PURE Math Residents' Program
Gröbner Bases and Applications
Week 2 Lectures

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

June 2012

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from each polynomial.

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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)

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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)
- $LM_{>_{lex}}(f) = x^3y^2$ (without the coefficient)

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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)
- $LM_{>_{lex}}(f) = x^3y^2$ (without the coefficient)
- $LC_{>_{lex}}(f) = 2$

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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)
- $LM_{>_{lex}}(f) = x^3y^2$ (without the coefficient)
- $LC_{>_{lex}}(f) = 2$
- In text: $\mathrm{multideg}(f) = \alpha$ if $LT(f) = cx^\alpha$

Leading terms, etc.

- Last week, we introduced monomial orders so that we can select a *leading term* from 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)
- $LM_{>_{lex}}(f) = x^3y^2$ (without the coefficient)
- $LC_{>_{lex}}(f) = 2$
- In text: $\mathrm{multideg}(f) = \alpha$ if $LT(f) = cx^\alpha$
- If order is clear from context we'll often omit it

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

- First major difference with 1-variable case – we'll allow more than one divisor $f_1, \ldots, f_s$ (reason: not every ideal is principal). So there will be as many quotients as divisors.

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

- First major difference with 1-variable case – we'll allow more than one divisor $f_1, \ldots, f_s$ (reason: not every ideal is principal). 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.

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

- First major difference with 1-variable case – we'll allow more than one divisor $f_1, \ldots, f_s$ (reason: not every ideal is principal). 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*.

The algorithm

```
Input: f_1,...,f_s,f, monomial order >
Output: a_1,...,a_s,r
a_1 := 0; ... a_s := 0; r := 0; p := f;
while p <> 0 do
   divocc := false; i := 1;
   while i <= s and divocc = false do
      if LT(f_i) divides LT(p) then
         a_i := a_i + LT(p)/LT(f_i)
         p := p - (LT(p)/LT(f_i)) f_i
         divocc := true
      else
         i := i + 1
   if divocc = false
      r := r + LT(p)
      p := p - LT(p)
```

Division theorem

Theorem 1

Given any input $f_1, \ldots, f_s$, f, and a monomial order, the algorithm above 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. See Exercise 11 in Chapter 2, §3.)

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 $f = x^4 + x^3 z$. (Work out on board).

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 $f = x^4 + x^3 z$. (Work out on board).

- Result is

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

More examples

- Let $f_1 = xy + x + 1$, $f_2 = y^2 - x$, $f = x^2y^2$, and use $>_{grlex}$ with $x > y$.

More examples

- Let $f_1 = xy + x + 1$, $f_2 = y^2 - x$, $f = x^2y^2$, and use $>_{grlex}$ with $x > y$.
- (Work out on board)

More examples

- Let $f_1 = xy + x + 1$, $f_2 = y^2 - x$, $f = x^2y^2$, and use $>_{grlex}$ with $x > y$.
- (Work out on board)
- Note how the term x^2 went into the remainder r, but division continued for one more step:

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

More examples

- Let $f_1 = xy + x + 1$, $f_2 = y^2 - x$, $f = x^2y^2$, and use $>_{grlex}$ with $x > y$.
- (Work out on board)
- Note how the term x^2 went into the remainder r, but division continued for one more step:

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

- If we reorder the divisors we get different quotients and remainder(!)

More examples

- Let $f_1 = xy + x + 1$, $f_2 = y^2 - x$, $f = x^2y^2$, and use $>_{grlex}$ with $x > y$.
- (Work out on board)
- Note how the term x^2 went into the remainder r, but division continued for one more step:

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

- If we reorder the divisors we get different quotients and remainder(!)
- $$x^2y^2 = (x^2)(y^2 - x) + 0 \cdot (xy + x + 1) + (x^3)$$

Observations

- The quotients and remainder can change if we just reorder the divisors(!)

Observations

- The quotients and remainder can change if we just reorder the divisors(!)
- Also, if $r = 0$, it follows that $f \in \langle f_1, \ldots, f_s \rangle$.

Observations

- The quotients and remainder can change if we just reorder the divisors(!)
- Also, if $r = 0$, it follows that $f \in \langle f_1, \ldots, f_s \rangle$.
- But the converse *fails*. Here is an example:

Observations

- The quotients and remainder can change if we just reorder the divisors(!)
- Also, 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

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

Observations

- The quotients and remainder can change if we just reorder the divisors(!)
- Also, 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!

Key idea

- In $k[x]$, we could tell whether $f(x) \in I$ by finding the (monic) generator $g(x)$ such that $I = \langle g(x) \rangle$.

Key idea

- In $k[x]$, we could tell whether $f(x) \in I$ by finding the (monic) generator $g(x)$ such that $I = \langle g(x) \rangle$.
- Then $f(x) \in I \Leftrightarrow r(x) = 0$ in $f(x) = q(x)g(x) + r(x)$ from the division algorithm

Key idea

- In $k[x]$, we could tell whether $f(x) \in I$ by finding the (monic) generator $g(x)$ such that $I = \langle g(x) \rangle$.
- Then $f(x) \in I \Leftrightarrow r(x) = 0$ in $f(x) = q(x)g(x) + r(x)$ from the division algorithm
- In $k[x_1, \ldots, x_n]$, to "fix" the apparent undesirable properties we saw in the examples above, we have to find "good" sets of generators with the same properties as the $g(x)$ of minimal degree.

Key idea

- In $k[x]$, we could tell whether $f(x) \in I$ by finding the (monic) generator $g(x)$ such that $I = \langle g(x) \rangle$.
- Then $f(x) \in I \Leftrightarrow r(x) = 0$ in $f(x) = q(x)g(x) + r(x)$ from the division algorithm
- In $k[x_1, \ldots, x_n]$, to "fix" the apparent undesirable properties we saw in the examples above, we have to find "good" sets of generators with the same properties as the $g(x)$ of minimal degree.
- Analogy will be $\{g(x)\} \leftrightarrow$ a Gröbner basis

Key idea

- In $k[x]$, we could tell whether $f(x) \in I$ by finding the (monic) generator $g(x)$ such that $I = \langle g(x) \rangle$.
- Then $f(x) \in I \Leftrightarrow r(x) = 0$ in $f(x) = q(x)g(x) + r(x)$ from the division algorithm
- In $k[x_1, \ldots, x_n]$, to "fix" the apparent undesirable properties we saw in the examples above, we have to find "good" sets of generators with the same properties as the $g(x)$ of minimal degree.
- Analogy will be $\{g(x)\} \leftrightarrow$ a Gröbner basis
- Euclidean algorithm $\leftrightarrow$ Buchberger's algorithm

Motivation for definition of Gröbner bases

- In examples like this: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$

Motivation for definition of Gröbner bases

- In examples like this: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$
- 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 $f \in \langle f_1, f_2 \rangle$

Motivation for definition of Gröbner bases

- In examples like this: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$
- 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

Motivation for definition of Gröbner bases

- In examples like this: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$
- 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

Motivation for definition of Gröbner bases

- In examples like this: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y - x^2 \in I = \langle f_1, f_2 \rangle$
- 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
- 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.

Questions

- Given an arbitrary ideal $I \subset k[x_1, \ldots, x_n]$, does there always exist $G = \{g_1, \ldots, g_t\} \subset I$ such that for every $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i?

Questions

- Given an arbitrary ideal $I \subset k[x_1, \ldots, x_n]$, does there always exist $G = \{g_1, \ldots, g_t\} \subset I$ such that for every $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i?
- If so, how do we find them?

Questions

- Given an arbitrary ideal $I \subset k[x_1, \ldots, x_n]$, does there always exist $G = \{g_1, \ldots, g_t\} \subset I$ such that for every $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i?
- If so, how do we find them?
- For instance, starting from an arbitrary set of generators for I, how compute a set G with the property above?

Questions

- Given an arbitrary ideal $I \subset k[x_1, \ldots, x_n]$, does there always exist $G = \{g_1, \ldots, g_t\} \subset I$ such that for every $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i?
- If so, how do we find them?
- For instance, starting from an arbitrary set of generators for I, how compute a set G with the property above?
- Can also ask: To what extent G depends on the choice of monomial order?

The ideal of leading terms

- Start from a given ideal I and a given monomial order $>$

The ideal of leading terms

- Start from a given ideal I and a given monomial order $>$
- For each $f \in I$, we have $LT(f)$

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 $\langle LT(I) \rangle = \langle LT(f) \mid f \in I \rangle$

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.

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.

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, as we'll see next

A technical result

Lemma 2

Let M be a monomial ideal generated by some collection of monomials $\{x^\alpha \mid \alpha \in A\}$ (possibly infinite). Let $x^\beta \in M$. Then x^β is a multiple of x^α for some $\alpha \in A$.

Proof.

By definition $x^\beta = \sum_\alpha h_\alpha x^\alpha$ (where h_α are some polynomials, only finitely many of which are nonzero). But then $x^\beta = x^\gamma x^\alpha$ for some x^γ appearing in one of the h_α. □

Dickson's Lemma

Theorem 3 (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.

Proof.

- By induction on n

Dickson's Lemma

Theorem 3 (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.

Proof.

- By induction on n
- If $n = 1$, then by what we did last week, we know M is principal and hence $M = \langle x^a \rangle$ where a is the smallest nonnegative integer such that $x^a \in M$.

Dickson's Lemma

Theorem 3 (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.

Proof.

- By induction on n
- If $n = 1$, then by what we did last week, we know M is principal and hence $M = \langle x^a \rangle$ where a is the smallest nonnegative integer such that $x^a \in M$.
- Now assume that the result is known for all monomial ideals in $k[x_1, \ldots, x_{n-1}]$ and consider $M \subset k[x_1, \ldots, x_{n-1}, y]$.

Proof of Dickson, continued

- Write monomials as $x^{\alpha} y^{b}$

Proof of Dickson, continued

- Write monomials as $x^\alpha y^b$
- The projection $M' = \langle \{ x^\alpha \mid x^\alpha y^b \in M \text{ for some } b \geq 0 \} \rangle$ is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$

Proof of Dickson, continued

- Write monomials as $x^\alpha y^b$
- The projection $M' = \langle \{ x^\alpha \mid x^\alpha y^b \in M \text{ for some } b \geq 0 \} \rangle$ is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$
- So induction hypothesis applies, and $M' = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ for some s.

Proof of Dickson, continued

- Write monomials as $x^\alpha y^b$
- The projection $M' = \langle \{ x^\alpha \mid x^\alpha y^b \in M \text{ for some } b \geq 0 \} \rangle$ is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$
- So induction hypothesis applies, and $M' = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ for some s.
- This means that for each $1 \leq i \leq s$, there is some b_i such that $x^{\alpha(i)} y^{b_i} \in M$.

Proof of Dickson, continued

- Write monomials as $x^\alpha y^b$
- The projection $M' = \langle \{x^\alpha \mid x^\alpha y^b \in M \text{ for some } b \geq 0\} \rangle$ is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$
- So induction hypothesis applies, and $M' = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ for some s.
- This means that for each $1 \leq i \leq s$, there is some b_i such that $x^{\alpha(i)} y^{b_i} \in M$.
- Let $b = \max_i \{b_i\}$ so $x^\alpha(i) y^b \in M$ for all $1 \leq i \leq s$

Proof of Dickson, continued

- For each $0 \leq c < b$, take the "horizontal slice" of M at height c and project that to get $M'_c = \langle x^\alpha \mid x^\alpha y^c \in M \rangle$

Proof of Dickson, continued

- For each $0 \leq c < b$, take the "horizontal slice" of M at height c and project that to get $M'_c = \langle x^\alpha \mid x^\alpha y^c \in M \rangle$
- The M'_c are also monomial ideals in $k[x_1, \ldots, x_{n-1}]$ so induction $\Rightarrow M'_c = \langle x^{\alpha(c,1)}, \ldots, x^{\alpha(c,s_c)} \rangle$

Proof of Dickson, continued

- For each $0 \leq c < b$, take the "horizontal slice" of M at height c and project that to get $M'_c = \langle x^\alpha \mid x^\alpha y^c \in M \rangle$
- The M'_c are also monomial ideals in $k[x_1, \ldots, x_{n-1}]$ so induction $\Rightarrow M'_c = \langle x^{\alpha(c,1)}, \ldots, x^{\alpha(c,s_c)} \rangle$
- *Claim is*: The $x^{\alpha(c,1)}, \ldots, x^{\alpha(c,s_c)}$ for $0 \leq c < b$ and the $x^{\alpha(1)}y^b, \ldots, x^{\alpha(s)}y^b$ generate M

Proof of Dickson, continued

- For each $0 \leq c < b$, take the "horizontal slice" of M at height c and project that to get $M'_c = \langle x^\alpha \mid x^\alpha y^c \in M \rangle$
- The M'_c are also monomial ideals in $k[x_1, \ldots, x_{n-1}]$ so induction $\Rightarrow M'_c = \langle x^{\alpha(c,1)}, \ldots, x^{\alpha(c,s_c)} \rangle$
- *Claim is*: The $x^{\alpha(c,1)}, \ldots, x^{\alpha(c,s_c)}$ for $0 \leq c < b$ and the $x^{\alpha(1)}y^b, \ldots, x^{\alpha(s)}y^b$ generate M
- That follows fairly easily from the construction. QED

Consequences of Dickson

- Return to the monomial ideal $\langle LT(I) \rangle$ for a given I and a given monomial order.

Consequences of Dickson

- Return to the monomial ideal $\langle LT(I)\rangle$ for a given I and a given monomial order.
- By Dickson, we know that $\langle LT(I)\rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$ for some finite collection of monomials.

Consequences of Dickson

- Return to the monomial ideal $\langle LT(I)\rangle$ for a given I and a given monomial order.
- By Dickson, we know that $\langle LT(I)\rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$ for some finite collection of monomials.
- Every monomial in $\langle LT(I)\rangle$ is $LT(g)$ for some $g \in I$ (why?)

Consequences of Dickson

- Return to the monomial ideal $\langle LT(I)\rangle$ for a given I and a given monomial order.
- By Dickson, we know that $\langle LT(I)\rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$ for some finite collection of monomials.
- Every monomial in $\langle LT(I)\rangle$ is $LT(g)$ for some $g \in I$ (why?)
- (Reason is Lemma 2 from before implies if $x^\beta \in \langle LT(I)\rangle$, then $x^\beta = x^\gamma LT(f)$ for some $f \in I$. But then $x^\gamma LT(f) = LT(x^\gamma f)$ by properties of monomial orders and $x^\gamma f \in I$ by definition of an ideal.)

Consequences of Dickson

- Return to the monomial ideal $\langle LT(I)\rangle$ for a given I and a given monomial order.
- By Dickson, we know that $\langle LT(I)\rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$ for some finite collection of monomials.
- Every monomial in $\langle LT(I)\rangle$ is $LT(g)$ for some $g \in I$ (why?)
- (Reason is Lemma 2 from before implies if $x^\beta \in \langle LT(I)\rangle$, then $x^\beta = x^\gamma LT(f)$ for some $f \in I$. But then $x^\gamma LT(f) = LT(x^\gamma f)$ by properties of monomial orders and $x^\gamma f \in I$ by definition of an ideal.)
- 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 4

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

Gröbner bases defined

- This leads to

Definition 4

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

- Dickson's Lemma $\Rightarrow$

Theorem 5

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

Gröbner bases defined

- This leads to

Definition 4

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

- Dickson's Lemma $\Rightarrow$

Theorem 5

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

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

Consequences of Dickson, continued

- We have

Theorem 6

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

Consequences of Dickson, continued

- We have

Theorem 6

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

Proof.

Let $f \in I$ and use the division algorithm. At every stage, the polynomial p is in I, so its leading term is divisible by $LT(g_i)$ for some i. The algorithm reduces p to 0 without putting any terms into r, so $r = 0$ and $f = a_1 g_1 + \cdots a_t g_t$. □

Consequences of Dickson, continued

- We have

Theorem 6

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

Proof.

Let $f \in I$ and use the division algorithm. At every stage, the polynomial p is in I, so its leading term is divisible by $LT(g_i)$ for some i. The algorithm reduces p to 0 without putting any terms into r, so $r = 0$ and $f = a_1 g_1 + \cdots a_t g_t$. □

- This also proves an unexpected "big theorem!"

Theorem 7 (Hilbert Basis Theorem)

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

The ACC

- No, not the Atlantic Coast Conference(!)

The ACC

- No, not the Atlantic Coast Conference(!)
- ACC = "Ascending Chain Condition"

Theorem 8

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Then there exists an index m such that $I_m = I_{m+1} = I_{m+2} = \cdots$.

The ACC

- No, not the Atlantic Coast Conference(!)
- ACC = "Ascending Chain Condition"

Theorem 8

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Then there exists an index m such that $I_m = I_{m+1} = I_{m+2} = \cdots$.

- That is, an ascending chain of ideals *cannot strictly increase forever* – it must *stabilize* after finitely many steps.

The ACC

- No, not the Atlantic Coast Conference(!)
- ACC = "Ascending Chain Condition"

Theorem 8

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Then there exists an index m such that $I_m = I_{m+1} = I_{m+2} = \cdots$.

- That is, an ascending chain of ideals *cannot strictly increase forever* – it must *stabilize* after finitely many steps.

Proof.

The union $I = \cup_{i \geq 1} I_i$ is also an ideal (why?) By the HBT, $I = \langle f_1, \ldots, f_s \rangle$ for some f_i. Each f_i "comes from" some I_j; after some number m of steps, I_m contains all f_j, so equals I. □

Comments on ACC

- In fact ACC $\Leftrightarrow$ every ideal is finitely generated (HBT for the polynomial ring). Can you see how the other implication might go?

Comments on ACC

- In fact ACC $\Leftrightarrow$ every ideal is finitely generated (HBT for the polynomial ring). Can you see how the other implication might go?
- Hint: Argue by contraposition. If there exists an ideal that is not finitely generated, then ACC cannot hold!

Comments on ACC

- In fact ACC $\Leftrightarrow$ every ideal is finitely generated (HBT for the polynomial ring). Can you see how the other implication might go?
- Hint: Argue by contraposition. If there exists an ideal that is not finitely generated, then ACC cannot hold!
- The class of commutative rings in which ACC holds, and in which all ideals are finitely generated is known as the class of *Noetherian* rings, after Emmy Noether.

Comments on ACC

- In fact ACC $\Leftrightarrow$ every ideal is finitely generated (HBT for the polynomial ring). Can you see how the other implication might go?
- Hint: Argue by contraposition. If there exists an ideal that is not finitely generated, then ACC cannot hold!
- The class of commutative rings in which ACC holds, and in which all ideals are finitely generated is known as the class of *Noetherian* rings, after Emmy Noether.
- The ACC might seem like a rather arcane theoretical statement, but as we'll see shortly, it has a big practical implication for our story(!)

Background for Buchberger's algorithm

- Recall the example we discussed earlier: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y + x^2 \in I = \langle f_1, f_2 \rangle$

Background for Buchberger's algorithm

- Recall the example we discussed earlier: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y + x^2 \in I = \langle f_1, f_2 \rangle$
- If we use $>_{grlex}$, then $LT(f_1) = xy$, $LT(f_2) = y^2$, but $LT(f) = x^2 \notin \langle LT(f_1), LT(f_2) \rangle$

Background for Buchberger's algorithm

- Recall the example we discussed earlier: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y + x^2 \in I = \langle f_1, f_2 \rangle$
- If we use $>_{grlex}$, then $LT(f_1) = xy$, $LT(f_2) = y^2$, but $LT(f) = x^2 \notin \langle LT(f_1), LT(f_2) \rangle$
- In other words, $\{f_1, f_2\}$ is *not a Gröbner basis* for I with respect to $>_{grlex}$.

Background for Buchberger's algorithm

- Recall the example we discussed earlier: $f_1 = xy + 1$, $f_2 = y^2 - x$, $f = yf_1 - xf_2 = y + x^2 \in I = \langle f_1, f_2 \rangle$
- If we use $>_{grlex}$, then $LT(f_1) = xy$, $LT(f_2) = y^2$, but $LT(f) = x^2 \notin \langle LT(f_1), LT(f_2) \rangle$
- In other words, $\{f_1, f_2\}$ is *not a Gröbner basis* for I with respect to $>_{grlex}$.
- Note that we "found" a new leading term by forming a polynomial combination of f_1, f_2 that was constructed to *cancel leading terms*

S-polynomials

- A general form of this:

Definition 9

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

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

S-polynomials

- A general form of this:

Definition 9

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

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

- This is defined to make the leading terms cancel.

A more elaborate example

- Another example: $f = 2x^2y + xy$, $g = xy^2 + 2x + y$, using *lex* order $x > y$:

$$\begin{aligned} S(f,g) &= \frac{x^2y^2}{2x^2y}(2x^2y + xy) - \frac{x^2y^2}{xy^2}(xy^2 + 2x + y) \\ &= x^2y^2 + \frac{1}{2}xy^2 - (x^2y^2 + 2x^2 + xy) \\ &= \frac{1}{2}xy^2 - 2x^2 - xy \end{aligned}$$

A more elaborate example

- Another example: $f = 2x^2y + xy$, $g = xy^2 + 2x + y$, using *lex* order $x > y$:

$$\begin{aligned} S(f,g) &= \frac{x^2y^2}{2x^2y}(2x^2y + xy) - \frac{x^2y^2}{xy^2}(xy^2 + 2x + y) \\ &= x^2y^2 + \frac{1}{2}xy^2 - (x^2y^2 + 2x^2 + xy) \\ &= \frac{1}{2}xy^2 - 2x^2 - xy \end{aligned}$$

- In this case, the leading term of the S-polynomial is a multiple of $LT(g)$.

A more elaborate example

- Another example: $f = 2x^2y + xy$, $g = xy^2 + 2x + y$, using *lex* order $x > y$:

$$\begin{aligned} S(f,g) &= \frac{x^2y^2}{2x^2y}(2x^2y + xy) - \frac{x^2y^2}{xy^2}(xy^2 + 2x + y) \\ &= x^2y^2 + \frac{1}{2}xy^2 - (x^2y^2 + 2x^2 + xy) \\ &= \frac{1}{2}xy^2 - 2x^2 - xy \end{aligned}$$

- In this case, the leading term of the S-polynomial is a multiple of $LT(g)$.
- But we would get something "new" if we subtracted $\frac{1}{2}g$

Idea of Buchberger algorithm

- When we find a “new” leading term like this, we will just append the new polynomial to our list of generators(!)

Idea of Buchberger algorithm

- When we find a “new” leading term like this, 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.

Idea of Buchberger algorithm

- When we find a "new" leading term like this, 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'
```

Comments and questions

- To understand what this is doing note that G' stores a copy of the collection of polynomials at the start of each pass through the repeat loop. The pairs p, q are selected from this copy, which is not changing.

Comments and questions

- To understand what this is doing note that G' stores a copy of the collection of polynomials at the start of each pass through the repeat loop. The pairs p, q are selected from this copy, which is not changing.
- Any nonzero S-polynomial remainders are adjoined to the *original* collection of polynomials, which is in G.

Comments and questions

- To understand what this is doing note that G' stores a copy of the collection of polynomials at the start of each pass through the repeat loop. The pairs p, q are selected from this copy, which is not changing.
- Any nonzero S-polynomial remainders are adjoined to the *original* collection of polynomials, which is in G.
- The algorithm will terminate the first time $G = G'$ (that is when all S-polynomial remainders are zero, so no new polynomials are adjoined to G)

Comments and questions

- To understand what this is doing note that G' stores a copy of the collection of polynomials at the start of each pass through the repeat loop. The pairs p, q are selected from this copy, which is not changing.
- Any nonzero S-polynomial remainders are adjoined to the *original* collection of polynomials, which is in G.
- The algorithm will terminate the first time $G = G'$ (that is when all S-polynomial remainders are zero, so no new polynomials are adjoined to G)
- Question 1: How do we know this process will ever stop?

Comments and questions

- To understand what this is doing note that G' stores a copy of the collection of polynomials at the start of each pass through the repeat loop. The pairs p, q are selected from this copy, which is not changing.
- Any nonzero S-polynomial remainders are adjoined to the *original* collection of polynomials, which is in G.
- The algorithm will terminate the first time $G = G'$ (that is when all S-polynomial remainders are zero, so no new polynomials are adjoined to G)
- Question 1: How do we know this process will ever stop?
- Question 2: If it does stop, is G a Gröbner basis?

Answers to the questions

- Question 2 is answered by the main technical result of Buchberger's theory:

Theorem 10 (Buchberger's *S*-polynomial Criterion)

Let $G = \{g_1, \ldots, g_t\}$ be a collection of polynomials. Then G is a Gröbner basis for the ideal it generates if and only if the remainder on division of $S(g_i, g_j)$ by G is zero for all pairs $i \neq j$.

Answers to the questions

- Question 2 is answered by the main technical result of Buchberger's theory:

Theorem 10 (Buchberger's *S*-polynomial Criterion)

Let $G = \{g_1, \ldots, g_t\}$ be a collection of polynomials. Then G is a Gröbner basis for the ideal it generates if and only if the remainder on division of $S(g_i, g_j)$ by G is zero for all pairs $i \neq j$.

- One implication is easy; the other one says the answer to Question 2 is *yes*! This is Theorem 6 in Chapter 2, §6 of IVA – a "hard slog of a proof if there ever was one"

Answers to the questions

- Question 2 is answered by the main technical result of Buchberger's theory:

Theorem 10 (Buchberger's *S*-polynomial Criterion)

Let $G = \{g_1, \ldots, g_t\}$ be a collection of polynomials. Then G is a Gröbner basis for the ideal it generates if and only if the remainder on division of $S(g_i, g_j)$ by G is zero for all pairs $i \neq j$.

- One implication is easy; the other one says the answer to Question 2 is *yes*! This is Theorem 6 in Chapter 2, §6 of IVA – a "hard slog of a proof if there ever was one"
- We won't discuss this in "class"

Termination of Buchberger's algorithm

- The remaining question is: Does this always terminate?

Termination of Buchberger's algorithm

- The remaining question is: Does this always terminate?
- Note that if the algorithm does not terminate, it is because the new G strictly contains G'

Termination of Buchberger's algorithm

- The remaining question is: Does this always terminate?
- Note that if the algorithm does not terminate, it is because the new G strictly contains G'
- That means $\langle LT(G') \rangle \subset \langle LT(G) \rangle$ (strict containment)

Termination of Buchberger's algorithm

- The remaining question is: Does this always terminate?
- Note that if the algorithm does not terminate, it is because the new G strictly contains G'
- That means $\langle LT(G') \rangle \subset \langle LT(G) \rangle$ (strict containment)
- The ACC implies this cannot go on forever. Eventually this increasing chain of monomial ideals must stabilize.

Termination of Buchberger's algorithm

- The remaining question is: Does this always terminate?
- Note that if the algorithm does not terminate, it is because the new G strictly contains G'
- That means $\langle LT(G') \rangle \subset \langle LT(G) \rangle$ (strict containment)
- The ACC implies this cannot go on forever. Eventually this increasing chain of monomial ideals must stabilize.
- When it does, the algorithm terminates.

An example, by hand

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$, use *grlex* order. We start with $G = \{f_1, f_2\}$.

An example, by hand

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$, use *grlex* order. We start with $G = \{f_1, f_2\}$.
- $S(f_1, f_2) = x^2 + y$, with leading term x^2, and this is its own remainder on division by f_1, f_2. So we update to $G = \{f_1, f_2, f_3 = x^2 + y\}$

An example, by hand

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$, use *grlex* order. We start with $G = \{f_1, f_2\}$.
- $S(f_1, f_2) = x^2 + y$, with leading term x^2, and this is its own remainder on division by f_1, f_2. So we update to $G = \{f_1, f_2, f_3 = x^2 + y\}$
- Now, the S-polynomial $S(f_1, f_2)$ reduces to zero, so we consider $S(f_1, f_3) = x(xy + 1) - y(x^2 + y) = x - y^2 = -f_2$. This reduces to a remainder of 0 because we have f_2.

An example, by hand

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$, use *grlex* order. We start with $G = \{f_1, f_2\}$.
- $S(f_1, f_2) = x^2 + y$, with leading term x^2, and this is its own remainder on division by f_1, f_2. So we update to $G = \{f_1, f_2, f_3 = x^2 + y\}$
- Now, the S-polynomial $S(f_1, f_2)$ reduces to zero, so we consider $S(f_1, f_3) = x(xy + 1) - y(x^2 + y) = x - y^2 = -f_2$. This reduces to a remainder of 0 because we have f_2.
- Next, $S(f_2, f_3) = x^2(y^2 - x) - y^2(x^2 - y^2) = -x^3 + y^4$. Dividing by $G = \{f_1, f_2, f_3\}$ (in that order), we find

$$y^4 - x^3 = (y + 1)f_1 + y^2 f_2 + (-x)f_3 + (-y - 1)$$

An example, by hand

- Let $f_1 = xy + 1$, $f_2 = y^2 - x$, use *grlex* order. We start with $G = \{f_1, f_2\}$.
- $S(f_1, f_2) = x^2 + y$, with leading term x^2, and this is its own remainder on division by f_1, f_2. So we update to $G = \{f_1, f_2, f_3 = x^2 + y\}$
- Now, the S-polynomial $S(f_1, f_2)$ reduces to zero, so we consider $S(f_1, f_3) = x(xy + 1) - y(x^2 + y) = x - y^2 = -f_2$. This reduces to a remainder of 0 because we have f_2.
- Next, $S(f_2, f_3) = x^2(y^2 - x) - y^2(x^2 - y^2) = -x^3 + y^4$. Dividing by $G = \{f_1, f_2, f_3\}$ (in that order), we find

$$y^4 - x^3 = (y + 1)f_1 + y^2 f_2 + (-x)f_3 + (-y - 1)$$

- After cleaning up the signs, we adjoin $f_4 = y + 1$ to G and continue.

Example, continued

- We have $S(f_1, f_4) = x - 1$ and that is its own remainder on division by $\{f_1, f_2, f_3, f_4\}$, so that polynomial must also be adjoined to G.

Example, continued

- We have $S(f_1, f_4) = x - 1$ and that is its own remainder on division by $\{f_1, f_2, f_3, f_4\}$, so that polynomial must also be adjoined to G.
- At this point, it can be checked that $G = \{xy + 1, y^2 - x, x^2 + y, y + 1, x - 1\}$ satisfies Buchberger's Criterion, so it is a Gröbner basis for $I = \langle f_1, f_2 \rangle$ with respect to the *grlex* order.

Example, continued

- We have $S(f_1, f_4) = x - 1$ and that is its own remainder on division by $\{f_1, f_2, f_3, f_4\}$, so that polynomial must also be adjoined to G.
- At this point, it can be checked that $G = \{xy + 1, y^2 - x, x^2 + y, y + 1, x - 1\}$ satisfies Buchberger's Criterion, so it is a Gröbner basis for $I = \langle f_1, f_2 \rangle$ with respect to the *grlex* order.
- Note that $LT(f_1), LT(f_2), LT(f_3)$ are multiples of $LT(f_4)$ or $LT(f_5)$ or both.

Example, continued

- We have $S(f_1, f_4) = x - 1$ and that is its own remainder on division by $\{f_1, f_2, f_3, f_4\}$, so that polynomial must also be adjoined to G.
- At this point, it can be checked that $G = \{xy + 1, y^2 - x, x^2 + y, y + 1, x - 1\}$ satisfies Buchberger's Criterion, so it is a Gröbner basis for $I = \langle f_1, f_2 \rangle$ with respect to the *grlex* order.
- Note that $LT(f_1), LT(f_2), LT(f_3)$ are multiples of $LT(f_4)$ or $LT(f_5)$ or both.
- This says that $\langle LT(I) \rangle$ is generated by $\langle LT(f_4), LT(f_5) \rangle$.

Example, continued

- We have $S(f_1, f_4) = x - 1$ and that is its own remainder on division by $\{f_1, f_2, f_3, f_4\}$, so that polynomial must also be adjoined to G.
- At this point, it can be checked that $G = \{xy + 1, y^2 - x, x^2 + y, y + 1, x - 1\}$ satisfies Buchberger's Criterion, so it is a Gröbner basis for $I = \langle f_1, f_2 \rangle$ with respect to the *grlex* order.
- Note that $LT(f_1), LT(f_2), LT(f_3)$ are multiples of $LT(f_4)$ or $LT(f_5)$ or both.
- This says that $\langle LT(I) \rangle$ is generated by $\langle LT(f_4), LT(f_5) \rangle$.
- Hence $\{f_4, f_5\}$ is *also* a Gröbner basis for I.

Reduced Gröbner bases

A useful theoretical result:

Theorem 11

Each nonzero ideal I has a unique reduced Gröbner basis with respect to each monomial order – a Gröbner basis $G = \{g_1, \ldots, g_t\}$ such that

i. $LC(g_i) = 1$ *for all* i*, and*

ii. *No term in* g_i *is divisible by* $LT(g_j)$ *for any* $j \neq i$*.*

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.

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

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

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.

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 12

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. If $1 \leq \ell \leq n - 1$, we define the ℓth elimination ideal of I to be

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

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

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 12

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. If $1 \leq \ell \leq n - 1$, we define the ℓth elimination ideal of I to be

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

(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 $V(I) \subset k^n$

Geometry of elimination

- If $I \subset k[x_1, \ldots, x_n]$, then we have the geometric object $V(I) \subset k^n$
- If we then eliminate the first ℓ variables, we can ask, what is the corresponding variety $V(I_\ell)$?

Geometry of elimination

- If $I \subset k[x_1, \ldots, x_n]$, then we have the geometric object $V(I) \subset k^n$
- If we then eliminate the first ℓ variables, we can ask, what is the corresponding variety $V(I_\ell)$?
- Partial answer – it's very closely related to the projection of $V(I)$ into the coordinate space $k^{n-\ell}$ of the variables $x_{\ell+1}, \ldots, x_n$.

Geometry of elimination

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

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.

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

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 $x_{\ell+1}, \ldots, x_n$.

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 13 (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
$$I = \langle x^2 y + y^2 + 2, xy - 3y + 1 \rangle \subset \mathbb{Q}[x, y]$$

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

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 $I_1 = I \cap \mathbb{Q}[y]$.

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

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

Example, continued

- Note the form of

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

- To find the points in $V(I) = V(x^2y + y^2 + 2, xy - 3y + 1)$, we could solve the one-variable equation $y^3 + 9y^2 - 4y + 1 = 0$ (numerically),

Example, continued

- Note the form of

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

- To find the points in $V(I) = V(x^2y + y^2 + 2, xy - 3y + 1)$, 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.

Example, continued

- Note the form of

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

- To find the points in $V(I) = V(x^2y + y^2 + 2, xy - 3y + 1)$, 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 $V(I)$ 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

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 $G_x =$

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

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.

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 $V(I)$ (and would yield the same results!)

"Implicitization" = elimination

- In the first week, we briefly discussed how some varieties can be given in parametric form as well as by implicit equations

"Implicitization" = elimination

- In the first week, 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"

"Implicitization" = elimination

- In the first week, 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

"Implicitization" = elimination

- In the first week, 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 $\mathbb{R}^5$).

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

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 $I_2 = I \cap \mathbb{R}[x, y, z]$.

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 contain no u, v terms:

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

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 contain no u, v terms:

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

- This defines 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.

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

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
-

$$(1 + 2y)v + x - y + z - y^2$$
$$(1 + 4z + 4x)v + 5x - y + z + 2yx + y^2 - 6zy - 2y^3$$
$$v - y + z + v^2$$

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
-

$$(1 + 2y)v + x - y + z - y^2$$
$$(1 + 4z + 4x)v + 5x - y + z + 2yx + y^2 - 6zy - 2y^3$$
$$v - y + z + v^2$$

- Final polynomial is $u - y + v$

Interpreting the basis elements

- The polynomials $v - y + z + v^2$ and $u - y + v$ show that given $(x, y, z) \in V(I_2)$, there are never more than 2 pairs (u, v) that yield that (x, y, z).

Interpreting the basis elements

- The polynomials $v - y + z + v^2$ and $u - y + v$ show that given $(x, y, z) \in V(I_2)$, 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).

Interpreting the basis elements

- The polynomials $v - y + z + v^2$ and $u - y + v$ show that given $(x, y, z) \in V(I_2)$, 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 $V(I_2)$ where $1 + 2y = 0$ and $1 + 4z + 4x = 0$. Those equations define a straight line that lies on the surface $V(I_2)$.

Interpreting the basis elements

- The polynomials $v - y + z + v^2$ and $u - y + v$ show that given $(x, y, z) \in V(I_2)$, 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 $V(I_2)$ where $1 + 2y = 0$ and $1 + 4z + 4x = 0$. Those equations define a straight line that lies on the surface $V(I_2)$.
- Precise statement of all this comes from the Extension Theorem in text.