An Algorithm for Finding Symmetric Gröbner Bases in Infinite Dimensional Rings

[Extended Abstract]

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095
matthias@math.ucla.edu

Christopher J. Hillar
Department of Mathematics
Texas A&M University
College Station, TX 77843
chillar@math.tamu.edu

ABSTRACT

A *symmetric ideal* $I \subseteq R = K[x_1, x_2, \ldots]$ is an ideal that is invariant under the natural action of the infinite symmetric group. We give an explicit algorithm to find Gröbner bases for symmetric ideals in the infinite dimensional polynomial ring R. This allows for symbolic computation in a new class of rings. In particular, we solve the ideal membership problem for symmetric ideals of R.

Categories and Subject Descriptors

G.4 [**Mathematical Software**]: Discrete Mathematics—*algorithm design and analysis*; G.2.m [**Discrete Mathematics**]: [miscellaneous]; J.2 [**Physical Sciences and Engineering**]: [chemistry, mathematics and statistics]

General Terms

Algorithms, Theory

Keywords

Invariant ideal, partial ordering, symmetric group, Gröbner basis, polynomial reduction, algorithm

1. INTRODUCTION

In computational algebra, one encounters the following general problem.

PROBLEM 1.1. *Let I be an ideal of a ring R and let $f \in R$. Determine whether $f \in I$.*

When $R = K[x_1, \ldots, x_n]$ is a polynomial ring in n indeterminates over a field K, this problem has a complete solution due to Buchberger [2] (for a nice exposition, see [4, 3]).

THEOREM 1.2 (BUCHBERGER). *Let $I = \langle f_1, \ldots, f_m \rangle_R$ be an ideal of $R = K[x_1, \ldots, x_n]$. Then, there is a computable, finite set of polynomials G such that for every polynomial f, we have $f \in I$ if and only if the polynomial reduction of f with G is 0.*

One remarkable feature of this result is that once such a *Gröbner basis* G for I is found, any new instance of the question "Is $f \in I$"? can be solved very quickly in principle (of course, in practice, there are many issues involving the coefficient heights of the polynomials involved). It is difficult not to stress the importance of Theorem 1.2; it forms the backbone of the field of computational algebraic geometry and has many applications, too numerous to list here. We should mention that there have been various improvements to Buchberger's algorithm. Currently, the algorithm of Faugere [6] is generally regarded as the fastest.

We shall consider a different but related membership problem; one that at first glance would not seem to be solvable as completely as Buchberger had done with $K[x_1, \ldots, x_n]$. 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

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

We motivate our discussion with the following concrete problem. Questions of this nature arise in applications to chemistry [8, 9, 10] and algebraic statistics [5].

PROBLEM 1.3. *Let $f_1 = x_1^3 x_3 + x_1^2 x_2^3$ and $f_2 = x_2^2 x_3^2 - x_2^2 x_1 + x_1 x_3^2$ and consider the ideal of $R = K[X]$ generated by all permutations of f_1 and f_2:*

$$I = \langle \mathfrak{S}_\infty f_1, \mathfrak{S}_\infty f_2 \rangle_R.$$

ISSAC'08, July 20–23, 2008, Hagenberg, Austria.
Copyright 2008 ACM 978-1-59593-904-3/08/07 ...$5.00.

Is the following polynomial with 10 *indeterminates in* I*?*

$$f = -x_{10}^2x_9^2x_5^6 - 2x_{10}^2x_9x_8^3x_5^5 - x_{10}^2x_8^6x_5^4 + 3x_{10}^2x_8^2 + 3x_{10}^2x_7 + 3x_{10}x_9x_7x_4^3x_3^2x_2^2x_1 + 3x_{10}x_9x_7x_4^3x_3^2x_1^2 - 3x_{10}x_9x_7x_4^3x_2^2x_1^2 - x_9^2x_8^7x_7x_6x_5^6 - 2x_9x_8^{10}x_7x_6x_5^5 + x_9x_5^3x_3x_2x_1^3 + x_9x_5^3x_2^4x_1^2 + x_9x_3x_2^3x_1^4 + x_9x_2^6x_1^3 - x_8^{13}x_7x_6x_5^4 - 3x_8^2x_7 + x_7^2x_6x_3^3x_2^7 + x_7^2x_6x_3^3x_2^5x_1 - x_7^2x_6x_3x_2^7x_1 + x_5x_4^2 - 3x_5x_3^2 + 2x_5x_1^2 + x_4^2x_3^2 - 2x_3^2x_1^2 + 5x_3x_1^5 + 5x_2^3x_1^4.$$

More generally, given $f \in R$*, how can we determine if* $f \in I$*?*

Naively, one could solve this problem using Buchberger's algorithm with truncated polynomial rings $R_n = K[x_1, \ldots, x_n]$. Namely, for each $n \geq 10$, compute a Gröbner basis G_n for the ideal $I_n = \langle \mathfrak{S}_n f_1, \mathfrak{S}_n f_2 \rangle_{R_n}$, and reduce f by G_n.

There are several problems with this approach. For one, this method requires computation of many Gröbner bases (the bottleneck in any symbolic computation), the number of which depends on the number of indeterminates appearing in f. Additionally, it lacks the ability to solve new membership problems quickly, a powerful feature of Buchberger's technique. One might hope to at least restrict the number of Gröbner basis computations in terms of the number of indeterminates appearing in f, however, the following simple example should temper one's optimism a little.

Example 1.4. *Let* I *be the ideal generated by all permutations of* $x_1 + x_2$*. Then,* $I = \langle x_1, x_2, \ldots \rangle_R$*, but*

$$x_1 \notin \langle x_1 + x_2 \rangle_{K[x_1,x_2]}.$$

Our main result in this paper is an effective algorithm that solves the general membership problem for symmetric ideals (such as those appearing in Problem 1.3) and has all of the important features of Buchberger's method. It is the first algorithm of its kind that we are aware of (although it is similar in spirit to Buchberger's original algorithm). Before we state our theorem explicitly (Theorem 1.6), we develop some notation. In general, we first give the main ideas in the text informally and clarify the notions later.

Let $R[\mathfrak{S}_\infty]$ denote 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) naturally gives R the structure of a (left) module over the ring $R[\mathfrak{S}_\infty]$. For instance, we have

$$[x_1(12) + x_2(23)] \cdot (x_1x_3 + x_2) = x_1x_2x_3 + x_1^2 + x_1x_2^2 + x_2x_3.$$

An ideal $I \subseteq R$ is called *symmetric* if

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

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

Also, 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. This notation greatly simplifies expressing symmetric ideals in terms of their generators.

Example 1.5. $I = \langle x_1, x_2, \ldots \rangle_R$ *is an invariant ideal of* R*. Written as a module over the group ring* $R[\mathfrak{S}_\infty]$*, it has the compact presentation* $I = \langle x_1 \rangle_{R[\mathfrak{S}_\infty]}$*.*

We may now state our main theorem.

Theorem 1.6. *Let* $I = \langle f_1, \ldots, f_m \rangle_{R[\mathfrak{S}_\infty]}$ *be a symmetric ideal of* R*. Then, there is a computable, finite set of polynomials* G *such that for every polynomial* f*, we have* $f \in I$ *if and only if the polynomial reduction of* f *with* G *is* 0*.*

We should remark here that the polynomial reduction appearing in Theorem 1.6 is only a slight modification of the reduction in the context of normal (finite dimensional) polynomial rings. We will also call the sets G appearing above *Gröbner bases* for reasons which will be evident in the section that follows.

Example 1.7. *The ideal* $I = \langle x_1^3x_3 + x_1^2x_2^3, x_2^2x_3^2 - x_2^2x_1 + x_1x_3^2 \rangle_{R[\mathfrak{S}_\infty]}$ *from Problem 1.3 has a Gröbner basis given by:*

$$G = \mathfrak{S}_3 \cdot \{x_3x_2x_1^2, x_3^2x_1 + x_2^4x_1 - x_2^2x_1, x_3x_1^3, x_2x_1^4, x_2^2x_1^2\}.$$

Once G *is found, testing whether a polynomial* f *is in* I *can be done using the reduction algorithm found in Section 4; for instance, one finds that* $f \in I$ *for the polynomial encountered in Problem 1.3.* □

In Section 2, we discuss the history of this problem and state some of the foundational results that are ingredients in the proof of Theorem 1.6. In particular, we discuss there an important partial order on monomials that respects the action of the symmetric group. Section 3 briefly reviews the notion of reduction that occurs in our more general context, and finally, in Section 4, we describe our algorithm. To keep the paper as expository as possible, we have left out many of the (technical) proofs that will appear in a much longer version of this paper.

2. GRÖBNER BASES FOR SYMMETRIC IDEALS

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

Theorem 2.1. *Every symmetric 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.*

Remark 2.2. *Symmetric ideals can be arbitrarily complex in the following sense. For each* n*, there are symmetric ideals of* R *that cannot have fewer than* n $R[\mathfrak{S}_\infty]$*-module generators [7]. Moreover, such ideals are not always monomial.*

Theorem 2.1 was motivated by finiteness questions in chemistry [8, 9, 10] and algebraic statistics [5] involving chains of symmetric 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 2.1, it was shown that, in a certain sense, a symmetric ideal I has a finite minimal Gröbner basis (see below for a review of these concepts). Moreover, the existence of such a set of generators solves the ideal membership problem in R.

Theorem 2.3. *Let* G *be a Gröbner basis for a symmetric ideal* I*. Then* $f \in I$ *if and only if* f *has normal form* 0 *with respect to* G*.*

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 below. 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 2.4. *Let $I = \langle f_1, \ldots, f_m \rangle_{R[\mathfrak{S}_\infty]}$ be a symmetric ideal of R. There exists an effective algorithm to compute a finite minimal Gröbner basis for I.*

COROLLARY 2.5. *There exists an effective algorithm to solve the ideal membership problem for symmetric ideals in the infinite dimensional ring $K[x_1, x_2, \ldots]$.*

The following is a brief review of the Gröbner basis theory for symmetric ideals (see [1] for more details). Let us first note that an infinite permutation acting on a polynomial may be replaced with a finite one.

LEMMA 2.6. *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 $\tau f = \sigma f$.*

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 2.7. *(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 2.8. *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 2.21 below.*

EXAMPLE 2.9. *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 2.12, 2.13, and 2.14 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 σ is a witness to a relation involving $\mathrm{lm}(f)$, while the latter can be viewed as a kind of "S-pair" leading term cancellation.

LEMMA 2.10. *Let f be a nonzero polynomial and $w \in \Omega$. Suppose that $\sigma \in \mathfrak{S}_\infty$ witnesses $lm(f) \preceq w$, and let $u \in \Omega$ with $u\sigma lm(f) = w$. Then $lm(u\sigma f) = u\sigma lm(f)$.*

LEMMA 2.11. *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*

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

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 2.12. *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 2.13. *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].

LEMMA 2.14. *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 $ux_{n+1}^a \preceq vx_{n+1}^b$.*

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

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

the span of all monomials which are $\preceq$ larger than leading monomials in I. If I happens to be a symmetric ideal, then it follows from Lemma 2.10 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 2.15. *We say that a subset B of a symmetric ideal $I \subseteq R$ is a* Gröbner basis *for I if $lm(B) = lm(I)$.*

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 symmetric ideals; it is an analog to the corresponding statement for finite dimensional polynomial rings. As a corollary, they obtain Theorem 2.1.

THEOREM 2.16. *A symmetric 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 a symmetric ideal I (see Example 2.24 below). However, we do have a description of minimal Gröbner bases for monomial ideals, and this is the content of Theorem 2.22 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. This description will be used in our algorithm that finds symmetric Gröbner bases.

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 2.17. *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 2.18. *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*

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

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

Lemma 2.19. *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 Lemma 2.17, 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 2.12. In general, we have two cases to consider. If $i = n > 1$, then the claim follows from Lemma 2.13 and induction. Alternatively, if $i < n$ and $n > 1$, then we may apply Lemma 2.14 and induction. The second claim is clear from the definitions. □

Remark 2.20. *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 a new characterization of the symmetric cancellation partial order.

Theorem 2.21. *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 2.19 and Definition 2.7. 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 2.14. 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 2.18.

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:

$$\begin{aligned} &(u \leq v \Rightarrow \sigma u \leq \sigma v \text{ for all } u \in \Omega) \\ &\Rightarrow (\sigma i_1 < \cdots < \sigma i_n \text{ and } i_k \leq \sigma i_k \text{ for all } k \leq n). \end{aligned} \qquad (2)$$

The result in the theorem is then implied by Lemma 2.18. 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) 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). 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 we have $u x_{i_{n+1}}^{v_{i_{n+1}}} \leq v$. By assumption,

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

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. □

The main result of this section is the following.

Theorem 2.22. *Let G be a finite set of monomials of the same degree, 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 be the set,*

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

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 $\operatorname{lm}(H) \subseteq \operatorname{lm}(I)$ 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 (its unordered vector of exponents) 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 2.19.

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 2.21, 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 2.23. *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 2.24. *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 our Gröbner basis 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 exists $g \in B$ such that we have $\mathrm{lm}(g) \preceq \mathrm{lm}(f)$, witnessed by some $\sigma \in \mathfrak{S}_\infty$ and

$$\mathrm{lt}(f) = aw\sigma\,\mathrm{lt}(g)$$

for some nonzero $a \in K$ and a monomial $w \in \Omega$ such that $w\sigma\,\mathrm{lm}(g) = \mathrm{lm}(f)$. In this case we write $f \xrightarrow[B]{} h$, where

$$h = f - \big(aw\sigma g\big),$$

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 $\mathrm{lm}(h) < \mathrm{lm}(f)$, by Lemma 2.11. 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 polynomials $g_1, \ldots, g_n \in B$, $\sigma_1, \ldots, \sigma_n \in \mathfrak{S}_\infty$ and $h_1, \ldots, h_n \in R$ such that*

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

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

Lemma 3.2. *Let I be a symmetric 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, $I = \langle B \rangle_{R[\mathfrak{S}_\infty]}$.)*

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 $\mathrm{lt}(f) \notin \mathrm{lt}(B)$ is reduced with respect to B, hence has two distinct normal forms (0 and f), a contradiction. Thus $\mathrm{lt}(I) = \mathrm{lt}(B)$. □

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 2.21. 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 $\mathbb{N}^\infty$.

Algorithm 4.1. *(Comparing monomials in the symmetric cancellation order)*
Input: Two monomials v and w with largest indeterminate in w having index 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 ∪ {(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 $\leq N$ not appearing as a
   first coordinate in match;
       If $j$ is not a second coordinate in match, then
   match := match ∪ (i, j);
5. Return the permutation that match represents;
```

Example 4.2. *Consider the vectors $v = (1, 2, 0, 2)$ and $w = (0, 3, 4, 1)$ representing monomials $x_4^2x_2^2x_1$ and $x_4x_3^4x_2^3$ 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 $x_1^3x_2^2x_5^5 \preceq x_1^5x_2x_3^4x_4^6x_5^9$.

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 2.10. Specifically, we set

$$SG_\sigma(f, g) = f - \frac{\operatorname{lt}(f)}{\sigma \operatorname{lt}(g)}\sigma g. \tag{3}$$

Notice that when $\sigma = (1)$, the polynomial $SG_\sigma(f, g)$ resembles 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 4.3. *(Reducing a polynomial f by an ordered set of polynomials B)*
Input: Polynomial f and an ordered set $B = (b_1, \dots, b_s) \in R^s$.
Output: A norma form (remainder) of f with respect to 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 witness $\sigma$ to $\operatorname{lm}(g) \preceq \operatorname{lm}(p)$, then
               $p := SG_\sigma(p, g)$;
               divoccured $:= 1$;
               Break inner loop;
           Else, $i := i + 1$;
       If divoccured $= 0$, then
           $r := r + \operatorname{lt}(p)$;
           $p := p - \operatorname{lt}(p)$;
3. Return $r$;
```

Example 4.4. *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 4.5. *(Constructing a truncated Gröbner basis for a symmetric ideal)*
Input: An integer N and polynomials $F = \{f_1, \dots, f_n\} \subset K[x_1, \dots, x_N]$.
Output: A truncated Gröbner basis for $I = \langle f_1, \dots, f_n\rangle_{R[\mathfrak{S}_\infty]}$.

```
1. Set $F' := F$;
2. For each pair $(f_i, f_j)$:
       For each pair $(\sigma, \tau)$ of permutations in $\mathfrak{S}_N$:
           $h :=$ the $S$-polynomial of $\sigma f_i$ and $\tau f_j$;
           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 4.6. *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 4.7. *(Constructing a Gröbner basis for a symmetric ideal)*
Input: Polynomials $F = \{f_1, \dots, f_n\} \subset K[x_1, \dots, x_N]$.
Output: A Gröbner basis for $I = \langle f_1, \dots, f_n\rangle_{R[\mathfrak{S}_\infty]}$.

```
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 $F$;
       $F := F'$;
       $i := i + 1$;
```

Example 4.8. *Consider $F = \{x_1 + x_2, x_1x_2\}$ from the introduction. One iteration of Algorithm 4.7 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 answer.*

5. REFERENCES

[1] M. Aschenbrenner and C. J. Hillar. Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.*, 359(11):5171–5192, 2007.

[2] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, 4:374–383, 1970.

[3] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[4] D. A. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[5] M. Drton, B. Sturmfels, and S. Sullivant. Algebraic factor analysis: tetrads, pentads and beyond. *Probab. Theory Related Fields*, 138(3-4):463–493, 2007.

[6] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic), New York, 2002. ACM.

[7] C. J. Hillar and T. Windfeldt. Minimal generators for symmetric ideals. *Proc. Amer. Math. Soc., to appear.*

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

[9] E. Ruch and A. Schönhofer. Theorie der chiralitätsfunktionen. *Theor. Chim. Acta*, 19:225–287, 1970.

[10] E. Ruch, A. Schönhofer, and I. Ugi. Die vandermondesche determinante als näherungsansatz für eine chiralitätsbeobachtung, ihre verwendung in der stereochemie und zur berechnung der optischen aktivität. *Theor. Chim. Acta*, 7:420–432, 1967.