AN ALGORITHM FOR FINDING SYMMETRIC GRÖBNER BASES

ABSTRACT. We give an explicit algorithm to find Gröbner bases for symmetric ideals in infinite dimensional polynomials rings. This allows for symbolic computation in a new class of rings.

1. INTRODUCTION

Let $X = \{x_1, x_2, \ldots\}$ be an infinite collection of indeterminates, indexed by the positive integers, and let $\mathfrak{S}_\infty$ be the group of permutations of X. For a positive integer N, we will also let $\mathfrak{S}_N$ denote the set of permutations of $\{1, \ldots, N\}$. Fix a field K and let $R = K[X]$ be the polynomial ring in the indeterminates X. The group $\mathfrak{S}_\infty$ acts naturally on R: if $\sigma \in \mathfrak{S}_\infty$ and $f \in K[x_1, \ldots, x_n]$, then

$$\sigma f(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n}) \in R. \tag{1.1}$$

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

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

Invariant ideals are then simply the $R[\mathfrak{S}_\infty]$-submodules of R.

The following was proved recently in [1]. It says that while ideals of R are too big in general, those with extra structure have finite presentations.

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

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 the elements of G.

Example 1.2. $I = \langle x_1, x_2, \ldots\rangle_R$ is an invariant ideal of R. Written as a module over the group ring $R[\mathfrak{S}_\infty]$, it has the compact presentation $I = \langle x_1\rangle_{R[\mathfrak{S}_\infty]}$.

Theorem 1.1 was motivated by finiteness questions in chemistry [4, 5, 6] and algebraic statistics [8] 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 2 for a review of these concepts). Moreover, the existence of such a set of generators solves the ideal membership problem in R.

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.

Theorem 1.3. *Let G be a Gröbner basis for an invariant ideal I. Then $f \in I$ if and only if f has normal form 0 with respect to G.*

Example 1.4. Let $I = \langle x_1 + x_2, x_1 x_2 \rangle_{R[\mathfrak{S}_\infty]}$. Then, a Gröbner basis for I is given by $G = \{x_1\}$. It is important to note that we may not simply restrict consideration to $K[x_1, x_2]$ to produce this result since

$$\langle x_1 + x_2, x_1 x_2 \rangle_{R[\mathfrak{S}_2]} \neq \langle x_1 \rangle_{R[\mathfrak{S}_2]}.$$

Example 1.5. The ideal $I = \langle x_1^3 x_3 + x_1^2 x_2^3, x_2^2 x_3^2 - x_2^2 x_1 + x_1 x_3^2 \rangle_{R[\mathfrak{S}_\infty]}$ has a Gröbner basis given by:

$$G = \mathfrak{S}_3 \cdot \{x_3 x_2 x_1^2, x_3^2 x_1 + x_2^4 x_1 - x_2^2 x_1, x_3 x_1^3, x_2 x_1^4, x_2^2 x_1^2\}.$$

Once G is found, testing whether a polynomial f is in I is computationally fast. □

The normal form reduction we are talking about here is a modification of the standard notion in polynomial theory and Gröbner bases; we describe it in more detail in Section 2. Unfortunately, the techniques used to prove finiteness in [1] are nonconstructive and therefore do not give methods for computing Gröbner bases in R. Our main result is an algorithm for finding these bases.

Theorem 1.6. *Let $I = \langle f_1, \ldots, f_n \rangle_{R[\mathfrak{S}_\infty]}$ be an invariant ideal of R. There exists an effective algorithm to compute a finite minimal Gröbner basis for I.*

Corollary 1.7. *There exists an effective algorithm to solve the ideal membership problem for symmetric ideals in the infinite dimensional ring $K[x_1, x_2, \ldots]$.*

A brief review of the terminology and results of [1] is found in Section 3, including a new characterization (Theorem 2.16) 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 2.17.

In Section 4, we describe our algorithm, and examples from an implementation can be found in the subsequent section. Finally, we prove correctness in Section 6.

2. Gröbner Bases for Invariant Ideals

We first note that an infinite permutation acting on a polynomial may be replaced with a finite one.

Lemma 2.1. *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 N be the largest integer in $\sigma S \cup S$. The injective function $\sigma : S \to \{1, \ldots, N\}$ extends (nonuniquely) to a permutation $\tau \in \mathfrak{S}_N$ such that $\tau f = \sigma f$. □

The following is a brief review of the Gröbner basis theory for invariant ideals necessary we will need (see [1] for more details).

Let Ω be the set of monomials in indeterminates $x_1, x_2, \ldots$, including the constant 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 $\leq$ and $\mathrm{lt}(f)$ to be its leading term. The following partial ordering on Ω respects the action of $\mathfrak{S}_\infty$ and refines the division partial order on Ω.

Definition 2.2. (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 2.3. A permutation σ in the definition need not be unique. Also, we say that such a permutation *witnesses* $v \preceq w$. We will give a more computationally useful description of this partial order in Theorem 2.16 below.

Example 2.4. 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.

Alternatively, one may use Lemmas 2.7, 2.8, and 2.9 to produce these and many other examples of such relations. □

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 2.5. *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 2.6. *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 $0 \neq c \in K$ 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 two lemmas allow us to generate many relations, including the ones in the above example. Proofs can also be found in [1].

Lemma 2.7. *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 2.8. *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 $a, b \in \mathbb{N}$ such that $a \leq b$, we have $x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n} \preceq x_1^b x_2^{b_1} \cdots x_{n+1}^{b_n}$.*

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

Lemma 2.9. *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, $x_i \neq x_m$. Assume now that $x_i < x_m$ so that $x_i < u$ and thus $\sigma x_i < \sigma u \leq v$. Again this contradicts $\sigma x_i > x_n$ and finishes the proof of the claim.

It follows that σ restricted to the set $\{x_i : i \leq m\}$ can be extended to a permutation σ' of $\{x_i : i \leq n\}$. 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

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

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 2.5 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 state the following definition from [1].

Definition 2.10. 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 2.11. *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 2.19 below). However, we do have a description of minimal Gröbner bases for monomial ideals, and this is the content Theorem 2.17 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 $h = x_3^3 x_4 x_6^2$.

The following fact should be clear.

Lemma 2.12. *If $g \sim_\sigma h$ and $h \sim_\tau k$, then $g \sim_{\tau\sigma} k$.*

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

Lemma 2.13. *Let g be a monomial, and let $i_1 < \cdots < i_n$ be those indices appearing in the indeterminates dividing g. Then σ is an upward shift permutation of g if and only if*

$$\sigma i_1 < \sigma i_2 < \cdots < \sigma i_n \quad \textit{and} \quad \sigma i_k \geq i_k, \qquad k = 1, \ldots, n.$$

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

Lemma 2.14. *Let g and h 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. By transitivity and Lemma 2.12, we may suppose that σ as in the statement of the lemma acts on g by transposing x_i and x_{i+1}. Write $g = x_1^{a_1} \cdots x_i^{a_i} x_{i+2}^{a_{i+2}} \cdots x_n^{a_n}$ with $a_n > 0$; we must verify that

$$x_1^{a_1} \cdots x_i^{a_i} x_{i+2}^{a_{i+2}} \cdots x_n^{a_n} \preceq x_1^{a_1} \cdots x_{i-1}^{a_{i-1}} x_{i+1}^{a_i} x_{i+2}^{a_{i+2}} \cdots x_n^{a_n}.$$

This is proved by induction on n. When $n = 1$, we have $i = 1$, and the claim reduces to Lemma 2.7. In general, we have two cases to consider. If $i = n > 1$, then the claim follows from Lemma 2.8 and induction. Alternatively, if $i < n$ and $n > 1$, then we may apply Lemma 2.9 and induction. The second claim is clear from the definitions. □

Remark 2.15. A word of caution is in order. Suppose that g and h are monomials with $g \sim_\sigma h$ for some $\sigma \in \mathfrak{S}_\infty$. Then it can happen that σ is *not* a witness for the (valid) relation $g \preceq h$. For example, if $\sigma = (14)(23)$, $g = x_2$, and $h = x_3$, then $g \sim_\sigma h$. However, the relation $x_1 \leq x_2$ does not imply $\sigma x_1 \leq \sigma x_2$ as one can easily check.

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

Theorem 2.16. *Two monomials v and w satisfy $v \preceq w$ if and only if there is an upward shift $\sigma \in \mathfrak{S}_N$ of v such that $\sigma v | w$, where N is the largest index of indeterminates appearing in w.*

Proof. We prove the only-if direction ($\Rightarrow$); the converse is clear from Lemma 2.14 and Definition 2.2. 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 2.9. 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 2.13.

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. We prove the following claim by induction on the number of indeterminates n appearing in v:

(2.1)
$$(u \leq v \Rightarrow \sigma u \leq \sigma v \text{ for all } u \in \Omega) \Rightarrow (\sigma i_1 < \cdots < \sigma i_n \text{ and } i_k \leq \sigma i_k \text{ for all } k \leq n).$$

The result in the theorem is then implied by Lemma 2.13. 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 $i_n > 1$.

Fix a monomial v with $n + 1$ indeterminates; we must show that (2.1) holds. Therefore, assume that σ is such that $u \leq v \Rightarrow \sigma u \leq \sigma v$ for all $u \in \Omega$. For a positive integer c, consider the monomial $u_c = (x_1 \cdots x_{i_{n+1}-1})^c \leq v$. Since $u_c \leq v$, we have by assumption that

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

If $\sigma i_{n+1} \leq \sigma i_j$ for some $j < n+1$, then by choosing c sufficiently large (say, larger than the degree of v), the above inequality is impossible. Therefore, it follows that $\sigma i_j < \sigma i_{n+1}$ for all $j < n+1$. Next, we show that $i_{n+1} \leq \sigma i_{n+1}$. Suppose by way of contradiction that $\sigma i_{n+1} < i_{n+1}$. Then, $\sigma i_j < i_{n+1}$ for all $j < n+1$. In particular, $\sigma v < v$, and thus $\sigma^s v \leq \sigma v < v$ for all positive integers s. Hence, $v = \sigma^{N!} v < v$, a contradiction.

Our final step is to invoke the induction hypothesis and prove the other inequalities on the right-hand side of (2.1). Suppose that $u = x_1^{u_1} \cdots x_{i_n}^{u_{i_n}} \leq x_{i_1}^{v_{i_1}} \cdots x_{i_n}^{v_{i_n}}$ so that $u x_{i_{n+1}}^{v_{i_{n+1}}} \leq v$. By assumption, we have

$$\sigma(u x_{i_{n+1}}^{v_{i_{n+1}}}) = (\sigma u) x_{\sigma i_{n+1}}^{v_{i_{n+1}}} \leq x_{\sigma i_k}^{v_{i_k}} \cdots x_{\sigma i_{n+1}}^{v_{i_{n+1}}} = \sigma v,$$

and thus (since we are using the lexicographic ordering),

$$\sigma u \leq x_{\sigma i_1}^{v_{i_1}} \cdots x_{\sigma i_n}^{v_{i_n}}.$$

It follows from induction applied to the monomial $x_{i_1}^{v_{i_1}} \cdots x_{i_n}^{v_{i_n}}$ in n indeterminates that $\sigma i_1 < \cdots < \sigma i_n$ and $i_k \leq \sigma i_k$ for all $k \leq n$. This proves the claim and completes the proof of the theorem. □

We may now prove the main result of this section.

Theorem 2.17. *Let G be a set of n monomials of degree d, and let N be the largest index of indeterminates appearing in any monomial 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*

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

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 2.14.

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 2.16, 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 2.18. *Let G be a finite set of monomials, and let N be the largest index of indeterminates appearing in any monomial in G. Then $\mathfrak{S}_N G$ is a (not necessarily minimal) Gröbner basis for $I = \langle G \rangle_{R[\mathfrak{S}_\infty]}$.*

Example 2.19. The ideal $I = \langle x_1^2 x_3 \rangle_{R[\mathfrak{S}_\infty]}$ has a Gröbner basis,

$$H = \{x_1x_2^2, x_1x_3^2, x_1^2x_2, x_2x_3^2, x_1^2x_3, x_2^2x_3\}.$$

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: $\{x_1x_2^2, x_1^2x_2\}$. □

3. Reduction of polynomials

Before describing the algorithm, we must recall the ideas of reduction from [1]. Let $f \in R$, $f \neq 0$, and let B be a set of nonzero polynomials in R. We say that f is *reducible by B* if there exist pairwise distinct $g_1, \dots, g_m \in B$, $m \geq 1$, such that for each i we have $\operatorname{lm}(g_i) \preceq \operatorname{lm}(f)$, witnessed by some $\sigma_i \in G$, and

$$\operatorname{lt}(f) = a_1 w_1 \sigma_1 \operatorname{lt}(g_1) + \cdots + a_m w_m \sigma_m \operatorname{lt}(g_m)$$

for nonzero $a_i \in A$ and monomials $w_i \in X^\diamond$ such that $w_i \sigma_i \operatorname{lm}(g_i) = \operatorname{lm}(f)$. In this case we write $f \xrightarrow[B]{} h$, where

$$h = f - \big(a_1 w_1 \sigma_1 g_1 + \cdots + a_m w_m \sigma_m g_m\big),$$

and we say that f *reduces to h* by B. We say that f is *reduced* with respect to B if f is not reducible by B. By convention, the zero polynomial is reduced with respect to B. Trivially, every element of B reduces to 0.

The smallest quasi-ordering on R extending the relation $\xrightarrow[B]{}$ is denoted by $\xrightarrow[B]{*}$. If $f, h \neq 0$ and $f \xrightarrow[B]{} h$, then $\operatorname{lm}(h) < \operatorname{lm}(f)$, by Lemma 2.5. In particular, every chain

$$h_0 \xrightarrow[B]{} h_1 \xrightarrow[B]{} h_2 \xrightarrow[B]{} \cdots$$

with all $h_i \in R \setminus \{0\}$ is finite. (Since the term ordering $\leq$ is well-founded.) Hence there exists $r \in R$ such that $f \xrightarrow[B]{*} r$ and r is reduced with respect to B; we call such an r a *normal form* of f with respect to B.

Lemma 3.1. *Suppose that $f \xrightarrow[B]{*} r$. Then there exist $g_1, \dots, g_n \in B$, $\sigma_1, \dots, \sigma_n \in G$ and $h_1, \dots, h_n \in R$ such that*

$$f = r + \sum_{i=1}^{n} h_i \sigma_i g_i \quad \textit{and} \quad \operatorname{lm}(f) \geq \max_{1 \leq i \leq n} \operatorname{lm}(h_i \sigma_i g_i).$$

(In particular, $f - r \in \langle B \rangle_{R[G]}$.)

Proof. See [1]. □

Lemma 3.2. *Let I be an invariant ideal of R and B be a set of nonzero elements of I. The following are equivalent:*

1. *B is a Gröbner basis for I.*
2. *Every nonzero $f \in I$ is reducible by B.*
3. *Every $f \in I$ has normal form 0. (In particular, $I = \langle B \rangle_{R[G]}$.)*
4. *Every $f \in I$ has unique normal form 0.*

Proof. The implications (1) ⇒ (2) ⇒ (3) ⇒ (4) are either obvious or follow from the remarks preceding the lemma. Suppose that (4) holds. Every $f \in I \setminus \{0\}$ with $\operatorname{lt}(f) \notin \operatorname{lt}(B)$ is reduced with respect to B, hence has two distinct normal forms (0 and f), a contradiction. Thus $\operatorname{lt}(I) = \operatorname{lt}(B)$. □

4. Description of the Algorithm

We begin by describing a method that checks when two monomials are $\preceq$ comparable, returning a permutation (if it exists) witnessing the relation. This is accomplished using the characterization given by Theorem 2.16. In this regard, it will be useful to view monomials in R as vectors of integers $v = (v_1, v_2, \ldots)$ with finite support in $\mathbb{N}^\omega$.

Algorithm 4.1. (Comparing monomials in the symmetric cancellation order)
Input: Two monomials v and w with largest indeterminate in w being N.
Output: A permutation $\sigma \in \mathfrak{S}_N$ if $v \preceq w$; otherwise, ***false***.

```
(1) Set $t := 1$, $match := \{\}$;
(2) For $i = 1$ to N:
        For $j = t$ to N:
            If $v_i \neq 0$ and $v_i \leq w_j$, then
                $t := j + 1$;
                $match := match \cup \{(i, j)\}$;
                Break inner loop;
        $t := \max\{i + 1, t\}$;
(3) If $match$ contains fewer elements than the support of $v$, return false;
(4) For $j = N$ down to 1:
        Set $i :=$ largest integer not appearing as a first coordinate in $match$;
        If $j$ is not a second coordinate in $match$, then $match := match \cup (i, j)$;
(5) Return the permutation that $match$ represents;
```

Remark 4.2. One must be somewhat careful when constructing the witness σ. Changing the recipe given in the algorithm above might produce incorrect results. See also Remark 2.15.

Example 4.3. Consider the vectors $v = (1, 2, 0, 2)$ and $w = (0, 3, 4, 1)$ representing monomials $x_4^2 x_2^2 x_1$ and $x_4 x_3^4 x_2^3$ respectively. Then, Algorithm 4.1 will return false since $match = \{(1, 2), (2, 3)\}$ contains less than three elements after Step (2).

On the other hand, running the algorithm on inputs $v = (3, 2, 0, 0, 5)$ and $w = (5, 1, 4, 6, 9)$ will produce an output of $\{(1, 1), (2, 3), (3, 2), (4, 4), (5, 5)\}$, which correctly gives the witness $\sigma = (23)$ to the relation $x_1^3 x_2^2 x_5^5 \preceq x_1^5 x_2 x_3^4 x_4^6 x_5^9$.

We also need to know how to compute a reduction of a polynomial f by another polynomial g (assuming that f is reducible by g). Given a witness σ, however, this is calculated in Lemma 2.5. Specifically, we set

$$SG_\sigma(f, g) = f - \frac{\operatorname{lt}(f)}{\sigma \operatorname{lt}(g)} \sigma g. \tag{4.1}$$

Notice that when $\sigma = (1)$, the polynomial $SG_\sigma(f, g)$ is the normal S-pair from standard Gröbner basis theory.

The general case of reducing a polynomial f by a set B is performed as follows; it is a modification of ordinary polynomial division in the setting of finite dimensional polynomial rings.

Algorithm 4.4. (Reducing a polynomial f by an ordered set of polynomials B)
Input: Polynomial f and an ordered set $B = (b_1, \ldots, b_s) \in R^s$.
Output: The reduction of f by B.

```
(1) Set $p := f$, $r := 0$, $divoccured := 0$;
```

```
(2) While $p \neq 0$:
        i := 1;
        $divoccured := 0$;
        While $i \leq s$;
            $g := b_i$;
            If there exists a $\sigma$ witnessing $\mathrm{lm}(g) \preceq \mathrm{lm}(p)$, then
                $p := SG_\sigma(p, g)$;
                $divoccured := 1$;
                Break inner loop;
            Else, $i := i + 1$;
        If $divoccured = 0$, then
            $r := r + \mathrm{lt}(p)$;
            $p := p - \mathrm{lt}(p)$;
(3) Return $r$;
```

Example 4.5. Let $f = x_3^2x_2^2 + x_2x_1$ and $B = (x_3x_1 + x_2x_1)$. Reducing f by B is the same as reducing f by $x_3x_1 + x_2x_1$ twice as one can check. The resulting polynomial is $x_2^3x_1 + x_2x_1$.

Before coming to our main result, we describe a truncated version of it.

Algorithm 4.6. (Constructing a truncated Gröbner basis for a symmetric ideal)
Input: An integer N and polynomials $F = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_N]$.
Output: A truncated Gröbner basis for $I = \langle f_1, \ldots, f_n \rangle_{R[\mathfrak{S}_\infty]}$.

```
(1) Set $F' := F$;
(2) For each pair $(f_i, f_j)$:
        For each pair $(\sigma, \tau)$ of permutations in $\mathfrak{S}_N$:
            $h := SG_{(1)}(\sigma f_i, \tau f_j)$;
            Set $r$ to be the reduction of $h$ by $\mathfrak{S}_N B'$;
            If $r \neq 0$, then $B' := B' \cup \{r\}$;
(3) Return $B'$;
```

Remark 4.7. As we have seen, it is not enough to choose N to be the largest indeterminate appearing in F (c.f. Remark 1.4).

We call the input N the *order* of a truncated basis for F.

Algorithm 4.8. (Constructing a Gröbner basis for a symmetric ideal)
Input: Polynomials $F = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_N]$.
Output: A Gröbner basis for $I = \langle f_1, \ldots, f_n \rangle_{R[\mathfrak{S}_\infty]}$.

```
(1) Set $F' := F$, $i := N$;
(2) While true:
        Set $F'$ to be a truncated Gröbner basis of $F$ of order $i$;
        If every element of $F'$ reduces to 0 by $\mathfrak{S}_N F$, then return $F$;
        $F := F'$;
        $i := i + 1$;
```

We postpone the proof of correctness of the algorithms above until Section 6

5. Examples

Here we list some examples of our algorithm.[1]

Consider $F = \{x_1 + x_2, x_1x_2\}$ from the introduction. One iteration of Algorithm 4.8 with $i = 2$ gives $F' = \{x_1 + x_2, x_1^2\}$. The next two iterations produce $\{x_1\}$ and thus the algorithm returns with this as its asnwer.

6. Proof of Correctness

Here we prove that our algorithm terminates and produces a Gröbner basis for an ideal I.

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] C. Hillar and T. Windfeldt, *Minimal generators for symmetric ideals*, preprint.

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

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

[6] 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.

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

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

[1] Code that performs the calculations in this section using SINGULAR 3.0 (http://www.singular.uni-kl.de) can be found at http://www.math.tamu.edu/∼chillar/.