Gröbner Bases

Victor Adamchik

Carnegie Mellon University

"There are two main activities of mathematics:
theorem-proving and equations-solving."
Wen-tsun Wu, "*Mathematics Mechanization*", 2000.

"All mathematics is divided into three parts :
cryptography (paid for by CIA, KGB and the like),
hydrodynamics (supported by manufacturers of atomic submarines)
and celestial mechanics (financed by military and NASA)"
V.Arnold, *Frontiers and Perspectives*, 2000.

16 Century Program [**Descartes**] - "Rules for the Direction of the Mind"

solving any problem →
solving problem in mathematics →
solving problem in algebra →
solving a system of polynomial equations →
solving a single polynomial equation.

Intersection of Surfaces

Consider a system of the following surfaces

$$\begin{cases} x^2 + y^2 + z^2 - 1 = 0 \\ x^2 + y^2 + z^2 - 2\,x = 0 \\ x - y + 2\,z = 0 \end{cases}$$

Use plots to see the surfaces represented by these equations

```
Show[{ContourPlot3D[x - y + 2 z == 0, {x, -1, 1}, {y, -1, 1}, {z, -1, 1}],
  ContourPlot3D[x^2 + y^2 + z^2 - 2 x == 0, {x, -1, 2}, {y, -1, 2},
   {z, -1, 2}, Mesh → None],
  ContourPlot3D[x^2 + y^2 + z^2 - 1 == 0, {x, -1, 1}, {y, -1, 1}, {z, -1, 1},
   ContourStyle → Directive[FaceForm[Red, Green],
     Specularity[White, 30]], Mesh → None]}]
```

Find the points of intersection of these three surfaces by using a Groebner basis computation.

```
GroebnerBasis[{x - y + 2 z, x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2 x}, {x, y, z}]
```

$$\{-1 + 4\,z + 10\,z^2,\ -1 + 2\,y - 4\,z,\ -1 + 2\,x\}$$

```
Solve[# == 0 & /@ %, {x, y, z}]
```

$$\left\{\left\{x \to \frac{1}{2},\ y \to \frac{1}{10}\left(1 - 2\sqrt{14}\right),\ z \to \frac{1}{10}\left(-2 - \sqrt{14}\right)\right\},\right.$$
$$\left.\left\{x \to \frac{1}{2},\ y \to \frac{1}{2}\left(\frac{1}{5} + \frac{2\sqrt{14}}{5}\right),\ z \to \frac{1}{10}\left(-2 + \sqrt{14}\right)\right\}\right\}$$

Introduction

■ Linear system

Consider a system of linear polynomials

$$\begin{cases} f_1 = x + y - z = 0 \\ f_2 = 2x + 3y + 2z = 0 \end{cases}$$

We recall the Gauss-Jordan elimination (or row reduction)

$$\begin{cases} f_1 = x + y - z = 0 \\ f_3 = y + 4z = 0 \end{cases}$$

where

$$f_3 = f_2 - 2 f_1.$$

This process in called *reduction* of f_2 by f_1, and we write

$$f_2 \xrightarrow{f_1} f_3$$

The new polynomial can be viewed as a remainder of a certain division

$$\begin{array}{r} 2 \\ \hline x + y - z \;)\; 2x + 3y + 2z \\ 2x + 2y - 2z \\ \hline y + 4z \end{array}$$

Note, if a system has more than two equations, the elimination will require more than ove divisons.

■ NonLinear system in one variable - I

Let

$$\begin{cases} f_1 = x^3 - 2x^2 + 2x + 8 = 0 \\ f_2 = 2x^2 + 3x + 1 = 0 \end{cases}$$

We reduce f_1 by f_2:

$$f_1 = \left(\frac{1}{2}\,x - \frac{7}{4}\right) f_2 + \frac{27}{4}\,x + \frac{39}{4}$$

and thus the original system was transformed to

$$\begin{cases} f_1 = x^3 - 2\,x^2 + 2\,x + 8 = 0 \\ \\ f_3 = \frac{27}{4}\,x + \frac{39}{4} = 0 \end{cases}$$

Solving the linear equation and subsituting its solution to the first equation, yields that the system has no solution.

■ **NonLinear system in one variable - II**

Let

$$\begin{cases} f_1 = x^6 - x^3 = 0 \\ \\ f_2 = x^8 - x^3 = 0 \\ \\ f_3 = x^{12} - x^7 = 0 \end{cases}$$

Reduction

$$f_2 \xrightarrow{f_1} f_4 \text{ and } f_3 \xrightarrow{f_2} 0$$

$$\begin{cases} f_1 = x^6 - x^3 = 0 \\ \\ f_4 = x^5 - x^3 = 0 \end{cases}$$

$$f_1 \xrightarrow{f_4} f_5$$

$$\begin{cases} f_5 = x^4 - x^3 = 0 \\ \\ f_4 = x^5 - x^3 = 0 \end{cases}$$

Finally

$$f_4 \xrightarrow{f_5} f_6 = x^4 - x^3$$

So we end up with one equation (as Descartes wanted :-))

$$x^4 - x^3 = 0$$

■ Polynomial GCD

$$\begin{cases} f_1 = x^6 - x^3 = 0 \\ f_2 = x^8 - x^3 = 0 \\ f_3 = x^{12} - x^7 = 0 \end{cases}$$

```
PolynomialGCD[x^6 - x^3, x^5 - x^3, x^12 - x^7]
```

```
-x^3 + x^4
```

Another example

$$\begin{cases} f_1 = x^4 - 2x^2 - 3x - 2 = 0 \\ f_2 = x^5 + x^4 + 1 = 0 \\ f_3 = x^2 + x + 1 \end{cases}$$

```
PolynomialGCD[x^4 - 2 x^2 - 3 x - 2, x^5 + x^4 + 1, 1 + x + x^2]
```

```
1 + x + x^2
```

$$\begin{cases} f_1 = x^3 - 2x^2 + 2x + 8 = 0 \\ f_2 = 2x^2 + 3x + 1 = 0 \end{cases}$$

```
PolynomialGCD[x^3 - 2 x^2 + 2 x + 8, 2 x^2 + 3 x + 1]
```

```
1
```

Definition.

A *greatest common divisor* (GCD) of polynomilas $f_1, \ldots, f_s$ is a polynomial h such that

1) h divides all $f_1, \ldots, f_s$

2) If p is another polynomial that divides $f_1, \ldots, f_s$ then p divides h.

Two Special Cases

1) If all f_i are linear.

Elementary row reduction

2) All polynomials are in one variable.

Polynomial GCD

How do you find a GCD of two polynomials,. say f and g?

Euclidian algorithm:

$$f = q_1 * g + r_1$$

$$\text{GCD}(f, g) = \text{GCD}(g, r_1 = f - q_1 g)$$

$$g = q_2 * r_1 + r_2$$

$$r_1 = q_3 * r_2 + r_3$$

$$r_2 = q_4 * r_3 + 0$$

Our goal is to extend the notion of a polynomial GCD to a multivariate case.

Forming a background

■ **Algebra of polynomials**

The two main data types on which our algorithms operate are numbers and polynomials. In general, we need a polynomial ring, and in some cases a field to support division...

Definition. A *group* $(G, *)$ is a nonempty set G, closed under a binary operation * satisfying the following axioms:

A1. associativity: $a * (b * c) = (a * b) * c$

A2. identity: $e * x = x * e = x, \ x \in G$

A3. inverse: $x * x^{-1} = x^{-1} * x = e$

An a*belian group* (commutative group) is a group that satisfies

A4. commutativity: $a * b = b * a$

Definition. A *ring* is a nonempty set R, closed under two binary operation * and + satisfying the following:

$(R, +)$ is an abelian group

holds axioms A1 and A2 wrt * (it's called *monoid*! no inverses)

A5. distributivity: $a * (b + c) = (a * b) + (a * c)$

$(a + b) * c = (a * c) + (b * c)$

NOTE, a ring does not necessarily satisfies A4 wrt *.

Field is a commutative ring in which every nonzero element has a multiplicative inverse.

We consider polynomilas $f(x_1, \ ..., \ x_n)$ in n variables with coefficients in F (field of numbers). $R = F[x_1, \ ..., \ x_n]$ denotes a set of all polynomials In other words, $F[x_1, \ ..., \ x_n]$ will denote a *polynomial ring* (commutative).

Example. Let $R = Q[x, y]$ be the ring of all polynomials in x and y with coefficients in Q.

Then $\sqrt{2}$ is not in R, as well as $\frac{x}{y+x}$.

Also $x^2 + z^2 + 1$does not belong to R.

The whole ring is huge, we will deal with a smaller subset:

■ Polynomial ideals

Definition.

An *ideal* I is a subset of a <u>commutative</u> ring $(R, *, +)$ satisfying the following properties:

1) $f_1, \ f_2 \in I \Longrightarrow f_1 + f_2 \in I$

2) $f \in I, \ r \in R \Longrightarrow f * r \in I$

Two trivial ideals: the ring itself and the additive identity.

Definition. Polynomials $f_1, \ ..., \ f_s \in R$ generate an ideal

$$I = < f_1, \ ..., \ f_s > = \{ \sum_{k=1}^{s} q_k \ f_k, \text{ where } q_k \in R\}$$

called a *polynomial ideal* in the ring of all polynomials.

Example.

Let $R = Q\{x, \ y]$ and consider the ideal

$I = < f_1, \ f_2 > = \ < 1 + x, \ 1 + y >$

The following are elements in I:

$$0, \qquad x - y, \qquad x + x\,y, \qquad x^2\,y + x^2 - y\,x - y$$

since

$$x^2 y + x^2 - y x - y = x^2 (1 + y) - y (1 + x)$$

These are not elements in I:

$$1, \qquad x y, \qquad 1 + x^2$$

There is an analogy between ideals and subspaces in linear algebra. The difference is that a basis of an ideal is NOT necessarily independent. Elements can be written in various ways. The second difference is that ideals may have bases with a different number of generators. Consider $< x, x^2 >$, that is the same as $< x >$ or $< x + x^2, x >$.

The polynomial ideal has a nice interpretation in terms of polynomial equation. We can think of the ideal is a solution set. Given an ideal $< f_1, .., f_s >$. We get the system of equation

$$f_1 = 0$$
$$...$$
$$f_s = 0$$

One can derive other equations out of system by doing simple algebra.

$$a_1 f_1 + ... + a_s f_s = 0$$

The left hand side is exactly an element of the ideal. The idea of using ideals for solving systems is not so straightforward. There are some important questions that we need to address

Q1. How do we know that an ideal is not empty?

Q2. How big an ideal? Is it finite?

Since bases are not unique, perhaps there are good and bad ones. How would you find a good base? In order to find the "better" base, we need to solve the following two problems

Problem 1 (*Ideal Membership Problem*).

Given a polynomial $f \in R$. Decide whether it belongs to the ideal $I = < f_1, ..., f_s >$.

Problem 2

Given a polynomial $f \in I = < f_1, ..., f_s >$. Determine coefficients $a_1, ..., a_s \in R$ such that

$$f = a_1 f_1 + ... + a_s f_s$$

We can easily solve the first problem in two particular cases

Two Special Cases

1) If all f_i are linear.

Elementary row reduction

2) All polynomials are in one variable.

Polynomial GCD

Theorem.

Given $R[x]$. Then there exist a polynomial f such that $I = < f >$. Moreover, $f = \gcd(f_1, \ ..., \ f_s)$.

Proof.

Let $0 \neq f \in I$ and minimal degree.Choose another $g \in I$.

$$g = f * q + r, \quad \deg(r) < \deg(f).$$

Clearly, r could be only 0, since f has a minimal degree. Therefore, $g = f * q$ is a multiple of f. QED.

Question. How do you find a GCD of two polynomials,. say f and g?

Euclidian algorithm:

$$f = q_1 * g + r_1$$

$$\text{GCD}(f, \ g) = \text{GCD}(g, \ r_1 = f - q_1 g)$$

$$g = q_2 * r_1 + r_2$$

$$r_1 = q_3 * r_2 + r_3$$

$$r_2 = q_4 * r_3 + 0$$

Question. What is an Euclidean algorithm in multivariate case? Divide $4x^3 - 5y^4 + 7xy^2z + 4xyz^2$ by $x + y$

Monomial order

In order to introduce division with remainder for multivariate polynomials, we need a way to order terms. For polynomials of one variable, the natural order is by degree

$$x^\alpha > x^\beta \quad \text{if} \quad \alpha > \beta$$

A polynomial of the form $x^\alpha = {x_1}^{\alpha_1} \ ... \ {x_n}^{\alpha_n}$ is called a *monomial*.

There is a bijection between monomials and n-tuples.

$${x_1}^{\alpha_1} \ ... \ {x_n}^{\alpha_n} \rightarrow (\alpha_1, \ \alpha_2, \ ..., \ \alpha_n) \in \mathbb{Z}^n_{\geq 0}$$

Therefore, any ordering on the space $\mathbb{Z}^n_{\geq 0}$ will give us an ordering on monomials.

Definition.

Monomial order on $F[x_1 ..., x_n]$ is a relation satisfying the following

1) total order: monomials are comparable in the order, i.e.

either $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ or $x^\alpha < x^\beta$

2) multiplicative property: if $x^\alpha > x^\beta \Longrightarrow x^\alpha x^\gamma > x^\beta x^\gamma$

3) well-order: a set of monomials has a least element.

Here sre standard examples of monomial orders:

Lexicographical Order: (with $x_1 > x_2 > ... > x_n$)

$x^\alpha >_{\text{lex}} x^\beta$ if the leftmost nonzero entry in α-β is positive.

In *lex* order a variable dominates over any monomials involving only smaller variables

Example 1.

$$x_1 x_2^2 >_{\text{lex}} x_2^3 x_3^4$$

$$\alpha=\{1, 2, 0\}$$

$$\beta =\{0, 3, 4\}$$

$$\alpha - \beta = (1, -1, -4)$$

Example 2.

$$x_1 >_{\text{lex}} x_2^3$$

Example 3.

$$x >_{\text{lex}} y^2 z^5$$

Graded Lexicographical Order:

$x^\alpha >_{\text{grlex}} x^\beta$ if $\sum\alpha_i > \sum\beta_i$ or

$\sum\alpha_i = \sum\beta_i$ and $x^\alpha >_{\text{lex}} x^\beta$

Examples,

$$x_2 x_3^2 >_{\text{grlex}} x_2^2 >_{\text{grlex}} x_1$$

$$x_2^3 >_{\text{grlex}} x_2 x_3^2$$

$$x_1 x_2 x_4 >_{\text{grlex}} x_1 x_3^2$$

Graded Reverse Lexicographical Order:

$x^\alpha >_{\text{grevlex}} x^\beta$ if $\sum\alpha_i > \sum\beta_i$ or

$$\sum \alpha_i = \sum \beta_i$$

and the right-most nonzero in α-β is negative

Example

$$x_1 x_3^2 >_{\text{grevlex}} x_1 x_2 x_4$$

since

$$(1,0,2,0) - (1,1,0,1) = (0,-1,2,-1)$$

Example

$$x^5 y z >_{\substack{\text{grevlex} \\ \text{grlex}}} x^4 y z^2$$

grlex is looking for a larger variable in a larger power

grevlex is looking for a smaller variable in a smaller power

Example. Consider $x > y > z$

$$4x^3 - 5y^4 + 7xy^2z + 4xyz^2 \in Q[x, y, z]$$

Lexicographical Order: $4x^3 + 7xy^2z + 4xyz^2 - 5y^4$

Graded Lexicographical Order: $7xzy^2 + 4xz^2y - 5y^4 + 4x^3$

Graded Reverse Lexicographical Order: $-5y^4 + 7xy^2z + 4xyz^2 + 4x^3$

Notations: Let $f = \sum c_k x^k$.

The *multidegree* f is mdeg(f) is the max exponent wrt to order.

The *leading coefficient* of f is LC(f)= c_{mdeg}

The *leading monomial* of f is LM(f) = x^{mdeg}

The *leading term* of f is LT(f) = LC(f) LM(f)

Example.

$f = 4x^3 - 5y^4 + 7xy^2z + 4xyz^2$

Lexicographical Order: $4x^3 + 7xy^2z + 4xyz^2 - 5y^4$

mdeg = {3,0,0); LC = 4; LM = x^3

Graded Lexicographical Order: $7xy^2z + 4xyz^2 - 5y^4 + 4x^3$

mdeg = {1,2,1); LC = 7; LM = xy^2z

■ **Multivariate division with remainder**

Fix a monomial order on $R = F[x_1, \ ..., \ x_n]$. and let $I = < f_1, \ ..., \ f_s >$ and $g \in R$. We want to determine whether $g \in I$. The basic idea is the same as in one-dimensional case, however some care will be needed to characterize the remainder. The goal is to divide g by $f_1, \ ..., \ f_s$ which means

$$g = a_1 \ f_1 + ... + a_s \ f_s + r$$

where a_k and r are in $F[x_1, \ ..., \ x_n]$.

Example: (lexicographical order) Determine whether $g \in < f_1, \ f_2 >$, where

$$< f_1, \ f_2 > = \ < x\,y - 1, \ y^2 - 1 >$$

$$g = x^2\,y + x\,y^2 + y^2$$

We will divide g by f_1 and then by f_2

$x\,y - 1$ $y^2 - 1$ rem

$x^2\,y + x\,y^2 + y^2$ x

$-\left(x^2\,y - x\right)$

$x\,y^2 + x + y^2$ y

$-\left(x\,y^2 - y\right)$

$x + y^2 + y$ x

$y^2 + y$ 1

$-\left(y^2 - 1\right)$

$y + 1$ y + 1

Therefore,

$$g = x^2\,y + x\,y^2 + y^2 = (x + y)\ f_1 + \ f_2 + (x + y + 1)$$

Seems that the division algorithm can solve the membership problem: if we obtain by division that the remainder is zero then a polynomial belongs to the ideal. Unfortunately, rem = 0 is only sufficient condition.

Example: (lexicographical order)

$$< f_1,\ f_2 > \ = \ < x\,y + 1,\ y^2 - 1 >$$

$$g \ = \ x\,y^2 - x$$

Dividing g by $< f_1,\ f_2 >$, yields $g \ = \ y\ f_1 \ + (-x - y)$

Dividing g by $< f_2,\ f_1 >$, yields $g \ = \ x\ f_2$

This example shows, that if $g \in I$ it is still possible to obtain a nonzero remainder. So our basis is not perfect! We need to search for a "better" one!

■ **Generalized Division Algorithm**

```
Input: f1,f2,...,fs, g
Output: a1,a2,...,as, r
ai := 0 1<=i<=s; r := 0; p := g
   WHILE (p<>0) DO
         i := 1
         dividing := true
         WHILE i<=s AND dividing DO
                  IF LT(fi) divides LT(p) THEN
                           ai := ai + LT(p)/LT(fi)
                           p := p - (LT(p)/LT(fi)) * fi
                           dividing := false
                  ELSE
                            i := i+1
         IF (dividing) THEN
                  r := r + LT(p)
                  p := p - LT(p)
```

Clearly the algorithm is a generalized form of the high school division algorithm. The variable p represents the intermediate dividend at each stage. As long as the leading term of a divisor divides the leading term of p, the algorithm proceeds as in the one-variable case. Otherwise, we remove the leading term of p and add it to the remainder.

References

[1] Wen-tsun Wu, *Mathematics Mechanization,* Kluwer Acad. Publ., Beijing, 2000.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer-Verlag, 1991.