Gröbner Bases III: Algorithms

Alexander Haupt

06 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)

- Imagine you are given a system of polynomial eqs., e.g.

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

- Qu.: what are the (real/complex) solutions to this? (i.e. find all points in the ideal variety $V(I)$)
- For a linear system, one learns in high school that **Gaussian elimination** yields an algorithmic answer (basic idea: eqsys $\rightarrow$ coeff. matrix $M \rightarrow$ bring M in upper triangular form using allowed row operations on M)
- It doesn't apply to (1). Instead: **GB theory**
- Up to this point, we learned that a GB exists for (1)
- What's missing is the following... (= topics of this talk):

1. How to decide whether a given basis is a GB?
2. How to construct a GB for a given system of polynomials? ($\rightarrow$ Algorithms)
3. How can it be useful? ($\rightarrow$ Applications)

- Key result & concept of last talk:

Hilbert Basis Theorem

Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.

Definition of Gröbner basis

Fix a variable & monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$ is called a **Gröbner basis** if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

- Corollary 1: every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a GB.
- Corollary 2: Let I be an ideal and $f \in k[x_1, \ldots, x_n]$. Then $f \in I \Leftrightarrow$ remainder on division of f by a GB of I is 0.
- Solves ideal membership problem **provided** you have a GB!

Part 1: How to decide whether a given basis is a GB?

Definition 1

We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a GB for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order).

Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.

Definition 2 (LCM)

If $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the **least common multiple** of $\text{LM}(f)$ and $\text{LM}(g)$, written $x^\gamma = \text{lcm}(\text{LM}(f), \text{LM}(g))$.

Definition 3 (S-polynomial)

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

(Note that we are inverting the leading coefficients here as well.)

Let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$ with grlex order. Then multideg$(f) = (3, 2)$, multideg$(g) = (4, 1)$, $\gamma = (4, 2)$ and

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3 \ . \end{aligned}$$

Remarks:

- $S(f, g) \in \langle f, g \rangle$.
- The total degree of $S(f, g)$ is larger than that of f and g.
- However: multideg$(S(f, g)) < \gamma$ (here $<_{grlex}$).
  $\rightarrow$ S-polynomial is "designed" to produce **cancellation of leading terms!**

Previous observation leads to criterion for deciding whether a given basis is a GB:

S-pair criterion (AKA Buchberger's Criterion)

Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a GB of I iff

$$\overline{S(g_i, g_j)}^{G} = 0 \qquad \forall i \neq j$$

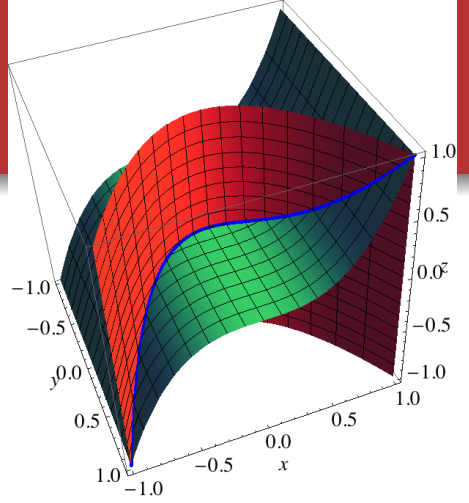
Proof:

$\Rightarrow$: If G is GB, then since $S(g_i, g_j) \in I$, by Cor. 2: $\overline{S(g_i, g_j)}^{G} = 0$.

$\Leftarrow$: see [1, pp. 86-88]

Remarks:

- Now, it's easy to show whether given basis is GB.
- S-pair criterion also leads naturally to an **algorithm** for computing GBs.



Consider $I = \langle y - x^2, z - x^3 \rangle$ (twisted cubic in $\mathbb{R}^3$).
Claim: $G = \{y - x^2, z - x^3\}$ is a GB for lex order with $y > z > x$.
Proof: Consider the S-polynomial ($f = y - x^2$, $g = z - x^3$, $\mathrm{LT}(f) = y$, $\mathrm{LT}(g) = z$, $\mathrm{multideg}(f) = (0, 1, 0)$, $\mathrm{multideg}(g) = (0, 0, 1)$, $\gamma = (0, 1, 1)$)

$$S(f, g) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Using the division algorithm, one finds that

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0,$$

so that $\overline{S(f, g)}^G = 0$.

BUT: Same $G = \{y - x^2, z - x^3\}$ is **not** a GB for lex order with $x > y > z$!

Proof: Consider the S-polynomial ($f = y - x^2$, $g = z - x^3$, $\mathrm{LT}(f) = -x^2$, $\mathrm{LT}(g) = -x^3$, $\mathrm{multideg}(f) = (2,0,0)$, $\mathrm{multideg}(g) = (3,0,0)$, $\gamma = (3,0,0)$)

$$S(f,g) = \frac{x^3}{-x^2}(y - x^2) - \frac{x^3}{-x^3}(z - x^3) = -xy + z.$$

Using the division algorithm, one finds that

$$-xy + z = 0 \cdot (y - x^2) + 0 \cdot (z - x^3) + (-xy + z),$$

(since $\mathrm{LT}(S(f,g)) = -xy \notin \langle \mathrm{LT}(f), \mathrm{LT}(g) \rangle$) so that $\overline{S(f,g)}^{G} \neq 0$.

Part 2: How to construct a GB?

- Up to now,
  - we know a GB always exists,
  - we can quickly decide whether a given basis is a GB.
- But, what to do if a given basis is not a GB? Are we doomed and have to guess into the blue? Surely not!
- Natural idea: extend original generating set by **adding more polynomials** in I.
- Adds nothing new (even introduces element of redundancy)
- But: worth it, due to extra info we get from a GB
- Q: **What new generators should we add?**
- A: Successively **add nonzero remainders** $\overline{S(f_i, f_j)}^G$ to G! (Natural consequence of S-pair criterion. Leads to the following **algorithm due to Buchberger**)

Consider previous example: $G = \{f_1, f_2\}$, $f_1 = y - x^2, f_2 = z - x^3$, for lex order with $x > y > z$.
We found $\overline{S(f_1, f_2)}^{G} = -xy + z$.
$\rightarrow$ set $f_3 = -xy + z$ and consider $G' = \{f_1, f_2, f_3\}$. Then $\overline{S(f_1, f_2)}^{G'} = 0$, but: $\overline{S(f_1, f_3)}^{G'} = xz - y^2$, $\overline{S(f_2, f_3)}^{G'} = 0$.
$\rightarrow$ set $f_4 = xz - y^2$ and consider $G'' = \{f_1, f_2, f_3, f_4\}$. Then $\overline{S(f_1, f_4)}^{G''} = 0$, $\overline{S(f_2, f_4)}^{G''} = \overline{S(f_3, f_4)}^{G''} = y^3 - z^2$.
$\rightarrow$ set $f_5 = y^3 - z^2$ and consider $G''' = \{f_1, f_2, f_3, f_4, f_5\}$. Then $\overline{S(f_i, f_5)}^{G'''} = 0$ for $i = 1, 2, 3, 4$ (and hence for all pairs).

$\Longrightarrow$ a lex GB for $I = \langle y - x^2, z - x^3 \rangle$ with $x > y > z$ is given by

$$\{f_1, f_2, f_3, f_4, f_5\} = \{y - x^2, z - x^3, -xy + z, xz - y^2, y^3 - z^2\}$$

Buchberger's Algorithm (Buchberger 1965)

Let $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a GB for I can be constructed in a finite number of steps by the following algorithm:

input : $F = (f_1, \ldots, f_s)$
output: a GB $G = (g_1, \ldots, g_t)$ for I, with $F \subseteq G$
$G := F$
repeat
  $G' := G$
  for each pair $\{p, q\}$, $p \neq q$ in G' **do**
    $r := \overline{S(p,q)}^{G'}$
    if $r \neq 0$ **then** $G := G \cup \{r\}$
until $G = G'$
return G

Comments and Remarks:

- Algorithm is only a rudimentary version for sake of clarity (e.g. not all remainders need to be checked at each step; enough to check $\overline{S(f_i, f_j)}^{G'}$, w/ $i \leq j-1$ & f_j new generator)
- Other, more refined/efficient, algorithms have been developed since Buchberger 1965
- # of steps (i.e. running time) depends on ordering of variables, monomials and input $F = (f_1, \ldots, f_s)$

GBs from prev. algorithm often bigger than necessary.
But: One can **eliminate some unneeded generators** owing to:

Lemma 1

Let G be a GB of $I \subseteq k[x_1, \ldots, x_n]$. Let $p \in G$ be a polynomial s.t. $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \backslash \{p\}) \rangle$. Then $G \backslash \{p\}$ is also a GB for I.

Proof: We know $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. If $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \backslash \{p\}) \rangle$, then $\langle \mathrm{LT}(G \backslash \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. $\overset{\text{by def.}}{\Longrightarrow}$ $G \backslash \{p\}$ is also a GB for I. $\square$

A GB for I is not unique. However, using Lemma 1, we can single out one "minimal" basis that is "better" than the others:

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 $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Reduced GBs have the following nice property.

Theorem 1

Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a reduced GB, and the reduced GB is **unique**.

- Example: twisted cubic for lex order with $x > y > z$.
- We found GB: $\{y - x^2, z - x^3, -xy + z, xz - y^2, y^3 - z^2\}$
- Is this a **reduced GB**?
  - (i) $\mathrm{LC}(p) = 1$? No $\rightarrow$ rescale: $\{x^2 - y, x^3 - z, xy - z, xz - y^2, y^3 - z^2\}$
  - (ii) Note: $x^3 \in \langle \mathrm{LT}(G \backslash \{x^3 - z\}) \rangle \rightarrow$ remove $x^3 - z$
- **Reduced GB**: $\{x^2 - y, xy - z, xz - y^2, y^3 - z^2\}$
- Note: this is the output you get from many computer algebra systems! E.g. Mathematica (`GroebnerBasis`), Maple (`with(Groebner)`, `Basis`), Sage (`groebner_basis()`), Magma (`GroebnerBasis`), ...
- Fr. Thm 1: **ideal equality algorithm**, i.e. two sets of polynomials $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ generate same ideal iff they have same reduced GB for fixed monomial ordering.