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 $K[x_1, x_2, \ldots]$.*

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 ??.