MINIMAL GENERATORS FOR INVARIANT IDEALS IN INFINITE DIMENSIONAL POLYNOMIAL RINGS

CHRISTOPHER J. HILLAR AND TROELS WINDFELDT

ABSTRACT. Let K be a field, and let $R = K[X]$ be the polynomial ring in an infinite collection X of indeterminates over K. Let $\mathfrak{S}_X$ be the symmetric group of X. The group $\mathfrak{S}_X$ acts naturally on R, and this in turn gives R the structure of a left module over the group ring $R[\mathfrak{S}_X]$. A recent theorem of Aschenbrenner and Hillar states that the module R is Noetherian. We address whether submodules of R can have any number of minimal generators, answering this question positively. As a corollary, we show that there are invariant ideals of R with arbitrarily large minimal Gröbner bases. We also describe minimal Gröbner bases for monomially generated submodules.

1. INTRODUCTION

Let X be an infinite collection of indeterminates, and let $\mathfrak{S}_X$ be the group of permutations of X. Fix a field K and let $R = K[X]$ be the polynomial ring in the indeterminates X. The group $\mathfrak{S}_X$ acts naturally on R: if $\sigma \in \mathfrak{S}_X$ and $f \in K[x_1, \ldots, x_n]$ where $x_i \in X$, then

$$\sigma f(x_1, x_2, \ldots, x_n) = f(\sigma x_1, \sigma x_2, \ldots, \sigma x_n) \in R. \tag{1.1}$$

We let $R[\mathfrak{S}_X]$ be the (left) group ring of $\mathfrak{S}_X$ over R with multiplication given by $f\sigma \cdot g\tau = fg(\sigma\tau)$ for $f, g \in R$, $\sigma, \tau \in \mathfrak{S}_X$. The action (1.1) naturally gives R the structure of a left module over the ring $R[\mathfrak{S}_X]$. An ideal $I \subseteq R$ is called *invariant under* $\mathfrak{S}_X$ (or simply *invariant*) if

$$\mathfrak{S}_X I := \{\sigma f : \sigma \in \mathfrak{S}_X,\ f \in I\} \subseteq I.$$

Invariant ideals are then simply the $R[\mathfrak{S}_X]$-submodules of R. The following was proved recently in [1]:

Theorem 1.1. *Every invariant ideal of R is finitely generated as an $R[\mathfrak{S}_X]$-module. In other words, R is a Noetherian $R[\mathfrak{S}_X]$-module.*

Theorem 1.1 was motivated by finiteness questions in chemistry [3, 4, 5] and algebraic statistics [7] involving chains of invariant ideals I_k $(k = 1, 2, \ldots)$ contained in finite dimensional polynomial rings R_k. We refer the reader to [1] for more details.

In the course of proving Theorem 1.1, it was shown that, in a certain sense, an invariant ideal I has a finite minimal Gröbner basis (see Section 3 for a review of

1991 *Mathematics Subject Classification.* 13E05, 13E15, 20B30, 06A07.

Key words and phrases. Invariant ideal, well-quasi-ordering, symmetric group, Gröbner basis, minimal generators.

The work of the first author is supported under a National Science Foundation Graduate Research Fellowship. This work was conducted during the Special Semester on Gröbner Bases, February 1 – July 31, 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

these concepts). However, it was not known whether one can have arbitrarily large numbers of elements in such a set of generators. In fact, the more basic question of whether the $R[\mathfrak{S}_X]$-module I is cyclic was already asked by Schicho [6].

To simplify our exposition, in what follows, we work with an infinite set $X = \{x_1, x_2, x_3, \ldots\}$ of indeterminates, indexed by the positive integers, although as already remarked in [1], this is not really a restriction. In this case, $\mathfrak{S}_X$ is naturally identified with $\mathfrak{S}_\infty$, the set of permutations of the positive integers, and $\sigma x_i = x_{\sigma i}$ for $\sigma \in \mathfrak{S}_\infty$. For a positive integer N, we will also let $\mathfrak{S}_N$ denote the set of permutations of $\{1, \ldots, N\}$. We give an answer to the above questions by proving that there are ideals with arbitrarily large number of generators.

Theorem 1.2. *For every positive integer n, there are invariant ideals of R generated by n polynomials which cannot have fewer than n $R[\mathfrak{S}_\infty]$-generators.*

Corollary 1.3. *There are invariant ideals of R with arbitrarily large minimal Gröbner bases.*

Using the results of Section 3, we also describe an explicit family of finite, minimal Gröbner bases that makes the statement of Corollary 1.3 more concrete. This will be the content of Theorem 3.14 below.

At first glance, Theorem 1.2 is a bit surprising. If one picks even a single polynomial $g \in R$, the cyclic submodule $R[\mathfrak{S}_X] \cdot g$ is very large, and it is not clear that every submodule of R doesn't arise in this way. Given a finite list of polynomials $f_1, \ldots, f_k$, one could conceivably choose a sufficiently large enough N so that the number of unknowns in a system

$$f_i = \sum_{\sigma \in \mathfrak{S}_N} r_{i\sigma} \sigma g, \quad r_{i\sigma} \in R, \ i = 1, \ldots, k,$$

greatly outnumbers the number of equations, thereby (presumably) ensuring a solution for the $r_{i\sigma}$.

We prove Theorem 1.2 in Section 4, using the notation found in Section 2. A brief review of the terminology and results of [1] is found in Section 3, including a new characterization (Theorem 3.13) of an important partial order on monomials introduced by the authors of [1]. Using this characterization, an explicit description of minimal Gröbner bases for monomial submodules is given by Thereom 3.14.

2. Monomials, Multisets, and Partitions

In this section, we provide the basic notation used in our proof of Theorem 1.2. Formally, a *multiset* $M = (A, m)$ is a set A along with a *multiplicity function* $m : A \to \mathbb{N}$ which assigns to each element $a \in A$ a *multiplicity* $m(a)$. In what follows, the set A will always be the set of positive integers and m will be a function with finite support; that is, m will be nonzero for only finitely many elements of A. For notational simplicity, we will frequently view M as a finite set of positive integers with repetitions allowed as in $\{1, 1, 2, 7\}$, and any indexing over elements of M will respect the multiplicities of M given by the function m.

Let $M = (A, m)$ be a multiset and let $i_1, i_2, \ldots, i_k$ be the list elements of A with nonzero multiplicity, arranged so that $m(i_1) \geq m(i_2) \geq \cdots \geq m(i_k)$. The *type* of a multiset M is the partition $\lambda(M) = (m(i_1), m(i_2), \ldots, m(i_k))$ that corresponds to the multiplicities of elements in M. For instance, the multiset $M = \{1, 1, 1, 2, 3, 3\}$ has type $\lambda(M) = (3, 2, 1)$.

Multisets are in natural bijection with monomials of $K[X]$. Given a multiset $M = (A, m)$, we can construct the monomial:

$$\mathbf{x}_M^{\lambda(M)} = \prod_{i \in M} x_i = \prod_{i \in A} x_i^{m(i)}.$$

Conversely, given a monomial, the associated multiset is the set of indices appearing in it, along with multiplicities.

The action of $\mathfrak{S}_\infty$ on monomials coincides with the natural action of $\mathfrak{S}_\infty$ on multisets $M = (A, m)$: $\sigma M = (A, \sigma m)$, in which $\sigma m : A \to \mathbb{Z}$ is the function $\sigma m(i) = m(\sigma i)$. It easy to see that the action of $\mathfrak{S}_\infty$ preserves the type of a multiset (resp. monomial).

Lemma 2.1. *Let M be a multiset, $\lambda = \lambda(M)$, and $\sigma \in \mathfrak{S}_\infty$. Then $\sigma \mathbf{x}_M^\lambda = \mathbf{x}_{\sigma M}^\lambda$.*

Finally, we note that an infinite permutation acting on a polynomial may be replaced with a finite one.

Lemma 2.2. *Let $\sigma \in \mathfrak{S}_\infty$ and $f \in R$. Then there exists a positive integer N and $\tau \in \mathfrak{S}_N$ such that $\tau f = \sigma f$.*

Proof. Let S be the set of indices appearing in the monomials of f and let m be the largest integer in $\sigma S \cup S$. The injective function $\sigma : S \to \{1, \ldots, m\}$ extends (nonuniquely) to a permutation $\tau \in \mathfrak{S}_m$ such that $\tau f = \sigma f$. □

3. Gröbner Bases for Invariant Ideals

We briefly review the Gröbner basis theory for invariant ideals necessary for our proof of Theorem 3.14 below (see [1] for more details). For the purposes of this work, we will use the following notation. Let B be a ring and let G be a subset of a B-module M. Then $\langle f : f \in G \rangle_B$ will denote the B-submodule of M generated by elements of G.

Let Ω be the set of monomials in indeterminates $x_1, x_2, \ldots$, including the empty monomial 1. Order the variables $x_1 < x_2 < \cdots$, and let $\leq$ be the induced lexicographic (total) well-ordering of monomials. Given a polynomial $f \in R$, we set $\mathrm{lm}(f)$ to be the leading monomial of f with respect to $\leq$. The following partial ordering on Ω respects the action of $\mathfrak{S}_\infty$ and refines the division partial order on Ω.

Definition 3.1. (The symmetric cancellation partial ordering)

$$v \preceq w \quad :\Longleftrightarrow \quad \begin{cases} v \leq w \text{ and there exist } \sigma \in \mathfrak{S}_\infty \text{ such that } \sigma v | w \\ \text{and } \sigma u \leq \sigma v \text{ for all } u \leq v. \end{cases}$$

Remark 3.2. A permutation σ in the definition need not be unique. Also, we say that such a permutation σ *witnesses* $v \preceq w$. We will give a more computationally useful description of this partial order in Theorem 3.13 below.

Example 3.3. As an example of this relation, consider the following chain,

$$x_1^3 \preceq x_1^2 x_2^3 \preceq x_1 x_2^2 x_3^3.$$

To verify the first inequality, notice that $x_1^2 x_2^3 = x_1^2 \sigma(x_1^3)$, in which σ is the transposition (12). If $u = x_1^{u_1} \cdots x_n^{u_n} \leq x_1^3$, then it follows that $n = 1$ and $u_1 \leq 3$. In particular, $\sigma u = x_2^{u_1} \leq x_2^3 = \sigma x_1^3$. Verification of the other inequality is similar. □

Although this partial order appears technical, it can be reconstructed from the following two properties. The first one says that the leading monomial of σf is the same as $\sigma \mathrm{lm}(f)$ whenever there is a witness σ for $\mathrm{lm}(f)$, while the latter can be viewed as a kind of "S-pair" leading term cancellation.

Lemma 3.4. *Let f be a nonzero polynomial and $w \in \Omega$. Suppose that $\sigma \in \mathfrak{S}_\infty$ witnesses $\mathrm{lm}(f) \preceq w$, and let $u \in \Omega$ with $u\sigma\mathrm{lm}(f) = w$. Then $\mathrm{lm}(u\sigma f) = u\sigma\mathrm{lm}(f)$.*

Lemma 3.5. *Suppose that $m_1 \preceq m_2$ and f_1, f_2 are two polynomials with lexicographic leading monomials m_1 and m_2, respectively. Then there exists a permutation σ and $c \in K^*$ such that*

$$h = f_2 - c\frac{m_2}{\sigma m_1}\sigma f_1$$

consists of monomials (lexicographically) smaller than m_2.

The following lemmas allow us to generate many relations, including the ones in the above example.

Lemma 3.6. *Suppose that $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^{b_1} \cdots x_n^{b_n}$ where $a_i, b_j \in \mathbb{N}$, $b_n > 0$. Then for any $c \in \mathbb{N}$ we have $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^c x_2^{b_1} \cdots x_{n+1}^{b_n}$.*

Lemma 3.7. *If $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^{b_1} \cdots x_n^{b_n}$, where $a_i, b_j \in \mathbb{N}$, $b_n > 0$, and $a, b \in \mathbb{N}$ are such that $a \leq b$, then $x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n} \preceq x_1^b x_2^{b_1} \cdots x_{n+1}^{b_{n+1}}$.*

The following fact is essentially a consequence of [1, Lemma 2.14], but we include an argument for completeness.

Lemma 3.8. *Let $u, v \in \Omega$ and set n to be the largest index of indeterminates appearing in v. If $u \preceq v$, then there is a witness $\sigma \in \mathfrak{S}_n$, and if $a, b \in \mathbb{N}$ are such that $a \leq b$, then $ux_{n+1}^a \preceq vx_{n+1}^b$.*

Proof. Let m (resp. n) be the largest integer such that $x_m | u$ (resp. $x_n | v$) and let σ be a witness to $u \preceq v$. We first claim that $\sigma x_i \leq x_n$ for all $i \leq m$. To see this, suppose by way of contradiction that $\sigma x_i > x_n$ for some $i \leq m$. We have $\sigma u | v$, so if $x_i | u$, then $\sigma x_i | v$, contradicting $\sigma x_i > x_n$. In particular $x_i < x_m$, which yields $x_i < u$ and thus $\sigma x_i < \sigma u \leq v$, again contradicting $\sigma x_i > x_n$. It follows that $\sigma \restriction \{x_i : i \leq m\}$ can be extended to a permutation σ' of the set $\{x_i : i \leq n\}$. Furthermore, extending σ' to a permutation in $\mathfrak{S}_\infty$ by setting $\sigma'(x_i) = x_i$ for all $i > n$, it is easy to see that σ' still witnesses $u \preceq v$. The second claim in the lemma follows immediately from the first. □

In this setting, we need a notion of the leading monomials of a set of polynomials that interacts with the symmetric group action. For a set of polynomials I, we define

$$\mathrm{lm}(I) = \langle w : \mathrm{lm}(f) \preceq w,\ 0 \neq f \in I \rangle_K,$$

the span of all monomials which are $\preceq$ larger than leading monomials in I. If I happens to be an invariant ideal, then it follows from Lemma 3.4 that

$$\mathrm{lm}(I) = \langle \mathrm{lm}(f) : f \in I \rangle_K$$

corresponds to a more familiar set of monomials. With these preliminaries in place, we make the following definition.

Definition 3.9. We say that a subset B of an invariant ideal $I \subseteq R$ is a *Gröbner basis* for I if $\mathrm{lm}(B) = \mathrm{lm}(I)$.

Additionally, a Gröbner basis is called *minimal* if no leading monomial of an element in B is $\preceq$ smaller than any other leading monomial of an element in B. In analogy to the classical case, a Gröbner basis B generates the ideal I:

$$I = \langle B \rangle_{R[\mathfrak{S}_\infty]}.$$

The authors of [1] prove the following finiteness result for invariant ideals; it is an analog to the corresponding statement for finite dimensional polynomial rings. As a corollary, they obtain Theorem 1.1.

Theorem 3.10. *An invariant ideal of R has a finite Gröbner basis.*

Although much of the intuition involving Gröbner bases from the finite dimensional case transfers over faithfully to the ring R, one needs to be somewhat careful in general. For example, monomial generators do not automatically form a Gröbner basis for an invariant ideal I (see example 3.16 below). However, we do have Theorem 3.14 below. To state it, we need to introduce a special class of permutations to give a more workable description of the symmetric cancellation partial order.

Fix a monomial $g = \mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$. A *downward elementary shift* (resp. *upward elementary shift*) of g is a permutation σ which acts on $\mathbf{a}$ as transposition of two consecutive coordinates, the smaller (resp. larger) of which is zero. A *downward shift* (resp. *upward shift*) of g is a product of downward elementary shifts (resp. upward elementary shifts) that begin with g. A *shift permutation* of g is either a downward shift or an upward shift of g. If $g, h \in \Omega$ and σ is an upward shift of g with $h = \sigma g$, then we write $g \sim_\sigma h$. For example, $\sigma = (341)$ is an upward elementary shift of $g = x_2^3 x_3 x_5^2$ and $\tau = (32)(56)(341)$ is an upward shift of g; in this case, $g \sim_\tau h$ for $h = x_3^3 x_4 x_6^2$.

A more concrete description of these permutations is given by the following straightforward lemma, which follows directly from the definitions.

Lemma 3.11. *Let g be a monomial, and let $\{i_1, \ldots, i_n\}$ be the set of indices appearing in the indeterminates dividing g. Then σ is an upward shift permutation of g if and only if*

$$\sigma i_1 < \sigma i_2 < \cdots < \sigma i_n \quad \text{and} \quad \sigma(i_k) \geq i_k, \ j = 1, \ldots, n.$$

The following fact gives a relationship between shift permutations and the symmetric cancellation partial order.

Lemma 3.12. *Let h and g be monomials with $g \sim_\sigma h$ for some $\sigma \in \mathfrak{S}_\infty$. Then $g \preceq h$. Moreover, we have $h \sim_{\sigma^{-1}} g$.*

Proof. Suppose that σ as in the statement of the lemma acts on g by transposing x_n and x_{n+1}. Write $g = x_1^{a_1} \cdots x_n^{a_n} x_{n+2}^{a_{n+2}} \cdots x_m^{a_m}$ with $a_m > 0$; we must verify that

$$x_1^{a_1} \cdots x_n^{a_n} x_{n+2}^{a_{n+2}} \cdots x_m^{a_m} \preceq x_1^{a_1} \cdots x_{n-1}^{a_{n-1}} x_{n+1}^{a_n} x_{n+2}^{a_{n+2}} \cdots x_m^{a_m}.$$

This is proved by induction on m. When $m = 1$, we have $n = 1$, and the claim reduces to Lemma 3.6. In general, we have two cases to consider. If $n = m > 1$, then the claim follows from Lemma 3.7 and induction. Alternatively, if $n < m$ and $m > 1$, then we may apply Lemma 3.8 and induction. The second claim is clear from the definitions. □

We now state and prove a characterization of the symmetric cancellation partial order.

Theorem 3.13. *Two monomials v and w satisfy $v \preceq w$ if and only if there is an upward shift σ of v and a monomial m such that $w = m\sigma v$.*

Proof. We prove the only-if direction ($\Rightarrow$); the converse is clear from Lemma 3.12 and Definition 3.1. Let N be the largest index of indeterminates appearing in w. If $v \preceq w$, then there is a monomial m and a witness $\sigma \in \mathfrak{S}_N$ such that $w = m\sigma v$ by Lemma 3.8. For the rest of the argument, we fix this permutation σ. We will prove that σ is an upward shift of v using the characterization found in Lemma 3.11.

Write $v = x_{i_1}^{v_{i_1}} \cdots x_{i_n}^{v_{i_n}}$, in which $i_1 < \cdots < i_n$ are all the indices appearing in v. The following claim will be proved by induction on the number of indeterminates n appearing in v:

$$u \leq v \Rightarrow \sigma u \leq \sigma v \text{ for all } u \in \Omega \text{ implies } \sigma i_1 < \cdots < \sigma i_n \text{ and } i_k \leq \sigma i_k \text{ for all } k \leq n.$$

The result in the theorem is then implied by Lemma 3.11. We take for our base case of induction $n = 0$ (so that $v = 1$), as the statement is vacuously true. Also, if $n = 1$ and $i_1 = 1$, then the statement is clear, so we suppose from now on that $i_n > 1$.

In general, let $u = (x_1 \cdots x_{i_n - 1})^c \leq v$ for a positive integer c, and suppose that for all c,

$$\sigma u = (x_{\sigma 1} \cdots x_{\sigma(i_n - 1)})^c \leq x_{\sigma i_1}^{v_{i_1}} \cdots x_{\sigma i_n}^{v_{i_n}} = \sigma v.$$

If $\sigma i_n \leq \sigma i_j$ for some $j < n$, then by choosing c sufficiently large, the above inequality is impossible. Therefore, it follows that $\sigma i_j < \sigma i_n$ for all $j < n$; it remains to show that $i_n \leq \sigma i_n$. Suppose by way of contradiction that $\sigma i_n < i_n$. Then, $\sigma i_j < i_n$ for all $j = 1, \ldots, n$. In particular, $\sigma v < v$, and thus $\sigma^k v \leq \sigma v < v$ for all positive integers k. Hence, $v = \sigma^{N!} v < v$, a contradiction.

Next, suppose that $u = x_1^{u_1} \cdots x_{i_{n-1}}^{u_{i_{n-1}}} \leq x_{i_1}^{v_{i_1}} \cdots x_{i_{n-1}}^{v_{i_{n-1}}}$. By assumption, we have

$$\sigma(u x_{i_n}^{v_{i_n}}) = (\sigma u) x_{\sigma i_n}^{v_{i_n}} \leq x_{\sigma i_k}^{v_{i_k}} \cdots x_{\sigma i_n}^{v_{i_n}} = \sigma v,$$

so that (since we are using the lexicographic ordering)

$$\sigma u \leq x_{\sigma i_k}^{v_{i_k}} \cdots x_{\sigma i_{n-1}}^{v_{i_{n-1}}}.$$

It follows from induction applied to $x_{i_1}^{v_{i_1}} \cdots x_{i_{n-1}}^{v_{i_{n-1}}}$ that $\sigma i_1 < \cdots < \sigma i_{n-1}$ and $i_k \leq \sigma i_k$ for all $k \leq n-1$. This proves the claim and completes the proof of the lemma. □

We may now prove the main result of this section.

Theorem 3.14. *Let G be a set of n monomials of degree d having distinct types, and let N be the largest index of indeterminates appearing in G. Then $H = \mathfrak{S}_N G$ is a (finite) Gröbner basis for $I = \langle G \rangle_{R[\mathfrak{S}_\infty]}$. Moreover, if we let*

$$S = \{h \in H : \text{ there exists } g \in H \backslash \{h\}, \sigma \in \mathfrak{S}_N \text{ with } g \sim_\sigma h\},$$

then $H \backslash S$ is a minimal Gröbner basis for I.

Proof. Let G, H, S, N, and I be as in the statement of the theorem; we first show that H is a Gröbner basis for I. The inclusion $\mathrm{lm}(H) \subseteq \mathrm{lm}(I)$ is clear from the definition. So suppose that $w \in \mathrm{lm}(I)$ is a monomial; we must show that $h \preceq w$ for some $h \in H$. Set $w = u\sigma g$ for some monomial u, witness $\sigma \in \mathfrak{S}_\infty$, and $g \in G$. Since $\sigma g \preceq u\sigma g = w$, it suffices to show that $h \preceq \sigma g$ for some $h \in H$. Let τ be a downward shift that takes σg to a monomial h with indices at most N. Then h has

the same type as g, and therefore there is a permutation $\gamma \in \mathfrak{S}_N$ such that $h = \gamma g$. It follows that $h \in H$ and $h \sim_{\tau^{-1}} \sigma g$ so that $h \preceq \sigma g$ by Lemma 3.12.

Next, we observe that $H \backslash S$ is still a Gröbner basis since $g \sim_\sigma h$ implies that $g \preceq h$. Therefore, it remains to prove that $H \backslash S$ is minimal. If $h, g \in H$ are related by $g \preceq h$, then $h = m\sigma g$ for a witness σ and a monomial m. Since each element of H has the same degree, we have $m = 1$. By Theorem 3.13, it follows that we may choose $\sigma \in \mathfrak{S}_N$ such that $g \sim_\sigma h$. Therefore, we are only removing unnecessary elements from the Gröbner basis H when we discard the monomials in S. This completes the proof. □

Corollary 3.15. *Let G be a finite set of monomials, and let N be the largest index of indeterminates appearing in G. Then $\mathfrak{S}_N G$ is a (not necessarily minimal) Gröbner basis for $I = \langle G \rangle_{R[\mathfrak{S}_\infty]}$.*

Example 3.16. The ideal $I = \langle x_1^2 x_3 \rangle_{R[\mathfrak{S}_\infty]}$ has a Gröbner basis,

$$H = \{x_1 x_2^2, x_1 x_3^2, x_1^2 x_2, x_2 x_3^2, x_1^2 x_3, x_2^2 x_3\}.$$

However, it is not minimal. Removing those elements that are the result of upward shifts, we are left with the following minimal Gröbner basis for I: $\{x_1 x_2^2, x_1^2 x_2\}$. □

4. Proof of Theorem 1.2

We will derive Theorem 1.2 as a direct corollary of the following result.

Theorem 4.1. *Let $G = \{g_1, \ldots, g_n\}$ be a set of monomials of degree d with distinct types and fix a matrix $C = (c_{ij}) \in K^{n \times n}$ of rank r. Then the submodule $\langle f_1, \ldots, f_n \rangle_{R[\mathfrak{S}_\infty]} \subseteq R$ generated by the n polynomials,*

$$f_j = \sum_{i=1}^{n} c_{ij} g_i, \ j = 1, \ldots, n,$$

cannot be generated with fewer than r polynomials.

Proof. Suppose that $p_1, \ldots, p_k$ are generators for $I = \langle f_1, \ldots, f_n \rangle_{R[\mathfrak{S}_\infty]}$ with the f_j as in the statement of the theorem; we prove that $k \geq r$. Note that each f_j is homogeneous of degree d. Since each $p_l \in I$, it follows that each is a linear combination, over $R[\mathfrak{S}_\infty]$, of monomials in G. Therefore, each monomial occurring in p_l has degree at least d, and, moreover, any degree d monomial in p_l has the same type as one of the monomials in G (c.f. Lemma 2.1).

Write each of the monomials in G in the form $g_i = \mathbf{x}_{M_i}^{\lambda_i}$ for multisets $M_1, \ldots, M_n$ with corresponding distinct types $\lambda_1, \ldots, \lambda_n$. Then we can express each generator p_l in the following form:

$$p_l = \sum_{i=1}^{n} \sum_{\lambda(M) = \lambda_i} u_{ilM} \mathbf{x}_M^{\lambda_i} \ + \ q_l, \tag{4.1}$$

in which $u_{ilM} \in K$ with only finitely many of them nonzero, each monomial appearing in q_l has degree greater than d, and the inner sum is over all multisets M with type λ_r.

Since each polynomial in $\{f_1, \ldots, f_n\}$ is a finite linear combination of the p_l, and since only finitely many positive integers are indices of monomials appearing in $p_1, \ldots, p_k$, it follows that we may pick a positive integer N large enough so that

all of these linear combinations can be expressed with coefficients in the subring $R[\mathfrak{S}_N]$ (c.f. Lemma 2.2). Therefore, we have,

$$f_j = \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} s_{lj\sigma} \sigma p_l, \tag{4.2}$$

for some polynomials $s_{lj\sigma} \in R$. Substituting the expressions found in (4.1) into (4.2) produces

$$\begin{aligned} f_j &= \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} s_{lj\sigma} \left(\sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} u_{ilM} \mathbf{x}_{\sigma M}^{\lambda_i} \; + \; \sigma q_l \right) \\ &= \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM} \mathbf{x}_{\sigma M}^{\lambda_i} \; + h, \end{aligned}$$

in which $h \in R$ has degree greater than d and $v_{lj\sigma}$ are the constant terms of $s_{lj\sigma}$. Since $\deg(f_j) = d$, we must have that $h = 0$. It follows that

$$\sum_{i=1}^{n} c_{ij} \mathbf{x}_{M_i}^{\lambda_i} = \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM} \mathbf{x}_{\sigma M}^{\lambda_i}.$$

Next, for a fixed i, take the sum on each side in this last equation of the coefficients of monomials with the type λ_i. This produces the n^2 equations:

$$\begin{aligned} c_{ij} &= \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM} \\ &= \sum_{l=1}^{k} \left(\sum_{\lambda(M)=\lambda_i} u_{ilM} \right) \left(\sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma} \right) \\ &= \sum_{l=1}^{k} U_{il} V_{lj}, \end{aligned} \tag{4.3}$$

in which

$$U_{il} = \sum_{\lambda(M)=\lambda_l} u_{ilM} \quad \text{and} \quad V_{lj} = \sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma}.$$

Set V to be the $k \times n$ matrix (V_{lj}) and similarly let U denote the $n \times k$ matrix (U_{il}). The n^2 equations (4.3) can be viewed compactly as matrix multiplication:

$$\begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{bmatrix} = \begin{bmatrix} U_{11} & \cdots & U_{1k} \\ \vdots & \ddots & \vdots \\ U_{n1} & \cdots & U_{nk} \end{bmatrix} \begin{bmatrix} V_{11} & \cdots & V_{1n} \\ \vdots & \ddots & \vdots \\ V_{k1} & \cdots & V_{kn} \end{bmatrix}.$$

Considering the rank of both sides of the equation $C = UV$ leads to the following chain of inequalities:

$$r = \operatorname{rank}(C) = \operatorname{rank}(UV) \leq \min\{\operatorname{rank}(U), \operatorname{rank}(V)\} \leq \min\{n, k\} \leq k.$$

Therefore, we have $k \geq r$, and this completes the proof. □

Corollary 4.2. *Let G be a set of n monomials of degree d having distinct types. Then $I = \langle G \rangle_{R[\mathfrak{S}_\infty]}$ cannot be generated by fewer than n elements.*

Proof. Apply Theorem 4.1 with the set G and the $n \times n$ identity matrix $C = (\delta_{ij})$. □

Theorem 1.2 from the introduction follows easily from this.

References

[1] M. Aschenbrenner and C. Hillar, *Finite generation of symmetric ideals*, Trans. Amer. Math. Soc., to appear.

[2] D. Cox, J. Little, D. O'Shea, *Using algebraic geometry*, Springer, New York, 1998.

[3] A. Mead, E. Ruch, A. Schönhofer, *Theory of chirality functions, generalized for molecules with chiral ligands.* Theor. Chim. Acta **29** (1973), 269–304.

[4] E. Ruch, A. Schönhofer, *Theorie der Chiralitätsfunktionen*, Theor. Chim. Acta **19** (1970), 225–287.

[5] E. Ruch, A. Schönhofer, I. Ugi, *Die Vandermondesche Determinante als Näherungsansatz für eine Chiralitätsbeobachtung, ihre Verwendung in der Stereochemie und zur Berechnung der optischen Aktivität*, Theor. Chim. Acta **7** (1967), 420–432.

[6] J. Schicho, private communication, 2006.

[7] B. Sturmfels and S. Sullivant, *Algebraic factor analysis: tetrads, pentads and beyond*, preprint. (math.ST/0509390).

Department of Mathematics, Texas A&M University, College Station, TX 77843
E-mail address: chillar@math.tamu.edu

Department of Mathematics, University of Copenhagen, Denmark.
E-mail address: windfeldt@math.ku.dk