AN ALGORITHM FOR FINDING GRÖBNER BASES IN INFINITE DIMENSIONAL POLYNOMIAL RINGS

CHRISTOPHER J. HILLAR, ROBERT KRONE, AND ANTON LEYKIN

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 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 1.3. *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 $I = \langle x_1 + x_2, x_1x_2\rangle_{R[\mathfrak{S}_\infty]}$. 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

$$\langle x_1 + x_2, x_1x_2\rangle_{R[\mathfrak{S}_2]} \neq \langle x_1\rangle_{R[\mathfrak{S}_2]}.$$

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

Example 1.5. The ideal $I = \langle x_1^3x_3+x_1^2x_2^3, x_2^2x_3^2-x_2^2x_1+x_1x_3^2\rangle_{R[\mathfrak{S}_\infty]}$ 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 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 **??**. Unfortunately, the techniques used to prove finiteness in [**?**] 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 $K[x_1,x_2,\ldots]$.*

Let G denote the monoid of strictly increasing functions $\pi : \mathbb{N} \to \mathbb{N}$. G has a natural action on the variables of R with π mapping x_i to $x_{\pi(i)}$. This defines an action of G on R and note that this action respects the term order defined on R. For any two monomials m, n, $m < n$ implies $\pi(m) < \pi(n)$ for all $\pi \in G$. In particular for any polynomial $g \in R$, $\text{in}_>(\pi g) = \pi\,\text{in}_>(g)$. We can define the G-invariant ideals as ideals $I \subset R$ with $GI \subset I$. Equivalently they are the $R[G]$-submodules of R.

Proposition 1.8. *R is a Noetherian $R[G]$-module.*

Proposition 1.9. *If I is a $\mathfrak{S}_\infty$-invariant ideal, then I is also G-invariant.*

Proof. For any $f \in I$ and $\pi \in G$, πf contains only a finite number of variables in R. Let n be the index of the largest variable occurring in πf. Then there exists $\sigma \in \mathfrak{S}_n$ such that $\pi f = \sigma f$. Because I is $\mathfrak{S}_\infty$-invariant, $\sigma f \in I$ so $\pi f \in I$. □

Given a finite set F that generates a $\mathfrak{S}_\infty$-invariant ideal I as a $R[\mathfrak{S}_\infty]$-module, we can easily construct a finite set that generates I as a $R[G]$-module as follows.

Proposition 1.10. *Let F be a finite set of polynomials and let n be the index of the largest variable occurring in F. Then $\langle F\rangle_{R[\mathfrak{S}_\infty]} = \langle \mathfrak{S}_nF\rangle_{R[G]}$.*

Proof. Clearly $\langle \mathfrak{S}_nF\rangle_{R[G]} \subset \langle F\rangle_{R[\mathfrak{S}_\infty]}$.

To prove the other containment, it's enough to show for any $f \in F$ and $\sigma \in \mathfrak{S}_\infty$, that $\sigma f \in \langle \mathfrak{S}_nF\rangle_{R[G]}$ since the elements of this form generate $\langle F\rangle_{R[\mathfrak{S}_\infty]}$ as an ideal. Let $\tau \in \mathfrak{S}_n$ be the permutation that puts the integers 1 to n in the same order as σ does, i.e. $\tau(i) < \tau(j)$ exactly when $\sigma(i) < \sigma(j)$ for all $i,j \in \{1,\ldots,n\}$. Then there is some monoid element $\pi \in G$ such that $\sigma(i) = \pi\circ\tau(i)$ for all $i \in \{1,\ldots,n\}$. Therefore $\sigma f = \pi(\tau f) \in \langle \mathfrak{S}_nF\rangle_{R[G]}$. □

Given a $\mathfrak{S}_\infty$-invariant ideal $I = \langle F\rangle_{\mathfrak{S}_\infty}$, we will use the set $\mathfrak{S}_nF$ which generates I as a $R[G]$-module to find a G-Gröbner basis of I (defined below) and from that obtain a $\mathfrak{S}_\infty$-Gröbner basis.

Definition 1.11. A G-Gröbner basis of a G-invariant ideal I is a finite set $B \subset I$ such that for any $f \in I$, there exists $g \in B$ with $\pi\,\text{in}_>\,g$ dividing $\text{in}_>\,f$ for some $\pi \in G$.

Note that if I is also $\mathfrak{S}_\infty$-invariant, then a G-Gröbner basis of I is also a $\mathfrak{S}_\infty$-Gröbner basis. Given $f \in I$, $g \in B$ and $\pi \in G$ with $\pi \operatorname{in}_> g | \operatorname{in}_> f$, π can also be expressed as a permutation $\sigma \in \mathfrak{S}_\infty$ and σ witnesses $\operatorname{in}_> g \preceq \operatorname{in}_> f$ since it only increases the indices of the variables in $\operatorname{in}_> g$ and maintains their relative order.

Using the work of Brouwer and Draisma, there is an algorithm for finding a G-Gröbner basis of I provided that the action of G satisfies certain criteria, which we will show it does.

Proposition 1.12 (Satisfaction of Criterion EGB4)**.** *For all $f, h \in R$, the set $Gf \times Gh$ is the union of a finite number of G-orbits (where G acts diagonally on $R \times R$), and generators of these orbits can be computed effectively.*

Proof. Let n be the index of the largest variable occurring in f and g. Let H be the set of strictly increasing maps $\tau : [n] \to [2n]$, which is finite. We will show that any pair $(\pi_1 f, \pi_2 g) \in Gf \times Gh$ can be expressed as $(\sigma\tau_1 f, \sigma\tau_2 g)$ for some $\sigma \in G$ and $\tau_1, \tau_2 \in H$. Note that $\pi_1 f$ and $\pi_2 g$ are fully determined by the images $\pi_1([n])$ and $\pi_2([n])$. Let

$$S_i = \{j \in [n] : \pi_i(j) \in \pi_1([n]) \cap \pi_2([n])\}$$

for $i = 1, 2$, and let $k = |S_1| = |S_2|$. □

2. Algorithms

We postpone the proof of correctness of the algorithms above until Section 4

3. 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 **??** 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.

4. Proof of Correctness

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

References

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

Redwood Center for Theoretical Neuroscience, University of California, Berkeley
E-mail address: chillar@msri.org

Georgia Tech University, Atlanta, GA
E-mail address: krone@math.gatech.edu

Georgia Tech University, Atlanta, GA
E-mail address: anton.leykin@gmail.com

[1] Code that performs the calculations in this section can be found at ??.