HILBERT IDEALS OF VECTOR INVARIANTS OF S_2 AND S_3

MÜFİT SEZER AND ÖZGÜN ÜNLÜ

Abstract. The Hilbert ideal is the ideal generated by positive degree invariants of a finite group. We consider the vector invariants of the natural action of S_n. For S_2 we compute the reduced and universal Gröbner bases for the Hilbert ideal. As well, we identify all initial form ideals of the Hilbert ideal and describe its Gröbner fan. In characteristic two, we show that the Hilbert ideal for S_3 can be generated by polynomials of degree at most 3 and the reduced Gröbner basis contains no polynomials that involve variables from four or more copies. Our results give support for conjectures for improved degree bounds and regularity conditions on the Gröbner bases for the Hilbert ideal of vector invariants of S_n.

Introduction

Let G be a finite group and V be a G-module which is finite dimensional over a field F. The action of G extends to the symmetric algebra $S(V)$ which is the polynomial algebra in a basis of V. A polynomial $f \in S(V)$ is called invariant if $g(f) = f$ for all $g \in G$. The Hilbert ideal, denoted $H(G, V)$, is the ideal in $S(V)$ generated by homogeneous invariant polynomials of strictly positive degree.

The Hilbert ideal plays an important role in constructive aspects of invariant theory and some papers have been published which determine this ideal for various classes of groups. It has been conjectured that $H(G, V)$ is always generated by invariants of degree up to group order, [4, 3.8.6]. This conjecture is known to hold if V is a trivial source module [5] or if $|G| \in F^*$ [5] or if $G = \mathbb{Z}/p$ and V is an indecomposable $\mathbb{Z}/p$-module [9], where p is a prime number. The reduced Gröbner bases for the Hilbert ideal of several representations of $\mathbb{Z}/p$ has been computed in [10] in connection with the study of the module structure of the coinvariant ring.

There has been also some work in the situation where G is a permutation group acting naturally on V with some interesting applications. The reduced Gröbner bases for the full symmetric group S_n has been given in [2], where these bases are used in a solution of Lagrange's problem. Gröbner bases of S_n can also be used in coding theory, see [7]. The reduced and the universal Gröbner bases for the alternating group A_n has been computed in [12]. In fact, they show that $H(S_n, V)$ and $H(A_n, V)$ coincide over some characteristics and whenever they are different the respective reduced Gröbner bases differ by a monomial only, [12, 2.4].

In this paper we study the case where $G = S_2$ or $G = S_3$ and V is the direct sum of arbitrarily many (finite) copies of the natural permutation representation of G. In Section 1, we compute the reduced and the universal Gröbner bases for $H(S_2, V)$. We give two bases; one for characteristic two and one for other characteristics. It turns out that in both cases these bases contain no polynomials that involve

Date: October 11, 2008, 21 h 22 min.
2000 *Mathematics Subject Classification.* 13P10, 13A50.

variables from three copies. Actually in characteristic two, bases polynomials come from only one copy. We note that in [3] a generating set has been computed for the vector invariants of $\mathbb{Z}/p$ acting on copies of two dimensional Jordan blocks in characteristic p. This set can be refined to a Gröbner basis for the Hilbert ideal again consisting of polynomials that depend on only one copy. Therefore our results in Section 1 should be seen as a reproduction of the nice Gröbner basis in [3] for a different (permutation) vector space basis for V. But our computations do not rely on knowing a generating set for the invariant ring. In section 2 we identify the equivalence classes of vectors that generate the same initial form ideal of $H(S_2, V)$ and this yields a description of the Gröbner fan. Moreover, we give generating sets for all initial form ideals of $H(S_2, V)$. In section 3 we consider $H(S_3, V)$ and restrict ourselves to characteristic two. Along the same lines we show that a parallel result holds for $H(S_3, V)$: There is a generating set of polynomials of degree at most three and the reduced Gröbner basis (with respect to lexicographic order) consists of polynomials that involve variables from at most three copies. Together with these results, our computations with the software GAP [6] for $H(S_n, V)$ for various characteristics and term orders give ground for the following conjecture.

Conjecture 1. *Let V be the direct some of finitely many copies of the natural representation of S_n. Then*

(1) *There is a minimal generating set for $H(S_n, V)$ consisting of polynomials up to degree n;*
(2) *For any term order, the reduced Gröbner basis for $H(S_n, V)$ consist of polynomials that involve variables from at most n copies.*

We remark that the first statement of the conjecture is a substantial improvement of the theorem of Fleischmann [5] for the degrees of the generators of the Hilbert ideal for a permutation module. Also, to the best of our knowledge there is no result indicating a type of regularity for the Gröbner basis for the Hilbert ideal of vector invariants as indicated by the second statement. As a general reference for invariant theory see [4] or [8]. As a reference for Gröbner bases we recommend [1] and [11].

The Reduced and Universal Gröbner bases for $H(S_2, V)$

In this section σ denotes the non-trivial element in $G = S_2$. Let k be a positive integer and V be the direct sum of k copies of the natural representation of S_2. We identify $S(V)$ with $R := F[x_i, y_i \mid 1 \leq i \leq k]$. We will denote by R^G the subalgebra in R of invariant polynomials. For each $1 \leq i \leq k$, $\{x_i, y_i\}$ spans the two dimensional permutation representation, i.e., $\sigma(x_i) = y_i$ and $\sigma(y_i) = x_i$. We denote the corresponding Hilbert ideal $H(G, V)$ by H. Let $<$ denote a term order on R with $y_i < x_i$ for $1 \leq i \leq k$. We begin with the easy case when the characteristic of F is not equal to two.

Proposition 2. *Assume that the characteristic of F is not equal to two. Then the set $A = \{x_i + y_i,\, y_i^2,\, y_p y_q \mid 1 \leq i \leq k\,, 1 \leq p < q \leq k\}$ is the reduced Gröbner basis for H with respect to $<$.*

Proof. Note that $y_i^2 = y_i(x_i + y_i) - x_i y_i$. Since $x_i y_i$ and $x_i + y_i$ are in R^G, we have that $y_i^2 \in H$ for $1 \leq i \leq k$. From the equality

$$y_p y_q = \frac{(x_p x_q + y_p y_q) - x_q(x_p + y_p) + y_p(x_q + y_q)}{2}$$

it also follows that $y_p y_q \in H$. Therefore we have established that all polynomials in A lie in H. Notice that the set of monomials in R that are not divisible by a leading monomial of an element in A is precisely the set $\{y_i \mid 1 \leq i \leq k\}$. Since for each i, x_i appears in every invariant polynomial of degree one in which y_i appears and $x_i > y_i$, it follows that none of y_i for $1 \leq i \leq k$ is a leading monomial of a polynomial in H. Therefore A is indeed the reduced Gröbner basis for H with respect to $<$. □

For the rest of the section the characteristic of F is two. We say a monomial $m = x_1^{a_1} y_1^{b_1} x_2^{a_2} y_2^{b_2} \cdots x_k^{a_k} y_k^{b_k} \in R$ is of multidegree $d(m) = (d_1, d_2, \ldots, d_k) \in \mathbb{N}^k$ if $d_i = a_i + b_i$ for $1 \leq i \leq k$. We let $o(m)$ denote the orbit sum of a monomial m. Also define $\operatorname{supp}(m) = \{0 \leq i \leq k \mid d_i > 0\}$ and $\operatorname{supp}_x(m) = \{0 \leq i \leq k \mid a_i > 0\}$ which we call the support and x-support of m respectively. Let I denote the ideal in R generated by $x_i + y_i$ for $1 \leq i \leq k$. We prove a reduction formula for a monomial with respect to I.

Lemma 3. *Let $m = x_1^{a_1} y_1^{b_1} x_2^{a_2} y_2^{b_2} \cdots x_k^{a_k} y_k^{b_k} \in R$ be a monomial with multidegree $d(m) = (d_1, d_2, \ldots, d_k)$. Then*

$$m \equiv \prod_{i \in \operatorname{supp}(m)} y_i^{d_i} \mod I.$$

Proof. The proof is by induction on $|\operatorname{supp}_x(m)|$. If $\operatorname{supp}_x(m) = \emptyset$, then no x_i for $1 \leq i \leq k$ appears in m, and therefore $m = \prod_{i \in \operatorname{supp}(m)} y_i^{d_i}$. If $|\operatorname{supp}_x(m)| > 0$, pick $j \in \operatorname{supp}_x(m)$. Then

$$m \equiv m + \frac{m(x_j + y_j)}{x_j} = \frac{m y_j}{x_j} \mod I.$$

Therefore by reducing successively modulo $x_j + y_j$, we see that $m \equiv \frac{m y_j^{a_j}}{x_j^{a_j}} \mod I$. Set $m' = \frac{m y_j^{a_j}}{x_j^{a_j}}$. Note that the multidegree of m and m' are the same. Moreover, we have $\operatorname{supp}(m') = \operatorname{supp}(m)$ and that $|\operatorname{supp}_x(m')| + 1 = |\operatorname{supp}_x(m)|$. Therefore by induction we get

$$m' \equiv \prod_{i \in \operatorname{supp}(m')} y_i^{d_i} = \prod_{i \in \operatorname{supp}(m)} y_i^{d_i} \mod I.$$

Hence $m \equiv \prod_{i \in \operatorname{supp}(m)} y_i^{d_i} \mod I$, as desired. □

Now we are ready to give the reduced Gröbner basis for the characteristic two case.

Proposition 4. *Assume that the characteristic of F is two. Then the set $A' = \{x_i + y_i,\ y_i^2 \mid 1 \leq i \leq k\}$ is the reduced Gröbner basis for H with respect to $<$.*

Proof. Let I' be the ideal generated by the polynomials in A'. Since $y_i^2 = y_i(x_i + y + i) + y_i x_i \in H$, we have $I' \subseteq H$. Since the leading monomials of polynomials in A' are relatively prime, A' is the reduced Gröbner basis for the ideal I'. Therefore it suffices to show that I' is equal to H. That is we need to show that $o(m) \in I'$ for any monomial m. Notice that if $o(m)$ contains one monomial only then m is divisible by $x_j y_j$ for some $1 \leq j \leq k$. But since $x_j y_j = y_j(x_j + y_j) + y_j^2 \in I'$, it follows that $m = o(m) \in I'$. Otherwise $o(m)$ contains two monomials, namely m

and $\sigma(m)$. Since σ permutes x_i and y_i, we have $\mathrm{supp}(m) = \mathrm{supp}(\sigma(m))$. Assume that the multidegree of m is $d(m) = (d_1, d_2, \ldots, d_k)$. By the previous lemma we get

$$m \equiv \prod_{i \in \mathrm{supp}(m)} y_i^{d_i} = \prod_{i \in \mathrm{supp}(\sigma(m))} y_i^{d_i} \equiv \sigma(m) \mod I.$$

Therefore

$$o(m) = m + \sigma(m) \equiv 2\Big(\prod_{i \in \mathrm{supp}(m)} y_i^{d_i}\Big) = 0 \mod I.$$

Since $I \subseteq I'$, we have $o(m) \in I'$, as desired. □

Let A be a subset of $\{1, 2, \ldots, k\}$ and let $A_<$ denote the set of term orders such that $x_i > y_i$ if and only if $i \in A$. Notice that the computation of the reduced Gröbner bases above just relied on the choice $x_i > y_i$ for $1 \leq i \leq k$. Therefore, by virtue of Propositions 2 and 4, we have the following.

Theorem 5. *Let $<$ be a term order in $A_<$ and let A^c denote the complement of A in $\{1, 2, \ldots, k\}$.*

(1) If the characteristic of F is not equal to two, then the set

$$\{x_i + y_i\}_{1 \leq i \leq k} \cup \{x_i^2\}_{i \in A^c} \cup \{y_i^2\}_{i \in A} \cup \{x_i y_j\}_{i \in A^c, j \in A}$$

is the reduced Gröbner basis for H with respect to $<$.

(2) If the characteristic of F is equal to two, then the set

$$\{x_i + y_i\}_{1 \leq i \leq k} \cup \{x_i^2\}_{i \in A^c} \cup \{y_i^2\}_{i \in A}$$

is the reduced Gröbner basis for H with respect to $<$.

By putting together the reduced Gröbner bases in Theorem 5, we get a universal Gröbner basis for H.

Theorem 6. *If the characteristic of F is not equal to two, the set $\{x_i + y_i\}_{1 \leq i \leq k} \cup \{x_i^2\}_{1 \leq i \leq k} \cup \{y_i^2\}_{1 \leq i \leq k}, \{x_i y_j\}_{i \neq j\, 1 \leq i,j \leq k}$ is a universal Gröbner basis for H. Similarly the set $\{x_i + y_i\}_{1 \leq i \leq k} \cup \{x_i^2\}_{1 \leq i \leq k} \cup \{y_i^2\}_{1 \leq i \leq k}$ is a universal Gröbner basis of H if the characteristic of F is equal to two.*

Initial form ideals of $H(S_2, V)$

We assume the notation and the convention of the previous section. For a term order $<$, a vector $w \in \mathbb{R}^{2k}$ and a polynomial $f \in R$, let $\mathrm{LT}_<(f)$ and $\mathrm{IN}_w(f)$ denote the lead term and initial form of f with respect to $<$ and w. Also we denote the corresponding lead term and initial form ideals of H by $\mathrm{LT}_<(H)$ and $\mathrm{IN}_w(H)$. Note that $\mathrm{IN}_w(H)$ does not need to be a monomial ideal. Nevertheless, for any term order $<$, there exists a non-negative vector $w \in \mathbb{N}^{2k}$ such that $\mathrm{LT}_<(H) = \mathrm{IN}_w(H)$. For a background on representation of term orders by vectors see [11, §1].

For disjoint subsets A and B of $\{1, 2, \ldots, k\}$, let $C(A, B)$ denote the set of vectors $(a_1, b_1, a_2, b_2, \ldots, a_k, b_k) \in \mathbb{R}^{2k}$ such that $a_i > b_i$ for $i \in A$, $a_j = b_j$ for $j \in B$ and $a_t < b_t$ for $t \in \{1, 2, \ldots, k\} \setminus (A \cup B)$. Note that the collection of $C(A, B)$ forms a partition of $\mathbb{R}^{2k}$. We say that two vectors in $\mathbb{R}^{2k}$ are in the same class if they both lie in $C(A, B)$ for some sets A, B. In the following lemma we show that these classes are exactly the equivalence classes of vectors with respect to the initial form ideals they produce.

Lemma 7. *Let w and w' be two vectors in $\mathbb{R}^{2k}$. Then, $\mathrm{IN}_w(H) = \mathrm{IN}_{w'}(H)$ if and only if w and w' are in the same class.*

Proof. If w and w' are in different classes, then there exists an index $1 \leq i \leq k$ such that $\mathrm{IN}_w(x_i+y_i) \neq \mathrm{IN}_{w'}(x_i+y_i)$. If x_i appears in an invariant polynomial of degree one, then y_i also appears in the polynomial. It follows that $\mathrm{IN}_w(H) \neq \mathrm{IN}_{w'}(H)$.

Conversely, assume that w and w' are in the same class. We show that the corresponding initial form ideals are the same. Since H is homogeneous, there exists vectors $w_+, w'_+ \in \mathbb{R}^{2k}_+$ such that $\mathrm{IN}_w(H) = \mathrm{IN}_{w_+}(H)$ and $\mathrm{IN}_{w'}(H) = \mathrm{IN}_{w'_+}(H)$, see [11, 1.12]. Since w and w_+ produce the same initial form ideal, they are in the same class from the previous paragraph. Similarly w' and w'_+ are in the same class. Therefore replacing w by w_+ and w' by w'_+ if necessary, we may assume that both w and w' are in $\mathbb{R}^{2k}_+$. Fix a term order $<$ and let S denote the reduced Gröbner basis of H with respect to $<_w$, where $<_w$ is the term order obtained by comparing the monomials first with using w and then with $<$ (we need positivity of w here). Since any reduced Gröbner basis of H consists of monomials together with $x_i + y_i$ for $1 \leq i \leq k$ by Theorem 5, we have $\mathrm{IN}_w(g) = \mathrm{IN}_{w'}(g)$ for all $g \in S$. But $\mathrm{IN}_w(H)$ is generated by $\{\mathrm{IN}_w(g) \mid g \in S\}$, see [11, 1.9]. Therefore it follows that $\mathrm{IN}_w(H) \subseteq \mathrm{IN}_{w'}(H)$ because initial forms of elements in S with respect to w and w' are the same. If this inclusion were proper, then it would stay proper after taking the lead term ideals with respect to $<$, i.e., $\mathrm{LT}_{<_w}(H) \subset \mathrm{LT}_{<_{w'}}(H)$. This is impossible since there can not be a proper inclusion between the lead term ideals of H arising from term orders, see for instance [11, 1.1]. □

Now we identify the classes of vectors with monomial initial form ideals. These are precisely the lead term ideals arising from term orders.

Lemma 8. *Let w be a vector in $C(A, B)$. Then $\mathrm{IN}_w(H)$ is a monomial ideal if and only if $B = \emptyset$.*

Proof. Let w be a vector in $C(A, B)$ with $B \neq \emptyset$. Pick $i \in B$. Then $\mathrm{IN}_w(x_i + y_i) = x_i+y_i$. Since x_i and y_i appear in a degree one invariant polynomial always together, it follows that $\mathrm{IN}_w(H)$ is not a monomial ideal.

Conversely, let $w \in C(A, \emptyset)$. We may assume that $w \in \mathbb{R}^{2k}_+$ by [11, 1.12]. Fix a term order $<$ and let S be the Gröbner basis of H with respect to $<_w$. Since S consists of monomials and $\{x_i + y_i\}_{1\leq i\leq k}$ by Theorem 5, we have that $\mathrm{IN}_w(g)$ is a monomial for all $g \in S$. So $\mathrm{IN}_w(H)$ is a monomial ideal since it is generated by $\{\mathrm{IN}_w(g) \mid g \in S\}$, [11, 1.9]. □

We now give a generating set for each non-monomial initial form ideal of H.

Proposition 9. *Let $w \in C(A, B)$ with $B \neq \emptyset$. Assume that the characteristic of F is equal to two and set $D = \{1, 2, \ldots, k\} \setminus (A \cup B)$. Then $\mathrm{IN}_w(H)$ is generated by $\{x_i\}_{i\in A} \cup \{x_i + y_i\}_{i\in B} \cup \{y_i\}_{i\in D} \cup \{x_i^2\}_{i\in D} \cup \{y_i^2\}_{i\in A\cup B}$.*

Proof. We may assume that $w \in \mathbb{R}^{2k}_+$ by [11, 1.12]. Also note that w lies in the closure of $C(A \cup B, \emptyset)$. Let $w' \in C(A \cup B, \emptyset) \cap \mathbb{R}^{2k}_+$ be arbitrary. Then $w + \epsilon w' \in C(A \cup B, \emptyset)$ for all $\epsilon > 0$. Since $\mathrm{IN}_{w'}(\mathrm{IN}_w(H)) = \mathrm{IN}_{w+\epsilon w'}(H)$ for sufficiently small ϵ, see [11, 1.13], it follows that

$$\mathrm{IN}_{w'}(\mathrm{IN}_w(H)) = \mathrm{IN}_{w'}(H).$$

By the previous lemma, $\mathrm{IN}_{w'}(H)$ is a monomial ideal and hence a lead term ideal with respect to a term order, say $<$. From Theorem 5, we see that the set

$$\{x_i + y_i\}_{1\leq i\leq k} \cup \{x_i^2\}_{i\in D} \cup \{y_i^2\}_{i\in A\cup B}$$

is the reduced Gröbner basis for H with respect to $<$. By taking the lead term ideal of both sides in the above equality of initial form ideals with respect to $<$, one sees that this set is also the reduced Gröbner basis with respect to $<'_w$, where $<'=<_{w'}$. It now follows from [11, 1.9]) that

$$\{\mathrm{IN}_w(x_i + y_i)\}_{1\leq i\leq k} \cup \{\mathrm{IN}_w(x_i^2)\}_{i\in D} \cup \{\mathrm{IN}_w(y_i^2)\}_{i\in A\cup B}$$

generates $\mathrm{IN}_w(H)$. But this set is equal to

$$\{x_i\}_{i\in A} \cup \{x_i + y_i\}_{i\in B} \cup \{y_i\}_{i\in D} \cup \{x_i^2\}_{i\in D} \cup \{y_i^2\}_{i\in A\cup B},$$

as desired. □

Remark 10. *Along the same lines, one can get the following result for a field of characteristic not equal to two. Let $w \in C(A, B)$ with $B \neq \emptyset$ and let D denote the complement of $A \cup B$ in $\{1, 2, \ldots, k\}$. Then $\mathrm{IN}_w(H)$ is generated by*

$$\{x_i\}_{i\in A} \cup \{x_i + y_i\}_{i\in B} \cup \{y_i\}_{i\in D} \cup \{x_i^2\}_{i\in D} \cup \{y_i^2\}_{i\in A\cup B} \cup \{x_i y_j\}_{i\in D,\, j\in A\cup B}.$$

Recall that the Gröbner fan of H is the polyhedral complex consisting of the (Euclidean) closures of equivalence classes of vectors with respect to the initial form ideals they produce. Therefore by Lemma 7, the Gröbner fan of H is the set of the closures $\overline{C(A, B)}$, where A, B varies over the disjoint subsets of $\{1, 2, \ldots, k\}$. We refer the reader to [11, §2] for basic facts regarding fans. We have the following face relations among these polyhedra.

Proposition 11. *$\overline{C(A_1, B_1)}$ is a face of $\overline{C(A_2, B_2)}$ if and only if $A_2 \cup B_2 \subseteq A_1 \cup B_1$ and $A_1 \subseteq A_2$.*

Proof. Since a Gröbner fan is a complex [11, 2.4], it suffices to show that $\overline{C(A_1, B_1)} \subseteq \overline{C(A_2, B_2)}$ if and only if $A_2 \cup B_2 \subseteq A_1 \cup B_1$ and $A_1 \subseteq A_2$.

Take any $w = (a_1, b_1, a_2, b_2, \ldots, a_k, b_k)$ in $\overline{C(A_1, B_1)}$. Then $A_2 \subseteq A_1 \cup B_1$ implies $a_i \geq b_i$ for all $i \in A_2$ and $B_2 \subseteq B_1$ implies $a_i = b_i$ for all $i \in B_2$ and $\{1, 2, \ldots, k\} \setminus (A_2 \cup B_2) \subseteq \{1, 2, \ldots k\} \setminus A_1$ implies $a_i \leq b_i$ for all $i \in \{1, 2, \ldots, k\} \setminus (A_2 \cup B_2)$. Hence w is in $\overline{C(A_2, B_2)}$.

Conversely if $A_1 \nsubseteq A_2$, then pick $i \in A_1 \setminus A_2$. For $w = (a_1, b_1, a_2, b_2, \ldots, a_k, b_k)$ in $C(A_1, B_1)$ we have $a_i > b_i$ and hence w is not in $\overline{C(A_2, B_2)}$. Similarly, if $A_2 \cup B_2 \nsubseteq A_1 \cup B_1$, then pick $i \in (A_2 \cup B_2) \setminus (A_1 \cup B_1)$. Then any element $w = (a_1, b_1, a_2, b_2, \ldots, a_k, b_k)$ in $C(A_1, B_1)$ satisfies $b_i > a_i$. Hence $w \notin \overline{C(A_2, B_2)}$. □

The Reduced Gröbner basis for $H(S_3, V)$

In this section $G = S_3$ and V denotes the direct sum of k copies of the natural representation of G and we assume that F is a field of characteristic two. Let H denote $H(S_3, V)$ and R denote $S(V) = F[x_i, y_i, z_i \mid 1 \leq i \leq k]$. For each $1 \leq i \leq k$, $\{x_i, y_i, z_i\}$ spans the three dimensional representation on which G acts by permuting the variables. We use the lexicographic order with $x_i > y_i > z_i$ for $1 \leq i \leq k$ and $z_i > x_{i+1}$ for $1 \leq i \leq k-1$. As before let R^G denote the subalgebra of invariant polynomials. We recall and extend the definitions for the support of a monomial. As in Section 1, a monomial $m = x_1^{a_1} y_1^{b_1} z_1^{c_1} \cdots x_k^{a_k} y_k^{b_k} z_k^{c_k} \in R$ is said to

be of multidegree $d(m) = (d_1, d_2, \ldots, d_k) \in \mathbb{N}^k$ if $d_i = a_i + b_i + c_i$ for $1 \leq i \leq k$. Define $\operatorname{supp}(m) = \{0 \leq i \leq k \mid d_i > 0\}$ which we call the support of m. Also let $\operatorname{supp}_x(m)$ denote the set $\{0 \leq i \leq k \mid a_i > 0\}$ which we call the x-support of m. The y-support and the z-support of m is defined similarly. Furthermore define the rank $r(m)$ of m to be the size of $\operatorname{supp}(m)$. Similarly we let $r_x(m)$, $r_y(m)$, $r_z(m)$ denote the sizes of $\operatorname{supp}_x(m)$, $\operatorname{supp}_y(m)$ and $\operatorname{supp}_z(m)$. We call these numbers x-rank, y-rank and z-rank, respectively.

Now let B denote the set of following polynomials in R:

$$\begin{aligned}
e_i &= o(x_i) = x_i + y_i + z_i \ \text{ for } 1 \leq i \leq k,\\
f_i &= o(x_i y_i) + (y_i + z_i)e_i = y_i^2 + y_i z_i + z_i^2 \ \text{ for } 1 \leq i \leq k,\\
g_i &= o(x_i y_i z_i) + z_i f_i + y_i z_i e_i = z_i^3 \ \text{ for } 1 \leq i \leq k,\\
u_{i,j} &= o(x_i y_j) + (y_j + z_j)e_i + (y_i + z_i)e_j\\
&= y_i z_j + y_j z_i \quad \text{for } 1 \leq i < j \leq k,\\
a_{i,j} &= o(x_i x_j^2) + (y_j^2 + z_j^2)e_i + x_i e_j^2 + z_i f_j + z_j u_{\min\{i,j\},\max\{i,j\}}\\
&= z_i z_j^2 \ \text{ for } 1 \leq i \neq j \leq k,\\
p_{i,j,l} &= o(x_i y_j y_l) + y_j u_{i,l} + x_l u_{i,j} + (y_j y_l + z_j z_l)e_i + (y_i + z_i)x_l e_j + (y_i y_j + z_i z_j)e_l\\
&= z_i y_j y_l + z_i z_j y_l \quad \text{for } 1 \leq i < j < l \leq k,\\
p_{i,j} &= o(x_i y_i y_j) + (y_i y_j + y_i x_j + z_i x_j + z_i z_j)e_i + y_i z_i e_j + (x_j + y_j)f_i + a_{j,i}\\
&= y_i z_i y_j + z_i^2 y_j \ \text{ for } 1 \leq i < j \leq k,\\
b_{i,j,l} &= z_j z_l u_{i,l} + y_i a_{j,l}\\
&= z_i z_j y_l z_l \ \text{ for } 1 \leq i < j < l \leq k.
\end{aligned}$$

Note that all these polynomials lie in H. Actually we want to show that these polynomials generate H. This needs some preparation. First let I denote the ideal generated by the set B in R. Let m be any monomial and s denote the maximum integer in $\operatorname{supp}(m)$. Define $\overline{m} = \left(\prod_{j \in \operatorname{supp}(m)\setminus\{s\}} z_j^{d_j}\right)\left(y_s z_s^{d_s - 1}\right)$. For example if $m = y_1 z_2 y_3 z_4$, then $\overline{m} = z_1 z_2 z_3 y_4$. Notice that the multidegree of a monomial m uniquely determines $\overline{m}$, i.e., if $d(m) = d(m')$, then $\overline{m} = \overline{m'}$.

Lemma 12. *If $r_x(m) = 0$, $r_y(m) > 0$, and $r_z(m) > 0$, then $m \equiv \overline{m} \mod I$.*

Proof. Let s denote the biggest integer in $\operatorname{supp}(m)$, and $t \leq s$ denote the smallest integer in $\operatorname{supp}_y(m)$. We proceed by reverse induction on t. We first consider the situation when y_t^2 divides m. Notice that in this case $m \equiv m + \frac{m f_t}{y_t^2} = \frac{m z_t}{y_t} + \frac{m z_t^2}{y_t^2} \mod I$. Since $r_z(m) > 0$, there exits $1 \leq j \leq k$ such that $z_t^2 z_j$ divides $\frac{m z_t^2}{y_t^2}$. Hence $\frac{m z_t^2}{y_t^2}$ is a multiple of either g_t or $a_{j,t}$. That is $\frac{m z_t^2}{y_t^2} \in I$. It follows that

$$m \equiv \frac{m z_t}{y_t} \mod I.$$

Furthermore $r_x(\frac{m z_t}{y_t}) = 0$ and both $r_y(\frac{m z_t}{y_t})$ and $r_z(\frac{m z_t}{y_t})$ are positive because y_t and z_t divide $\frac{m z_t}{y_t}$. Also, since m and $\frac{m z_t}{y_t}$ have the same multidegree we have $\overline{m} = \overline{(\frac{m z_t}{y_t})}$. Therefore by replacing m with $\frac{m z_t}{y_t}$ repeatedly, we may assume that y_t^2 does not divide m.

Assume that $t = s$. Since y_t^2 does not divide m, we have $m = \overline{m}$ and the assertion holds trivially. Hence we may take $t < s$. We now consider two cases. First assume that there exists an integer $t < t' \leq s$ such that $t' \in \mathrm{supp}_z(m)$. Then m is divisible by $y_t z_{t'}$. Consider the monomial $m' = m + \frac{mu_{t,t'}}{y_t z_{t'}}$. Then we have $m \equiv m' \mod I$. Also, since m' is obtained from m by just replacing y_t with z_t and replacing $z_{t'}$ with $y_{t'}$, we have $r_x(m) = r_x(m')$, $r_y(m) = r_y(m')$ and $r_z(m) = r_z(m')$ and the multidegree of m is equal to the multidegree of m'. Moreover, the smallest integer in $\mathrm{supp}_y(m')$ is strictly bigger than t. Hence the result follows by induction because $\overline{m} = \overline{m'}$.

Next assume that $\mathrm{supp}_z(m)$ does not contain any integer that is strictly bigger than t. Hence m is also divisible by y_s. As we did in the first case it suffices to show that there exists a monomial $m' \equiv m \mod I$ with same multidegree and the same ranks with respect to each variable such that the smallest integer in $\mathrm{supp}_y(m')$ is strictly bigger that t. Note that since $r_z(m) > 0$, there exists $i \leq t$ such that z_i divides m. If $i < t$, then m is divisible by $z_i y_t y_s$ and so $m' = m + \frac{mp_{i,t,s}}{z_i y_t y_s}$ is a monomial that meets the requirements. If $i = t$, then m is divisible by $y_t z_t y_s$ and so $m' = m + \frac{mp_{t,s}}{y_t z_t y_s}$ meets the requirements. This completes the proof. □

For a monomial m with multidegree $(d_1, d_2, \ldots, d_k)$ define $m_y = \prod_{i \in \mathrm{supp}(m)} y_i^{d_i}$ and $m_z = \prod_{i \in \mathrm{supp}(m)} z_i^{d_i}$. Also define $\alpha_y(m) = 1$ if $r_y(m) = 0$ and $\alpha_y(m) = 0$ if $r_y(m) > 0$. And similarly set $\alpha_z(m) = 1$ if $r_z(m) = 0$ and $\alpha_z(m) = 0$ if $r_z(m) > 0$. We are ready to show that the ideal I generated by B is actually H.

Theorem 13. *We have $H = I$*

Proof. It is clear that $I \leq H$. Hence it suffices to show that the orbit sum $o(m)$ lies in I for any monomial m. Set $m = x_1^{a_1} y_1^{b_1} z_1^{c_1} \cdots x_k^{a_k} y_k^{b_k} z_k^{c_k}$

Reducing successively modulo the polynomials $e_i = x_i + y_i + z_i$ for $i \in \mathrm{supp}_x(m)$, we see that

$$m \equiv \frac{m}{\prod_{i \in \mathrm{supp}_x(m)} x_i^{a_i}} \Big(\prod_{i \in \mathrm{supp}_x(m)} (y_i + z_i)^{a_i} \Big) \mod I.$$

Clearly, the x-rank of the monomials in the above expansion are all zero and they share the common multidegree with m. Notice also that all monomials in the above expansion have strictly positive y-rank if and only if the y-rank of m is strictly positive. Moreover if the y-rank of m is zero, then there is precisely one monomial in the above expansion with zero y-rank which is m_z. Similarly the assertions of the last two sentences still hold if one interchanges y with z in these sentences. Therefore all monomials in the above expansion except possibly two have strictly positive y-rank and z-rank and therefore reduce to the same monomial $\overline{m}$ by the previous lemma. Therefore we have

$$\begin{aligned} m &\equiv \alpha_y(m) m_z + \alpha_z(m) m_y + (2^{a_1 + a_2 + \cdots + a_k} - \alpha_y(m) - \alpha_z(m)) \overline{m} \\ &\equiv \alpha_y(m) m_z + \alpha_z(m) m_y + (\alpha_y(m) + \alpha_z(m)) \overline{m} \mod I. \end{aligned}$$

Taking the summation over the monomials $\sigma(m)$ in the orbit of m, we see that $o(m)$ is equivalent to

$$\sum_{\sigma(m)} \alpha_y(\sigma(m)) \sigma(m)_z + \sum_{\sigma(m)} \alpha_z(\sigma(m)) \sigma(m)_y + \sum_{\sigma(m)} (\alpha_y(\sigma(m)) + \alpha_z(\sigma(m))) \overline{\sigma(m)},$$

modulo the ideal I. Note that since $\mathrm{supp}(m) = \mathrm{supp}(\sigma(m))$ for all $\sigma \in G$, it follows that $\overline{m} = \overline{\sigma(m)}$ and $m_y = \sigma(m)_y$ and $m_z = \sigma(m)_z$. Notice also that $\sum_{\sigma(m)} \alpha_y(\sigma(m))$ and $\sum_{\sigma(m)} \alpha_z(\sigma(m))$ are exactly the numbers of monomials in the orbit $o(m)$ that have zero y-rank and zero z-rank respectively, where the summation is taken over the monomials that are in the orbit of m. Since G is the full symmetric group on $\{x_i, y_i, z_i\}$ for $1 \leq i \leq k$, these numbers are equal. Combining all this information we get

$$\begin{aligned} o(m) &\equiv \sum_{\sigma(m)} \alpha_y(\sigma(m))\sigma(m)_z + \sum_{\sigma(m)} \alpha_z(\sigma(m))\sigma(m)_y \\ &\equiv \sum_{\sigma(m)} \alpha_y(\sigma(m))m_z + \sum_{\sigma(m)} \alpha_z(\sigma(m))m_y \mod I, \end{aligned}$$

where we also used that we are in characteristic two in the first equivalence. Note also that since $G = S_3$, the number of monomials in $o(m)$ of zero y-rank and z-rank are simultaneously either zero, one or two. Therefore from the last identity we have $o(m) \in I$ except for the situation $\sum_{\sigma(m)} \alpha_y(\sigma(m)) = \sum_{\sigma(m)} \alpha_z(\sigma(m)) = 1$. So it suffices to consider this case. Let $m = x_1^{a_1} z_1^{c_1} \cdots x_k^{a_k} z_k^{c_k}$ be a monomial with zero y-rank such that all other monomials in its orbit have positive y-rank. Assume that $(d_1, d_2, \ldots, d_k)$ is the multidegree of m. Then we have $a_i = c_i$ for $1 \leq i \leq k$ because otherwise the permutation that interchanges x_i with z_i for $1 \leq i \leq k$ would send m to another distinct monomial in the orbit with zero y-rank, contradicting that m is the only monomial with zero y-rank in the orbit. Hence if d_i is non-zero for some i, it is at least two. First assume that $r(m)$ is one, that is $m = x_i^{a_i} z_i^{a_i}$ for some i. Then $o(m)$ is in the ideal generated by e_i, f_i, g_i by [7], hence $o(m) \in I$. We next assume $r(m) > 1$. Then there exist $1 \leq i < j \leq k$ such that $d_i \geq 2$ and $d_j \geq 2$. Then m_z is divisible by $z_i^2 z_j^2$, that is m_z is divisible $a_{i,j}$ and hence m_z is in I. We finish the proof by showing that $m_y \in I$ as well. Note that m_y is divisible by $y_i^2 y_j^2$. Then $m_y \equiv m_y + \frac{m_y f_i}{y_i^2} \equiv \frac{m_y z_i}{y_i} + \frac{m_y z_i^2}{y_i^2} \mod I$. But since y_j divides m_y, both $\frac{m_y z_i}{y_i}$ and $\frac{m_y z_i^2}{y_i^2}$ have positive y-rank and z-rank. Moreover they have the same multidegree and zero x-rank. Therefore by the previous lemma we get $\overline{(\frac{m_y z_i}{y_i})} = \overline{(\frac{m_y z_i^2}{y_i^2})}$. Therefore $m_y \equiv \frac{m_y z_i}{y_i} + \frac{m_y z_i^2}{y_i^2} \equiv 2\overline{(\frac{m_y z_i}{y_i})} = 0 \mod I$, as desired. □

Remark 14. *Note that the polynomial $b_{i,j,l} \in B$ for $1 \leq i < j < l \leq k$ is a combination of $u_{i,l}$ and $a_{j,l}$ hence is not needed in a minimal generating set for H. Therefore the previous theorem shows that H is always generated by polynomials up to degree three independently of the number k of the copies of the natural representation we consider. The reason for including $b_{i,j,l}$ is that they are needed in the Gröbner basis.*

We next show that the set B is the reduced Gröbner basis for the ideal H with respect to the order we fixed in the beginning of the section. A standard way to do this is to show that the polynomials in B satisfy the Buchberger's Criterion. We need to recall some definitions to describe this criterion. The s-polynomial $s(f_1, f_2)$ of two polynomials f_1, f_2 in R is defined to be $\frac{M}{\mathrm{LT}(f_1)} f_1 - \frac{M}{\mathrm{LT}(f_2)} f_2$, where M is the monic least common multiple of the leading monomials of f_1 and f_2, and $\mathrm{LT}(f)$

denotes the lead term of the polynomial f. Also for polynomials f, g, h in R, with $g \neq 0$, we say f reduces to h modulo g in one step if $\mathrm{LT}(g)$ divides a non-zero term T in f and $h = f - \frac{T}{\mathrm{LT}(g)}g$. We denote this by $f \equiv h \mod g$. For a set of non-zero polynomials $J = \{f_1, \ldots, f_s\}$ we say that f reduces to h modulo J, if there exists a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, s\}$ and a sequence of polynomials $f = h_0, h_1, \ldots, h_{t-1}, h_t = h$ such that $h_j \equiv h_{j+1} \mod f_{i_{j+1}}$ for $0 \leq j \leq t-1$. We denote this by $f \equiv h \mod J$. Buchberger Criterion says that a set of polynomials $J = \{f_1, f_2, \ldots, f_s\}$ in R is a Gröbner basis for the ideal they generate in R if and only if for $i \neq j$, we have $s(f_i, f_j) \equiv 0 \mod J$. For more back ground on this criterion we direct the reader to [1, §1].

Remark 15. *Assume the notation of Lemma 12. Note that all the reductions modulo B in the proof of Lemma 12 are obtained by dividing a monomial in the remainder with a leading monomial of a polynomial in B. Therefore the proof of Lemma 12 actually shows that $m \equiv \overline{m} \mod B$. It follows that two monomials m and m' with the same multidegree satisfying $r_x(m) = r_x(m') = 0$ and $r_y(m), r_y(m') > 0$, and $r_z(m), r_z(m') > 0$ reduce to the same monomial modulo B. Hence $m + m' \equiv 0 \mod B$. In this case we say m and m' cancel.*

Theorem 16. *The set B is the reduced Gröbner basis for H with respect to the lexicographic order with $x_i > y_i > z_i$ for $1 \leq i \leq k$ and $z_i > x_{i+1}$ for $1 \leq i \leq k-1$.*

Proof. It suffices to show that the s-polynomial of any pair of polynomials in B reduces to zero modulo B. A well known fact that we will use is that if the leading monomials of two polynomials are relatively prime then the s-polynomial of this pair reduces to zero. We will also be using the assertion of the previous remark frequently.

Let $\overline{B}$ be the subset of B containing the polynomials $\{u_{i,j} \mid 1 \leq i < j \leq k\}$, $\{p_{i,j,l} \mid 1 \leq i < j < l \leq k\}$ and $\{p_{i,j} \mid 1 \leq i < j \leq k\}$. We show that the s-polynomial of any two polynomials in $\overline{B}$ reduce to zero modulo B as follows. Notice that each polynomial in $\overline{B}$ is a sum of two monomials both of which have positive y-rank and z-rank. In particular, the s-polynomial of two polynomials in $\overline{B}$ will be either zero or a sum of two monomials with positive ranks with respect to y and z. It follows that this sum reduces to zero by the previous remark because these monomials have zero x-rank and the same multidegree.

We check the s-polynomial of every pair of polynomials in B when these polynomials are not simultaneously monomials. We follow the order of appearance in the list in the beginning of the section except for the cases cleared by the previous paragraph.

Note that since x_i does not divide any leading monomial in B other than itself we see that the s-polynomial of e_i with all other polynomials in B reduce to zero.

The polynomials in B whose leading term are not relatively prime to y_i^2 are $u_{i,j}$, $p_{t,i,l}$, $p_{t,j,i}$, $p_{i,j}$, $p_{t,i}$, $b_{j,t,i}$. We consider the s-polynomial of f_i with these ones. Note $s(f_i, u_{i,j}) = y_i z_i y_j + y_i z_i z_j + z_i^2 z_j$. By the previous remark, first two monomials cancel and third one is divisible by $a_{j,i}$. We have $s(f_i, p_{t,i,l}) = z_i^2 z_t y_l$ and this is zero modulo $a_{t,i}$. And $s(f_i, p_{t,j,i}) = y_i z_i z_t y_j + z_i^2 z_t y_j + y_i^2 z_t y_j$ reduces to zero because $z_i^2 z_t y_j$ is divisible by $a_{t,i}$ and the remaining two monomials cancel. Also $s(f_i, p_{i,j}) = z_i^3 y_j$ and this is divisible by g_i. Similarly, $s(f_i, p_{t,i}) = y_t z_t y_i z_i + z_t z_i^2 + z_t^2 y_i^2$ reduces to zero because the first and the third monomials cancel and the second one is divisible by $a_{t,i}$. Finally, $s(f_i, b_{j,t,i}) = z_j z_t z_i^2 y_i + z_j z_t z_i^3$ reduces to zero modulo $a_{j,i}$.

Next we consider the s-polynomials of g_i with other polynomials down the list. We have $s(g_i, u_{t,i}) = z_t y_i z_i^2$ and this is divisible by $a_{t,i}$. Also $s(g_i, p_{i,j,l}) = z_i^3 z_j y_l$ and $s(g_i, p_{i,j}) = z_i^4 y_j$ are both divisible by g_i.

Next polynomial down the list is $u_{i,j}$. Note that $s(u_{i,j}, a_{j,t}) = z_t^2 z_i y_j$ is divisible by $a_{i,t}$. Also $s(u_{i,j}, a_{t,j}) = z_i z_j z_t y_j$. This monomial is divisible by $a_{j,i}$ if $i = t$ and is equal to $b_{i,t,j}$ or $b_{t,i,j}$ otherwise, hence it reduces to zero. And $s(u_{i,j}, b_{q,l,i}) = y_j z_i^2 z_q z_l$ is divisible by $a_{q,i}$. We also have $s(u_{i,j}, b_{q,j,l}) = y_j z_i z_q y_l z_l$. This is divisible by $b_{i,q,l}$ if $i < q$, divisible by $b_{q,i,l}$ if $q < i$, and divisible by $a_{l,i}$ if $i = q$. Also $s(u_{i,j}, b_{q,l,j}) = z_q z_l z_i y_j^2$ reduces to $z_q z_l z_i y_j z_j + z_q z_l z_i z_j^2$ modulo f_j. This further reduces to zero modulo $b_{q,l,j}$ and $a_{i,j}$. The polynomial $s(u_{i,j}, b_{j,q,l})$ is seen to reduce to zero along the same lines.

Next we consider the s-polynomials of $a_{i,j}$ with the other members down the list. These polynomials are easily seen to reduce to zero modulo B because $s(a_{i,j}, p_{i,q,l})$, $s(a_{i,j}, p_{j,q,l})$, $s(a_{i,j}, p_{i,q})$ and $s(a_{i,j}, p_{j,q})$ are all divisible by $a_{i,j}$.

As for the s-polynomials of $p_{i,j,l}$, it is easy to see that $s(p_{i,j,l}, b_{i,q,t})$, $s(p_{i,j,l}, b_{i,q,j})$, $s(p_{i,j,l}, b_{i,q,l})$, $s(p_{i,j,l}, b_{q,i,t})$, $s(p_{i,j,l}, b_{q,i,j})$ and $s(p_{i,j,l}, b_{q,i,l})$ are divisible by $b_{i,q,t}$, $a_{i,j}$, $b_{i,q,l}$, $b_{q,i,t}$, $a_{i,j}$ and $b_{q,i,l}$ respectively. Moreover $s(p_{i,j,l}, b_{q,t,i})$, $s(p_{i,j,l}, b_{q,t,j})$ and $s(p_{i,j,l}, b_{q,t,l})$ are divisible by $b_{q,t,i}$, $a_{i,j}$ and $b_{q,t,l}$ respectively.

We finish with the s-polynomials of $p_{i,j}$ with $b_{q,t,l}$. Let m denote the least common multiple of $p_{i,j}$ and $b_{q,t,l}$ where the sets $\{i,j\}$ and $\{q,t,l\}$ not necessarily disjoint. Then $r_z(\frac{m}{y_i z_i y_j})$ is positive and so there exists $1 \leq r \leq k$ such that z_r divides $\frac{m}{y_i z_i y_j}$ and therefore $s(p_{i,j,l}, b_{q,t,l})$ is divisible by $z_i^2 z_r$. Hence this monomial is divisible by $a_{r,i}$ if $i \neq r$ and by g_i if $i = r$. □

References

[1] William W. Adams and Philippe Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[2] Jean-Marie Arnaudiès and Annick Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118:23–40, 1997. Algorithms for algebra (Eindhoven, 1996).

[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(1):1–20, 1997.

[4] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[5] Peter Fleischmann. The Noether bound in invariant theory of finite groups. *Adv. Math.*, 156(1):23–32, 2000.

[6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007.

[7] Teo Mora and Massimiliano Sala. On the Gröbner bases of some symmetric systems and their application to coding theory. *J. Symbolic Comput.*, 35(2):177–194, 2003.

[8] Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.

[9] Müfit Sezer. A note on the Hilbert ideals of a cyclic group of prime order. *J. Algebra*, 318(1):372–376, 2007.

[10] Müfit Sezer and R. James Shank. On the coinvariants of modular representations of cyclic groups of prime order. *J. Pure Appl. Algebra*, 205(1):210–225, 2006.

[11] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

[12] Takashi Wada and Hidefumi Ohsugi. Gröbner bases of Hilbert ideals of alternating groups. *J. Symbolic Comput.*, 41(8):905–908, 2006.

Department of Mathematics, Bilkent University, Ankara 06800 Turkey