Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DESY

Particles, Strings,
and the Early Universe
Collaborative Research Center SFB 676

Gröbner Bases IV: Applications

Alexander Haupt

13 June 2016

Slides available at: `bit.ly/1t0Ubp3`

Primary refs.:

[1] Cox, Little, O'Shea, "Ideals, Varieties, and Algorithms," (2015)

[2] Cox, Little, O'Shea, "Using Algebraic Geometry," (2005)

Summary of previous talk

Definition 3 (S-polynomial)

The **S-polynomial** of f and g: $S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$.

("Designed" to produce cancellation of leading terms)

S-pair criterion

Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a GB of I iff: $\overline{S(g_i, g_j)}^G = 0 \qquad \forall i \neq j$

$\rightarrow$ Buchberger's Algorithm (successively add nonzero remainders $\overline{S(f_i, f_j)}^G$ to G until S-pair criterion satisfied)

Definition 4

A **reduced GB** for a polynomial ideal I is a GB G for I s.t.:

(i) $\mathrm{LC}(p) = 1$ for all $p \in G$.

(ii) For all $p \in G$, no monomial of p lies in $\langle \mathrm{LT}(G \backslash \{p\}) \rangle$.

(Always exists and unique)

Part 3: How can it be useful?

- **Ideal membership problem**: ✓
  (1. find GB G, 2. use Cor. 2, i.e. $f \in I \Leftrightarrow \overline{f}^G = 0$)
- Proving that polynomials have **no common roots**: ✓
  (1. find GB G, 2. no common roots iff $1 \in G$)
  (e.g. reduced GB of $\langle x + y, x^2 - 1, y^2 - 2x \rangle$ is $\{1\}$)
- **Ideal Equality Algorithm**: ✓
  ($\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ generate same ideal iff they have same reduced GB for fixed monomial ordering)
- Next:
  1. **Solving Polynomial Equations** ($\rightarrow$ Elimination Theory)
  2. **Implicitization Problem**

- Back to our very first example: **What are the solutions of the following system of polynomial eqs.?**

$$\begin{aligned} 3x^2 + 2yz - 2wx &= 0, \\ 2xz - 2wy &= 0, \\ 2xy - 2z - 2wz &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0. \end{aligned} \tag{1}$$

- Consider ideal $I = \langle 3x^2+2yz-2wx, 2xz-2wy, 2xy-2z-2wz, x^2+y^2+z^2-1 \rangle$
- Let's **compute a reduced GB** of I for lex order with $w > x > y > z$.
- E.g. use Mathematica's `GroebnerBasis` (running time < 0.005 s)

$$w - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2,$$
$$x^2 + y^2 + z^2 - 1,$$
$$xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z,$$
$$xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z,$$
$$y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z,$$
$$y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z,$$
$$yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2,$$
$$z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z.$$

- Looks like a horrible mess (Note: coefficients of elements of GB can be **significantly messier** than coefficients of original generating set.)
- However, last polynomial **depends only on** z (i.e. "eliminated" other variables):

$$g_8 = z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z$$

- Miraculously, this factorizes into

$$\frac{1}{1152}z(z+1)(z-1)(3z+2)(3z-2)(128z^2-11)$$

- So, setting $g_8 = 0$ leads to "simple" solutions:

$$z = 0, \ \pm 1, \ \pm 2/3, \ \pm\sqrt{11}/(8\sqrt{2})$$

- Setting z equal to each of these values in turn, the remaining eqs. can be solved successively for y, x and w

In total 10 solutions:

$$
\begin{array}{llll}
z = 0; & y = 0; & x = 1; & w = 3/2, \\
z = 0; & y = 0; & x = -1; & w = -3/2, \\
z = 0; & y = \pm 1; & x = 0; & w = 0, \\
z = \pm 1; & y = 0; & x = 0; & w = -1, \\
z = 2/3; & y = 1/3; & x = -2/3; & w = -4/3, \\
z = -2/3; & y = -1/3; & x = -2/3; & w = -4/3, \\
z = \sqrt{11}/(8\sqrt{2}); & y = -3\sqrt{11}/(8\sqrt{2}); & x = -3/8; & w = 1/8, \\
z = -\sqrt{11}/(8\sqrt{2}); & y = 3\sqrt{11}/(8\sqrt{2}); & x = -3/8; & w = 1/8.
\end{array}
$$

- If you run in Mathematica

```
I={3x^2+2yz-2wx, 2xz-2wy, 2xy-2z-2wz, x^2+y^2+z^2-1};
Solve[I == 0, {w, x, y, z}]
```

  this is exactly the output you get
- And this is **what Mathematica is doing for you in the background**
- So, chances are you've already **unknowingly used GB techniques** (e.g. in Mathematica, Maple, ...)!

Observations:

- GB w.r.t. lex order simplifies form of eqs. considerably.
- In particular, get eqs. where variables are **eliminated** successively.
- Also, note: order of elimination seems to correspond to ordering of the variables.
- E.g. in example, $w > x > y > z$ and in GB w is eliminated first, x second, and so on.
- Easy to solve (last eq. contains only one variable) $\rightarrow$ **successively apply one-variable techniques**
- Note the analogy between this procedure and the method of **"back-substitution"** used to solve a linear system in triangular form.

- **What enabled us to find these solutions?** There were two things that made our success possible:
  - **(Elimination Step)** We could find a consequence $g_8 = 0$ of original eqs. which involved only z (i.e. eliminated x, y and w from system of eqs).
  - **(Extension Step)** Once we solved the simpler eq. $g_8 = 0$ to determine the values of z, we could extend these solutions to solutions of the original eqs.
- Basic idea of elimination theory: both Elimination Step and Extension Step can be done in great generality
- Indeed, notice that our observation concerning g_8 can be written as $g_8 \in I \cap \mathbb{C}[z]$
- In fact, $I \cap \mathbb{C}[z]$ consists of **all** consequences of our eqs. which eliminate x, y and w.

- These observations can be generalized:

Definition 5

Given $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$, the ℓ-th **elimination ideal** I_ℓ is the ideal of $k[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

- I_ℓ consists of **all consequences** of $f_1 = \ldots = f_s = 0$ which eliminate the variables $x_1, \ldots, x_\ell$.
- Note that **different orderings** of the variables lead to **different elimination ideals**.

Elimination Theorem

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let G be a GB of I w.r.t. lex order where $x_1 > x_2 > \cdots > x_n$. Then, for every $0 \leq \ell \leq n$, the set

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

is a GB of the ℓ-th elimination ideal I_ℓ.

- E.g. consider eq-sys (1) again. From Elimination Theorem

$$I_3 = I \cap \mathbb{C}[z] = \langle z^7 - \frac{1763}{1152} z^5 + \frac{655}{1152} z^3 - \frac{11}{288} z \rangle =: \langle g_8 \rangle$$

- Thus, g_8 is not random $\rightarrow$ **best possible way** (any other polynomial that eliminates x, y and w is a multiple of g_8)
- GB for **lex order** eliminates not only the first variable, but also the first two variables, the first three variables, etc.

- Next extend partial solution to full solution

Definition 6 (Ideal variety)

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. We will denote by $V(I)$ the set

$$V(I) = \{(a_1, \ldots, a_n) \in k^n | f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

- **partial solution** $:\Leftrightarrow (a_{\ell+1}, \ldots, a_n) \in V(I_\ell)$
- Now, **extend** $(a_{\ell+1}, \ldots, a_n)$ to a complete solution in $V(I)$
  - add one more coordinate to the solution, i.e. find a_ℓ s.t. $(a_\ell, a_{\ell+1}, \ldots, a_n) \in V(I_{\ell-1})$
  - suppose that $I_{\ell-1} = \langle g_1, \ldots, g_r \rangle$ in $k[x_\ell, x_{\ell+1}, \ldots, x_n]$. Want to find solutions $x_\ell = a_\ell$ of

$$g_1(x_\ell, a_{\ell+1}, \ldots, a_n) = \cdots = g_r(x_\ell, a_{\ell+1}, \ldots, a_n) = 0.$$

  - polynomials of one variable $x_\ell \implies$ possible a_ℓ's: roots of the gcd of the above r polynomials
  - basic problem: above polynomials may not have a common root (i.e. partial solution may not extend to complete solution)

The following theorem tells us when this can be done:

Extension Theorem

Let $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \leq i \leq s$, write f_i in the form

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{terms in which } x_1 \text{ has degree} < N_i,$$

where $N_i \geq 0$ and $c_i \in \mathbb{C}[x_2, \ldots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \ldots, a_n) \in V(I_1)$. If $(a_2, \ldots, a_n) \notin V(c_1, \ldots, c_s)$, then there exists $a_1 \in \mathbb{C}$ s.t. $(a_1, a_2, \ldots, a_n) \in V(I)$.

Note: $k = \mathbb{C}$ (in fact, Extension Theorem is false over $\mathbb{R}$), more generally need an **algebraically closed field** k here.

- Some more **examples** (revealing **caveats**):

1. Consider $I = \langle xy - 4, x^3 - y^2 - 1 \rangle$.
    - Compute GB G for lex order with $x > y$:

$$\{16x - y^4 - y^2, y^5 + y^3 - 64\}$$

    - Second polynomial, $y^5 + y^3 - 64$, has **no** rational roots.
    - No closed form expressions. E.g. using Mathematica's `Solve[]`:

$$\{\mathtt{y} \rightarrow \mathtt{Root[-64+\#1\hat{}3+\#1\hat{}5\&,1]},\ldots\}$$

    - Can only find numerical approximations:

$$x = 1.80699, y = 2.21363;$$
$$x = -1.38823 \mp 1.08623i, y = -1.78719 \pm 1.3984i;$$
$$x = 0.484732 \mp 1.61705i, y = 0.680372 \pm 2.26969i$$

    - **Finite numerical precision** can lead to subtle problems

2. Twisted cubic again. GB for lex order with $x > y > z$

$$I = \langle x^2 - y, xy - z, xz - y^2, y^3 - z^2 \rangle$$

- Elimination ideals

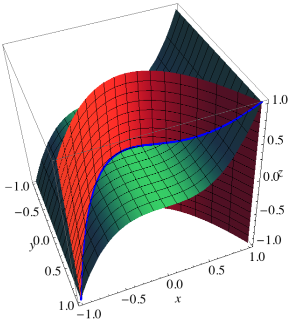
$$I_1 = I \cap \mathbb{C}[y, z] = \langle y^3 - z^2 \rangle = \langle g_4 \rangle,$$
$$I_2 = I \cap \mathbb{C}[z] = \langle 0 \rangle.$$

- So $V(I_2) = \mathbb{C}$ (i.e. every $a_3 \in \mathbb{C}$ is a partial solution).
- Which partial solutions $a_3 \in \mathbb{C}$ extend to $(a_1, a_2, a_3) \in V(I)$?
- Note: I_2 is elimination ideal of I_1
- Coefficient of y^3 in g_4 is 1, so $c_1 = 1$. Extension Thm says that solution extends to $(a_2, a_3) \in V(I_1)$ if $a_3 \notin V(1) = \emptyset$. So, it extends $\forall a_3 \in \mathbb{C}$
- Leading x-coefficients in remaining polynomials $g_1, \ldots, g_3$ are 1, y and z. Since 1 never vanishes, the Extension Thm guarantees that $a_3 \in \mathbb{C}$ always exists.
- New: free parameter $a_3 \in \mathbb{C} \to$ Implicitization Problem

- Points in twisted cubic variety $V(y - x^2, z - x^3)$ can be **parameterized** by setting $x = t$ in $y - x^2 = z - x^3 = 0$:

$$(x, y, z) = (t, t^2, t^3)$$

- This is used e.g. in plotting the graph of the twisted cubic:



- Inverse direction known as **Implicitization Problem**:
- Given a set of parametric equations (here: polynomials),

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned}$$

  defining a subset of an algebraic variety V in k^n.
- How can we find polynomial equations in the x_i that define V?

- Basic idea: **eliminate** the variables $t_1, \dots, t_m$ using GB
- We will take the **lex order** in $k[t_1, \dots, t_m, x_1, \dots, x_n]$ defined by the variable ordering

$$t_1 > \cdots > t_m > x_1 > \cdots > x_n.$$

- Now suppose we have a GB of the ideal

$$\tilde{I} = \langle x_1 - f_1, \dots, x_n - f_n \rangle.$$

- Since we are using lex order, we expect the GB to have polynomials that eliminate variables, and $t_1, \dots, t_m$ should be eliminated first since they are biggest in our monomial order.
- Thus, the GB for $\tilde{I}$ should contain polynomials that only involve $x_1, \dots, x_n$ $\rightarrow$ **candidates** for the equations of V.

Example: Parameterized twisted cubic curve V:
$(x, y, z) = (t, t^2, t^3)$ Compute GB of $\tilde{I} = \langle t - x, t^2 - y, t^3 - z \rangle$ for lex order in $\mathbb{C}[t, x, y, z]$:

$$\{y^3 - z^2, -y^2 + xz, xy - z, x^2 - y, t - x\}$$

From Elimination Thm:

$$\tilde{I}_1 = \tilde{I} \cap \mathbb{C}[x, y, z] = \langle y^3 - z^2, -y^2 + xz, xy - z, x^2 - y \rangle$$

Thus $V \subseteq V(y^3 - z^2, -y^2 + xz, xy - z, x^2 - y)$.
However, difficult and more work required to decide whether

$$V = V(y^3 - z^2, -y^2 + xz, xy - z, x^2 - y)$$

$\rightarrow$ **Geometry of Elimination** (not considered here)

- Even with best currently known versions of the algorithm:
- Many examples of ideals for which the computation of a GB takes a **tremendously long time** and/or consumes a **huge amount of storage space**
- Several reasons
  - total degrees of intermediate polynomials can be **quite large**
  - Coefficients in GB can be **quite complicated** rational numbers, even when the coefficients of the original ideal generators were small integers
- $\rightarrow$ search for **upper bounds** on complixity of computation
- measure to what extent GB techniques will continue to be **tractable** as larger and larger problems are attacked

- Bounds on degrees of generators in a GB are **quite large**
- E.g. Mayr and Meyer (1982): ideal generated by polynomials of degree less than or equal to some d can involve polynomials of degree proportional to 2^{2^d}
- 2^{2^d} grows **very rapidly** as $d \to \infty$!
- E.g. GB of $I = \langle x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w \rangle$ for grevlex order with $x > y > z > w$ (Mora (1983)): reduced GB contains the polynomial $z^{n^2+1} - y^{n^2} w$.
- However, experience shows that "on average" computations **often much more manageable** than in worst cases
- Experimentation with **changes of variables** and varying the **ordering of the variables** often can reduce the difficulty of the computation drastically
- in most cases, **grevlex** order produces GB with polynomials of the **smallest total degree** (Bayer and Stillmann (1987a))

Take home message (regarding Complexity Issues)

- Lex ordering very useful for **solving** system of polynomials
- But: lex ordering can be very **computationally intensive**!
- Hence, always choose the monomial ordering wisely
- It should be adapted to the problem at hand (lex ordering not always needed)

- E.g. for implicitization problem it's overkill (elimination order suffices)
- Also not needed for deciding whether $V(I) \subseteq k^n$ is a finite set
- (Lex ordering s.t. $x_1 > \cdots > x_n$ is an elimination ordering for every partition $\{x_1, \ldots, x_k\}, \{x_{k+1}, \ldots, x_n\}$. Thus a GB for this ordering carries much more information than usually necessary. This may explain why GB for lex ordering are usually the most difficult to compute.)

- What to do if lex ordering is still needed (e.g. for solving polynomial equations)?

1. Clever trick: compute GB for another monomial ordering (grevlex often fastest) and then do a **“basis conversion”** (→ FGLM basis conversion algorithm, Gröbner Walk)
2. Instead of Buchberger’s algorithm, use a **more advanced algorithm** to compute GB
(→ Faugère F4, F5)

- Most modern **computer algebra systems** (e.g. Maple, Magma, Singula, Sage, Macaulay2) feature implementations of various versions and combinations of 1) and 2)

Thank you for your attention.

Slides available at: `bit.ly/1t0Ubp3`

Backup slides

Example (1): GB for grlex order (running time 0.002 s)

$$x^2 + y^2 + z^2 - 1,$$
$$wz - xy + z,$$
$$wy - xz,$$
$$2wx + 3y^2 - 2yz + 3z^2 - 3,$$
$$-xy + 17xz + 17yz^2 - 13z^3 + 13z,$$
$$-6xy + 17y^2z + 7z^3 - 7z,$$
$$-7xy - 17xz + 17y^3 - 17y + 11z^3 - 11z,$$
$$12w^2 + 10w + 24xz^2 - 15x + 27y^2 + 9yz + 25z^2 - 27,$$
$$12w^2 + 2w + 24xyz - 3x + 27y^2 - 3yz + 17z^2 - 27,$$
$$12w^2 + 10w + 24xy^2 - 15x + 27y^2 - 15yz + 25z^2 - 27,$$
$$12w^3 - 23w - 6x - 6yz - 11z^2,$$
$$1164w^2 + 466w - 699x + 2619y^2 - 699yz + 1152z^4 + 769z^2 - 2619.$$

(Note: 12 instead of 8 polynomials; all mixed)

Example (1): GB for grevlex order (running time 0.002 s)

$$
\begin{aligned}
& -wz + xy - z, \\
& wy - xz, \\
& x^2 + y^2 + z^2 - 1, \\
& 2wx + 3y^2 - 2yz + 3z^2 - 3, \\
& -wz + 17xz + 17yz^2 - 13z^3 + 12z, \\
& 12w^2 + 10w + 24xz^2 - 15x + 27y^2 + 9yz + 25z^2 - 27, \\
& 12w^2 + 24wz^2 + 2w - 3x + 27y^2 - 3yz + 41z^2 - 27, \\
& -6wz + 17y^2z + 7z^3 - 13z, \\
& 17w^2z + 23wz + 10z^3 - 4z, \\
& -7wz - 17xz + 17y^3 - 17y + 11z^3 - 18z, \\
& 12w^3 - 23w - 6x - 6yz - 11z^2, \\
& 1164w^2 + 466w - 699x + 2619y^2 - 699yz + 1152z^4 + 769z^2 - 2619.
\end{aligned}
$$

(Note: 12 instead of 8 polynomials; all mixed)