

$$G \cdot I = I \implies I = \langle f_1, \dots, f_m \rangle_{R[G]}$$

An Algorithm for Finding Symmetric Groebner Bases In Infinite Dimensional Rings

Christopher Hillar
(Texas A&M University)

Joint with Matthias Aschenbrenner
(UCLA)

Motivational Problem

Let $R = K[x_1, x_2, x_3, \dots]$ over a field K ,
 $G = S_\infty = \text{Perm}(\{1, 2, 3, \dots\})$.

Let $I = G \cdot \langle f_1, f_2 \rangle_R$ be the ideal generated by
all permutations of the two polynomials

$$f_1 = x_1^3 x_3 + x_1^2 x_2^3$$

$$f_2 = x_2^2 x_3^2 - x_2^2 x_1 + x_1 x_3^2$$

Problem: Let g be a polynomial in R . Can you
tell me if g is in I ?

Motivational Problem

Concretely, for instance, what if

$$\begin{aligned} g = & -x_{10}^2 x_9^2 x_5^6 - 2x_{10}^2 x_9 x_8^3 x_5^5 - x_{10}^2 x_8^6 x_5^4 + 3x_{10}^2 x_8^2 + 3x_{10}^2 x_7 + \\ & 3x_{10} x_9 x_7 x_4^3 x_3^2 x_2^2 x_1 + 3x_{10} x_9 x_7 x_4^3 x_3^2 x_1^2 - 3x_{10} x_9 x_7 x_4^3 x_2^2 x_1^2 - x_9^2 x_8^7 x_7 x_6 x_5^6 - \\ & 2x_9 x_8^{10} x_7 x_6 x_5^5 + x_9 x_5^3 x_3 x_2 x_1^3 + x_9 x_5^3 x_2^4 x_1^2 + x_9 x_3 x_2^3 x_1^4 + x_9 x_2^6 x_1^3 - \\ & x_8^{13} x_7 x_6 x_5^4 - 3x_8^2 x_7 + x_7^2 x_6 x_3^3 x_2^7 + x_7^2 x_6 x_3^3 x_2^5 x_1 - x_7^2 x_6 x_3 x_2^7 x_1 + x_5 x_4^2 - \\ & 3x_5 x_3^2 + 2x_5 x_1^2 + x_4^2 x_3^2 - 2x_3^2 x_1^2 + 5x_3 x_1^5 + 5x_2^3 x_1^4 \end{aligned}$$

How would you try to answer the **question**:

Can you express g as a **finite linear combination** over R of polynomials σf_i (σ a permutation, $i = 1, 2$)?

Computation in Infinite Dimensional Polynomial Rings

Let $R = K[x_1, x_2, x_3, \dots]$ be the (infinite Krull dimensional) polynomial ring over K . We will discuss methods for *computing* with ideals in R .

- Group actions and **Invariant Ideals**
- **Noetherianity** (finite generation)
- **Partial orders** (respecting group action)
- **Reduction** (normal form computation)
- (Symmetric) **Groebner Bases**
- **Algorithms**

Invariant Ideals

Group Rings: Let G be a group and R a ring.

The (left) group ring $R[G]$ over R is formally all linear combinations:

$$R[G] = \{ r_1g_1 + \cdots + r_mg_m : r_i \text{ in } R, g_i \text{ in } G \}$$

Multiplication is given by $(r_1g_1) \cdot (r_2g_2) = (r_1r_2)g_1g_2$

Assume that R is a G -module; that is, G gives an action on R (i.e. $G \rightarrow \text{Perm}(R)$) that is linear:

$$g(r+s) = gr + gs, \quad g \text{ in } G, r, s \text{ in } R$$

- R has the structure of a (left) module over $R[G]$

Invariant Ideals

Definition: An ideal I of R is **invariant under G** if

$$G \cdot I = \{g \cdot f : f \text{ in } I, g \text{ in } G\} = I$$

I.e. **invariant ideals** are the $R[G]$ -submodules of R .

1. $R = K[x_1, x_2, \dots]$, $G = S_\infty$, $I = G \cdot \langle f_1, f_2 \rangle_R$

2. $R = K[x_1, x_2]$ and $G = S_2 = \{(1), (12)\}$

$$\underbrace{(x_1(1) + x_2(12))}_{R[G]} \cdot \underbrace{(x_1 + x_2 x_1^2)}_R = \underbrace{x_1^2 + x_2^2 + x_2 x_1^3 + x_2^3 x_1}_R$$

$I = \langle x_1 + x_2^2, x_2 + x_1^2 \rangle_R = \langle x_1 + x_2^2 \rangle_{R[G]}$ is an **invariant ideal**

Noetherianity

Setup: $R = K[x_1, x_2, x_3, \dots]$, $G = S_\infty = \text{Perm}(\{1, 2, 3, \dots\})$

Theorem [AH07]: Invariant ideals of R are finitely generated over $R[G]$. (R is a **Noetherian** $R[G]$ -module)

Simplest Example: We cannot have

$$I = \langle x_1, x_2, x_3, \dots \rangle_R = \langle f_1, \dots, f_m \rangle_R$$

However, I has extra structure: it is invariant under $G = S_\infty$. This theorem should apply:

$$I = \langle x_1, x_2, \dots \rangle_R = \langle x_1 \rangle_{R[G]} = \{h \cdot x_1 : h \text{ in } R[G]\}$$

- Note: I might need **arbitrarily large numbers** of generators

Partial Order on Monomials

Let $<_{\text{lex}}$ be the **lexicographic ordering** of monomials with

$$x_1 <_{\text{lex}} x_2 <_{\text{lex}} x_3 <_{\text{lex}} \dots. \text{ E.g., } x_2x_3^3 <_{\text{lex}} x_1x_4$$

Definition: Symmetric partial order (**version 1**)

$$u \leq v \Leftrightarrow \left\{ \begin{array}{l} u \leq_{\text{lex}} v, \text{ there exists } \sigma \text{ in } G \\ \text{with } \sigma u \mid v, \text{ and for all} \\ w \leq_{\text{lex}} u, \text{ we have } \sigma w \leq_{\text{lex}} \sigma u \end{array} \right.$$

Theorem[AH08] : Symmetric partial order (**version 2**)

$$u \leq v \Leftrightarrow \text{ a shift of } u \text{ divides } v$$

$$x_1^2 < x_1x_2^2 < x_1^3x_2x_3^2 \quad \color{red}{!<} \quad x_1^3x_3^2x_4$$

Symmetric SG-Polynomial

This looks quite **technical**, but is remembered by the

Cancellation Property: If $m_1 < m_2$ and if f_1 and f_2 have leading (lexicographic) terms m_1 and m_2 , then the **SG-polynomial**

$$\mathbf{SG}_\sigma(f_1, f_2) = f_2 - \frac{m_2}{\sigma m_1} \sigma f_1$$

has a smaller (lex) leading monomial than f_2 .

Main Point: if $m_1 < m_2$ one can cancel m_2 by using a permutation σ in S_∞ . Thus,

$$\mathbf{SG}_\sigma(f_1, f_2) \in I = \langle f_1, f_2 \rangle_{R[G]}$$

Basic Theory of Reduction

We now explain **reduction** in the $R[G]$ -module R , $G = S_\infty$

Definition: $\text{lm}(f)$ = largest lexicographic monomial in f .

Definition: f in R is **reducible** by a set of polynomials B means that for some g in B , we have

$$\text{lm}(g) \leq \text{lm}(f) \quad \text{so } \sigma \text{lm}(g) \mid \text{lm}(f)$$

In this case, we write $f \dashrightarrow h$ where

$$h = f - cm(\sigma g)$$

m is a monomial and c is the coefficient of $\text{lm}(f)$ in f

Reduction Intuition

The point: if I is invariant, f and g in I , and $f \rightarrow h$, then h is in I with smaller (lex) leading monomial

In analog to classical GB, we would like to find a (finite) subset B of I such that being in I is same as there being a sequence of reductions

$$f \rightarrow h_1 \rightarrow h_2 \rightarrow \dots \rightarrow 0$$

Example: $B = \{x_1x_2^2 + x_2, x_1 - 1\}$, $f = x_1^3x_2x_3^2 + x_1^4x_3$

$$f \rightarrow x_1^4x_3 - x_1^3x_3 \rightarrow 0$$

So $f = x_1^3(123)(x_1x_2^2 + x_2) + x_1^3x_3(x_1 - 1)$ is in $\langle B \rangle_{R[G]}$

Groebner Bases

Definition/Proposition: Let I be an invariant ideal and B a set of nonzero polynomials. The following are equivalent

- (1) B is a **Groebner Basis** for I
- (2) Every f in I has **unique normal form** 0

Notice that (2) implies that $I = \langle B \rangle_{R[G]}$

So our previous theorem may be deduced from the

Theorem [AH07]: An invariant ideal of R has a **finite Groebner basis** B

Example Groebner Basis

Achtung! Classical intuition sometimes fails here.

Example: Let $I = \langle x_1 x_2^2 \rangle_{R[G]}$, which is a monomial ideal.

The set $B = \{x_1 x_2^2\}$ is **not** a Groebner Basis for I .

Reason: $x_1^2 x_2$ is in I , however,

$$x_1^2 x_2 \not\rightarrow 0$$

so that $x_1^2 x_2$ does not have normal form 0 wrt B

But $B = \{x_1 x_2^2, x_1^2 x_2\}$ is a minimal **Groebner basis**.

Example: $x_3 x_4 x_6^3 = x_4 x_6 (13)(26) x_1 x_2^2$ is in I , and indeed

$$x_3 x_4 x_6^3 \rightarrow 0$$

Algorithms

Can we compute a Groebner basis for an invariant ideal I given a finite list of generators? If so, then we really could do computations in the infinite dimensional (module) R .

Theorem [AH08]: Let $I = \langle f_1, f_2, \dots, f_n \rangle_{R[G]}$ be an invariant ideal of R . There exists an **effective** algorithm to compute a minimal Groebner Basis B for I

Corollary: There is a (Buchberger-like) algorithm to solve the **ideal membership problem**.

- This algorithm has been implemented and is currently being optimized for use in **SINGULAR**

Motivational Problem Again

Example: Let I be generated by

$$F = \{x_1^3x_3 + x_1^2x_2^3, x_2^2x_3^2 - x_2^2x_1 + x_1x_3^2\}.$$

A symmetric **Groebner basis** is given by 5 polynomials:

$$G = \{x_3x_2x_1^2, x_3^2x_1 + x_2^4x_1 - x_2^2x_1, x_3x_1^3, x_2x_1^4, x_2^2x_1^2\}$$

To see if any polynomial g is in I , we simply **reduce g by G** and see if the result is **0**.

Traditionally, we would have to (at the very least) compute a (normal) Groebner basis of the S_n orbit of the generators of I , where n is the number of indeterminates in f .

Motivational Problem Again

So, is

$$\begin{aligned} & -x_{10}^2 x_9^2 x_5^6 - 2x_{10}^2 x_9 x_8^3 x_5^5 - x_{10}^2 x_8^6 x_5^4 + 3x_{10}^2 x_8^2 + 3x_{10}^2 x_7 + 3x_{10} x_9 x_7 x_4^3 x_3^2 x_2^2 x_1 + \\ & 3x_{10} x_9 x_7 x_4^3 x_3^2 x_1^2 - 3x_{10} x_9 x_7 x_4^3 x_2^2 x_1^2 - x_9^2 x_8^7 x_7 x_6 x_5^6 - 2x_9 x_8^{10} x_7 x_6 x_5^5 + \\ & x_9 x_5^3 x_3 x_2 x_1^3 + x_9 x_5^3 x_2^4 x_1^2 + x_9 x_3 x_2^3 x_1^4 + x_9 x_2^6 x_1^3 - x_8^{13} x_7 x_6 x_5^4 - 3x_8^2 x_7 + \\ & x_7^2 x_6 x_3^3 x_2^7 + x_7^2 x_6 x_3^3 x_2^5 x_1 - x_7^2 x_6 x_3 x_2^7 x_1 + x_5 x_4^2 - 3x_5 x_3^2 + 2x_5 x_1^2 + x_4^2 x_3^2 - \\ & 2x_3^2 x_1^2 + 5x_3 x_1^5 + 5x_2^3 x_1^4 \end{aligned}$$

in the ideal I ?

One way to check: Compute a traditional GB with a priori $2 \cdot 10!$ polynomials in 10 variables! (and it still might not work!)

Better way: Reduce it modulo the symmetric Groebner bases and check if you get 0 (you do).

Research Problems

1. Extensions to other group actions G .
2. Applications to finite dimensional situation.
3. Can we read off properties of the ideals I from their Groebner bases as in the traditional case?
4. Applications to toric ideals (with S. Sullivant)
5. Noncommutative applications?

The End

(of talk)