Canad. Math. Bull. Vol. **52** (1), 2009 pp. 72–83

A SAGBI Basis For $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$

Alexander Duncan, Michael LeBlanc, 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_n the indecomposable n dimensional representation of C_p over a field $\mathbb{F}$ of characteristic p. We compute a set of generators, in fact a SAGBI basis, for the ring of invariants $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$.

1 Introduction

Let $\mathbb{F}$ be any field of characteristic $p > 0$. We denote by C_p the cyclic group of order p. Let $\rho\colon C_p \to \mathrm{GL}(V_n, \mathbb{F})$ be an n-dimensional indecomposable representation of C_p defined over $\mathbb{F}$.

Fix σ, a non-trivial element of C_p, and select 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. Further, since σ has order p, we have $\rho_n(\sigma)^p = \mathrm{I}_n$, and so the eigenvalues of $\rho_n(\sigma)$ must be p^{th} roots of unity. Since the only root of unity in $\mathbb{F}$ is 1, we have

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

Note that this matrix has order p if and only if $2 \leq n \leq p$. Any $n \times n$ matrix of this form generates a representation of C_p over $\mathbb{F}$ if $n \leq p$, and so ρ_n is of the form above for all $1 \leq n \leq p$ and is the unique n-dimensional indecomposable representation of C_p over $\mathbb{F}$.

Let $\rho\colon C_p \to \mathrm{GL}(W, \mathbb{F})$ be a representation of C_p. The action of C_p on W naturally induces an action on W^* given by

$$(g \cdot f)(w) = f(g^{-1} \cdot w)$$

where $g \in C_p$, $f \in W^*$ and $w \in W$. This action extends to an action by algebra automorphisms on $\mathbb{F}[W]$, the symmetric algebra of W^*.

Since $\mathbb{F}[V_1 \oplus W]^{C_p} \cong \mathbb{F}[V_1] \otimes_{\mathbb{F}} \mathbb{F}[W]^{C_p}$, we may assume that W does not contain V_1 as a summand. Such a representation is called *reduced*.

In 1913, L. Dickson[5] gave generators for the two rings of invariants $\mathbb{F}[V_2]^{C_p}$ and $\mathbb{F}[V_3]^{C_p}$. In 1990, David Richman[9] described a conjectural set of generators for

Received by the editors June 15, 2006; revised October 1, 2006.
Research partially supported by grants from ARP and NSERC
AMS subject classification: Primary: 13A50.

$\mathbb{F}[V_2 \oplus V_2 \oplus \cdots \oplus V_2]^{C_p}$ (for any number of copies of V_2). In 1997, Campbell and Hughes[3] proved Richman's conjecture.

In 1998, Shank [11] introduced a new method using SAGBI bases and used it to find generating sets for the both the rings of invariants $\mathbb{F}[V_4]^{C_p}$ and $\mathbb{F}[V_5]^{C_p}$. This method gives, in fact, not just a generating set but indeed a SAGBI basis for the ring of invariants. In 2002, Shank and Wehlau [13] extended this method and found a SAGBI basis for $\mathbb{F}[V_2 \oplus V_3]^{C_p}$. Recently Campbell, Fodden and Wehlau [2] gave a SAGBI basis for $\mathbb{F}[V_3 \oplus V_3]^{C_p}$

It seems that this method for finding algebra generators will be effective for representations of C_p for which the Cohen–Macaulay defect of the ring of invariants (*i.e.,* the dimension of the ring minus its depth) is at most 2. For larger values of the Cohen–Macaulay defect the chain complex (6) described below is increasingly complicated, and furthermore we have no analogue of [8, Theorem 3] to apply. In particular, this restriction on the Cohen–Macaulay defect requires that every indecomposable summand V_n of W satisfy $n \leq 5$. Furthermore Shank [12] has shown other reasons why this method should not be expected to work for representations with an indecomposable summand of dimension 6 or more.

The above rings of invariants include those of all reduced representations of C_p whose Cohen–Macaulay defect is at most 2 with the two exceptions $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$ and $\mathbb{F}[V_4 \oplus V_2]^{C_p}$. The former we treat here, leaving only the latter unknown. Since it is known that form of the Hilbert series of the latter ring depends upon the residue of p modulo 4, we know *a priori* that analysis of that ring of invariants will involve extra complications.

Since $\rho_3(\sigma)$ has order 4 when $p = 2$ (and not order p), we will assume $p \geq 3$. However, for $p = 2$ a short Magma [1] computation reveals that $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_4}$ is generated by 18 invariants in degrees 1, 1, 1, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 5.

For all $p \geq 3$, we will describe a finite set of invariants in $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$ and prove that it is a SAGBI basis and thus also an algebra generating set for $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$.

There are a number of computational steps in the proof of our main theorem. Each of these steps has been confirmed for small primes by computer computations using the computer algebra system Magma [1]. We were able to compute generators directly for $\mathbb{F}_p[V_2 \oplus V_2 \oplus V_3]^{C_p}$ with $p = 3, 5$. We computed lead terms of transfers and confirmed that the free resolution (6) is exact and that the summing and simplification described in the final paragraph of the paper are correct for many small values of p. While these computer calculations may lend confidence in our result, there is no reliance on them in the proof of Theorem 1.

2 Preliminaries

We direct the reader to [4, Chapter 2] for the appropriate definitions and a detailed discussion of monomial orders. We use the convention that a monomial is a product of variables and that a term is a monomial multiplied by a non-zero scalar coefficient.

For $f \in \mathbb{F}[W]$, $\mathrm{LT}(f)$ denotes the leading term of f, and $\mathrm{LM}(f)$ denotes the leading monomial of f.

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

Note that the lead monomial and lead term of an element depend on the choice of basis and ordering.

For $Q \subset \mathbb{F}[W]$, $LT(Q) := \mathrm{span}_{\mathbb{F}}\{\mathrm{LM}(f) | f \in Q\}$. If the set Q is a subalgebra, then $\mathrm{LT}(Q)$ is also a subalgebra.

If Q is a graded subalgebra of $\mathbb{F}[W]$ and $\mathcal{B} \subseteq Q$ is some subset of Q then $\mathcal{B}$ is a *SAGBI basis* for Q if the algebra generated by $\{\mathrm{LM}(f) \mid f \in \mathcal{B}\}$ is equal to $\mathrm{LT}(Q)$.

For more about SAGBI bases see [7, 10] or [14, Chapter 11].

For a graded $\mathbb{F}$ vector space, $Q = \oplus_{i=0}^{\infty} Q_i$, the *Hilbert Series* of Q is

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

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 $H \leq H'$ if $d_i \leq d_i'$ for all i.

An important property, which is easily verified, is $\mathcal{H}(Q, \lambda) = \mathcal{H}(\mathrm{LT}(Q), \lambda)$. For any SAGBI basis $\mathcal{B}$ of Q, we have $\mathrm{LT}(\mathbb{F}[\mathcal{B}]) \supseteq \mathbb{F}[\mathrm{LT}(\mathcal{B})] = \mathrm{LT}(Q)$, so $\mathcal{H}(\mathbb{F}[\mathcal{B}], \lambda) \geq \mathcal{H}(Q, \lambda)$. Combined with $\mathbb{F}[\mathcal{B}] \subseteq Q$, this shows that any SAGBI basis $\mathcal{B}$ for Q is also an algebra generating set for Q.

The *Transfer Homomorphism* or *Trace* is given by

$$\begin{aligned} \mathrm{Tr}\colon \mathbb{F}[W] &\longrightarrow \mathbb{F}[W]^{C_p}, \\ f &\longmapsto \sum_{g \in C_p} g \cdot f. \end{aligned}$$

The *Norm Homomorphism* is given by

$$\begin{aligned} \mathrm{N}\colon \mathbb{F}[W] &\longrightarrow \mathbb{F}[W]^{C_p} \\ f &\longmapsto \prod_{g \in C_p} g \cdot f. \end{aligned}$$

3 A SAGBI Basis for $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$

We write W to denote the representation $V_2 \oplus V_2 \oplus V_3$. Fix a non-trivial element $\sigma \in C_p$. We choose a basis $\{x_1, y_1, x_2, y_2, x_3, y_3, z_3\}$ for W^* such that the matrix of σ is in Jordan normal form. In particular, we have $\sigma \cdot x_i = x_i$ and $\sigma \cdot y_i = y_i + x_i$ for $i = 1, 2, 3$ and $\sigma \cdot z_3 = z_3 + y_3$. We use the graded reverse lexicographic monomial order on $\mathbb{F}[W]$ with $x_1 < y_1 < x_2 < y_2 < x_3 < y_3 < z_3$.

Consider $\rho'\colon \mathbb{Z} \to \mathrm{GL}(V_2 \oplus V_2 \oplus V_3, K)$, a 7-dimensional representation of $\mathbb{Z}$ over a field K of characteristic 0 generated by

$$\rho'(1) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

Let $\phi_1 : \mathbb{Z} \to C_p$ and $\phi_2 : K[V_2 \oplus V_2 \oplus V_3] \to \mathbb{F}[W]$ be defined as reduction modulo p. Then for $\sigma \in C_p$ and $v \in \mathbb{F}[W]$ we define $\sigma \cdot v = \phi_2(\sigma' \cdot v')$ where $\phi_1(\sigma') = \sigma$ and $\phi_2(v') = v$. It is easy to see that this operation is well defined and that it induces the same action of C_p as ρ. This shows that for $v \in K[V_2 \oplus V_2 \oplus V_3]^{\mathbb{Z}}$, we have $\phi_2(v) \in \mathbb{F}[W]^{C_p}$. Such elements are called rational invariants. Using a Magma script, we find that the rational invariants are generated by the following polynomials:

$$\begin{aligned} u_{ij} &= y_i x_j - x_i y_j \text{ for } 1 \le i < j \le 3, \\ w_i &= x_i y_i x_3 + y_i^2 x_3 - 2x_i y_i y_3 + 2x_i^2 z_3 \text{ for } i = 1, 2, \\ s &= y_1 x_2 x_3 + y_1 y_2 x_3 - y_1 x_2 y_3 - x_1 y_2 y_3 + 2x_1 x_2 z_3, \\ d_3 &= x_3 y_3 - y_3^2 + 2x_3 z_3 \end{aligned}$$

We now consider the set $h = \{x_1, N(y_1), x_2, N(y_2), x_3, d_3, N(z_3)\}$. The set h is a homogeneous system of parameters for $\mathbb{F}[W]$, and therefore for $\mathbb{F}[W]^{C_p}$. Therefore there exists a finite subset $\hat{C} \subset \mathbb{F}[W]^{C_p}$ such that

$$\mathbb{F}[W]^{C_p} = \bigoplus_{f \in \hat{C}} fB,$$

where $B = \mathbb{F}[x_1, N(y_1), x_2, N(y_2), x_3, d_3, N(z_3)]$.

Theorem 1 *Let $\mathbb{F}$ be any field of characteristic p where $p \ge 3$. Let C denote the set consisting of the following elements of $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$:*

$$\begin{aligned} u_{12}^i w_1^j w_2^k \quad &\textit{for all} \quad i + 2j + 2k < p, \\ s u_{12}^i w_1^j w_2^k \quad &\textit{for all} \quad i + 2j + 2k < p - 2, \\ u_{23} w_1^j w_2^k \quad &\textit{for all} \quad 2j + 2k + 1 < p, \\ u_{13} w_1^j w_2^k \quad &\textit{for all} \quad 2j + 2k + 1 < p, \\ Tr(z_3^i y_2^j y_1^k) \quad &\textit{for all} \quad j + k > 0, 2i + j + k \ge 2p - 1, \textit{ and } 0 \le i, j, k \le p - 1, \\ Tr(z_3^{p-1} y_3 y_2^i y_1^j) \quad &\textit{for all} \quad 0 \le i, j \le p - 1. \end{aligned}$$

Then

$$\{x_1, N(y_1), x_2, N(y_2), x_3, d_3, N(z_3)\} \cup C$$

is a SAGBI basis for $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$.

Let $A = \mathrm{LT}(B) = \mathbb{F}[x_1, y_1^p, x_2, y_2^p, x_3, y_3^2, z_3^p]$. Let $M = \sum_{f \in C} \mathrm{LT}(f)A$ and consider the subalgebra R of $\mathbb{F}[W]$ generated by the elements of $h \cup C$. Then $M \subseteq \mathrm{LT}(R)$ and $R \subseteq \mathbb{F}[W]^{C_p}$. Therefore

$$\mathcal{H}(M, \lambda) \le \mathcal{H}(\mathrm{LT}(R), \lambda) = \mathcal{H}(R, \lambda) \le \mathcal{H}(\mathbb{F}[W]^{C_p}, \lambda)\,.$$

We will show that $\mathcal{H}(M, \lambda) = \mathcal{H}(\mathbb{F}[W]^{C_p}, \lambda)$ and thus $R = \mathbb{F}[W]^{C_p}$ (and $M = \mathrm{LT}(R)$) and $h \cup C$ is a SAGBI basis for $\mathbb{F}[W]^{C_p}$.

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

4 Hilbert Series of $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$

Using the method of Hughes and Kemper [6], one can compute the Hilbert series of $\mathbb{F}[W]^{C_p}$. Gregor Kemper has written a Magma script implementing this algorithm. This script yields the following expression for $\mathcal{H}(\mathbb{F}[W]^{C_p}, \lambda)$ as a rational function:

$$\begin{aligned}
&2\lambda^{6+3q} + 12\lambda^{5+3q} - \lambda^{4+3p} - 3\lambda^{4+2p} - 3\lambda^{4+p} + 18\lambda^{4+3q} - \lambda^4 \\
&\quad - 6\lambda^{3+2p} - 6\lambda^{3+p} + 18\lambda^{3+3q} - 3\lambda^{2+3p} - 9\lambda^{2+2p} - 9\lambda^{2+p} + 12\lambda^{2+3q} \\
&\quad -3\lambda^2 - 6\lambda^{1+2p} - 6\lambda^{1+p} + 2\lambda^{1+3q} - \lambda^{3p} - 3\lambda^{2p} - 3\lambda^p - 1 \\
\hline
&\lambda^{11+3p} - 3\lambda^{11+2p} + 3\lambda^{11+p} - \lambda^{11} - 3\lambda^{10+3p} + 9\lambda^{10+2p} - 9\lambda^{10+p} \\
&\quad + 3\lambda^{10} + 2\lambda^{9+3p} - 6\lambda^{9+2p} + 6\lambda^{9+p} - 2\lambda^9 + 3\lambda^{7+3p} - 9\lambda^{7+2p} \\
&\quad + 9\lambda^{7+p} - 3\lambda^7 - 3\lambda^{6+3p} + 9\lambda^{6+2p} - 9\lambda^{6+p} + 3\lambda^6 - 3\lambda^{5+3p} \\
&\quad + 9\lambda^{5+2p} - 9\lambda^{5+p} + 3\lambda^5 + 3\lambda^{4+3p} - 9\lambda^{4+2p} + 9\lambda^{4+p} - 3\lambda^4 \\
&\quad + 2\lambda^{2+3p} - 6\lambda^{2+2p} + 6\lambda^{2+p} - 2\lambda^2 - 3\lambda^{1+3p} + 9\lambda^{1+2p} - 9\lambda^{1+p} \\
&\quad + 3\lambda + \lambda^{3p} - 3\lambda^{2p} + 3\lambda^p - 1,
\end{aligned}$$

where $q = (p-1)/2$.

Factoring the numerator and denominator gives

$$\frac{(1+\lambda)(1-\lambda^3)^2 \hat{f}_p(\lambda)}{(1-\lambda)^3(1-\lambda^2)(1-\lambda^p)^3(1+\lambda)(1-\lambda^3)^2} = \frac{\hat{f}_p(\lambda)}{(1-\lambda)^3(1-\lambda^2)(1-\lambda^p)^3}$$

where $\hat{f}_p$ is a polynomial dependent on p.

5 Leading Terms

5.1 Rational Invariants

The set C contains four families of rational invariants. Since $\mathrm{LT}(fh) = \mathrm{LT}(f)\,\mathrm{LT}(h)$ for all $f, h \in \mathbb{F}[W]$ we see that their leading monomials are

Family	Leading Term
$u_{12}^i w_1^j w_2^k$	$y_1^{i+2j} x_2^i y_2^{2k} x_3^{j+k}$
$su_{12}^i w_1^j w_2^k$	$y_1^{i+2j+1} x_2^i y_2^{2k+1} x_3^{j+k+1}$
$u_{23} w_1^j w_2^k$	$y_1^{2j} y_2^{2k+1} x_3^{1+j+k}$
$u_{13} w_1^j w_2^k$	$y_1^{2j+1} y_2^{2k} x_3^{1+j+k}$

5.2 Transfers

Using the fact that $\sigma^q(z_3^i y_2^j y_1^k) = (z_3 + qy_3 + \binom{q}{2})^i (y_2 + qx_2)^j (y_1 + qx_1)^k$ and that

$$\sum_{q \in \mathbb{F}_p} q^l = \begin{cases} -1, & \text{if } p-1 \text{ divides } l; \\ 0, & \text{otherwise;} \end{cases} \tag{1}$$

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

we see that the coefficient of $z_3^{c_3} y_3^{b_3} x_3^{a_3} y_2^{b_2} x_2^{a_2} y_1^{b_1} x_1^{a_1}$ (where $a_1 + b_1 = k$, etc.) in $\mathrm{Tr}(z_3^i y_2^j y_1^k)$ is

$$\frac{1}{2^{a_3}} \binom{i}{a_3, b_3} \binom{j}{a_2} \binom{k}{a_1} \sum_{n=0}^{a_3} \sum_{q=0}^{p-1} (-1)^{a_3-n} q^{a_1+a_2+a_3+b_3+n}.$$

Since $i, j, k \leq p-1$, the above multinomial coefficients are all nonzero. Thus by (1) the coefficient is nonzero if and only if there is an n with $0 \leq n \leq a_3$ such that $p-1$ divides $a_1 + a_2 + a_3 + b_3 + n$. Thus if $i \geq \frac{p-1}{2}$ then $\mathrm{Tr}(z_3^i y_2^j y_1^k)$ contains the term $y_3^{2i-p+1} x_3^{p-1-i} y_2^j y_1^k$ (arising from $n = p-1-i$) and no greater terms. If $i < \frac{p-1}{2}$ the greatest term in $\mathrm{Tr}(z_3^i y_2^j y_1^k)$ is $x_3^i y_2^{j+2i+1-p} x_2^{p-1-2i} y_1^k$ arising from $n = i$.

Now

$$\sigma^q(z_3^{p-1} y_3 y_2^j y_1^k) = (y_3 + qx^3)\sigma^q(z_3^{p-1} y_2^j y_1^k),$$

and so the coefficient in $\mathrm{Tr}(z_3^{p-1} y_3 y_2^j y_1^k)$ of $z_3^{c_3} y_3^{b_3} x_3^{a_3} y_2^{b_2} x_2^{a_2} y_1^{b_1} x_1^{a_1}$ (with $a_3+b_3+c_3 = p$, etc.) is

$$\frac{1}{2^{a_3}} \binom{j}{a_2} \binom{k}{a_1} \sum_{q=0}^{p-1} \left[\binom{p-1}{a_3, b_3 - 1} (-1)^{a_3} q^{a_1+a_2+a_3+b_3-1} + \left(\binom{p-1}{a_3, b_3 - 1} - 2\binom{p-1}{a_3 - 1, b_3} \right) \sum_{n=1}^{a_3} (-1)^{a_3-n} q^{a_1+a_2+a_3+b_3+n-1} \right].$$

Thus by (1) the coefficient is nonzero if and only if there is an n with $0 \leq n \leq a_3$ such that $p-1$ divides $a_1 + a_2 + a_3 + b_3 + n - 1$ and either $n = 0$ or $b_3 \neq 2a_3$. Thus the lead monomial of $\mathrm{Tr}(z_3^{p-1} y_3 y_2^j y_1^k)$ is $y_3^p y_2^j y_1^k$ (corresponding to $n = 0$).

6 Computing $\mathcal{H}(M, \lambda)$

Let G denote the group $C_p \times C_p \times C_2$. We introduce a G-grading on M by declaring the multidegree of y_1 to be $(1, 0, 0)$, of y_2 to be $(0, 1, 0)$, of y_3 to be $(0, 0, 1)$, and of the other four variables to be $(0, 0, 0)$.

Note that the action of A on M leaves the multidegree invariant. Thus M decomposes as the direct sum of finitely generated A-modules, $M = \bigoplus_{\omega \in G} M_\omega$ where M_ω consists of those of M elements with multidegree ω. Therefore $\mathcal{H}(M, \lambda) = \sum_{\omega \in G} \mathcal{H}(M_\omega, \lambda)$.

For all $0 \leq i, j \leq p-1$ the submodule $M_{(i,j,1)}$ is generated by the single monomial $y_1^i y_2^j y_3^p$, and so $\mathcal{H}(M_{(i,j,1)}, \lambda) = \mathcal{H}(A, \lambda)\lambda^{i+j+p}$.

For $1 \leq i, j \leq p-1$, and $i + j \geq p$, the submodule $M_{(i,j,0)}$ is generated by

$$\tilde{u}_{ij}(s) := y_1^i y_2^j x_3^s y_3^{p-1-2s} \quad \text{for } 0 \leq s \leq \frac{p-3}{2},$$

$$\tilde{v}_{ij}(s) := y_1^i x_2^{p-1-2s} y_2^j x_3^s \quad \text{for } \lceil \frac{j}{2} \rceil \leq s \leq \frac{p-1}{2}.$$

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

For $0 \leq i, j \leq p-1$ and $i+j \leq p-1$ and $i+j \equiv 0 \pmod 2$ the submodule $M_{(i,j,0)}$ is generated by

$$\tilde{u}_{ij}(s) := y_1^i y_2^j x_3^s y_3^{p-1-2s} \quad \text{for } 0 \leq s \leq \frac{i+j}{2} - 1,$$
$$\tilde{v}_{ij}(s) := y_1^i x_2^{i+j-2s} y_2^j x_3^s \quad \text{for } \lceil \frac{j}{2} \rceil \leq s \leq \frac{i+j}{2}.$$

For $0 \leq i, j \leq p-1$ and $i+j \leq p-1$ and $i+j \equiv 1 \pmod 2$ the submodule $M_{(i,j,0)}$ is generated by

$$\tilde{u}_{ij}(s) := y_1^i y_2^j x_3^s y_3^{p-1-2s} \quad \text{for } 0 \leq s \leq \frac{i+j-1}{2},$$
$$\tilde{v}_{ij}(s) := y_1^i x_2^{i+j-2s} y_2^j x_3^s \quad \text{for } \lceil \frac{j}{2} \rceil \leq s \leq \frac{i+j-1}{2},$$
$$\tilde{v}_{ij}(\frac{i+j+1}{2}) := y_1^i y_2^j x_3^{(i+j+1)/2}.$$

To calculate $\mathcal{H}(M_{(i,j,0)}, \lambda)$ we will construct a free resolution of $M_{(i,j,0)}$ as an A-module. Define $P := \mathbb{F}[x_2, x_3, y_3^2]$ and $P' := \mathbb{F}[x_1, y_1^p, y_2^p, z_3^p]$. Then $A = P \otimes_{\mathbb{F}} P'$.

We will denote by u_s the monomial $u_s = \tilde{u}_{ij}(s)/(y_1^i y_2^j) \in P$. Similarly we define $v_s := \tilde{v}_{ij}(s)/(y_1^i y_2^j) \in P$. Let q_0 and q_1 denote respectively the minimum and maximum values of s for which u_s is defined, *i.e.,* for which $\tilde{u}_{ij}(s)$ is one of the generators of $M_{(i,j,0)}$ listed above. Similarly let r_0 and r_1 denote respectively the minimum and maximum values of s for which v_s is defined. Note that $q_0 \leq r_0$ and $q_1 = r_1 - 1$. Let $V = V_{ij}$ be the set of monomials

$$V := \{u_s \mid q_0 \leq s \leq q_1\} \cup \{v_s \mid r_0 \leq s \leq r_1\}.$$

Let $\overline{M}_{(i,j,0)}$ denote the P-module generated by the elements of V_{ij}. We begin by constructing a free resolution of $\overline{M}_{(i,j,0)}$ as a P-module.

We consider the following graph $\Gamma = \Gamma_{ij}$ with vertices $V = V(\Gamma)$ and edge set:

$$E(\Gamma) := \{\langle u_{s-1}, u_s\rangle \mid q_0 + 1 \leq s \leq q_1\} \cup \{\langle v_{s-1}, v_s\rangle \mid r_0 + 1 \leq s \leq r_1\}$$
$$\cup \{\langle u_s, v_s\rangle \mid r_0 \leq s \leq q_1\} \cup \{\langle u_{q_1}, v_{r_1}\rangle\}.$$

Note that we only include the edge $\langle u_{q_1}, v_{r_1}\rangle$ if both of its endpoints are among the vertices in V (which only fails to occur for $i = j = 0$).

We view the vertices $u_{q_0}, u_{q_0+1}, \ldots, u_{q_1}$ as lying on a straight line in a plane and the vertices $v_{r_0}, v_{r_0+1}, \ldots, v_{r_1}$ as lying on another. This shows that Γ is a planar graph. With this embedding the bounded regions enclosed by Γ are a single triangle (provided $r_1 > r_0$) and $q_1 - r_0$ quadrilaterals. We let $F(\Gamma)$ denote the set of these regions:

$$F(\Gamma) := \quad \{\langle v_{r_1}, u_{q_1}, v_{q_1}\rangle\} \cup \{\langle u_{s-1}, v_{s-1}, u_s, v_s\rangle \mid r_0 + 1 \leq s \leq q_1\}.$$

Again we only include the face $\langle v_{r_1}, u_{q_1}, v_{q_1}\rangle$ if all of its edges are included in E, *i.e.,* if $r_1 > r_0$.

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

We use the planar graph Γ to construct a complex as follows. See [8, Section 4] for another discussion of this construction. For any edge $\Delta \in E(\Gamma)$ or face $\Delta \in F(\Gamma)$ we define $\mathrm{LCM}(\Delta) = x_2^a x_3^b y_3^c$ to be the least common multiple of the monomials of V which form the vertices of Δ.

For each edge, $e = \langle w_a, w_b \rangle \in E(\Gamma)$ and each face $\Delta \in F(\Gamma)$ we define $\varepsilon(e, \Delta)$ to be 0 if e is not an edge of Δ, otherwise it is $+1$ if Δ lies on the left as one goes from w_a to w_b, and -1 if Δ is on the right.

Define three free graded P-modules by

$$\overline{K}_0 := \bigoplus_{w \in V(\Gamma)} P(-\deg(\mathrm{LCM}(w)))\langle w \rangle,$$

$$\overline{K}_1 := \bigoplus_{e \in E(\Gamma)} P(-\deg(\mathrm{LCM}(e)))e,$$

$$\overline{K}_2 := \bigoplus_{\Delta \in F(\Gamma)} P(-\deg(\mathrm{LCM}(\Delta)))\Delta,$$

and consider the complex

$$0 \to \overline{K}_2 \xrightarrow{\partial_2} \overline{K}_1 \xrightarrow{\partial_1} \overline{K}_0 \xrightarrow{\partial_0} \overline{M}_{(i,j,0)} \to 0\,.$$

Here the P-module map ∂_0 is given by $\partial_0(\langle w \rangle) = w$. The P-module map ∂_1 is defined by $\partial_1(\langle w_0, w_1 \rangle) = \frac{m}{w_0}\langle w_0 \rangle - \frac{m}{w_1}\langle w_1 \rangle$, where $m = \mathrm{LCM}(w_0, w_1)$. Finally the P-module map ∂_2 is defined by $\partial_2(\Delta) = \sum_{e \in E(\Gamma)} \varepsilon(e, \Delta)\frac{\mathrm{LCM}(\Delta)}{\mathrm{LCM}(e)}e$.

It is easily verified that (6) is a complex, *i.e.,* that $\partial_i \circ \partial_{i+1} = 0$ for i=0,1. We claim moreover that it is exact.

By [8, Theorem 3] there is some planar graph G for which the corresponding complex is the minimal resolution of $\overline{M}_{(i,j,0)}$. We will show that $G = \Gamma$. Note that [8, Theorem 3] requires the hypothesis that the base ring P be a polynomial ring on *three* variables. This is our reason for replacing A by P. This is also why the method used here may fail if the Cohen–Macaulay defect of the ring of invariants exceeds 2.

As an aside we note here that in [8] the situation is slightly different. In [8] the goal is to find the Hilbert series of a ring modulo a monomial ideal rather than the Hilbert series of a module M generated by monomials. To compare the two settings, let I denote the ideal of P generated by a set of monomials. In both cases we have a P-module map ∂_0 carrying the generators of a free P-module onto the monomials in the generating set. For us this is the final (non-zero) map in our resolution, with image M. In [8] however the authors consider the image of ∂_0 as lying in P, and their resolution has one extra map, $\partial_{-1}\colon P \twoheadrightarrow P/I$. Thus in the two settings the exact resolutions are the same except for the additonal final map in the ideal setting.

By construction the two graphs Γ and G have the same vertex set V. We will show $\Gamma = G$ by showing they also share the same edge set and the same face set. For ease of notation, we will show that $\Gamma = G$ only in the case where $1 \leq i, j \leq p-1$ and $i + j \geq p$. The other two cases are entirely similar.

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

Note that for $k \geq 2$ we have the following four equalities:

$$\begin{aligned}
\partial_1(\langle u_s, u_{s+k}\rangle) &= x_3^{k-1}\partial_1(\langle u_s, u_{s+1}\rangle) + y_3^2\partial_1(\langle u_{s+1}, u_{s+k}\rangle),\\
\partial_1(\langle v_s, v_{s+k}\rangle) &= x_3^{k-1}\partial_1(\langle v_s, v_{s+1}\rangle) + x_2^2\partial_1(\langle v_{s+1}, v_{s+k}\rangle),\\
\partial_1(\langle u_s, v_{s+k}\rangle) &= y_3^2\partial_1(\langle u_{s+1}, v_{s+k}\rangle) + x_2^{p-1-2s-2k}x_3^{k-1}\partial_1(\langle u_s, u_{s+1}\rangle),\\
\partial_1(\langle u_{s+k}, v_s\rangle) &= x_2^2\partial_1(\langle u_{s+k}, v_{s+1}\rangle) - x_3^{k-1}y_3^{p-1-2s-2k}\partial_1(\langle v_s, v_{s+1}\rangle)\,.
\end{aligned}$$

These equations show that $\partial_1(\langle w_1, w_2\rangle)$ is contained in $\partial_1(E(\Gamma)) = \ker\partial_0 = \partial_1(E(G))$ for every pair $w_1, w_2 \in V$. Thus none of the edges not in $E(\Gamma)$ is required for the minimal resolution, and therefore $E(G) \subseteq E(\Gamma)$.

Consider $e = \langle u_{s-1}, u_s\rangle \in E(\Gamma)$. Note that $\deg(\mathrm{LCM}(e)) = (0, s, p+1-2s)$, and thus $\mathrm{LCM}(e)$ is divisible only by two monomials of V, namely u_{s-1} and u_s. This implies that $\partial_1(e) \notin \partial_1(E(G)\setminus\{e\})$, and thus that e must lie in $E(G)$. Similarly for each $r_0 + 1 \leq s \leq r_1$ we must have $\langle v_{s-1}, v_s\rangle \in E(G)$.

Finally we consider edges of the form $e = \langle u_s, v_s\rangle \in E(\Gamma)$. Here $\deg(\mathrm{LCM}(e)) = (p-1-2s, s, p-1-2s)$, and thus $\mathrm{LCM}(e)$ is again divisible by exactly two monomials of V: u_s and v_s. This shows that $\partial_1(e) \notin \partial_1(E(G)\setminus\{e\})$, and thus that $e \in E(G)$. Thus we see that $E(\Gamma) = E(G)$.

It only remains to show that the faces of G are exactly those lying in $F(\Gamma)$. Although this may seem obvious, we have to allow for the possibility that G has been embedded into the plane in some way other than that described above.

First we consider the triangle $\Delta = \langle v_{r_1}, u_{q_1}, v_{q_1}\rangle$ contained in $F(\Gamma)$. Expressly,

$$u_{q_1} = x_3^{(p-3)/2}y_3^2, \quad v_{q_1} = x_2^2x_3^{(p-3)/2}, \quad v_{r_1} = x_3^{(p-1)/2}$$

and $\deg(\mathrm{LCM}(\langle v_{r_1}, u_{q_1}, v_{q_1}\rangle)) = (2, (p-1)/2, 2)$. Thus the only monomials of V which divide $\mathrm{LCM}(\langle v_{r_1}, u_{q_1}, v_{q_1}\rangle)$ are v_{r_1}, u_{q_1}, and v_{q_1}. Therefore $\partial_2(\Delta) \notin \partial_2(F(G)\setminus\{e\})$, and thus Δ must be contained in $F(G)$.

Let $r_0 + 1 \leq s \leq q-1$. Since

$$\deg(\mathrm{LCM}(\langle u_{s-1}, v_{s-1}, u_s, v_s\rangle)) = (p+1-2s, s, p+1-2s),$$

the only monomials of V which divide $\mathrm{LCM}(\langle u_{s-1}, v_{s-1}, u_s, v_s\rangle$ are $u_{s-1}, v_{s-1}, u_s, v_s$. Thus $F(G)$ must contain at least one of the faces $\langle u_{s-1}, v_{s-1}, u_s\rangle$, $\langle u_{s-1}, v_{s-1}, v_s\rangle$, $\langle u_{s-1}, u_s, v_s\rangle$, $\langle v_{s-1}, u_s, v_s\rangle$, and $\langle u_{s-1}, v_{s-1}, u_s, v_s\rangle$. However, since each of the four triangles contains an edge not lying in $E(G)$, the region in $F(G)$ must be the quadrilateral.

Hence we have shown that $F(G) \subseteq F(\Gamma)$.

We have that $|E(G)| = (q_1-q_0)+(r_1-r_0)+(q_1-r_0+1)+1$, $|V(G)| = (q_1-q_0+1)+(r_1-r_0+1)$, and therefore by Euler's formula, $|F(G)| = |E(G)|-|V(G)|+1 = q_1-r_0+1$ which is exactly the size of $F(\Gamma)$. Therefore $F(G) = F(\Gamma)$, and thus $G = \Gamma$. This shows that the complex arising from Γ is the same as the exact complex arising from G, and thus that the complex (6) is an exact sequence of P-modules.

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

Now we may tensor this exact sequence with the free (hence flat) cyclic P-module, $P' y_1^i y_2^j$, to obtain an exact sequence of A-modules:

$$0 \to K_2 \xrightarrow{\partial_2} K_1 \xrightarrow{\partial_1} K_0 \xrightarrow{\partial_0} M_{(i,j,0)} \to 0\,,$$

where

$$K_0 := \bigoplus_{w \in V(\Gamma)} A(-\deg(\mathrm{LCM}(w)))w y_1^i y_2^j,$$
$$K_1 := \bigoplus_{e \in E(\Gamma)} A(-\deg(\mathrm{LCM}(e)))e y_1^i y_2^j,$$
$$K_2 := \bigoplus_{\Delta \in F(\Gamma)} A(-\deg(\mathrm{LCM}(\Delta)))\Delta y_1^i y_2^j\,.$$

Therefore

$$\mathcal{H}(M_{(i,j,0)}, \lambda) = \mathcal{H}(K_0\lambda) - \mathcal{H}(K_1, \lambda) + \mathcal{H}(K_2, \lambda). \tag{2}$$

Now

$$\mathcal{H}(K_0, \lambda) = \lambda^{i+j} \sum_{w \in V} \lambda^{\deg(w)} \mathcal{H}(A, \lambda),$$
$$\mathcal{H}(K_1, \lambda) = \lambda^{i+j} \sum_{\Delta_1 \in E} \lambda^{\deg(\mathrm{LCM}(\Delta_1))} \mathcal{H}(A, \lambda),$$
$$\mathcal{H}(K_2, \lambda) = \lambda^{i+j} \sum_{\Delta_2 \in F} \lambda^{\deg(\mathrm{LCM}(\Delta_2))} \mathcal{H}(A, \lambda).$$

This gives the following expressions.
If $i + j \geq p$ then

$$\mathcal{H}(K_0, \lambda) = \mathcal{H}(A, \lambda)\lambda^{i+j}\Big(\sum_{s=0}^{\frac{p-3}{2}} \lambda^{p-1-s} + \sum_{s=\lceil \frac{j}{2} \rceil}^{\frac{p-1}{2}} \lambda^{p-1-s}\Big),$$
$$\mathcal{H}(K_1, \lambda) = \mathcal{H}(A, \lambda)\lambda^{i+j}\Big(\sum_{s=1}^{\frac{p-1}{2}} \lambda^{p+1-s} + \sum_{s=\lceil \frac{j}{2} \rceil+1}^{\frac{p-1}{2}} \lambda^{p+1-s} + \sum_{s=\lceil \frac{j}{2} \rceil}^{\frac{p-3}{2}} \lambda^{2p-2-3s}\Big),$$
$$\mathcal{H}(K_2, \lambda) = \mathcal{H}(A, \lambda)\lambda^{i+j}\Big(\sum_{s=\lceil \frac{j}{2} \rceil+1}^{\frac{p-1}{2}} \lambda^{2p+2-3s}\Big).$$

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press

If $i+j \leq p-1$ and $i+j \equiv 0 \pmod 2$, then

$$\mathcal{H}(K_0,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\sum_{s=0}^{\frac{i+j}{2}-1}\lambda^{p-1-s} + \sum_{s=\lceil\frac{i}{2}\rceil}^{\frac{i+j}{2}}\lambda^{i+j-s}\Big),$$

$$\mathcal{H}(K_1,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\sum_{s=1}^{\frac{i+j}{2}}\lambda^{p+1-s} + \sum_{s=\lceil\frac{j}{2}\rceil+1}^{\frac{i+j}{2}}\lambda^{i+j+2-s} + \sum_{s=\lceil\frac{j}{2}\rceil}^{\frac{i+j}{2}-1}\lambda^{i+j+p-1-3s}\Big),$$

$$\mathcal{H}(K_2,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\sum_{s=\lceil\frac{j}{2}\rceil+1}^{\frac{i+j}{2}}\lambda^{p+3+i+j-3s}\Big).$$

If $i+j \leq p-1$ and $i+j \equiv 1 \pmod 2$ then

$$\mathcal{H}(K_0,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\lambda^{\frac{i+j+1}{2}} + \sum_{s=0}^{\frac{i+j-1}{2}}\lambda^{p-1-s} + \sum_{s=\lceil\frac{j}{2}\rceil}^{\frac{i+j-1}{2}}\lambda^{i+j-s}\Big),$$

$$\mathcal{H}(K_1,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\sum_{s=1}^{\frac{i+j+1}{2}}\lambda^{p+1-s} + \sum_{s=\lceil\frac{j}{2}\rceil+1}^{\frac{i+j+1}{2}}\lambda^{i+j+2-s} + \sum_{s=\lceil\frac{j}{2}\rceil}^{\frac{i+j-1}{2}}\lambda^{p-1+i+j-3s}\Big),$$

$$\mathcal{H}(K_2,\lambda) = \mathcal{H}(A,\lambda)\lambda^{i+j}\Big(\sum_{s=\lceil\frac{j}{2}\rceil+1}^{\frac{i+j+1}{2}}\lambda^{p+1+i+j+2-3s}\Big).$$

Using the above formulae and equation (2) and summing over all $\omega \in G$, we get a huge expression for $\mathcal{H}(M,\lambda)$. Now it is clear that $\mathcal{H}(A,\lambda) = (1-\lambda)^3(1-\lambda^2)(1-\lambda^p)^3$. Multiplying the numerator and denominator by $(1+\lambda)(1-\lambda^3)^2$ causes the sums to telescope, and we get the desired result that $\mathcal{H}(M,\lambda) = \mathcal{H}(\mathbb{F}[W]^{C_p},\lambda)$. Therefore $h \cup C$ is a SAGBI basis for $\mathbb{F}[W]^{C_p}$, and the proof of Theorem 1 is complete.

Acknowledgment The authors gratefully acknowledge the assistance of Mike Roth.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I. The user language.* J. Symbolic Comput. **24**(1997), no. 3-4, 235–265.

[2] H. E. A. Campbell, B. Fodden, and D. L. Wehlau, *Invariants of the diagonal C_p-action on V_3.* J. Algebra **303**(2006), no. 2, 501–513. *Also see the appendix with additional details contained in the online version of this paper at the Journal of Algebra web site.*

[3] H. E. A. Campbell and I. P. Hughes, *Vector invariants of $U_2(\mathbf{F}_p)$: A proof of a conjecture of Richman.* Adv. Math. **126**(1997), no. 1, 1–20.

[4] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[5] L. E. J. Dickson, *On invariants and the theory of numbers.* Dover Publications, Inc., New York, 1966.

[6] I. Hughes and G. Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds.* Comm. Algebra **28**(2000), no. 4, 2059–2088.
[7] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis of a k-subalgebra.* Computers and Mathematics, Springer, New York, 1989, pp. 1–11.
[8] E. Miller and B. Sturmfels, *Monomial Ideals and Planar Graphs.* In: Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci. 1719, Springer, Berlin, 1999, pp. 19–28.
[9] D. Richman, *On vector invariants over finite fields.* Adv. Math. **81**(1990), no. 1, 30–65.
[10] L. Robbiano and M. Sweedler, *Subalgebra bases*, In: Commutative algebra, Lecture Notes in Math. 1430, Springer, Berlin, 1990, pp. 61–87.
[11] R. J. Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants.* Comment. Math. Helv. **73**(1998), no. 4, 548–565.
[12] ———, *Classical Covariants and Modular Invariants.* In: Invariant Theory in All Characteristics, CRM Proc. Lecture Notes 35, Amer. Math. Soc., Providence, RI, 2004, pp. 241–249.
[13] R. J. Shank and D. L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order.* Bull. London Math. Soc. **34**(2002), no. 4, 438–450.
[14] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series 8, American Mathematical Society, Providence, RI, 1996.

Department of Mathematics, The University of British Columbia, Vancouver, B.C., V6T 1Z2
e-mail: duncan@math.ubc.ca
mleblanc@math.ubc.ca

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

https://doi.org/10.4153/CMB-2009-009-2 Published online by Cambridge University Press