Introduction to Gröbner Bases and Computational Algebraic Geometry

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross
jlittle@holycross.edu

April 7, 2017

Varieties – the definition

- Let k be a field (usually $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ in this talk)
- $k[x_1, \ldots, x_n]$ is the polynomial ring in indeterminates x_i, coefficients in k
- If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then we define

  $$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0, i = 1, \ldots, s\}$$

  in k^n.
- If we want to be specific about where a variety "lives," we might write something like $V_{\mathbb{R}}(f_1, \ldots, f_s)$ for the real points, etc.

First examples

To draw pictures, we will almost always take $k = \mathbb{R}$

- $\mathbf{V}\left(\frac{x^2}{9} - \frac{y^2}{4} - 1\right)$ is a hyperbola in the plane
- $\mathbf{V}\left(x^2 + y^2 - 1, x - y + \frac{1}{2}\right)$ consists of the two intersection points of the circle defined by $x^2 + y^2 - 1 = 0$ and the line defined by $x - y + \frac{1}{2} = 0$.
- $\mathbf{V}(z - xy)$ is a hyperbolic paraboloid ("saddle surface") in $\mathbb{R}^3$
- $\mathbf{V}(y - x^2, z - x^3)$ is the *twisted cubic curve* in $\mathbb{R}^3$. It is contained in the saddle surface from the previous bullet.

Parametrizations

Some, but not all varieties can also be described as the images of *parametrization mappings*

$$\begin{aligned} F : k^m &\rightarrow k^n, \\ (t_1, \ldots, t_m) &\mapsto (F_1(t_1, \ldots, t_m), \ldots, F_n(t_1, \ldots, t_m)) \end{aligned}$$

where the F_i are polynomial or rational functions

- For instance, the circle $\mathbf{V}(x^2 + y^2 - 1)$ can be parametrized by $F(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$; image is the circle minus $\{(-1, 0)\}$.
- The twisted cubic $\mathbf{V}(y - x^2, z - x^3)$ is the image of $F(t) = (t, t^2, t^3)$

An Example (I think) you have studied

- Key idea: probabilities for discrete random variables often depend *polynomially* on some parameters
- So can think of parametrized families of distributions
- Example: If X is a *binomial random variable* based on n trials, with success probability θ, then X takes values in $\{0, 1, \ldots, n\}$ with probabilities given by:

$$P(X = k) = p_k(\theta) = \binom{n}{k} \theta^k (1-\theta)^{n-k}$$

- Gives:

$$\begin{aligned} \varphi : \mathbb{R} &\to \mathbb{R}^{n+1} \\ \theta &\mapsto (p_0(\theta), p_1(\theta), \ldots, p_n(\theta)) \end{aligned}$$

Example, continued

- Since $\sum_i p_i(\theta) = 1$, the image $\varphi(\mathbb{R})$ is subset of the hyperplane $\mathbf{V}(p_0 + \cdots + p_n - 1)$
- If $\theta \in [0, 1]$, then $\varphi(\theta) \in \Delta_{n+1}$, the probability simplex defined by $\sum_i p_i = 1$, and $0 \le p_i \le 1$ for $i = 0, \ldots, n$.
- Question: Is this image a variety?
- With $n = 2$,

$$p_0(\theta) = (1-\theta)^2,\ p_1(\theta) = 2\theta(1-\theta),\ p_2(\theta) = \theta^2$$

  and $\varphi(\mathbb{R}) = \mathbf{V}(p_1^2 - 4p_0p_2, p_0 + p_1 + p_2 - 1)$.
- For general n, we get what's called a *rational normal curve* of degree n – a (simple) example of a *toric variety*

What do we want to know about varieties?

Given a variety $V = \mathbf{V}(f_1, \ldots, f_s)$ might ask

- Is $V = \emptyset$? If not, what points does it contain?
- If V is finite as a set in k^n, how many points does it have?
- If V is not finite, how does it decompose as a union of varieties, what are their dimensions, etc.?
- The answers are nicest if k is algebraically closed(!) Then there's an especially close connection between varieties and *ideals* in $k[x_1, \ldots, x_n]$.
- Then, invariants of a variety like degree, genus (for curves – dim $V = 1$), ...

To Ideals

The set of defining equations $f_1 = 0, \ldots, f_s = 0$ defining a variety $V = \mathbf{V}(f_1, \ldots, f_s)$ is *never unique*.

- First notice that if $g, \ldots, g_s$ are any polynomials at all and $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$, then $f = g_1 f_1 + \cdots + g_s f_s$ satisfies

$$f(a_1, \ldots, a_n) = g_1(a_1, \ldots, a_n) \cdot 0 + \cdots + g_1(a_1, \ldots, a_n) \cdot 0 = 0$$

- Hence f *also vanishes at every point of* $V = \mathbf{V}(f_1, \ldots, f_s)$, and
- It follows that $\mathbf{V}(f_1, \ldots, f_s, f) = \mathbf{V}(f_1, \ldots, f_s)$

More motivation

- This gives a way to detect extra, unneeded equations in some cases: If $V = \mathbf{V}(f_1, \ldots, f_s)$ and $f_s = g_1 f_1 + \ldots + g_{s-1} f_{s-1}$ for some polynomials $g_1, \ldots, g_{s-1}$, then $V = \mathbf{V}(f_1, \ldots, f_{s-1})$ also.
- Finding polynomials $f = g_1 f_1 + \ldots + g_s f_s$ with "special" features like *factorizations* can also be useful.
- Example: Consider $W = \mathbf{V}\left(x^2 + y^2 + z^2 - 1, x^2 + y^2 - \frac{1}{4}\right)$ in $\mathbb{R}^3$. Notice:

$$\begin{aligned}(1)(x^2 + y^2 + z^2 - 1) \;&+\; (-1)(x^2 + y^2 - \frac{1}{4}) = z^2 - \frac{3}{4} \\ &= (z - \sqrt{3}/2)(z + \sqrt{3}/2)\end{aligned}$$

What does this tell us about the variety W?

Ideal generated by $f_1, \ldots, f_s$

Definition 1

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. The *ideal generated by the* $f_1, \ldots, f_s$ is the subset of $k[x_1, \ldots, x_n]$ defined by

$$\langle f_1, \ldots, f_s \rangle = \{g_1 f_1 + \cdots + g_s f_s \mid g_i \in k[x_1, \ldots, x_n]\}$$

For instance the example on the last slide shows

$$z^2 - \frac{3}{4} \in \left\langle x^2 + y^2 + z^2 - 1, x^2 + y^2 - \frac{1}{4} \right\rangle.$$

Ideals

Note that $I = \langle f_1, \ldots, f_s \rangle$ has the following properties:

a. If $f, g \in I$, then $f + g \in I$
b. If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $h \cdot f \in I$

Definition 2

A nonempty subset I of a $k[x_1, \ldots, x_n]$ is said to be *an ideal* if

a. $f, g \in I$ implies $f + g \in I$, and
b. $f \in I$ and $h \in k[x_1, \ldots, x_n]$ implies $h \cdot f \in I$.

Given any $f_1, \ldots, f_s$, $\langle f_1, \ldots, f_s \rangle$ satisfies this definition. But are there other ideals too in $k[x_1, \ldots, x_s]$ – (perhaps ones with only infinite generating sets)? The answer is "no" – we'll see an explanation shortly.

Other examples of ideals

The answer is not so clear at first:

- Let $S \subset k^n$ be any subset (for example a variety),

  $$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ all } a = (a_1, \ldots, a_n) \in S\}$$

  Easy to check this satisfies the definition. (Why?)
- If I is an ideal in $k[x_1, \ldots, x_n]$, $\sqrt{I}$ *(the radical of I)* is

  $$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^k \in I \text{ for some } k \geq 1\}.$$

- Have:

Theorem 3

Let I be an ideal in $k[x_1, \ldots, x_n]$. Then $\sqrt{I}$ is an ideal.

An observation

Theorem 4

Let $V = V(f_1, \ldots, f_s)$ be a variety, and let $\langle g_1, \ldots, g_t\rangle = \langle f_1, \ldots, f_s\rangle$. Then $V = V(g_1, \ldots, g_t)$ also.

- In other words, it's better to think that varieties are defined by ideals, not particular sets of equations – we'll write $\mathbf{V}(I)$.
- Proof: $V \subset \mathbf{V}(g_1, \ldots, g_t)$ is more or less clear since each $g_i = h_{i1}f_1 + \cdots + h_{is}f_s$ for some polynomials h_{ij}.
- The reverse inclusion follows in the same way since each $f_j = p_{j1}g_1 + \cdots p_{jt}g_t$ for some polynomials p_{ji}. QED

$\mathbf{I}(\mathbf{V}(I))$

- Suppose we start with an ideal and look at the variety $\mathbf{V}(I)$. Is $\mathbf{I}(\mathbf{V}(I)) = I$?
- One inclusion is always true. Which one?
- Answer to first question: *not always!* Example: Let $I = \langle x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $\mathbf{V}(I)$ is the y-axis in the plane, and it's not too hard to show $\mathbf{I}(\mathbf{V}(I)) = \langle x \rangle \neq I$.
- In fact, it follows directly that $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$: If $f \in \sqrt{I}$, then $f^k \in I$ for some $k \geq 1$. At any point a in $\mathbf{V}(I)$, $(f^k)(a) = (f(a))^k = 0$, which implies $f(a) = 0$. Therefore, $f \in \mathbf{I}(\mathbf{V}(I))$.

$\mathbf{I}(\mathbf{V}(I))$, continued.

- On the other hand, here is another example where $\mathbf{I}(\mathbf{V}(I)) = I$ is true. As above $I \subset \mathbf{I}(\mathbf{V}(I))$ always holds.
- Say $I = \langle y - x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $\mathbf{V}(I)$ is the usual parabola.
- Given any $f(x, y)$ we can substitute $f(x, y) = f(x, (y - x^2) + x^2)$ expand out and collect terms to obtain:

$$f(x, y) = q(x, y)(y - x^2) + r(x)$$

- If $f \in \mathbf{I}(\mathbf{V}(I))$ (that is if f vanishes at every point of the parabola $y - x^2$), then we must have $r(x) = 0$ for all $x \in \mathbb{R}$.
- But that implies $r(x)$ is the zero polynomial, so $f \in \langle y - x^2 \rangle$. This shows $\mathbf{I}(\mathbf{V}(I)) \subset I$ in this case, so they are equal.

Nullstellensätze

Theorem 5 (Weak Nullstellensatz)

If k is algebraically closed, $\mathbf{V}(I) = \emptyset \Leftrightarrow I = k[x_1, \ldots, x_n]$.

(Can be understood as the "multivariable Fundamental Theorem of Algebra")

Theorem 6 (Hilbert's Nullstellensatz)

If k is algebraically closed, then $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Both statements can fail without the hypothesis, e.g. $\mathbf{V}_{\mathbb{R}}(x^2 + y^2) = \emptyset$, but $\langle x^2 + y^2 \rangle \neq \mathbb{R}[x, y]$.

The key idea – "big picture"

- Particular generating sets ("bases") for ideals contain the information we need to answer questions posed before
- Among the "nicest" are the *Gröbner bases*
- Moreover each ideal I has many different Gröbner bases depending on *monomial orders*
- Potential downside: computing them takes a lot of computational effort and storage space in realistic cases (too much to do by hand); software like Singular, Macaulay 2, CoCoA, Magma, Sage, Maple typically used.
- In *big* examples, a very fast computer and or significant cleverness might be required!
- In *really big* examples, might be infeasible altogether

A first monomial order – lexicographic order

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

Definition 7

We say $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

-
- Example: In $k[x, y, z]$, let $x^\alpha = x^3y^4z$ and $x^\beta = x^2yz^8$.
- Then $\alpha = (3, 4, 1)$, $\beta = (2, 1, 8)$, $\alpha - \beta = (1, 3, -7)$
- So $x^3y^4z >_{lex} x^2yz^8$ (with $x > y > z$).

Another *lex* example

- Consider the polynomial $f(x,y) = x^3y^3 + x^5 + xy^4$ from before
- Which is the *lex* leading term (taking $x > y$)?
- The exponent vectors are $(3,3),(5,0),(1,4)$.
- In *lex* order, we have $(5,0) >_{lex} (3,3) >_{lex} (1,4)$
- Note: *lex* order is analogous to dictionary order for words(!)

A second order – graded reverse lex order

Definition 8

We say $x^\alpha >_{grevlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and in $\alpha - \beta$ the rightmost nonzero entry is *negative*.

- Example: $x^3y^2z >_{grevlex} x^4z$ as for *grlex*
- Example: $x^4yz >_{grevlex} x^3y^2z$ since total degrees are both 6, but $(4,1,1) - (3,2,1) = (1,-1,0)$
- Note that $f(x,y,z) = x^2y^2z^2 + xy^4z + x^5$ has different leading terms depending on which of the orders *lex, grevlex* we use

Why different monomial orders?

- When we introduce Gröbner bases, we'll see a monomial order is built into the definition
- Best answer – GB's with respect to different monomial orders do different (and all useful) things!
- *lex* order GB's systematically eliminate variables (good for direct approach to solving systems of equations, but computationally "expensive")
- GB's with respect to graded orders (including *grevlex*, are usually less "expensive" computationally
- There are also *conversion algorithms* to go from a GB with respect to one order to a GB with respect to another order

Leading terms, etc.

- Given a monomial order, we get a *leading term* in each polynomial.
- For instance, if $f(x, y, z) = 2x^3y^2 + \frac{1}{3}xy^2z + 4z^5$ and we use $>_{lex}$ (with $x > y > z$), then
- $LT_{>_{lex}}(f) = 2x^3y^2$ (including the coefficient)
- If order is clear from context we'll often omit it

Division in $k[x_1, \ldots, x_n]$

- Major difference with 1-variable case – we'll allow more than one divisor $f_1, \ldots, f_s$ (reason: not every ideal is generated by a single polynomial). So there will be as many quotients as divisors.
- There can be several $LT(f_i)$ that divide LT of the dividend. If so, we'll go down the list of the f_i from the start and use the first one found.
- Second major difference with 1-variable case – when a term is not divisible by any of the $LT(f_i)$, it goes into the remainder, but *division is not necessarily finished*.

Division theorem

Theorem 9

Given any input $f_1, \ldots, f_s$, f, and a monomial order, there is a division algorithm that terminates and yields an expression

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

where

i. *If $a_i f_i \neq 0$, then $LT(a_i f_i) \leq LT(f)$*
ii. *If $r \neq 0$, then no monomial in r is divisible by $LT(f_i)$ for any i, $1 \leq i \leq s$.*

(Note: there is a sense in which this expression is unique too, but it's more subtle than in the 1-variable case)

Example

Here's a first example. Suppose $f_1 = xz - y^2$, $f_2 = x^3 - yz$ and use *lex* order with $x > y > z$ so the first term in each is the leading term. Say $f = x^4 + x^3z$. [work out on board]

- Result is

$$x^4 + x^3z = (x^2 + y)(xz - y^2) + (x)(x^3 - yz) + (x^2y^2 + y^3)$$

Observations – an ideal membership test?

- If $r = 0$, it follows that $f \in \langle f_1, \ldots, f_s \rangle$.
- But the converse *fails*. Here is an example:
- Say f_i are as above: $f_1 = xy + x + 1$, $f_2 = y^2 - x$. If we take $f = yf_1 - xf_2 = xy + y + x^2$, and divide by (f_1, f_2) in that order, we get

$$xy+y+x^2 = (1)(xy+x+1)+(0)\cdot(y-x^2)+(x^2+y-x-1)$$

- Doesn't seem especially useful (yet)!

Motivation for definition of Gröbner bases

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$,
  $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$
- If we use $>_{grlex}$, then $LT(f_1) = xy$, $LT(f_2) = y^2$, but
  $LT(f) = -x^2$
- If we divide f by (f_1, f_2), then $r \neq 0$, even though $f \in \langle f_1, f_2 \rangle$
- The leading terms of the given generators f_1, f_2 don't account for *all possible leading terms* of elements of I
- Goal: "good" generating sets satifying $f \in I \Leftrightarrow r = 0$ on division (would give an *ideal membership test*!)
- Equivalently, we want generators $\{g_1, \ldots, g_t\}$ for I such that for every $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i.

The ideal of leading terms

- Start from a given ideal I and a given monomial order $>$
- For each $f \in I$, we have $LT_>(f)$
- Define $\langle LT_>(I)\rangle = \langle LT_>(f) \mid f \in I\rangle$
- That is $\langle LT_>(I)\rangle$ is the *ideal generated by the leading terms of all elements of I* according to the given monomial order.
- An example of a *monomial ideal* – an ideal generated by a collection of monomials – these have some nice properties

Dickson's Lemma

Theorem 10 (Dickson's Lemma)

Let M be a monomial ideal in $k[x_1, \ldots, x_n]$. Then M is generated by a finite collection of monomials.

- Return to the monomial ideal $\langle LT(I)\rangle$ for a given I and a given monomial order.
- By Dickson, we know that $\langle LT(I)\rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$.
- Every monomial in $\langle LT(I)\rangle$ is $LT(g)$ for some $g \in I$
- Consequence: There exist $g_i \in I$ such that $LT(g_i) = x^{\alpha(i)}$ for all $1 \leq i \leq t$.

Gröbner bases defined

- This leads to

Definition 11

Let I be a nonzero ideal and $>$ be a monomial order. A *Gröbner basis* for I with respect to $>$ is a finite set $G = \{g_1, \ldots, g_t\} \subset I$ such that $\langle LT_>(I)\rangle = \langle LT_>(g_1), \ldots, LT_>(g_t)\rangle$.

- Dickson's Lemma $\Rightarrow$

Theorem 12

If I is a nonzero ideal and $>$ is a monomial order, then Gröbner bases of I with respect to $>$ exist.

- Not unique, though, since generating sets for the monomial ideal $\langle LT(I)\rangle$ are not unique.

Consequences of Dickson, continued

Theorem 13

A Gröbner basis $G = \{g_1, \ldots, g_t\}$ for I generates I.

Proof.

Let $f \in I$ and divide by G – no terms end up in r, so we get $f = a_1 g_1 + \cdots + a_t g_t$. □

This also proves an unexpected "big theorem!"

Theorem 14 (Hilbert Basis Theorem)

Every ideal in $k[x_1, \ldots, x_n]$ is finitely generated.

Main tool for computing Gröbner bases – S-polynomials

- The definition:

Definition 15

Let $f, g \in k[x_1, \ldots, x_n]$ and $>$ be a monomial order. The *S-polynomial* of f, g is

$$S(f,g) = \frac{\mathrm{lcm}(LM(f), LM(g))}{LT(f)} f - \frac{\mathrm{lcm}(LM(f), LM(g))}{LT(g)} g$$

- This is defined to make the leading terms cancel.

Idea of Buchberger algorithm

- When we find a "new" leading term in an S-polynomial, we will just append the new polynomial to our list of generators(!)
- Even if the S-polynomial itself does not have a "new" leading term, we can still try to "strip away" terms we already know by computing *the remainder on division of the S-polynomial* by the generators of the ideal we already have.
- Note that if $S(f_i, f_j) = a_1 f_1 + \cdots + a_s f_s + r$ then by definition $r \in I = \langle f_1, \ldots, f_s \rangle$ so if $r \neq 0$, then its leading term will be something we want to know(!)

Buchberger's algorithm – basic form

```
Input: F = {f_1,...,f_s}
Output: G containing F
G := F
repeat
   G' := G
   for each pair p <> q in G' do
      S := remainder of S(p,q) on division by G'
      if S <> 0 then
         G = G union {S}
until G = G'
```

A technical result and the algorithm

- Buchberger's Criterion (proof is hard!) says that a finite basis G for I is a Gröbner basis of I if and only if the remainder on division of $S(g_i, g_j)$ by G is zero for all $1 \leq i < j \leq t$.
- The process of adding non-zero S-polynomial remainders terminates (after a finite number of iterations) because the ideals of leading terms of the G form an *ascending chain* (HBT $\Rightarrow$ ACC) and then we have a Gröbner basis.
- Many "tweaks" and improvements are also possible.

Reduced Gröbner bases – a test for $\mathbf{V}(I) = \emptyset$

- A GB $G = \{g_1, \ldots, g_t\}$ is *reduced* if the $LM_>(g_i)$ are a *minimal basis* of $\langle LT_>(I)\rangle$, and no term in g_i is divisible by $LT_>(g_j)$ for $j \neq i$ (analogous to row-reduced echelon form for linear equations!)
- Every ideal has reduced GB's wrt all monomial orders, and they are unique(!)
- For instance, $\{1\}$ is the unique reduced GB of $I = k[x_1, \ldots, x_n]$
- $\Rightarrow$ if k alg. closed, then $\mathbf{V}(I) = \emptyset \Leftrightarrow \{1\}$ is the unique reduced GB of I. (Note: $\Leftarrow$ is true for all k, so we now have a test for when $\mathbf{V}(I) = \emptyset$(!))

Elimination

- In elementary algebra, linear algebra, etc., a standard method for solving simultaneous equations in several variables is to form polynomial combinations that *eliminate variables*.
- Example: In the system

$$\begin{aligned} 2x - 3y &= 1 \\ 4x + 5y &= 3 \end{aligned}$$

- second equation minus $2\times$ first equation yields $11y = 1$, so $y = \frac{1}{11}$, and then $x = \frac{7}{11}$

Elimination ideals

- In our terms,

$$(-2)(2x-3y-1)+(1)(4x+5y-3)=11y-1$$

is in $I=\langle 2x-3y-1, 4x+5y-3\rangle$, *and* contains no x.

- Generalizing this,

Definition 16

Let $I \subset k[x_1,\ldots,x_n]$ be an ideal. The ℓth elimination ideal of I is

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

(in which the variables $x_1,\ldots,x_\ell$ have been eliminated).

- For example, $11y-1 \in I_1 = I \cap \mathbb{Q}[y]$.

Geometry of elimination

- If $I \subset k[x_1, \ldots, x_n]$, then we have the geometric object $\mathbf{V}(I) \subset k^n$
- If we then eliminate the first ℓ variables, we can ask, what is the corresponding variety $\mathbf{V}(I_\ell)$?
- Partial answer – it's very closely related to the projection of $\mathbf{V}(I)$ into the coordinate space $k^{n-\ell}$ of the variables $x_{\ell+1}, \ldots, x_n$.
- But a projection of a variety is not always a variety. (Example: project $\mathbf{V}(xy - 1)$ onto the x-axis.) However over $\mathbb{C}$ at least, $\mathbf{V}(I_\ell)$ is the *smallest variety* containing the projection of $\mathbf{V}(I)$.

Lex Gröbner bases and elimination

- A special property of *lex* order: Say the variables are ordered $x_1 > x_2 > \cdots > x_n$. If a monomial contains any positive power of x_1, then it is larger in *lex* order than all monomials that contain only $x_2, \ldots, x_n$. Similarly, any monomial that contains a positive power of x_2 is larger than all monomials containing only $x_3, \ldots, x_n$, etc.
- Suppose I is an ideal for which $I_\ell \neq \{0\}$, and let $f \neq 0$ be an element of I_ℓ
- If G is a *lex* Gröbner basis for I, there must be some $g_i \in G$ such that $LT(g_i)$ divides $LT(f)$, hence $LT(g_i)$ contains only $x_{\ell+1}, \ldots, x_n$.
- But then the observation above shows $g_i \in I \cap k[x_{\ell+1}, \ldots, x_n] = I_\ell$

Elimination Theorem

This is the key idea in the proof of:

Theorem 17 (Elimination Theorem)

Let I be an ideal in $k[x_1, \ldots, x_m]$ and let G be a Gröbner basis for I with respect to lex order with $x_1 > x_2 > \cdots > x_n$. For all ℓ let $G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$. Then G_ℓ is a Gröbner basis for the elimination ideal I_ℓ.

(Note: If $G_\ell = \emptyset$, this says $I_\ell = \{0\}$.)
In other words, *lex Gröbner bases systematically eliminate variables "as much as possible"*

A first example

- Let
$$I = \langle x^2y + y^2 + 2, xy - 3y + 1\rangle \subset \mathbb{Q}[x, y]$$
- If we compute a (reduced) *lex* Gröbner basis for I with $x > y$, we get $G_y =$
$$\{y^3 + 9y^2 - 4y + 1, x - y^2 - 9y + 1\}$$
- Note that the first polynomial depends only on y. It is the monic generator for $I_1 = I \cap \mathbb{Q}[y]$.
- The second polynomial contains x too.

Example, continued

- Note the form of

$$G_y = \{y^3 + 9y^2 - 4y + 1, x - y^2 - 9y + 1\}$$

- To find the points in $\mathbf{V}(I) = \mathbf{V}(x^2y + y^2 + 2, xy - 3y + 1)$, we could solve the one-variable equation $y^3 + 9y^2 - 4y + 1 = 0$ (numerically),
- Then, substitute the values into the other equation and determine x.
- There are three points in $\mathbf{V}(I)$ over $\mathbb{C}$, one with coordinates in $\mathbb{R}$, approx.

$$(-3.10598633669341, -9.43517845033930)$$

Example, continued

- If we reverse the order of the variables (i.e. look at *lex* order with $y > x$), then the reduced Gröbner basis changes
- Get $G_x =$

$$\{x^3 - 5x^2 + 12x - 19, y + x^2 - 2x + 6\}$$

- Now, the first basis element generates $I \cap \mathbb{Q}[x]$, and the second contains x, y.
- This other basis could be used in the same way to determine $\mathbf{V}(I)$ (and would yield the same results!)

Finite varieties

- Note that in this last example, for *lex* order with $x > y$, the complement of $\langle LT_>(I)\rangle$ contains just $\{1, y, y^2\}$
- In general $\mathbf{V}(I)$ finite over an algebraically closed field $\Leftrightarrow$ the *complement of the monomials in* $\langle LT_>(I)\rangle$ *in the set of all monomials* is a finite set for some ($\Rightarrow$ all) monomial order(s).
- Moreover the cardinality of the complement gives an upper bound on $|\mathbf{V}(I)|$
- See the Finiteness Theorem in Chapter 5 of “IVA”

"Implicitization" = elimination

- Before, we briefly discussed how some varieties can be given in parametric form as well as by implicit equations
- The process of deriving implicit equations from a parametrization is called "implicitization"
- This can also be performed by means of elimination and *lex* Gröbner bases, when the coordinate functions are *polynomial* (or rational) functions
- Example: A parametric surface in $\mathbb{R}^3$:

$$\begin{aligned} x &= u^2 \\ y &= u + v \\ z &= u - v^2 \end{aligned}$$

Implicitization example, continued

- The ideal $I = \langle x - u^2, y - u - v, z - u + v^2\rangle$ defines the *graph* of the parametrization map (a subset of $\mathbb{R}^5$).
- Geometrically, we want to project that into the x, y, z-coordinate space to find the image of the parametrization map
- In algebraic terms, we want to order the variables with u, v bigger than x, y, z (for instance as $u > v > x > y > z$) and find the elimination ideal $I_2 = I \cap \mathbb{R}[x, y, z]$.
- Computing a lex Gröbner basis we find 5 polynomials in all; only the last one contains no u, v terms:

$$I_2 = \langle -x + z^2 + 2xz - 4yx + x^2 + 2zy^2 - 2xy^2 + y^4\rangle$$

- $\mathbf{V}(I_2)$ is a surface in $\mathbb{R}^3$ that contains the image of the parametrization.

Implicitization example, continued

- The rest of the Gröbner basis is an “illustrated book” of exactly the way this parametrization works.
- For instance, the next three polynomials in the basis have x, y, z, v, but no u, so $I_1 = I \cap \mathbb{R}[v, x, y, z]$ has *lex* Gröbner basis consisting of the generator for I_2 above, plus
-
$$
\begin{aligned}
&(1 + 2y)v + x - y + z - y^2 \\
&(1 + 4z + 4x)v + 5x - y + z + 2yx + y^2 - 6zy - 2y^3 \\
&v - y + z + v^2
\end{aligned}
$$
- Final polynomial is $u - y + v$

Interpreting the basis elements

- The polynomials $v - y + z + v^2$ and $u - y + v$ show that given $(x, y, z) \in \mathbf{V}(I_2)$, there are never more than 2 pairs (u, v) that yield that (x, y, z).
- The polynomials $(1 + 2y)v + x - y + z - y^2$ and $(1 + 4z + 4x)v + \cdots$ show that for "most" (x, y, z), there is only one pair (u, v).
- The only possible "different" points would come from places on $\mathbf{V}(I_2)$ where $1 + 2y = 0$ and $1 + 4z + 4x = 0$. Those equations define a straight line that lies on the surface $\mathbf{V}(I_2)$.
- Precise statement of all this comes from the Extension Theorem in Chapter 3 of "IVA"

Where next?

- GB's can be used to compute the *Hilbert function* of a (homogeneous) ideal (or its variety) – encodes degree, dimension, other invariants, etc. (Idea: comes from dimensions of degree-s pieces of the complement of $\langle LT(I)\rangle$ when the complement is not finite.) See Chapter 9 of "IVA"
- GB's are used in algorithms for primary decomposition and finding irreducible components of varieties.
- Many applications in areas of pure and applied math
- Much ongoing research in improving algorithms for computing GB's. See Chapter 10 in "IVA," 4th edition for something close to the "state of the art."
- Thanks for your attention!