifically, for $g \in C_p$, $f \in \mathbf{F}[W]$ and $v \in W$, $(g \cdot f)(v) = f(g^{-1} \cdot v)$. The ring of invariants of C_p is the subring of $\mathbf{F}[W]$ given by

$$\mathbf{F}[W]^{C_p} := \{f \in S \mid g \cdot f = f \text{ for all } g \in C_p\}.$$

For an introduction to the invariant theory of finite groups see BENSON[2] or SMITH[18].

Suppose $\rho_n : C_p \to \mathrm{GL}(V_n)$ is an n dimensional indecomposable representation of C_p. Choose a basis for V_n such that the matrix of $\rho_n(\sigma)$ is in Jordan normal form. Since ρ_n is indecomposable, $\rho_n(\sigma)$ consists of a single Jordan block. Since $\rho_n(\sigma)$ has order p, the eigenvalues of $\rho_n(\sigma)$ are p^{th} roots of unity and thus must be 1 since 1 is the only p^{th} root of unity in $\mathbf{F}$. Therefore

$$\rho_n(\sigma) = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Date: January 20, 2005.

1991 *Mathematics Subject Classification.* 13A50.

Research partially supported by grants from ARP and NSERC.

It is easy to verify that this matrix has order p if and only if $n \leq p$. Since ρ_n is a representation of C_p we must therefore have $n \leq p$. Furthermore the above discussion shows that V_n yields the unique indecomposable representation of C_p for each $1 \leq n \leq p$.

Consider a finite dimensional representation $\rho : \mathbf{C}_p \to \mathrm{GL}(W)$ of C_p. We are interested in the ring of invariants $\mathbf{F}[W]^{C_p}$. Since $\mathbf{F}[V_1 \oplus W]^{C_p} \cong \mathbf{F}[V_1] \otimes_{\mathbf{F}} \mathbf{F}[W]^{C_p}$, we will suppose that W does not contain V_1 as a summand. Up until now, the only such representations of C_p for which corresponding rings of invariants are known (for all p) are precisely the representations $mV_2 = \underbrace{V_2 \oplus V_2 \cdots \oplus V_2}_{m \text{ copies}}$ for all $m \in \mathbf{N}$, V_3, V_4, V_5 and $V_2 \oplus V_3$. In 1913, L. Dickson[7] described the two rings of invariants $\mathbf{F}[V_2]^{C_p}$ and $\mathbf{F}[V_3]^{C_p}$. In 1990, Richman[12] conjectured that a certain set of invariants were generators for $\mathbf{F}[m\,V_2]^{C_p}$ where $m \in \mathbf{N}$. In 1997, Campbell and Hughes[4] proved this conjecture for all p and all $m \in \mathbf{N}$. In 1998, Shank[14] gave generating sets for the both the rings of invariants $\mathbf{F}[V_4]^{C_p}$ and $\mathbf{F}[V_5]^{C_p}$. In 2002, Shank and Wehlau[16] gave a list of generators for $\mathbf{F}[V_3 \oplus V_2]^{C_p}$. Here we will give generators for $\mathbf{F}[V_3 \oplus V_3]^{C_p}$.

Consider then the 6 dimensional representation of C_p given by

$$\rho = \rho_3 \oplus \rho_3 : C_p \to \mathrm{GL}(V)$$

where $V = V_3 \oplus V_3$. Let $\{x_1, y_1, z_1, x_2, y_2, z_2\}$ be a basis of V^*. We choose this basis so that the representation of σ on V^* is in Jordan normal form, i.e., $\sigma(x_i) = x_i$, $\sigma(y_i) = y_i + x_i$ and $\sigma(z_i) = z_i + y_i$ for $i = 1, 2$. This action of C_p on V^* extends naturally to an action by algebra automorphisms on the symmetric algebra of V^*, $S = \mathbf{F}[V_3 \oplus V_3] = \mathbf{F}[x_1, y_1, z_1, x_2, y_2, z_2]$.

An important set of invariants are the so-called *rational invariants*. Intuitively, these are invariants which are "independent" of the prime, p. More precisely, if we view C_p as a quotient of $\mathbf{Z}$ and consider the matrix of σ as an element of $\mathrm{GL}(6, \mathbf{Z})$ then it generates an infinite cyclic group, that is to say, a copy of $\mathbf{Z}$. Reduction modulo p gives a map from $\mathbf{Z}[x_1, y_1, z_1, x_2, y_2, z_2]^{\mathbf{Z}}$ to $\mathbf{Z}/p\mathbf{Z}[x_1, y_1, z_1, x_2, y_2, z_2]^{C_p}$. Elements in the image of this map are called *rational invariants*. Applying the functor $\cdot \otimes_{\mathbf{Z}} \mathbf{C}$ gives a map from $\mathbf{Z}[x_1, y_1, z_1, x_2, y_2, z_2]^{\mathbf{Z}}$ to $\mathbf{C}[x_1, y_1, z_1, x_2, y_2, z_2]^{\mathbf{Z}}$. This latter ring is an example of an invariant ring considered by classical invariant theorists in the later half of the 1900's. Shank[15] contains a discussion of this point and rational invariants in general. Furthermore, [15] includes a discussion of the difficulties involved in trying to compute $\mathbf{F}[V_6]^{C_p}$.

In addition to rational invariants we consider two other types of invariants. Firstly, we can construct invariants using the *transfer* (also

called the *trace*) *homomorphism* which is defined by

$$\begin{array}{rccc} \mathrm{Tr}: & \mathbf{F}[V] & \longrightarrow & \mathbf{F}[V]^{C_p} \\ & f & \longmapsto & \displaystyle\sum_{g\in C_p} g\cdot f \end{array}$$

Secondly we may construct *norms* as follows. If $x \in V^*$ then the *norm of* x is the invariant

$$\mathbf{N}(x) = \prod_{g\in C_p} g(x) \ .$$

In [15], Shank conjectured that for any representation W of C_p, the ring of invariants, $\mathbf{F}[W]^{C_p}$, is generated by a combination of rational invariants, norms of linear forms and transfers. Our results here conform this conjecture for the representation $W = V_3 \oplus V_3$.

Note, that for $p = 2$ the matrix $\rho(\sigma) \in \mathrm{GL}(V_3 \oplus V_3)$ has order 4 and thus yields a representation of C_4. We do not consider the case $p = 2$ here although it is a relatively simple matter, using a computer algebra system, to compute the ring of invariants, $\mathbf{F}[V_3 \oplus V_3]^{C_4}$, when $\mathbf{F}$ has characteristic 2. This ring has a minimal system of eighteen generators of degrees 1, 1, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 6.

A SAGBI basis for a subalgebra of S is the analog of a Gröbner basis for an ideal of S and as such is a generating set which is particularly useful for computations. SAGBI bases were introduced independently by Robbiano and Sweedler [13] and Kapur and Madlener [11]. In general the ring of invariants of a finite group may fail to have a finite SAGBI basis (see Göbel[8, Lemma 2.1], Göbel[9] or Sturmfels[19, Example 11.2]). However it was shown by Shank and Wehlau in [17, Corollary 3.3] that the ring of invariants of a p-group in characteristic p always has a finite SAGBI basis.

The computations by Shank of $\mathbf{F}[V_4]^{C_p}$ and $\mathbf{F}[V_5]^{C_p}$ and by Shank and Wehlau of $\mathbf{F}[V_3 \oplus V_2]^{C_p}$ exploited SAGBI bases. We will extend the method used there and compute a SAGBI basis for $\mathbf{F}[V_3 \oplus V_3]^{C_p}$.

For reasons of brevity and clarity a number of details of some of the proofs and of some of the computations are omitted here. Most readers will not gain any further insights by being exposed to these details but the interested reader may find these details online in [20].

2. Preliminaries

We use the convention that a monomial is a product of variables (a power product) and a term is a monomial multiplied by a scalar coefficient. We refer the reader to Cox, Little and O'Shea [6, Chapter 2] for a detailed discussion of monomial orders. Here we will use the graded reverse lexicographic monomial order on $S = \mathbf{F}[V] = \mathbf{F}[x_1, y_1, z_1, x_2, y_2, z_2]$ with $x_1 < y_1 < z_1 < x_2 < y_2 < z_2$. For $f \in S$, we denote by $\mathrm{LT}(f)$ the leading term of f and $\mathrm{LM}(f)$ the leading monomial of f. For example $\mathrm{LT}(2x_1z_1 + 3y_1^2) = 3y_1^2$ and $\mathrm{LM}(2x_1z_1 + 3y_1^2) = y_1^2$.

For $w = (a_1, b_1, c_1, a_2, b_2, c_2) \in \mathbf{N}^6$ we denote by $\mathbf{x}^w$ the monomial $x_1^{a_1} y_1^{b_1} z_1^{c_1} x_2^{a_2} y_2^{b_2} z_2^{c_2}$. Given a non-empty finite subset $\{w_1, w_2, \ldots, w_m\} \subset \mathbf{N}^6$ we define $\mathrm{LCM}(\{w_1, w_2, \ldots, w_m\})$ by requiring that the following equation hold:

$$\mathrm{LCM}\{\mathbf{x}^{w_1}, \mathbf{x}^{w_2}, \ldots, \mathbf{x}^{w_m}\} = \mathbf{x}^{\mathrm{LCM}(w_1, w_2, \ldots, w_m)} .$$

Thus for example, $\mathrm{LCM}(\{(2,2,0,1,2,0), (1,7,1,2,1,0), (1,3,3,5,1,0)\} = (2,7,3,5,2,0)$. For $w = (a_1, b_1, c_1, a_2, b_2, c_2) \in \mathbf{N}^6$ we define $\deg(w) := \deg(\mathbf{x}^w) = a_1 + b_1 + \cdots + c_2$.

If Q is a graded subspace of S, we denote by $\mathrm{LT}(Q)$, the subspace spanned by the leading monomials of elements of Q:

$$\mathrm{LT}(Q) := \mathrm{span}_{\mathbf{F}}\{\mathrm{LM}(f) \mid f \in Q\} .$$

If Q is also an algebra then so is $\mathrm{LT}(Q)$, called the *lead term algebra* of Q. Notice that the lead term algebra depends on the monomial order chosen as well the choice of linear variables which determine what is a monomial.

If Q is a graded subalgebra and B is a subset of Q such that the algebra generated by $\{\mathrm{LM}(f) \mid f \in B\}$ equals $\mathrm{LT}(Q)$, then B is called a *SAGBI basis* for Q.

For a graded $\mathbf{F}$-vector space, $Q = \oplus_{i=0}^{\infty} Q_i$, we denote by $\mathcal{H}(Q, \lambda)$ the Hilbert series of Q:

$$\mathcal{H}(Q, \lambda) := \sum_{i=0}^{\infty} \dim_{\mathbf{F}} Q_i \lambda^i .$$

Given two Hilbert series $H = \sum_{i=0}^{\infty} d_i \lambda^i$ and $H' = \sum_{i=0}^{\infty} d_i' \lambda^i$ we write $H \leq H'$ to indicate that $d_i \leq d_i'$ for all $i = 0, 1, \ldots$.

One of the most important properties of lead term algebras is that $\mathcal{H}(Q, \lambda) = \mathcal{H}(\mathrm{LT}(Q), \lambda)$. In particular, this property shows that a SAGBI basis for Q is a generating set for Q.

3. The Method in General

We describe a set of invariants which we will show is a SAGBI basis for $\mathbf{F}[V_3 \oplus V_3]^{C_p}$. The method used to prove that this set is indeed a SAGBI basis is based upon the method introduced by Shank in [14] and also used by Shank and Wehlau in Section 5 of [16].

We will find a finite set $B \subset S^G$ of invariants and consider the following two rings:

$$\begin{aligned} T &:= \text{the algebra generated by } B \\ R &:= \text{the algebra generated by } \{\mathrm{LM}(f) : f \in B\} . \end{aligned}$$

By definition, B is a SAGBI basis for T if $R = \mathrm{LT}(T)$. Since $R \subseteq \mathrm{LT}(T)$ and $T \subseteq S^G$, $\mathcal{H}(R, \lambda) \leq \mathcal{H}(\mathrm{LT}(T), \lambda) = \mathcal{H}(T, \lambda) \leq \mathcal{H}(S^G, \lambda)$ and thus B is a SAGBI basis of S^G if and only if $\mathcal{H}(R, \lambda) = \mathcal{H}(S^G, \lambda)$.

In order to study R we choose $h_1, h_2, \ldots, h_n \in T$ such that $\mathrm{LM}(h_1)$, $\mathrm{LM}(h_2)$, ..., $\mathrm{LM}(h_n)$ is a homogeneous system of parameters of S, hence also for R. We consider R as an A-module where A is the polynomial algebra $A = \mathbf{F}[\mathrm{LM}(h_1), \mathrm{LM}(h_2), \ldots, \mathrm{LM}(h_n)]$. Since $\mathrm{LM}(h_1)$, $\mathrm{LM}(h_2)$, ..., $\mathrm{LM}(h_n)$ is a a homogeneous system of parameters, R is a finitely generated A-module. Therefore we may write

$$R = \sum_{f \in \widehat{C}} A \cdot \mathrm{LM}(f)$$

for some finite subset $\widehat{C}$ of T.

We choose a finite subset C of $B \cup \{1\}$ and consider the A-module, M, generated by $\{\mathrm{LM}(f) \mid f \in C\}$:

$$M = \sum_{f \in C} A \cdot \mathrm{LM}(f) \ .$$

Clearly $M \subset R$ and thus $\mathcal{H}(M, \lambda) \leq \mathcal{H}(R, \lambda)$. Finally, if $\mathcal{H}(M, \lambda) = \mathcal{H}(S^G, \lambda)$ then $M = R = \mathrm{LT}(S^G)$ and $C \cup \{h_1, h_2, \ldots, h_n\}$ and B are both SAGBI bases for S^G.

In [1], G. Almkvist and R. Fossum gave a formula for $\mathcal{H}(\mathbf{F}[W]^{C_p}, \lambda)$ for any finite dimensional representation W of C_p. In [10], I. Hughes and G. Kemper generalized this formula. Kemper has written a MAGMA script which computes a closed expression for $\mathcal{H}(\mathbf{F}[W]^{C_p}, \lambda)$. Using this script we obtained the following which expresses the Hilbert series, $\mathcal{H}(\mathbf{F}[V_3 \oplus V_3]^{C_p}, \lambda)$, as a rational function in λ.

(3.0.1)

$$\frac{\lambda^{2p+2} + 2p\lambda^{p+2} - \lambda^2 + \lambda^{2p} - 2p\lambda^p - 1}{\begin{array}{c}\big(\lambda^{2p+8} - 2\lambda^{p+8} + \lambda^8 - 2\lambda^{2p+7} + 4\lambda^{p+7} - 2\lambda^7 - 2\lambda^{2p+6} + 4\lambda^{p+6} - 2\lambda^6 \\ +6\lambda^{2p+5} - 12\lambda^{p+5} + 6\lambda^5 - 6\lambda^{2p+3} + 12\lambda^{p+3} - 6\lambda^3 \\ +2\lambda^{2p+2} - 4\lambda^{p+2} + 2\lambda^2 + 2\lambda^{2p+1} - 4\lambda^{p+1} + 2\lambda - \lambda^{2p} + 2\lambda^p - 1\big)\end{array}}$$

Thus our main tasks are to find the sets B and C and to compute $\mathcal{H}(M, \lambda)$.

4. A SAGBI basis for $\mathbf{F}[V_3 \oplus V_3]^{C_p}$

Dickson[7] showed that $\mathbf{F}[V_3]^{C_p} = \mathbf{F}[x, y, z]^{C_p}$ is the hypersurface ring generated by the four functions x, $d = y^2 - 2xz - xy$, $\mathrm{Tr}(yz^{p-1})$ and $\mathbf{N}(z) = \prod_{g \in C_p} g(z)$.

We can use knowledge of $\mathbf{F}[V_3]^{C_p}$ to construct six invariants in $\mathbf{F}[V_3 \oplus V_3]^{C_p}$. These are the six invariants $x_1, x_2, d_1, d_2, N_1, N_2$ where $d_i = y_i^2 - 2x_iz_i - x_iy_i$ and $N_i = \mathbf{N}(z_i) = z_i^p + \ldots$ for i=1,2. Although we will not use this, it is not hard to show these invariants are a homogeneous system of parameters for S^G. What we *will* use is that their lead

terms, $(x_1, x_2, y_1^2, y_2^2, z_1^p, z_2^p)$ are a homogeneous system of parameters for $\mathrm{LT}(S^G)$.

The invariants x_1, x_2, d_1 and d_2 are *rational invariants*. In addition to x_1, x_2, d_1, d_2, there are two other generating rational invariants: $u = x_2y_1 - x_1y_2$ and $w = z_1x_2 - y_1y_2 + x_1z_2 + x_1y_2$.

Theorem 4.1. *The following eight families of invariants form a SAGBI basis for the ring of invariants* $\mathbf{F}[V_3 \oplus V_3]$.

(0) $x_1, x_2, d_1, d_2, N_1, N_2$
(1) w^s *for* $1 \leq s \leq (p-3)/2$
(2) uw^s *for* $0 \leq s \leq (p-1)/2$
(3) $\mathrm{Tr}(y_1 z_1^{p-1} z_2^s)$ *for* $0 \leq s \leq p-1$
(4) $\mathrm{Tr}(z_1^s y_2 z_2^{p-1})$ *for* $0 \leq s \leq p-1$
(5) $\mathrm{Tr}(z_1^t z_2^s)$ *for* $1 \leq t, s \leq p-1$ *and* $p \leq t+s$
(6) $\mathrm{Tr}(y_1 z_1^t z_2^s)$ *for* $0 \leq t \leq p-2, 1 \leq s \leq p-1$ *and* $p-1 \leq t+s$
(7) $\mathrm{Tr}(y_1 z_1^s y_2 z_2^{p-1})$ *for* $0 \leq s \leq p-1$

The proof of Theorem 4.1 is given in the remainder of the paper.

Remark 4.2. *Of course, it would be sufficient to include only* w *and* u *in place of* w^s *for* $1 \leq s \leq (p-3)/2$ *and* uw^s *for* $0 \leq s \leq (p-1)/2$ *in the SAGBI basis. We find it convenient to explicitly include the extra invariants since their lead terms are required as module generators below.*

Let B denote the set of invariants listed in Theorem 4.1.

Remark 4.3. *We note that the final family above is not required in a minimal generating set for* $\mathbf{F}[V_3 \oplus V_3]^{C_p}$. *This family of invariants is included because their lead terms are required in order that* B *be a SAGBI basis. However, it can be shown that if* $0 \leq s \leq p-2$ *then* $\mathrm{LM}(\mathrm{Tr}(y_1 z_1^s y_2 z_2^{p-1})) = \mathrm{LM}(x_2 \,\mathrm{Tr}(z_1^{s+1} z_2^{p-1}) + d_2 \,\mathrm{Tr}(z_1^{s+1} z_2^{p-2}) - cx_2^2 \,\mathrm{Tr}(z_1^{s+1} z_2^{p-2}) + w^{s+1} x_2^{p-s-1}) = y_1 z_1^s y_2^p$ *where* $c = \begin{cases} \frac{p-1}{4} & \text{if } p \equiv 1 \pmod 4 \\ \frac{3p-1}{4} & \text{if } p \equiv 3 \pmod 4 \end{cases}$. *Similarly for* $s = p-1$ *it can be shown that* $\mathrm{LM}(\mathrm{Tr}(y_1 z_1^{p-1} y_2 z_2^{p-1})) = \mathrm{LM}(w \,\mathrm{Tr}(z_2^{p-1} z_1^{p-1}) - x_2 N_1 \,\mathrm{Tr}(z_2^{p-1})) = y_1 z_1^{p-1} y_2^p$

5. Computing the Hilbert Series

We define the algebra $A := \mathbf{F}[x_1, x_2, \mathrm{LM}(d_1), \mathrm{LM}(d_2), \mathrm{LM}(N_1), \mathrm{LM}(N_2)]$ $= \mathbf{F}[x_1, x_2, y_1^2, y_2^2, z_1^p, z_2^p]$. Clearly $x_1, x_2, y_1^2, y_2^2, z_1^p, z_2^p$ is a homogeneous system of parameters in $\mathbf{F}[V_3 \oplus V_3]$. In particular, this implies that $\mathrm{LT}(\mathbf{F}[V_3 \oplus V_3]^{C_p})$ is a finitely generated A-module.

We take M to be the A-module generated by the lead monomials of the elements of $C := \{1\} \cup (B \setminus \{x_1, x_2, d_1, d_2, N_1, N_2\})$.

In order to study M, and in particular to compute its Hilbert series, we need to explicitly find all of its generators. That is, we need to

compute the lead monomial of each of the invariants in C. To do this we use simple generalizations of [14, Theorem 3.3] and [14, Theorem 3.6]. As well, we need the following lemma which may be proved by methods similar to those used to prove [14, Theorem 3.3 and Theorem 3.6].

Lemma 5.1. *Suppose* $0 \leq t, s \leq p-1$ *and* $2s+t \geq p-1$. *Then*

$$\mathrm{LM}(\mathrm{Tr}(z_1^t z_2^s)) = \begin{cases} z_1^t x_2^{p-1-s} y_2^{2s-(p-1)} & \text{if } s \geq (p-1)/2 \\ y_1^{p-1-2s} z_1^{t+2s-(p-1)} x_2^s & \text{if } s \leq (p-1)/2 \end{cases}$$

In order to compute the Hilbert series of M, we define the group

$$H := C_2 \times C_2 \times C_p = \{(i,j,k) \mid 0 \leq i \leq 1, 0 \leq j \leq 1, 0 \leq k \leq p-1\}.$$

We introduce an H-grading on M as follows. We declare that y_1 has multi-degree $(1,0,0) \in H$, that y_2 has multi-degree $(0,1,0) \in H$, that z_1 has multi-degree $(0,0,1) \in H$ and that x_1, x_2 and z_2 have multi-degree $(0,0,0) \in H$. Thus, for example, the monomial $x_1^2 x_2 y_1^3 y_2^4 z_1^{p+5} z_2^2$ has multi-degree $(1,0,5) \in C_2 \times C_2 \times C_p$.

Decompose M by multi-degree as follows:

$$M \quad = \quad \bigoplus_{\omega \in C_2 \times C_2 \times C_p} M_\omega \quad = \quad \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{1} \bigoplus_{k=0}^{p-1} M_{(i,j,k)} \ .$$

Notice that the lead monomial of each of the six functions x_1, x_2, d_1, d_2, N_1, N_2 has multi-degree (0,0,0). Thus every monomial, $m \in A$ has multi-degree (0,0,0) and so multiplication by m preserves multi-degree. Since M is a finitely generated A-module, each homogeneous component $M_{(i,j,k)}$ is itself a finitely generated A-module.

By the above direct sum decomposition,

$$\mathcal{H}(M,\lambda) = \sum_{i=0}^{1} \sum_{j=0}^{1} \sum_{k=0}^{p-1} \mathcal{H}(M_{(i,j,k)}, \lambda)$$

and we compute $\mathcal{H}(M,\lambda)$ by computing each of the individual $\mathcal{H}(M_{(i,j,k)}, \lambda)$.

To do this we take our explicit descriptions of the generators of M and sort them according to their H-degree. This yields the following.

For $i = 0$ and all $0 \leq j \leq 1$ and $0 \leq k \leq p-1$, if $k + j \leq (p-1)/2$ we have the following (minimal) generators of $M_{(0,j,k)}$.

(1) $y_1^{p-1+j-2t} z_1^k x_2^t$ for $\lceil k/2 \rceil \leq t \leq k+j-1$.
(2) $y_1^j z_1^k x_2^{k+j}$
(3) $y_1^j z_1^k x_2^{p-1-t} y_2^{2t-(p-1)}$ for $p-j-k \leq t \leq p-1$

For $i = 0$ and all $0 \leq j \leq 1$ and $0 \leq k \leq p-1$ if $k + j > (p-1)/2$ we have the following (minimal) generators of $M_{(0,j,k)}$.

(1) $y_1^{p-1+j-2t} z_1^k x_2^t$ for $\lceil k/2 \rceil \leq t \leq (p-1)/2$.
(2) $y_1^j z_1^k x_2^{p-1-t} y_2^{2t-(p-1)}$ for $(p+1)/2 \leq t \leq p-1$

For $i = 1$, and all $0 \leq j \leq 1$ and $0 \leq k \leq p-1$ we have the following generator of $M_{(1,j,k)}$.

(1) $y_1^j z_1^k y_2^p$

Since each $M_{(1,j,k)}$ is generated over A by a single element, it is a free rank one A-module. Therefore

$$\mathcal{H}(M_{(1,j,k)}, \lambda) = \mathcal{H}(A, \lambda) \cdot \lambda^{p+k+j} \tag{5.1.1}$$

for all $0 \leq j \leq 1$ and $0 \leq k \leq p-1$.

To compute $\mathcal{H}(M_{(0,j,k)}, \lambda)$ we will construct a resolution of $M_{(0,j,k)}$ by free A-modules.

Let $V_{(0,j,k)}$ denote the set of exponent sequences of the minimal generators of $M_{(0,j,k)}$ listed above:

$$V_{(0,j,k)} := \{w \in \mathbf{N}^6 \mid \mathbf{x}^w \text{ is a minimal generator of } M_{(0,j,k)}\} .$$

Notice that in all cases, all but at most one point of $V_{(0,j,k)}$, lie on two distinct lines of $\mathbf{R}^6 = \mathbf{N}^6 \otimes_{\mathbf{N}} \mathbf{R}$. These two lines intersect at the point $w_0 = (0, j, k, (p-1)/2, 0, 0)$. We denote by $u_1, u_2, \ldots, u_r$ the points of $V_{(0,j,k)}$ of the form $(0, p-j-2t, k, t, 0, 0)$ ordered so that u_m is closer than u_n to w_0 if and only if $m < n$. Similarly, we denote the points of $V_{(0,j,k)}$ of the form $(0, j, k, p-1-t, 2t-(p-1), 0)$ by $v_1, v_2, \ldots, v_s$ also ordered so that v_m is closer than v_n to w_0 if and only if $m < n$. Finally we denote $(0, j, k, 0, 0, 0)$ by both u_0 and by v_0.

We consider the two dimensional cell complex $\mathbf{X}$ with vertices $V_{(0,j,k)}$, and whose 1-cells $E_{(0,j,k)}$, and and 2-cells, $F_{(0,j,k)}$, are described as follows.

If $j+k \leq (p-1)/2$ we define $E_{(0,j,k)}$ to be the following line segments and $F_{(0,j,k)}$, to be the following trapezoids and single triangle

$$\begin{aligned} E_{(0,j,k)} &:= \{\langle u_{t-1}, u_t\rangle : 1 \leq t \leq r\} \sqcup \{\langle v_{t-1}, v_t\rangle : 1 \leq t \leq s\} \\ &\qquad \sqcup \{\langle u_t, v_t\rangle \mid 1 \leq t \leq \min\{r, s\}\} \\ F_{(0,j,k)} &:= \{\langle u_{t-1}, v_{t-1}, u_t, v_t\rangle \mid 2 \leq t \leq \min\{r, s\}\} \sqcup \{\langle u_0, u_1, v_1\rangle\}. \end{aligned}$$

Conversely if $j + k \geq (p+1)/2$, we define $E_{(0,j,k)}$ to be the following line segments and $F_{(0,j,k)}$, to be the following trapezoids

$$\begin{aligned} E_{(0,j,k)} &:= \{\langle u_{t-1}, u_t\rangle : 2 \leq t \leq r\} \sqcup \{\langle v_{t-1}, v_t\rangle : 2 \leq t \leq s\} \\ &\qquad \sqcup \{\langle u_t, v_t\rangle \mid 1 \leq t \leq \min\{r, s\}\} \\ F_{(0,j,k)} &:= \{\langle u_{t-1}, v_{t-1}, u_t, v_t\rangle \mid 2 \leq t \leq \min\{r, s\}\} \end{aligned}$$

A drawing of a typical situation showing the cellular complex $\mathbf{X}$ (with a chosen orientation) is shown in Figure 1. Note that all the vertices lie in a two dimensional plane, except the vertex $u_0 = v_0$, if it occurs.

For an edge $\Delta_1 = \langle w_1, w_2\rangle \in E_{(0,j,k)}$ we define $\mathrm{LCM}(\Delta_1) := \mathrm{LCM}(w_1, w_2)$. Similarly for a two dimensional face $\Delta_2 \in F_{(0,j,k)}$, we define $\mathrm{LCM}(\Delta_2) := \mathrm{LCM}(w \mid w \text{ is a vertex of } \Delta_2)$.

Define

$$\begin{aligned} K_0 &:= \bigoplus_{w \in V_{(0,j,k)}} A(-w) \ , \\ K_1 &:= \bigoplus_{\Delta_1 \in E_{(0,j,k)}} A(-\operatorname{LCM}(\Delta_1)) \ , \text{ and} \\ K_2 &:= \bigoplus_{\Delta_2 \in F_{(0,j,k)}} A(-\operatorname{LCM}(\Delta_2)) \ . \end{aligned}$$

We choose an orientation of $\mathbf{X}$ and consider the following complex:

$$0 \longrightarrow K_2 \xrightarrow{\partial_2} K_1 \xrightarrow{\partial_1} K_0 \xrightarrow{\partial_0} M_{(0,j,k)} \longrightarrow 0 \qquad (\dagger)$$

Here we have shifted the $\mathbf{N}^6$ grading on the summands of the K_1, K_2 and K_3 to arrange that the boundary maps are degree 0 maps. The boundary map ∂_0 is given by $\partial_0(w) = \mathbf{x}^w$. The boundary maps ∂_2 and ∂_1 are the usual cellular complex boundary maps. That is to say $\partial_1(\langle w_1, w_2\rangle) = \pm(w_1 - w_2)$ and $\partial_2(\langle w_1, w_2, w_3, w_4\rangle) = \pm(\langle w_1, w_2\rangle + \langle w_2, w_3\rangle + \langle w_3, w_4\rangle + \langle w_4, w_2\rangle)$ and $\partial_2(\langle u_0, u_1, v_1\rangle) = \pm(\langle u_0, u_1\rangle + \langle u_1, v_1\rangle + \langle v_1, u_0\rangle)$. The signs in these boundary maps are determined by the orientation of $\mathbf{X}$.

The homology of the complex $(\dagger)$ computes the reduced cellular homology of the contractible cell complex $\mathbf{X}$. Therefore the complex $(\dagger)$ is exact and thus gives a resolution of $M_{(0,j,k)}$ by free A-modules.

This resolution $(\dagger)$ shows that

$$\mathcal{H}(M_{(0,j,k)}, \lambda) = \mathcal{H}(K_0, \lambda) - \mathcal{H}(K_1, \lambda) + \mathcal{H}(K_2, \lambda) \qquad (5.1.2)$$

From the definition of the free modules K_0, K_1 and K_2 we see that

$$\begin{aligned} \mathcal{H}(K_0, \lambda) &= \sum_{w \in V_{(0,j,k)}} \lambda^{\deg(w)} \mathcal{H}(A, \lambda) \\ \mathcal{H}(K_1, \lambda) &= \sum_{\Delta_1 \in E_{(0,j,k)}} \lambda^{\deg(\operatorname{LCM}(\Delta_1))} \mathcal{H}(A, \lambda) \\ \mathcal{H}(K_2, \lambda) &= \sum_{\Delta_2 \in F_{(0,j,k)}} \lambda^{\deg(\operatorname{LCM}(\Delta_2))} \mathcal{H}(A, \lambda) \end{aligned}$$

It is a straightforward (but tedious) task to compute the two sets $\{\operatorname{LCM}(\Delta_1) \mid \Delta_1 \in E_{(0,j,k)}\}$ and $\{\operatorname{LCM}(\Delta_2) \mid \Delta_2 \in F_{(0,j,k)}\}$ for each $M_{(0,j,k)}$. From these we immediately obtain expressions for each $\mathcal{H}(K_\ell, \lambda)$ for $\ell = 0, 1, 2$ for each summand, $M_{(0,j,k)}$.

Using Equation 5.1.2 together with the formula for the sum of a geometric series, we find the expressions for the $\mathcal{H}(K_\ell, \lambda)$ combine to form telescoping sums and we get the following expressions for $\mathcal{H}(M_{(0,j,k)}, \lambda)$.

If $j+k \leq (p-1)/2$ then

$$\begin{aligned}\mathcal{H}(M_{(0,j,k)},\lambda) &= \big(2\lambda^p - \lambda^{p+j+\lfloor k/2\rfloor} - \lambda^{p+j+k} + \lambda^{2j+2k} \\ &\quad + \sum_{t=\lceil k/2\rceil}^{j+k-1} (\lambda^{2p+j+k-3t-1} - \lambda^{2p+j+k-3t-2})\big)\mathcal{H}(A,\lambda) \qquad (5.1.3)\end{aligned}$$

If $j+k \geq (p+1)/2$ then

$$\begin{aligned}\mathcal{H}(M_{(0,j,k)},\lambda) &= \big(\lambda^{(p-1)/2+j+k} + 2\lambda^{(p+1)/2+j+k} - \lambda^{p+j+\lfloor k/2\rfloor} - \lambda^{p+j+k} \\ &\quad + \sum_{t=\lceil k/2\rceil}^{(p-2)/2} (\lambda^{2p+j+k-3t-1} - \lambda^{2p+j+k-3t-2})\big)\mathcal{H}(A,\lambda) \qquad (5.1.4)\end{aligned}$$

It is clear that

$$\mathcal{H}(A,\lambda) = (\lambda-1)^{-2}(\lambda^2-1)^{-2}(\lambda^p-1)^{-2}\ .$$

Summing the above expressions for $\mathcal{H}(M_{(0,j,k)},\lambda)$ and the expression (5.1.1) for $\mathcal{H}(M_{(1,j,k)},\lambda)$ over all the homogeneous components of M, i.e., over $i=0,1$, $j=0,1$ and $k=0,1,\ldots,p-1$ we get a huge expression for $\mathcal{H}(M,\lambda)$.

We simplify this expression using mainly the formula for the sum of a geometric series. Doing this carefully shows that $\mathcal{H}(M,\lambda)$ is equal to the following rational function

$$\mathcal{H}(M,\lambda) = \frac{2p\lambda^p + 1 + 2\lambda^2 + 2\lambda^4 + \cdots + 2\lambda^{2p-4} + 2\lambda^{2p-2} + \lambda^{2p}}{(\lambda-1)^2(\lambda^2-1)^2(\lambda^p-1)^2}$$

Conversely factoring the numerator and denominator in (3.0.1) gives the following expression for $\mathcal{H}(\mathbf{F}[V_3\oplus V_3]^{C_p},\lambda)$

$$\frac{(2p\lambda^p + 1 + 2\lambda^2 + 2\lambda^4 + \cdots + 2\lambda^{2p-4} + 2\lambda^{2p-2} + \lambda^{2p})(\lambda^2-1)}{(\lambda-1)^2(\lambda^2-1)^3(\lambda^p-1)^2}$$

Therefore $\mathcal{H}(\mathbf{F}[V_3\oplus V_3]^{C_p},\lambda) = \mathcal{H}(M,\lambda)$ and this proves that the set B comprised of the eight families of invariants listed at the beginning of Section 4 is indeed a SAGBI basis for $\mathbf{F}[V_3\oplus V_3]^{C_p}$.

Acknowledgements. Various calculations were performed using the computer algebra package MAGMA [3]. These calculations included computing $\mathbf{F}[V]^{C_2}$ for $p=2$ and confirming that B is a SAGBI basis for $\mathbf{F}[V]^{C_p}$ for $p\leq 19$. The computations were done using the facilities of the computing laboratory Medicis, http://www.medicis.polytechnique.fr/.

References

[1] G. Almkvist and R. Fossum, *Decompositions of exterior and symmetric powers of indecomposable* $\mathbf{Z}/p\mathbf{Z}$*-modules in characteristic* p, Lecture Notes in Math. **641**, pp. 1–114, Springer-Verlag, 1978.

[2] D.J. Benson, *Polynomial invariants of finite groups*, Cambridge University Press, 1993.

[3] W. Bosma, J.J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Sym. Comp. **24** (1997) 235–265.
[4] H E A Campbell and I P Hughes, *On the vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of David Richman*, Advances in Math, **126** No 1 (1997) 1–20.
[5] H E A Campbell, I P Hughes, R J Shank, and D L Wehlau, *Bases for rings of covariants*, Transformation Groups, **1** No 4 (1996) 307–336.
[6] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, 1992.
[7] L.E.J. Dickson, *On invaraints and the theory of numbers*, The Madison Colloquium (1913) A.M.S., reprinted by Dover, 1966.
[8] M. Göbel, *Computing Bases for Rings of Permutation-invariant Polynomials*, J. Sym. Comp. **19** (1995) 285–291.
[9] M. Göbel, *A Constructive Description of SAGBI Bases for Polynomial Invariants of Permutation Groups*, J. Sym. Comp. **26** (1998) 261–272.
[10] I. Hughes and G. Kemper, *Symmetric powers of modular representations Hilbert series and degree bounds*, Comm. in Alg. **28** (2000) 2059–2088.
[11] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis of a k-subalgebra*, Proceedings of Computers and Mathematics 89, editors: E. Kaltofen and S. Watt, 1–11, MIT, 1989.
[12] D R Richman,*On vector invariants over finite fields*, Advances in Math., **81** (1990) 30–65.
[13] L. Robbiano and M. Sweedler, *Subalgebra bases*, LNM **1430** 61–87, Springer–Verlag, 1990.
[14] R. James Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants*, Comment. Math. Helv. **73** (1998) 548–565.
[15] R.J. Shank, *Classical Covariants and Modular Invariants*, in H.E.A. Campbell and D.L. Wehlau (eds), Invariant Theory in All Characteristics, CRM Proceedings and Lecture Notes **35** AMS, (2004) 241–249.
[16] R. J. Shank and D.L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc., **34** No. 4 (2002) 438-450.
[17] R.J. Shank and D.L. Wehlau, *Computing Modular Invariants of p-groups*, J. Symbolic Computation, **34** (2002) 307–327.
[18] L. Smith, *Polynomial invariants of finite groups*, A.K Peters, Wellesley, MA USA, 1995.
[19] B. Sturmfels, *Gröbner bases and convex polytopes*, ULS 8, Amer. Math. Society, 1996.
[20] H E A Campbell, B Fodden, and David L Wehlau, *Invariants of the Diagonal C_p-action on V_3 — Additional Details*, J. Algebra, **?** No ? (2005?) ?–?.

Department of Mathematics & Statistics, Memorial University of Newfoundland, St John's NL, Canada A1C 5S7
E-mail address: vpacad@mun.ca

Department of Mathematics & Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6
E-mail address: fodden@mast.queensu.ca

Department of Mathematics & Computer Science,
Royal Military College, Kingston, Ontario, Canada K7K 7B4
E-mail address: wehlau@rmc.ca

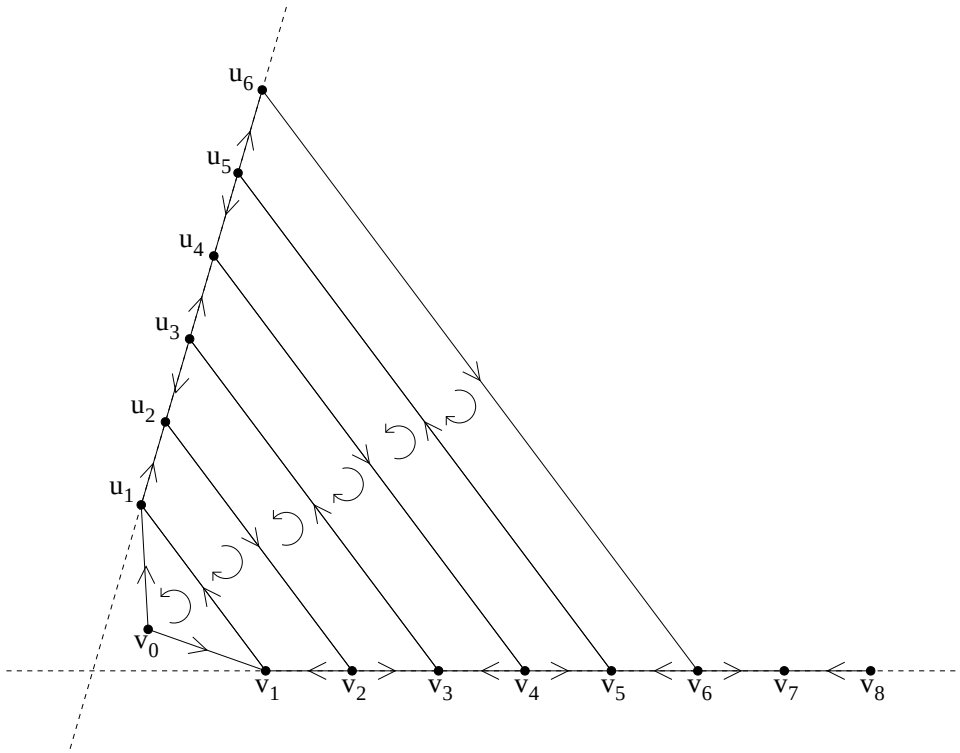

FIGURE 1. The Cellular Complex, $\mathbf{X}$, with an Orientation