ALGORITHMS FOR EQUIVARIANT GRÖBNER BASES

CHRISTOPHER J. HILLAR, ROBERT KRONE, AND ANTON LEYKIN

A polynomial ring over a countably infinite number of variables presents some obstacles to computation because it is not Noetherian. However, often ideals of interest in this setting are endowed with certain symmetry. Given an action of a monoid G on the set of variables, we consider G-equivariant ideals finitely generated up to the action of G. We describe an algorithm to compute *equivariant Gröbner bases* that may exist for such ideals in certain settings and its implementation, `EquivariantGB` package [8] for `Macaulay2` [5].

Included are two examples of computation of the kernels of toric maps of infinite-dimensional rings. One reproves the result of de Loera, Sturmfels, and Thomas [4] obtained theoretically. The other establishes that the kernel is finitely generated up to symmetry in the smallest open case of [1, Conjecture 5.10].

1. Introduction

Let $X = \{x_1, x_2, \ldots\}$ be a countably infinite collection of indeterminates. Fixing a field k, let $R = k[X]$ be the polynomial ring over k with indeterminates X. Let G be a monoid with a left action on X, so there is a natural left action of G on R. For a polynomial $f \in R$ and a monoid element $\sigma \in G$, the action of g on f is defined as

$$\sigma \cdot f(x_1, x_2, \ldots) = f(\sigma(x_1), \sigma(x_2), \ldots).$$

Indexing X by the natural numbers, two monoids of particular interest are

- $\mathfrak{S}_\infty$, the group of all permutations of $\mathbb{N}$, and
- $\mathrm{Inc}(\mathbb{N})$, the monoid of all strictly increasing functions $\mathbb{N} \to \mathbb{N}$.

Other examples of monoid actions of interest come from indexing the variables in other ways:

- Index X by $\mathbb{N} \times [n]$ for some positive integer n and act with either $\mathfrak{S}_\infty$ or $\mathrm{Inc}(\mathbb{N})$ on only the first index.
- Index X by $\mathbb{N} \times \mathbb{N}$ and act with either $\mathfrak{S}_\infty$ or $\mathrm{Inc}(\mathbb{N})$ diagonally on both indices.

The left actions of G and R on R can be combined into an action of the twisted monoid ring of G over R, denoted $R * G$. The additive structure of $R * G$ is the same as the monoid ring $R[G]$. Multiplication is defined term-wise by

$$f\sigma \cdot g\tau = f\sigma(g)(\sigma\tau)$$

for $f, g \in R$ and $\sigma, \tau \in G$, and extended by linearity. Note that elements of R and G do not commute with each other in $R * G$, mirroring the lack of commutativity of acting on R by permuting the variables and by multiplying by a polynomial. R has a natural $R * G$-module structure.

Definition 1.1. An ideal $I \subseteq R$ is *G-equivariant* (or simply *equivariant*) if

$$GI := \{\sigma f : \sigma \in G,\ f \in I\} \subseteq I.$$

G-equivariant ideals are exactly the $R * G$-submodules of R.

Definition 1.2. R is *G-Noetherian* if it satisfies the ascending chain condition for G-equivariant ideals.

In particular G-Noetherianity implies every G-equivariant ideal is finitely generated as an $R*G$-module, which is of particular interest to us. The notation $\langle f_1, \ldots, f_s \rangle_{R*G}$ will be used to denote the equivariant ideal generated by polynomials $f_1, \ldots, f_s$ as an $R * G$-module.

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

Theorem 1.3. [1] *R with variables indexed by $\mathbb{N}$ is $\mathfrak{S}_\infty$-Noetherian. Similarly R is* $\mathrm{Inc}(\mathbb{N})$*-Noetherian.*

Example 1.4. $I = \langle x_1, x_2, \ldots \rangle_R$ is a $\mathfrak{S}_\infty$-equivariant ideal of R. It can be expressed as $I = \langle x_1 \rangle_{R * \mathfrak{S}_\infty}$.

2. Equivariant Gröbner Bases

In order to define Gröbner bases, we give R a monomial order $>$, and impose the following requirement on the relationship between G and the order:

- For any monomials $x^\alpha, x^\beta \in R$, and $\sigma \in G$,

$$x^\alpha > x^\beta \quad \Leftrightarrow \quad \sigma x^\alpha > \sigma x^\beta.$$

If this condition is met we say G respects the order $>$. Note that there is no monomial order which the action of $\mathfrak{S}_\infty$ respects, so we won't be able to define $\mathfrak{S}_\infty$-equivariant Gröbner bases. However there are monomial orders which respect $\mathrm{Inc}(\mathbb{N})$, for example lexicographic order with

$$x_1 < x_2 < x_3 < \cdots .$$

We can use $\mathrm{Inc}(\mathbb{N})$ as a substitute for $\mathfrak{S}_\infty$ using the following fact.

Theorem 2.1. *For any finite $F \subset R$, there exists n such that $F \subset k[x_1, \ldots, x_n]$. Then*

$$\langle F \rangle_{\mathfrak{S}_\infty} = \langle \mathfrak{S}_n F \rangle_{\mathrm{Inc}(\mathbb{N})}.$$

So any $\mathfrak{S}_\infty$-equivariant ideal generated by F can be represented as a $\mathrm{Inc}(\mathbb{N})$-equivariant ideal with a finite generating set easily constructed from F.

Definition 2.2. A G-equivariant Gröbner basis for equivariant ideal I with monomial order $>$ that respects G is a set $B \subset I$ such that for any $f \in I$, there is $g \in B$ such that

$$\mathrm{in}_> f = m \cdot \mathrm{in}_> g$$

for some monomial $m \in R * G$.

The normal form of a polynomial f with respect to a set of polynomials B, denoted $\mathrm{NF}_B(f)$, is defined in the usual way. We reduce by an element $g \in B$ if there is some $\sigma \in G$ such that $\sigma \cdot \mathrm{in}_> g$ divides $\mathrm{in}_> f$.

An implementation issue with this equivariant normal form algorithm is efficiently finding $\sigma \in G$ such that $\sigma \, \mathrm{in}_> g$ divides $\mathrm{in}_> f$. This can be difficult depending on the monoid action. In the case of $G = \mathrm{Inc}(\mathbb{N})$ acting on a single index, there is a linear time greedy algorithm, by mapping each variable in $\mathrm{in}_> g$ in turn to the first possible variable in $\mathrm{in}_> f$ with a large enough exponent. For $G = \mathrm{Inc}(\mathbb{N})$ acting diagonally on variables indexed by $\mathbb{N} \times \mathbb{N}$, we are not aware of a polynomial time algorithm. Computing σ as efficiently as possible is an opportunity for improvement.

Theorem 2.3. *Let B be a G-equivariant Gröbner basis for equivariant ideal I. Then $f \in I$ if and only if f has normal form 0 with respect to B.*

3. Equivariant Buchberger algorithm

If the ring R is G-Noetherian, then every equivariant ideal has a finite equivariant Gröbner basis. Even if R is not G-Noetherian some finitely generated ideals may still have a finite equivariant Gröbner basis. In either case, given a set of generators for an equivariant ideal we can run our variant of the Buchberger algorithm. If the computation terminates, then the output is an equivariant Gröbner basis.

The main departure from the usual Buchberger algorithm comes when computing S-polynomials from a given pair of polynomials f, h. In the standard Buchberger algorithm, there is only one S-polynomial to consider, $S(f, h)$. In the equivariant case, there is no longer a single S-polynomial which generates all differences $m_1 f - m_2 h$ where $\mathrm{in}_> m_1 f = \mathrm{in}_> m_2 h$ for m_1, m_2 monomials in $R * G$. Instead we need to generate all S-polynomials in the set

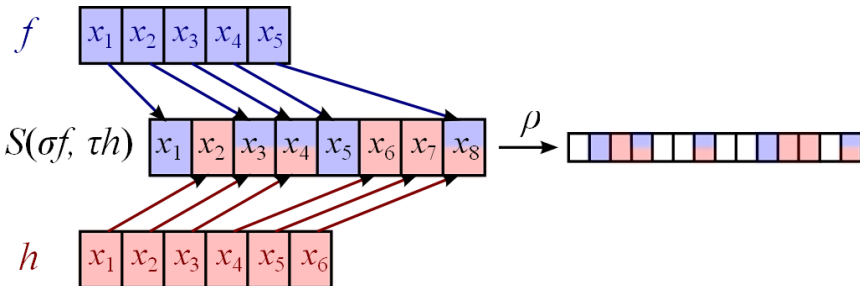
$$S(Gf, Gh) := \{S(\sigma f, \tau h) : \sigma, \tau \in G\}.$$

Typically this set is infinite, so for the algorithm to succeed we need to impose another requirement on the action of G:

- For each $f, h \in R$, the set $Gf \times Gh$ is contained in the union of of a finite number of G-orbits $G(\sigma_1 f, \tau_1 h), \ldots, G(\sigma_r f, \tau_r h)$, and we can compute the pairs $(\sigma_1, \tau_1), \ldots, (\sigma_r, \tau_r)$.

Theorem 3.1. *Fixing $f, h \in R$, there is some n such that $f, h \in k[x_1, \ldots, x_n]$. Then for any $\sigma', \tau' \in \mathrm{Inc}(\mathbb{N})$, there exist strictly increasing functions $\sigma, \tau : [n] \to [2n]$ and $\rho \in \mathrm{Inc}(\mathbb{N})$ such that*

$$\rho(\sigma f, \tau h) = (\sigma' f, \tau' h).$$



Therefore we can consider only S-polynomials of the form $S(\sigma f, \tau h)$ with $\sigma, \tau : [n] \to [2n]$. The theorem also holds for $\mathrm{Inc}(\mathbb{N})$ acting on variables indexed by $\mathbb{N} \times \mathbb{N}$ or $\mathbb{N} \times [n]$. Note that the number of pairs of strictly increasing functions $[n] \to [2n]$ is $\binom{2n}{n}^2$, which is large but finite.

We can make some improvements on the number of S-polynomials considered for each pair $f, h \in B$. In particular it's not necessary to consider all pairs of increasing maps $[n] \to [2n]$, but just the ways of "interlacing" the indices of f and h. These are the pairs (σ, τ) such that $\sigma[n] \cup \tau[n] = [n + r]$ for some $0 \leq r \leq n$. We call r the number of "gaps" in the pair since it is the number of values skipped in the image of each of the two maps. To count the number of interlacings with r gaps, we can choose any r elements of $[n + r]$ to be $\sigma[n] \setminus \tau[n]$ and any r of the remaining n elements to be $\tau[n] \setminus \sigma[n]$. So the total number of pairs is

$$\sum_{r=0}^{n-1} \binom{n+r}{r} \binom{n}{r}.$$

Note that gap size n can be ruled out. In this case the variable support of σf and τh will be disjoint, and so $S(\sigma f, \tau h)$ will always reduce to zero.

To further reduce the number of S-polynomials considered, we use the fact that, in practice, most elements of the Gröbner basis can be found from examining only the S-polynomials coming from interlacings with gap size 0 or 1. As a result, at each iteration, we only consider interlacings with gap size r if no new elements were found with gap size less than r. We must still consider all interlacings on the last pass to verify that the Buchberger criterion is satisfied.

4. Macaulay2 Package

We have implemented Buchberger's algorithm for equivariant Gröbner bases in a `Macaulay2` [5] package `EquivariantGB` [8]. The main function in the package is `egb` which takes a list of generators F for an equivariant ideal and returns an equivariant Gröbner basis for the ideal.

The generators passed to `egb` must belong to a ring R generated by the function `buildERing`. Such a ring has stored certain information about the how the monoid $G = \mathrm{Inc}(\mathbb{N})$ acts on the variables. R with the set of variables indexed by $\mathbb{N}^k$ is supported for any finite k, where G acts diagonally on the indices. R can also have multiple blocks of variables of this form. The algorithm uses lexicographic order, with the variables sorted by block, however we plan to allow the user to specify other orders in the future.

The optional argument `Symmetrize` determines whether `egb` computes a Gröbner basis for $\langle F \rangle_{\mathrm{Inc}(\mathbb{N})}$ or for $\langle F \rangle_{\mathfrak{S}_\infty}$.

Example 4.1. Let $Y = \{y_{i,j} : i > j;\ i,j \in \mathbb{N}\}$ and $X = \{x_i : i \in \mathbb{N}\}$. Let K be the kernel of the toric map $\varphi : k[Y] \to k[X]$ defined by $y_{i,j} \mapsto x_i x_j$. While K is not finitely generated in the usual sense, de Loera, Sturmfels, and Thomas [4] have shown that it is finitely generated up to symmetry.

We build the ring $R = k[Y, X]$ and note that the graph of φ has ideal $I = \langle y_{1,0} - x_1 x_0 \rangle_{\mathrm{Inc}(\mathbb{N})}$. We find an equivariant Gröbner basis for I with a monomial order eliminating X.

```
i1 : loadPackage "EquivariantGB";
i2 : R = buildERing({symbol y,symbol x},{2,1}, QQ, 2);
i3 : F = {y_(1,0) - x_1*x_0};
i4 : egb(F, Symmetrize => false)
                                                                    2
o4 = {x x  - y    , x y    - x y    , x y    - x y    , x y    - y   y    ,
       1 0    1,0   2 1,0    0 2,1   1 2,0    0 2,1   0 2,1    2,0 1,0

      y   y    - y   y    , y   y    - y   y    }
       3,1 2,0    3,0 2,1   3,2 1,0    3,0 2,1
```

This output matches the results communicated to us by Jan Draisma. Because the algorithm completed, we can conclude that the kernel of φ is finitely generated as a $\mathrm{Inc}(\mathbb{N})$-equivariant ideal, with generators

$$y_{3,1}y_{2,0} - y_{3,0}y_{2,1}, y_{3,2}y_{1,0} - y_{3,0}y_{2,1}.$$

This reproves the result of [4] without using any other argument other than the computation above.

Example 4.2. In the same way as in Example 4.1, we set up a computation of $K = \ker(y_{i,j} \mapsto x_i^2 x_j)$ and obtained the following equivariant Gröbner basis of $I = \langle y_{1,0} - x_1^2 x_0 \rangle_{\mathrm{Inc}(\mathbb{N})}$:

$$\begin{aligned}
\{\ & y_{3,1}y_{2,0} - y_{3,0}y_{2,1},\ y_{3,2}^2 y_{1,0} - y_{3,1}y_{3,0}y_{2,1},\ y_{4,2}y_{3,2}y_{1,0} - y_{4,0}y_{3,1}y_{2,1},\\
& x_0^3 y_{2,1}^2 - y_{2,0}^2 y_{1,0},\ x_0^3 y_{3,1}y_{2,1} - y_{3,0}y_{2,0}y_{1,0},\ x_1 y_{2,0} - x_0 y_{2,1},\ x_1 x_0^2 y_{2,1} - y_{2,0}y_{1,0},\\
& x_1 x_0^2 y_{3,2}^2 - y_{3,0}^2 y_{2,1},\ x_1 x_0^2 y_{4,2}y_{3,2} - y_{4,0}y_{3,0}y_{2,1},\ x_1^2 x_0 - y_{1,0},\ x_2 y_{3,2}y_{1,0} - x_0 y_{3,1}y_{2,1},\\
& x_2 x_1 x_0 y_{3,2} - y_{3,0}y_{2,1},\ x_2 x_1 x_0 y_{4,3}^2 - y_{4,1}y_{4,0}y_{3,2},\ x_2 x_1 x_0 y_{5,3}y_{4,3} - y_{5,0}y_{4,1}y_{3,2},\ x_2^2 y_{1,0} - x_1 x_0 y_{2,1}\ \}
\end{aligned}$$

The first three elements generate K up to symmetry.

Initiated by finiteness questions of Andreas Dress arising from chemistry, chains of toric ideals that are invariant under a group action have been studied by several authors. Surprisingly, even the basic question of whether chains induced by toric maps are finite up to symmetry has been open for a number of years (see [1, Conjecture 5.10]). The result of our computation in Example 4.2 proves the smallest open case of this conjecture, verifying [6, Conjecture 37] with $\alpha = (2, 1)$.

5. Conclusion

Since its revival by Aschenbrenner and Hillar [1], the topic of equivariant ideals enjoyed a lot of attention due to potential applications. This was amplified by an implementation of an equivariant Buchberger algorithm by Brouwer and Draisma [3], an implementation custom-made to solve computationally an open problem in algebraic statistics.

Proof-of-concept implementations of an equivariant Buchberger algorithm were carried out also in `Singular` and `Sage` (in [2] and [7], respectively). We have created `EquivariantGB` to attack problems in more general settings with a long-term goal to improve the efficiency and extend the reach of this algorithm, whose theoretical and practical complexities are extremely high.

Currently the package is written in the interpreted script language of `Macaulay2`, part of the code can be sped up tremendously by a low-level implementation. We also envision using sparsity of monomial exponents by implementing a new type of a polynomial ring in the kernel of `Macaulay2`.

References

[1] Matthias Aschenbrenner and Christopher J. Hillar. Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.*, 359(11):5171–5192, 2007.

[2] Matthias Aschenbrenner and Christopher J. Hillar. An algorithm for finding symmetric grobner bases in infinite dimensional rings. In *ISSAC*, pages 117–124, 2008.

[3] Andries E. Brouwer and Jan Draisma. Equivariant Gröbner bases and the Gaussian two-factor model. *Math. Comp.*, 80(274):1123–1133, 2011.

[4] Jesús A. de Loera, Bernd Sturmfels, and Rekha R. Thomas. Gröbner bases and triangulations of the second hypersimplex. *Combinatorica*, 15(3):409–424, 1995.

[5] Daniel R. Grayson and Michael E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[6] Christopher J. Hillar and Abraham Martín del Campo. Finiteness theorems and algorithms for permutation invariant chains of Laurent lattice ideals. *J. Symbolic Comput.*, 50:314–334, 2013.

[7] Simon King. Sage manual: Symmetric Ideals of Infinite Polynomial Rings. `http://www.sagemath.org/doc/reference/sage/rings/polynomial/symmetric_ideal.html`.

[8] Robert Krone. EquivariantGB: equivariant Gröbner bases in Macaulay2. `http://people.math.gatech.edu/~rkrone3/EquivariantGB.html`.

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

Georgia Institute of Technology, Atlanta, GA
E-mail address: `krone@math.gatech.edu`

Georgia Institute of Technology, Atlanta, GA
E-mail address: `leykin@math.gatech.edu`