Algorithms for Equivariant Gröbner Bases

Robert Krone

Georgia Institute of Technology

June 6, 2013

(joint with Chris Hillar and Anton Leykin)

Computational Difficulties of Infinite Variables

For polynomial ring $S = k[x_1, \ldots, x_n]$ with k a field,

- S is Noetherian.
- Every ideal $I \subset S$ is finitely generated (Hilbert Basis Theorem).
- We can calculate finite Gröbner bases of I to facilitate computations with I.

For polynomial ring $R = k[x_1, x_2, \ldots]$ with k a field,

- R is not Noetherian.
- Generally an ideal $I \subset R$ is not finitely generated.
- Gröbner bases are therefore out of reach.

Variable Sets with an Action

Let Π be a monoid which acts on $\mathbb{N}$, e.g.

- $\mathrm{Sym}(\mathbb{N})$ the infinite symmetric group,
- $\mathrm{Inc}(\mathbb{N})$ the monoid of strictly increasing functions $\mathbb{N} \to \mathbb{N}$.

Let X be a countably infinite set of variables, indexed by natural numbers e.g.

- $X_1 := \{x_i \mid i \in \mathbb{N}\}$,
- $X_k := \{x_{(j_1,\dots,j_k)} \mid (j_1,\dots,j_k) \in \mathbb{N}^k,\ \text{each } j_i \text{ distinct}\}$,
- $X_{k_1,\dots,k_N} := X_{k_1} \sqcup \cdots \sqcup X_{k_N}$.

For $x_{(j_1,\dots,j_k)} \in X$, $\pi \in \Pi$

$$\pi x_{(j_1,\dots,j_k)} = x_{(\pi(j_1),\dots,\pi(j_k))}.$$

This gives an action of Π on $R = K[X]$.

Invariant Ideals

Definition

A Π-*invariant ideal* $I \subset R$ is an ideal closed under the action of Π.

$$\pi I \subseteq I \quad \text{for all } \pi \in \Pi.$$

Example

- The maximal ideal $\mathfrak{m} = \langle x_0, x_1, \ldots \rangle \subset K[X_1]$ is a $\mathrm{Sym}(\mathbb{N})$-invariant ideal.
- $\langle x_{(i,j)} \mid i, j \in \mathbb{N},\ i > j \rangle \subset K[X_2]$ is an $\mathrm{Inc}(\mathbb{N})$-invariant ideal.

$\langle F \rangle_\Pi$ denotes the Π-invariant ideal generated by the orbits of set $F \subset R$.

Definition

A ring R with Π-action is Π-*Noetherian* if all Π-invariant ideals of R are generated by the Π-orbits of finitely many polynomials (Π-finitely generated).

Example

- $\mathfrak{m} = \langle x_0, x_1, \ldots \rangle = \langle x_0 \rangle_{\mathrm{Sym}(\mathbb{N})} = \langle x_0 \rangle_{\mathrm{Inc}(\mathbb{N})}$.
- $\langle x_{(i,j)} \mid i, j \in \mathbb{N},\ i > j \rangle = \langle x_{(1,0)} \rangle_{\mathrm{Inc}(\mathbb{N})}$.

$\mathrm{Sym}(\mathbb{N})$ and $\mathrm{Inc}(\mathbb{N})$

For $f \in R$ with index support in $[n]$,

- any $\sigma \in \mathrm{Inc}(\mathbb{N})$ has $\sigma f = \pi f$ for some $\pi \in \mathrm{Sym}(\mathbb{N})$.
- any $\pi \in \mathrm{Sym}(\mathbb{N})$ has $\pi f = \sigma \rho f$ for some $\rho \in \mathrm{Sym}([n])$ and some $\sigma \in \mathrm{Inc}(\mathbb{N})$.

Example

$$(1\ 7\ 3\ 5\ 2)(x_1^2 x_3 - x_2) = x_7^2 x_5 - x_1 = \sigma(1\ 3\ 2)(x_1^2 x_3 - x_2)$$

where $\sigma(1) = 1$, $\sigma(2) = 5$, $\sigma(3) = 7$.

Remark

If $F \subset R$ is finite, it has index support in some $[n]$ and then

$$\langle F \rangle_{\mathrm{Sym}(\mathbb{N})} = \langle \mathrm{Sym}([n]) F \rangle_{\mathrm{Inc}(\mathbb{N})}.$$

- $\mathrm{Sym}(\mathbb{N})$-invariance $\Rightarrow$ $\mathrm{Inc}(\mathbb{N})$-invariance.
- $\mathrm{Inc}(\mathbb{N})$-Noetherianity $\Rightarrow$ $\mathrm{Sym}(\mathbb{N})$-Noetherianity.

Some Noetherianity Results

- (Cohen; Aschenbrenner, Hillar, Sullivant):
  $K[X_{1,\dots,1}]$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian.
- (Hillar, Sullivant):
  $K[X_k]$ is not $\mathrm{Sym}(\mathbb{N})$-Noetherian for $k > 1$.

$$I = \langle x_{(0,1)}x_{(1,0)},\ x_{(0,1)}x_{(1,2)}x_{(2,0)},\ x_{(0,1)}x_{(1,2)}x_{(2,3)}x_{(3,0)}, \dots \rangle_{\mathrm{Sym}(\mathbb{N})} \subset K[X_2].$$

- (Draisma, Eggermont, Leykin, K):
  For any $K[X_{k_1,\dots,k_N}]$ and $\mathrm{Sym}(\mathbb{N})$-equivariant monomial map $\phi : K[X_{k_1,\dots,k_N}] \to K[X_{1,\dots,1}]$, $\ker\phi$ is $\mathrm{Sym}(\mathbb{N})$-finitely generated.
- (Krasilnikov):
  $\mathrm{Inc}(\mathbb{N})$-invariant subalgebras of $K[X_{1,\dots,1}]$ are generally not $\mathrm{Inc}(\mathbb{N})$-Noetherian.

$$S = K[x_{1,i}x_{2,j} \mid i < j] \subset K[X_{1,1}],$$

$$I = \langle x_{1,1}x_{2,n}\prod_{i=1}^{n-1} x_{1,i}x_{2,i+1} \mid n \geq 1\rangle_{\mathrm{Inc}(\mathbb{N})} \subset S.$$

- (Draisma, Eggermont, Leykin, K):
  $\mathrm{Sym}(\mathbb{N})$-invariant subalgebras of $K[X_{1,\dots,1}]$ are $\mathrm{Sym}(\mathbb{N})$-Noetherian.

Equivariant Gröbner Bases

Let $\geq$ be a monomial order on R.

Definition

The action of Π is *compatible* with $\geq$ if

$$a \geq b \Rightarrow \pi(a) \geq \pi(b) \quad \text{for all } \pi \in \Pi.$$

Equivalently $\text{in}_{\geq} \pi f = \pi(\text{in}_{\geq} f)$ for all $f \in R$.

Definition

For Π compatible with $\geq$, a Π-*equivariant Gröbner basis* of a Π-invariant ideal $I \subset R$ is a set $G \subset I$ such that

$$\langle \text{in}_{\geq} G \rangle_{\Pi} = \text{in}_{\geq} I.$$

Normal Form

The Π-divisibility partial order $\preceq$ on the monomials of R is given by

$$u \preceq v \quad \text{if} \quad \pi u | v \text{ for some } \pi \in \Pi.$$

Equivalently $u \preceq v$ if $v \in \langle u \rangle_\Pi$.

Definition

$A \subset R$ be finite and $f \in R$. Then $\mathrm{NF}_A(f)$ is obtained by the algorithm:

- If $\mathrm{in}_\geq a \not\preceq \mathrm{in}_\geq f$ for all $a \in A$, return f.
- If $\mathrm{in}_\geq a \preceq \mathrm{in}_\geq f$, let

$$f' = f - \frac{\mathrm{in}_\geq f}{\pi(\mathrm{in}_\geq a)} \pi(a),$$

  and repeat with $f = f'$.

Proposition

For G a Π-equivariant Gröbner basis of Π-invariant ideal I,

$$f \in I \quad \Leftrightarrow \quad \mathrm{NF}_G(f) = 0.$$

Equivariant Buchberger "Algorithm"

- Begin with finite generating set F.
- For each pair $f, h \in F$, compute $S_\Pi(f,h)$, a finite set of S-polynomials such that $\Pi \cdot S_\Pi(f,h) = S(\Pi f, \Pi g)$ where

$$S(a,b) := \frac{\gcd(\mathrm{in}_\geq a, \mathrm{in}_\geq b)}{\mathrm{in}_\geq a} a - \frac{\gcd(\mathrm{in}_\geq a, \mathrm{in}_\geq b)}{\mathrm{in}_\geq b} b.$$

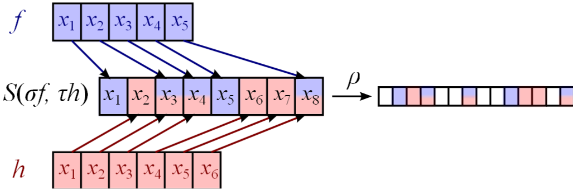
- If for some $s \in S_\Pi(f,g)$, $\mathrm{NF}_F(s) \neq 0$, then add s to F.
- Once all S-polynomials reduce to zero, return F. Otherwise repeat.

Inc($\mathbb{N}$) S-pairs

For $f, h \in R$ with index supports $[n]$ and $[m]$ respectively and $\rho_1, \rho_2 \in \text{Inc}(\mathbb{N})$,

$$S(\rho_1 f, \rho_2 h) = \rho S(\sigma f, \tau h)$$

with $\sigma : [n] \to [n+m]$ and $\tau : [m] \to [n+m]$.



σ and τ determine how the variables from f and h “interlace”.

$$|S_{\text{Inc}(\mathbb{N})}(f, g)| = \sum_{k=1}^{\min(m,n)} \binom{n+m-k}{n-k} \binom{m}{m-k}.$$

What do we need to run equivariant Buchberger on $I \subset R$?

- A monomial order compatible with Π
- For any pairs $f, g \in R$, the set $S(\Pi f, \Pi g)$ is the union of a finite number of Π-orbits, and these orbits can be computed.
- A finite generating set of I.

Will equivariant Buchberger terminate?

- If R is Π-Noetherian, then yes.
- Otherwise no guarantee.

Macaulay2 Package

`EquivariantGB`: top level Macaulay2 implementation of equivariant Buchberger for $\Pi = \text{Inc}(\mathbb{N})$ and $R = K[X_{k_1,\ldots,k_N}]$.
`http://people.math.gatech.edu/ rkrone3/EquivariantGB.html`

- `buildERing`: Constructs a ring of the correct form to input generators.
- `egb`: Computes an $\text{Inc}(\mathbb{N})$-equivariant Gröbner basis.
- `reduce`: Finds the normal form of a polynomial with respect to a set.

Some Computations with EquivariantGB

Example (de Loera, Sturmfels, Thomas)

Let $\phi : K[y_{(i,j)} \mid i,j \in \mathbb{N},\ i > j] \to K[x_i \mid i \in \mathbb{N}]$ be the Inc($\mathbb{N}$)-equivariant map

$$\phi : y_{(i,j)} \mapsto x_i x_j .$$

To find generators of $\ker \phi$, we compute an Inc($\mathbb{N}$)-equivariant Gröbnber basis for $I = \langle y_{(0,1)} - x_0 x_1 \rangle_{\mathrm{Inc}(\mathbb{N})}$, and eliminate x_i variables.

$$\ker \phi = \langle y_{(3,2)} y_{(1,0)} - y_{(3,0)} y_{(1,2)}, y_{(3,1)} y_{(2,0)} - y_{(3,0)} y_{(2,1)} \rangle_{\mathrm{Inc}(\mathbb{N})}.$$

Example

$$\phi : y_{(i,j)} \mapsto x_i^2 x_j .$$

$$\ker \phi = \langle y_{(3,1)} y_{(2,0)} - y_{(3,0)} y_{(2,1)}, y_{(3,2)}^2 y_{(1,0)} - y_{(3,1)} y_{(3,0)} y_{(2,1)},$$
$$y_{(4,2)} y_{(3,2)} y_{(1,0)} - y_{(4,0)} y_{(3,1)} y_{(2,1)} \rangle_{\mathrm{Inc}(\mathbb{N})}.$$

Going Forward

Technical improvements:

- Incorporate existing optimized GB algorithms.
- Implement lower level functionality.
- Parallelization.

Algorithmic improvements:

- Can the number of S-pairs considered be reduced?
- Is there a poly(n) time algorithm to decide if for monomials $u, v \in R[X_2]$ with index support in $[n]$, there is $\sigma \in \mathrm{Inc}(\mathbb{N})$ such that $\sigma u | v$?