Gröbner Bases

Victor Adamchik

Carnegie Mellon University

■ The main idea

Given a system of polynomial equations

$$\begin{cases} f_1 = 0 \\ \quad \ldots \\ f_s = 0 \end{cases}$$

It forms an ideal $I = \langle f_1, \ldots, f_s \rangle$ for which we cannot solve a membership problem

It's better to choose a monomial ideal

But how would you build a monomial ideal out of a given set of polynomials?

Monomial Ideal

■ Understanding the structure

Definition: A *monomial ideal* $I \subset R$ is an ideal generated by monomials in R. For example,

$$I = \langle x^2 y^5, \; x^4 y^3, \; x^5 y \rangle$$

Such an ideal I consists of all polynomials which are finite sums of $\sum q_\alpha x^\alpha$, where $q_k \in R$. We will write $I = \{x^\alpha, \; \alpha \in A \subset \mathbb{Z}^n_{\geq 0}\}$

Example. Given

$$I = \langle x^2, \; x y^3, \; y^4 z, \; x y z \rangle$$

Then

$$f = 3 x^7 + 7 x y^3 z + 2 y^4 z + x y^2 z^2 \text{ is in } I,$$

since

$$x^7 = (x^2)(x^5)$$

$$x\,y^3\,z = \left(x\,y^3\right)(z)$$
$$x\,y^2\,z^2 = (x\,y\,z)\,(y\,z)$$

Exercise. Given

$$I = \langle x^3,\ x^2\,y \rangle$$

Verify

$$f_1 = 3\,x^4 + 5\,x^2\,y^3 \quad \text{is it in } I?$$
$$f_2 = 2\,x^4\,y + 7\,x^2 \qquad \text{is it in } I?$$

Lemma. *Let $I = \langle x^\alpha \mid \alpha \in A \rangle$ and let x^β be a monomial in R. Then $x^\beta \in I \Longleftrightarrow x^\alpha \mid x^\beta$ for some $\alpha \in A$.*

Proof.

$\Longleftarrow$) is clear.

$\Longrightarrow$) Let $x^\beta \in I$, we can write $x^\beta = \sum q_k\,x^{\alpha_k}$, where $q_k \in R$. Each monomial in the sum is divisible by some x^α, and thus x^β is divisible by some x^α.■

Consider $I = \langle x^2\,y^5,\ x^4\,y^3,\ x^5\,y \rangle$.Here is a picture of all monomials in I.

Lemma.

Let I be a monomial ideal in R and let $f \in R$. Then the following are equivalent

1. $f \in I$
2. every monomial of f is in I
3. f is a linear combination of monomials in I.

This lemma will allow us to solve **the membership ideal problem:**

a given polynomial is in the monomial ideal $\Longleftrightarrow$ if the remainder of f on *division by generators is zero.*

■ Size of a monomial ideal

Lemma (*Emmy Noether*) (1882-1935)

Let R be a ring. The the following are equivalent

1. every ideal $I_k \subset R$ is finitely generated

2. every ascending sequence of ideals

$$I_0 \subset I_1 \subset \ldots$$

terminates, i.e. $I_n = I_{n+1}$ for sufficiently large n.

Then we say that the ring R is Noetherian.

The Noetherian-ness of polynomial rings allows us to prove that any infinite set of polynomial equations can be replaced with a finite set with the same solutions.

Proof.

1⟹2) Every ideal is finitely generated

$$I_1 = \; < f_1, \;\ldots,\; f_{p_1} >$$

$$I_2 \;=\; < \; f_1, \ldots, \; f_{p_1}, \;\ldots, \; f_{p_1+p_2} >$$

Take their union

$$I_\infty = \; < \; f_1, \; f_2, \; \ldots >$$

which is also finitely generated. Thus we may assume that the generators are taken from the ideals $I_{n_1}, \ldots, I_{n_r}$. If $N = \max(n_1 \ldots, n_r)$ then $I_\infty = I_N$.

2⟹1) Suppose every ascending sequence terminates.

Let I be an ideal $I = \; < f_\alpha >$ that is not generated by a finite number of α.

Then we can construct an infinite sequence such that

$$I_r = \; < f_{\alpha_1}, \;\ldots, \; f_{\alpha_r} > \; \not\subset \; I_{r+1} < f_{\alpha_1}, \;\ldots, \; f_{\alpha_{r+1}} >$$

for every r that violates the ascending chain condition.■

Lemma (*Dickson*, 1913)

Every monomial ideal $J \subset F[x_1, \;\ldots, \; x_n]$ is generated by a finite number of monomials.

The statement looks suspicious... Let $R = Q\{x, \; y]$, and consider $< x^2, \; x^2\, y, \; x^2\, y^2, \; \ldots >$. The catch: we must elimininate redundant generators

$$< x^2,\ x^2 y,\ x^2 y^2,\ \ldots > \ = \ < x^2 >$$

Proof. By induction on the number of variables.

If $n = 1$, then let $\beta = \min \{\alpha \mid x^\alpha \in A\}$.

Inductive step. The result is valid for $F[x_1, \ \ldots, \ x_{n-1}]$. We need to deduce it for $F[x_1, \ \ldots, \ x_{n-1}, \ y]$.

Let $J \subset F[x_1, \ \ldots, \ x_{n-1}, \ y]$ be a monomial ideal with n variables. We write a monomial in $F[x_1, \ \ldots, \ x_{n-1}, \ y]$ as $x^\alpha y^m$. Consider the following set of monomial ideals

$$J_m \subset F[x_1, \ \ldots, \ x_{n-1}]$$
$$J_m = \{x^\alpha \in F[x_1, \ \ldots, \ x_{n-1}] \mid x^\alpha y^m \in J\}$$

satisfying the ascending sequence

$$J_0 \subset J_1 \subset \ldots$$

Each J_k is finitely generated. This sequence terminates by the Noether theorem. Then the ideal J is a set of all monomials from the sequence. ■

■ Ideal of leading terms

Fix a monomial order and $I \subset R$ is an ideal. We define $\mathrm{LT}(I)$ as a set of the leading terms of the elements of the ideal I (with respect to a given monomial order).

$$\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I\}.$$

The *leading term ideal* of I, denoted by $< \mathrm{LT}(I) >$ is the ideal generated by $\mathrm{LT}(I)$. Observe, that is unpractical to build < LT(I) >, since we will have to consider all polynomials in the ideal and take their leading terms. We would rather take the ideal of leading terms of generators

$$< \mathrm{LT}(f_1), \ \ldots, \ \mathrm{LT}(f_s) >$$

There are two ideals are NOT necessarily equal.

Example. Consider $I = \ < f_1, \ f_2 > \ = \ < x^2 + 2\, x\, y^2, \ x\, y + 2\, y^3 - 1 >$. We can show that

$$x \in \ < f_1, \ f_2 >, \text{since } \ y * f_1 - x * f_2 == x$$

Moreover, $\mathrm{LT}(x) = x \in \ < \mathrm{LT}(I) >$. Now, we consider the ideal of leading terms of generators

$$< \mathrm{LT}(f_1), \ \mathrm{LT}(f_2) > \ = \ < x^2, \ x\, y >$$

It follows that $x \notin \ < \mathrm{LT}(f_1), \ \mathrm{LT}(f_2) >$.

The main question: is it possible to find such a set of generators that

$$< \mathrm{LT}(I) >= < \mathrm{LT}(f_1), \ \ldots \mathrm{LT}(f_s) >$$

Theorem. (*Hilbert Basis Theorem*)

Every ideal I in R is finitely generated. More precisely, there exists a finite subset $G = \{g_1, \ \ldots, \ g_s\} \subset I$ such that $I = \{g_1, \ \ldots, g_s\}$ with a property

$$< \mathrm{LT}(I) >= < \mathrm{LT}(g_1), \ \ldots, \ \mathrm{LT}(g_s) >$$

The Hilbert theorem tells us that any ideal (monomial or otherwise) is finitely generated. One CAN find such subset $G = \{g_1, \ \ldots, \ g_s\}$ of generators! The basis $\{g_1, \ \ldots, \ g_s\}$ that have a property $< \mathrm{LT}(I) >= < \mathrm{LT}(g_1), \ \ldots \mathrm{LT}(g_s) >$ is quite special!!

Gröbner Basis

Definition: Fix a monomial order and let I be an ideal. A finite subset $G = \{g_1, \ \ldots, \ g_r\} \subset I$ is said to be a *Gröbner basis* if

$$< \mathrm{LT}(I) >= < \mathrm{LT}(g_1), \ \ldots, \ \mathrm{LT}(g_s) >$$

This means that a subset $G = \{g_1, \ \ldots, \ g_r\} \subset I$ of an ideal I is a Gröbner basis if and only if the leading term of any element of I is divisible by one of the $\mathrm{LT}(g_k)$.

Example. Fix *lex* order and consider

$$I = < f_1, \ f_2 > = < x^3 - 2\,x\,y, \ x^2\,y - 2\,y^2 - x >$$

$< f_1, \ f_2 >$ is not a Gröbner basis. To prove this we first show that

$$x^2 \in < \mathrm{LT}(I) >$$

Indeed,

$$x^2 = y\,f_1 - x\,f_2 \Longrightarrow x^2 \in I \Longrightarrow x^2 = \mathrm{LT}\left(x^2\right) \in < \mathrm{LT(I)} >$$

However,

$$x^2 \notin < \mathrm{LT}(f_1), \ \mathrm{LT}(f_2) > = < x^3, \ x^2\,y >$$

since x^2 is not divisible by x^3 and $x^2\,y$.

We will show that divison with remainder by a Gröbner basis is a valid ideal membership test.

Theorem. *Let G be a Gröbner basis for an ideal $I \subset R$. Then $f \in I \Longleftrightarrow$ the remainder r on division of f by G is zero. In other words,*

$$f \in I \Longleftrightarrow f \xrightarrow{*}_G 0$$

Proof.

$\Longrightarrow$) Let f be an arbitrary polynomial in I, then division yields

$$f = e_1\, g_1 + \ldots + e_s\, g_s + r$$

Thus, $f - r \in I$, it follows that $r \in I$. Assume that $r \neq 0$. Then there exists k such that LT(g_k) divides LT(r), since G is a Gröbner basis. This is a contradiction to the fact that r is reduced wrt to G. Thus, $r = 0$.■

Corollary. *If* $G = \{g_1, \ldots, g_s\}$ *is a Gröbner basis for the ideal* I*, then* $I = \langle g_1, \ldots, g_s \rangle$.

Proof.

Clearly $G = \{g_1, \ldots, g_s\} \subseteq I$, since each $g_k \in I$.

To prove $I \subseteq G$, choose any $f \in I$. By the above theorem f is reducible by G with a zero remainder. Thus, $I \subseteq G$.■

Using the idea of Gröbner bases, we can easily solve a membership problem.

Algorithm

First we compute a Gröbner basis G of I.

Then we divide f by G and get the remainder r.

If $r = 0$ then f lies in I, otherwise it does not.

The Hilbert theorem states that a Gröbner basis exists, though it does not address a way of how to construct it.

How do we compute a Gröbner basis?

We will give an alternate characterization of Gröbner bases which shows us a practical way to construct them. To do this, we need to introduce the notion of *S-polynomial*.

■ S-polynomials

Recalle the definition of a Gröbner basis.

> A subset $G = \{g_1, \ldots, g_r\} \subset I$ of an ideal I is a Gröbner basis if and only if the leading term of any element of I is divisible by one of the LT(g_k).

It might happen that a polynomial f has a leading power that is divisible by two (or more) LT(g_k) and LT(g_n), where $k \neq n$. If we reduce f using g_k we get a polynomial h_1

$$h_1 = f - \frac{P}{\mathrm{LT}(g_k)}\, g_k$$

and

$$h_2 = f - \frac{P}{\mathrm{LT}(g_n)}\, g_n$$

We introduced an ambiguity! But what if we consider $h_2 - h_1$??

$$h_2 - h_1 = \frac{P}{\mathrm{LT}(g_k)}\, g_k - \frac{P}{\mathrm{LT}(g_n)}\, g_n$$

This is a so-called S-polynomial. The S-polynomial is constructed in such a way that leading terms of two polynomials cancel each other.

Definition. Let f and g be two polynomials in R. The S-polynomial of f and g is the following combination

$$S(f,\ g) = \frac{p}{\mathrm{LT}(f)} * f - \frac{p}{\mathrm{LT}(g)} * g$$

where p is the least common multiple

$$p = \mathrm{LCM}(\ \mathrm{LM}(f),\ \mathrm{LM}(g)\,).$$

Example. Compute $S(f,\ g)$ where $f = x^2\, y + 2\, x\, y^2,\ g = 3\, y^2 + 2$.

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

The following theorem gives an alternate characterization of Gröbner bases.

Theorem. (*Buchberger's S-pair criterion*)

A finite set $G = \{g_1,\ \ldots,\ g_s\}$ for an ideal I is a Gröbner basis if and only if

$$S(g_k,\ g_n) \xrightarrow{*}_G 0$$

(the remainder of division $S(g_k,\ g_n)$ by G is zero) for any k and n.

This theorem suggests how we can transform an arbitrary ideal basis into a Gröbner basis. Given a finite set G in $F[x_1,\ \ldots,\ x_n]$, we can immediately test G by checking the remainder.

Example. We will prove that $I = \ < y - x^2,\ z - x^3 >$ is a Gröbner basis for *lex* order $y > z > x$

Consider the S-polynomial

$$S = \frac{y\, z}{y}\left(y - x^2\right) - \frac{y\, z}{z}\left(z - x^3\right) = y\, x^3 - z\, x^2$$

This polynomial must be divisible by the basis

$$y\, x^3 - z\, x^2 = x^3\left(y - x^2\right) - x^2\left(z - x^3\right) + 0$$

Exercise. Change the lex order to $x > y > z$ and verify that that the above basis is NOT a Gröbner basis.

```
GroebnerBasis[{y - x^2, z - x^3}, {x, y, z}, MonomialOrder → Lexicographic]
```

```
{y^3 - z^2, -y^2 + x z, x y - z, x^2 - y}
```

Example. Let $f_1 = x\,y - x$ and $f_2 = x^2 - y$ with the *grlex* ordering and $x > y$. Build a Gröbner basis.

1. We compute a S-polynomial of f_1 and f_2

$$S(f_1,\ f_2) = \frac{x^2\,y}{x\,y}\ f_1 - \frac{x^2\,y}{x^2}\ f_2 = x\ f_1 - y\ f_2 = -x^2 + y^2$$

2. Then we reduce this polynomial wrt our basis $< f_1,\ f_2 >$

$$-x^2 + y^2 \to_{f_2} = y^2 - y$$

3. Since y^2 is not divisible by ant $\mathrm{LT}(f_k)$, we add $f_3 = y^2 - y$ to the basis, which is now is $G = < f_1,\ f_2,\ f_3 > = < x\,y\ -\ x,\ x^2 - y,\ y^2 - y >$.

4. Repeat the first step.

Compute S-polynomials and reduce them over basis G

$$S(f_1,\ f_2) \longrightarrow_G\ 0$$

$$S(f_1,\ f_3) = \frac{x\,y^2}{x\,y}\ f_1 - \frac{x\,y^2}{y^2}\ f_3 = y\ f_1 - x\ f_3 =\ 0$$

$$S(f_2,\ f_3) = \frac{x^2\,y^2}{x^2}\ f_2 - \frac{x^2\,y^2}{y^2}\ f_3 = y^2\ f_2 - x^2\ f_3 =\ x^2\ y - y^3$$

$$x^2\ y - y^3\ =\ q * f_2 + h = q\left(x^2 - y\right)\ +\ h = y\left(x^2 - y\right) + h$$

$$x^2\ y - y^3 \longrightarrow_{f_2} -y^3 + y^2$$

$$-y^3 + y^2\ =\ q * f_3 + h = q\left(y^2 - y\right)\ +\ h = -y\left(y^2 - y\right) + h$$

$$-y^3 + y^2 \longrightarrow_{f_3}\ 0$$

Thus, $< f_1,\ f_2,\ f_3 >$ is a Gröbner basis

```
GroebnerBasis[{x y - x, x^2 - y}, {x, y},
 MonomialOrder → DegreeLexicographic]
```

```
{-y + y^2, -x + x y, x^2 - y}
```

References

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