$$G \cdot I = I \quad \Longrightarrow \quad I = \langle f_1, \ldots, f_m \rangle_{R[G]}$$

Finiteness Theorems and Algorithms for Polynomial Equations in an Infinite Number of Variables

Chris Hillar
Redwood Center for Theoretical Neuroscience
UC Berkeley

discusses joint work with

Matthias Aschenbrenner, Robert Krone, Anton Leykin, Abraham Martin del Campo, Seth Sullivant

Computation in Infinite Dimensional Polynomial Rings

Let $R = K[x_1,x_2,x_3,\ldots]$ be the (infinite krull dimensional) polynomial ring over a field K. We discuss how to *compute* with ideals I in R.

- Group actions and Invariant Ideals
- Noetherianity (finite generation)
- Applications (algebraic stats, tensor rank)
- Partial orders and Reduction (normal forms)
- (Symmetric) Groebner Bases
- Algorithms that run on a computer

Motivational Problem

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

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

$$f_1 = x_1^3x_3 + x_1^2x_2^3$$
$$f_2 = x_2^2x_3^2 - x_2^2x_1 + x_1x_3^2$$

Problem: Given a polynomial g in R, is it in I?

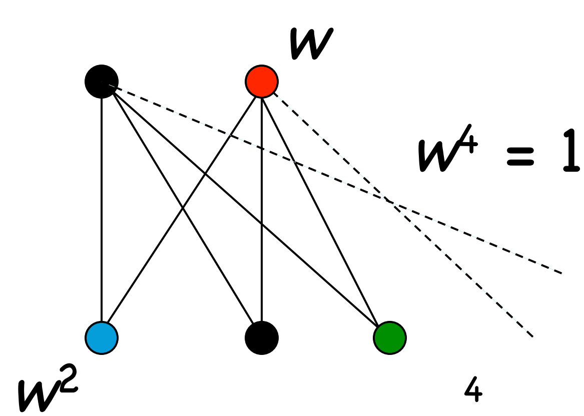
Motivational Problem

Concretely, if

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

Question: Can you write g as a finite linear combination over R of polynomials σf_i (σ are permutations and $i = 1,2$)?

- [HKL12] Applications of equation solving and ideal membership algorithms to coloring infinite highly symmetric graphs



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:

$$R[G] = \{\ r_1 g_1 + \cdots + r_m g_m \ :\ r_i \text{ in } R,\ g_i \text{ in } G\ \}$$

Multiplication is given by $(r_1 g_1)\cdot(r_2 g_2) = (r_1 r_2) g_1 g_2$

Assume that R is a G-module; that is, G gives an action on R that is linear:

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

- 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. $R = K[x_1,x_2,\ldots]$, $G = S_\infty$, $I = G{\cdot}\langle f_1, f_2\rangle_R$ is invariant
2. $R = K[x_1,x_2]$ and $G = S_2 = \{(1),(12)\}$

$$\underbrace{(x_1(1) + x_2(12))}_{R[G]} \cdot \underbrace{(x_1+x_2x_1^2)}_{R} = \underbrace{x_1^2 + x_2^2 + x_2x_1^3 + x_2^3x_1}_{R}$$

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

Noetherianity

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

Theorem [DE Cohen 67, AH07, Kemer 08, HS12]:
Invariant ideals of R are finitely generated over $R[G]$.
(R is a Noetherian $R[G]$-module)

Simplest Example: We cannot have

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

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

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

- Note: I might need arbitrarily large numbers of generators

Noetherianity

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

Theorem [DE Cohen 67, AH07, Kemer 08, HS12]:

Invariant ideals of R are finitely generated over $R[G]$.

(R is a Noetherian $R[G]$-module)

Applications:

Tensor algebra: Bounded-rank tensors are defined in bounded degree [Draisma-Kuttler 2011]

Algebraic Statistics: Finiteness for k-factor model [Draisma 10], Independent Set Conjecture [HS12]

Computational Algebra: Finite termination of ideal membership algorithms [AH08, HKL12]

Partial Order on Monomials

Let $<_{\text{lex}}$ be the lexicographic ordering of monomials with $x_1 <_{\text{lex}} x_2 <_{\text{lex}} x_3 <_{\text{lex}} \cdots$. 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**)

$u \leq v \;:\Leftrightarrow\;$ a shift of u divides v

$$x_1^2 \;<\; x_1x_2^2 \;<\; x_1^3x_2x_3^2 \;\not<\; x_1^3x_3^2x_4$$

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

$$SG_\sigma(f_1,f_2) = f_2 - \frac{m_2}{\sigma m_1}\sigma f_1$$

has a smaller (lex) leading monomial than f_2.

Reduction: if $m_1 < m_2$ one can reduce f_2 by f_1 by using a permutation σ to produce a smaller $<_{lex}$ lead monomial:

$$f_2 \dashrightarrow SG_\sigma(f_1,f_2) \in \langle f_1,f_2\rangle_{R[G]}$$

Reduction

The point: if I is invariant, f and g in I, and f --> h using g, then h in I with smaller (lex) leading monomial

In analogy to classical GB, we want to find a (finite) subset B of I such that to be in I is same as there being a sequence of reductions to zero by elements of B

$$f \dashrightarrow h_1 \dashrightarrow h_2 \dashrightarrow \dots \dashrightarrow 0$$

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

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

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

Equivariant Groebner Bases

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

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

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

So our previous theorem may be deduced from

Theorem [AH07, HS12]: An invariant ideal of R has a finite Groebner basis B

Termination: Higman's Lemma (1952) replaces Dickson's

Algorithms

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

Algorithm [AH08, HKL12]: Let $I = \langle f_1, f_2, \ldots, f_n \rangle_{R[G]}$ be an invariant ideal of R. There exists a terminating algorithm to compute a minimal Groebner Basis B for I

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

- Initial implementation in SAGE by Simon King
- [HKL12] More implementations in M2 and termination results

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 Groebner basis is given by 7 polynomials:

$$G = \{x_1^2x_0^2,\ x_1^3x_0,\ x_1x_0,\ x_2x_1x_0^2,\ x_2x_1^2 - x_2^2x_0,\ x_2^2x_0 - x_1^2x_0,\ x_2x_1^2 - x_1x_0\}$$

Then g in I iff when we reduce g by G the result is 0.

Note: Traditionally, we would compute a (normal) Groebner basis of the S_n orbit of the generators of I, where n is the number of indeterminates in g.

Motivational Problem Again

So, is

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

in the ideal I ?

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

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

Additional Research

1. (Open) Extensions to other group actions G.
2. (Open) Applications to finite dimensional situation.
3. (Open) Can we read off properties of the ideals I from their Groebner bases as in the traditional case?
4. Applications to finiteness questions in algebraic statistics (with S. Sullivant) and chains of toric ideals (with A. Martin del Campo)
5. (Open) Noncommutative applications.

The End

(of talk)