Gröbner bases and elimination theory

Shing Tak Lam

March 22, 2023

1 Motivation

In Algebraic geometry, given polynomials $f_1, \dots, f_m \in \mathbb{C}[x_1, \dots, x_n]$, we want to study

$$V = \mathbb{V}(f_1, \dots, f_m)$$

One natural question is whether $V = \varnothing$. From the (weak) Nullstellensatz, we know that

$$V = \varnothing \iff 1 \in I = (f_1, \dots, f_m)$$

More generally, consider the *ideal membership problem*. Given an ideal $I = (f_1, \dots, f_m) \trianglelefteq k[x_1, \dots, x_n]$, and $g \in k[x_1, \dots, x_n]$, is there an algorithm for determining whether $g \in I$?

2 Reduction and Gröbner bases

First of all, we need to generalise the notion of polynomial division f/g in $k[x]$ to division by polynomials $g_1, \dots, g_r$ in $\mathbb{C}[x_1, \dots, x_n]$.

Recall long division of polynomials.

[Long division of polynomials]

Issue: $k[x]$ is a Euclidean domain with Euclidean function deg, and deg gives us a well ordering

$$1 \prec x \prec x^2 \prec \dots$$

of the monomials in $k[x]$. However, deg no longer defines a well ordering on the set of monomials in $k[x_1, \dots, x_n]$. For example,

$$x_1^2, x_1x_2, x_2^2$$

all have the same degree. Furthermore, we needed the fact that we have a well ordering to justify the fact that polynomial division terminates.

2.1 Monomial orders

Therefore, what we want is a well ordering of the monomials in $k[x_1, \dots, x_n]$, which behaves nicely under multiplication.

Definition 2.1 (Monomial order)

A monomial ordering $\succ$ on $k[x_1, \dots, x_n]$ is a relation $\succ$ on $\mathbb{N}^n$ such that

- $\succ$ defines a well ordering on $\mathbb{N}^n$.
- If $\alpha \succ \beta$, then for any γ, $\alpha + \gamma \succ \beta + \gamma$.

We write $x^\alpha \succ x^\beta$ if $\alpha \succ \beta$.

Example 2.2 (Lexicographic order)

$$\alpha \succ_{\mathrm{L}} \beta \iff \text{first nonzero entry of } \alpha - \beta \in \mathbb{Z}^n \text{ is positive}$$

Example 2.3 (Graded lexicographic order)

$$\alpha \succ_{\mathrm{GL}} \beta \iff (|\alpha| > |\beta|) \text{ or } (|\alpha| = |\beta| \text{ and } \alpha \succ_{\mathrm{L}} \beta)$$

Example 2.4 (Graded reverse lexicographic order)

$$\alpha \succ_{\mathrm{GRL}} \beta \iff (|\alpha| > |\beta|) \text{ or } (|\alpha| = |\beta| \text{ and the right most entry of } \alpha - \beta \text{ is negative})$$

Definition 2.5
For a polynomial $f = \sum_\alpha a_\alpha x^\alpha$, we define

- The multidegree $\mathrm{mdeg}(f) = \max\{\alpha \mid a_\alpha \neq 0\}$
- The leading monomial $\mathrm{lm}(f) = x^{\mathrm{mdeg}(f)}$
- The leading coefficient $\mathrm{lc}(f) = a_{\mathrm{mdeg}(f)}$
- The leading term $\mathrm{lt}(f) = \mathrm{lc}(f)\,\mathrm{lm}(f)$

2.2 Reduction

Theorem 2.6 (Division algorithm). Let $\succ$ be a monomial order on $k[x_1, \ldots, x_n]$, $G = (g_1, \ldots, g_s)$ be a s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = q_1 g_1 + \cdots + q_n g_n + r$$

where $q_1, \ldots, q_n, r \in k[x_1, \ldots, x_n]$ where either $r = 0$, or each monomial in r is not divisible by any of $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$.

[Sketch of algo here]

Remark 2.7. This depends on a lot of things.

For example, this depends on the monomial ordering. Consider reducing $f = x^2 + xy$ by $g_1 = x^2$, $g_2 = x + y$. If we have an ordering such that $x^2 \succeq xy$, then $q_1 = 1$, $q_2 = y$ and $r = -y^2$. Whereas if $xy \succeq x^2$, then we have $q_1 = 0$, $q_2 = x$ and $r = 0$.

In addition, this depends on the ordering of the g_i, for example, if $f = x^2 y$, $g_1 = x^2$, $g_2 = xy$, then we get $q_1 = y, q_2 = 0$ whereas if $g_1 = xy$, $g_2 = x^2$ then we get $q_1 = x, q_2 = 0$.

Proposition 2.8 (Sufficient condition for ideal membership). If f, G as above, and we divide f by G and get $r = 0$, i.e.

$$f = q_1 g_1 + \cdots + q_n g_n$$

then $f \in (g_1, \ldots, g_n)$.

However this is not a necessary condition. For example, consider $g_1 = xy - 1, g_2 = y^2 - 1 \in k[x, y]$, and $f = xy^2 - x$. Suppose we use the lex order on $k[x, y]$. If we divide f by (g_1, g_2) we get

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

whereas if we divide f by (g_2, g_1) we get

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

2.3 Gröbner bases

Definition 2.9

Let $I \trianglelefteq k[x_1, \dots, x_n]$ be a nonzero ideal, and fix a monomial ordering $\succ$ on $k[x_1, \dots, x_n]$. Then define $\mathrm{lt}(I) = \{\mathrm{lt}(f) \mid f \in I \setminus \{0\}\}$.

Proposition 2.10. If $I = (f_1, \dots, f_s)$, then

$$(\mathrm{lt}(f_1), \dots, \mathrm{lt}(f_n)) \subseteq (\mathrm{lt}(I))$$

Proof. By definition $\mathrm{lt}(f_1) \in \mathrm{lt}(I)$. □

However, the reverse inclusion is usually false. For example, consider $f_1 = x^2 + x, f_2 = x^2$. Then $(\mathrm{lt}(f_1), \mathrm{lt}(f_2)) = (x^2)$ but $(\mathrm{lt}(I)) = (x)$.

Definition 2.11 (Gröbner basis)

Fix a monomial order on $k[x_1, \dots, x_n]$, a finite subset $G = \{g_1, \dots, g_t\}$ of a nonzero ideal $I \trianglelefteq k[x_1, \dots, x_n]$ is called a Gröbner basis if

$$(\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_t)) = (\mathrm{lt}(I))$$

Lemma 2.12. Suppose $x^\beta \in (x^{\alpha(1)}, \dots, x^{\alpha(n)})$. Then $x^{\alpha(i)} \mid x^\beta$ for some i.

Proof. Write $x^\beta = \sum_i h_i x^{\alpha(i)}$, $h_i \in k[x_1, \dots, x_n]$. We only care about the monomials which contribute to the leading term, so we have that

$$x^\beta = \mathrm{lt}(x^\beta) \sum_j \mathrm{lt}(h_{i_j}) x^{\alpha(i_j)}$$

where the i_j are such that $\mathrm{lt}(h_{i_j})x^{\alpha(i_j)}$ contributes to the leading term. Thus, all of the $x^{\alpha(i_j)}$ divide x^β. □

Proposition 2.13. If $G = \{g_1, \dots, g_t\}$ is a Gröbner basis for I, then

$$I = (g_1, \dots, g_t)$$

Proof. Clearly $(g_1, \dots, g_t) \subseteq I$. Conversely, given $f \in I$, divide f by $(g_1, \dots, g_t)$ to get

$$f = q_1 g_1 + \dots + q_t g_t + r$$

As each $g_i \in I$ and $f \in I$, we must have that $r \in I$. If $r \neq 0$, then $\mathrm{lt}(r) \in (\mathrm{lt}(I)) = (\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_t))$. But this means that $\mathrm{lt}(g_i) \mid \mathrm{lt}(r)$ for some i. Contradiction. □

There are tests to determine whether a set G is a Gröbner basis, and algorithms to compute them. However we will not discuss them here, and just assume their existence.

3 Ideal membership

First of all, we can use a Gröbner basis to determine ideal membership.

Proposition 3.1. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I. Then for any $f \in k[x_1, \ldots, x_n]$, there exists a unique r such that

- No term of r is divisible by any of $\operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_t)$,
- $f = g + r$ for some $g \in I$.

Proof. For existence, we use the division algorithm and write

$$f = \underbrace{q_1 g_1 + \cdots + q_t g_t}_{g} + r$$

For uniqueness, if $f = g + r = g' + r'$, then $r - r' = g - g' \in I$. If $r \neq r'$, then $\operatorname{lt}(r - r') \in (\operatorname{lt}(I))$. So by the same argument as before, we see that $\operatorname{lt}(g_i) \mid \operatorname{lt}(r - r')$ for some i. But this can't happen as no term in r or r' is divisible by any of $\operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_t)$. □

Corollary 3.2. No matter which order we do the division by elements of G, we always get the same result.

Proof. By uniqueness in the proposition. □

Definition 3.3

Let G be a Gröbner basis for an ideal I. Then define the reduction of f by G

$$\operatorname{red}_G(f) = r$$

where r is from the proposition.

Corollary 3.4. Let G be a Gröbner basis for an ideal I, $f \in k[x_1, \ldots, x_n]$. Then

$$f \in I \iff \operatorname{red}_G(r) = 0$$

4 Elimination theory

4.1 Elimination

Example 4.1

If $I = (x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1)$, then a Gröbner basis is given by

$$\begin{aligned}
g_1 &= x + y + z^2 - 1 \\
g_2 &= y^2 - y - z^2 + z \\
g_3 &= 2yz^2 + z^4 - z^2 \\
g_4 &= z^6 - 4z^4 + 4z^3 - z^2
\end{aligned}$$

Then $\mathbb{V}(I) = \mathbb{V}(g_1, g_2, g_3, g_4)$. But the second system of equations is much easier to solve. We can solve for z using g_4, substitute into g_2 and g_3 to find y, and substitute into g_1 to find x.

Definition 4.2 (Elimination ideal)
Let $I \trianglelefteq k[x_1, \ldots, x_n]$ be an ideal, the l-th elimination ideal of I is

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

Theorem 4.3 (Elimination theorem). Let G be a Gröbner basis for an ideal I with respect to the lexicographic order $x_1 \succ x_2 \succ \cdots \succ x_n$. Then for any $0 \leq l \leq n$, we have that

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

is a Gröbner basis for I_l.

Proof. By construction, $G_l \subseteq I_l$ and $(\mathrm{lt}(G_l)) \subseteq (\mathrm{lt}(I_l))$. We need to show the reverse inclusion $(\mathrm{lt}(I_l)) \subseteq (\mathrm{lt}(G_l))$.

Suppose $f \in I_l$. As $f \in I$, $\mathrm{lt}(f)$ is divisible by $\mathrm{lt}(g)$ for some $g \in G$. Since $f \in I_l$, $\mathrm{lt}(f)$ and $\mathrm{lt}(g)$ are in $k[x_{l+1}, \ldots, x_n]$. But we are using lex order, so $g \in k[x_{l+1}, \ldots, x_n]$ and $g \in G_l$. $\square$

Using the elimination theorem, we can solve for the coordinates of a point $p \in V = \mathbb{V}(I)$ one coordinate at a time. Define the l-th projection map

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l}$$

Lemma 4.4. We have that $\pi_l(V) \subseteq \mathbb{V}(I_l)$.

Proof. Fix $f \in I_l$. Suppose $(a_1, \ldots, a_n) \in V$, then $f(a_1, \ldots, a_n) = 0$. But f only involves $x_{l+1}, \ldots, x_n$, so we can write

$$f(a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)) = 0$$

$\square$

Proposition 4.5. In fact, $\mathbb{V}(I_l)$ is the Zariski closure of $\pi_l(V)$ and $\pi_l(V)$ is a Zariski open subset of $\mathbb{V}(I_l)$.

4.2 Implicitisation

Now suppose we have a parametrised set X given by

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m) \end{aligned}$$

where the f_i are polynomials, $(t_1, \ldots, t_m) \in k^m$. The equations above define a variety

$$V = \mathbb{V}(x_1 - f_1, \ldots, x_n - f_n) \in k^{m+n}$$

where points on V are of the form

$$(t_1, \ldots, t_m, f_1(t), \ldots, f_n(t))$$

Then it is easy to see that

$$X = \pi_m(V)$$

Hence if $I = (x_1 - f_1, \ldots, x_n - f_n) \in k[t, x]$ and I_m is the m-th elimination ideal, then $\mathbb{V}(I_m)$ is the Zariski closure of X.

4.2.1 Rational parametrisations

Now suppose we have

$$x_1 = \frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}$$
$$\vdots$$
$$x_n = \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)}$$

where $f_i, g_i \in k[t]$ and $t \in k^m \setminus W$, where $W = \mathbb{V}(g_1, \dots, g_n)$. We want to repeat the above process. However, the naïve guess $V = \mathbb{V}(g_1 x - f_1, \dots, g_n x - f_n)$ is too big. For example, consider

$$I = (vx - u^2, uy - v^2, z - u) \trianglelefteq k[u, v, x, y, z]$$

Then $I_2 = I \cap k[x, y, z] = (z(x^2 y - z^3))$. We also want to add in the condition that $g_1, \dots, g_n$ is not zero. We can do this as such:

1. Let $g = g_1 \cdots g_n$.
2. Let $I = (g_1 x - f_1, \dots, g_n x - f_n, 1 - gy) \trianglelefteq k[y, t, x]$.
3. Let $V = \mathbb{V}(I) \subseteq k^{1+m+n}$, so points on V are of the form
$$\left(\frac{1}{g(t)}, t, \frac{f_1(t)}{g_1(t)}, \dots, \frac{f_n(t)}{g_n(t)}\right)$$
and $\pi_{1+m}(V) = X$.
4. Then the Zariski closure of X is $\mathbb{V}(I_{1+m})$.

5 Ideal intersections

Theorem 5.1. Let $I, J \trianglelefteq k[x_1, \dots, x_n]$ be ideals. Then

$$I \cap J = (tI, (1-t)J) \cap k[x_1, \dots, x_n]$$

Proof. Given $f \in I \cap J$, $f = tf + (1-t)f \in (tI, (1-t)J)$. Conversely, if we have $f \in (tI, (1-t)J) \cap k[x_1, \dots, x_n]$. Then we can write

$$f = tg + (1-t)h$$

where $g \in I$ and $h \in J$. Setting $t = 0$ we see $f \in J$ and setting $t = 1$ we see $f \in I$. □

Therefore, with this, we can compute the intersection of two ideals by eliminating t.

Example 5.2
If we have $I = (x^2 + y, x + yz)$ and $J = (xy, x^2 y + z)$, then $(tI, (1-t)J)$ has Gröbner basis

$$\begin{aligned} g_1 &= tx + yz \\ g_2 &= ty + y^2 z^2 \\ g_3 &= -z + tz \\ g_4 &= xy + y^2 z \\ g_5 &= xz + yz^2 \\ g_6 &= yz + y^2 z^3 \end{aligned}$$

6 Minimal polynomial

Let $L = k(\alpha_1, \dots, \alpha_n)$ be an algebraic extension, α_i has minimal polynomial p_i over $k(\alpha_1, \dots, \alpha_{i-1})$.

Let $\bar{p}_i \in k[x_1, \dots, x_i]$ be such that $\bar{p}_i(\alpha_1, \dots, \alpha_{i-1}, x_i) = p_i(x_i)$ (and $\bar{p}_1 = p_1$). Then we have

Theorem 6.1. Suppose $\beta \in L$, i.e.

$$\beta = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$$

where $f, g \in k[x_1, \dots, x_n]$. Then let

$$J = (\bar{p}_1, \dots, \bar{p}_n, gy - f) \trianglelefteq k[x_1, \dots, x_n, y]$$

Then the elimination ideal $J_n = J \cap k[y]$ is a principal ideal, and the unique monic element is the minimal polynomial of β.

Example 6.2

Consider the field extension $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Then

- Minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x_1^2 - 2$.
- Minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}(\sqrt{2})$ is $x_2^3 - 5$.

If we wanted to compute the minimal polynomial of $\sqrt{2} + \sqrt[3]{5}$, we set

$$J = (x_1^2 - 2, x_2^3 - 5, y - (x_1 + x_2))$$

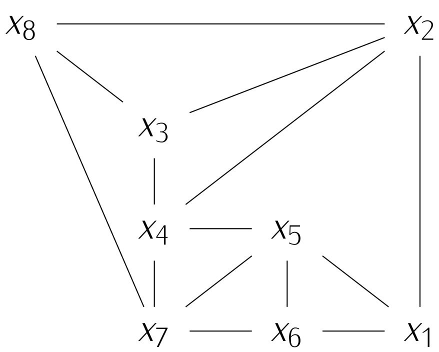
and we get the Gröbner basis

$$\begin{aligned} g_1 &= 1187x_1 - 48y^5 - 45y^4 + 320y^3 + 780y^2 - 735y + 1820 \\ g_2 &= 1187x_2 + 48y^5 + 45y^4 - 320y^3 - 780y^2 - 452y - 1820 \\ g_3 &= y^6 - 6y^4 - 10y^3 + 12y^2 - 60y + 17 \end{aligned}$$

So g_3 is the minimal polynomial of $\sqrt{2}+\sqrt[3]{5}$. In particular, as $[L : \mathbb{Q}] = 6$, we have that $L = \mathbb{Q}(\sqrt{2}+\sqrt[3]{5})$.

7 Graph colouring

Suppose we have the following graph



and we wanted to see whether we can 3-colour the graph. This is equivalent to finding $x_1, \dots, x_8 \in \{1, \zeta, \zeta^2\}$ where if x_i and x_j are adjacent, $\zeta_i \neq \zeta_j$. In particular,

$$0 = x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_ix_j + x_j^2)$$

so $x_i \neq x_j$ if and only if $x_i^2 + x_ix_j + x_j^2 = 0$. So if we define

- $v(x_j) = x_j^3 - 1$
- $a(x_i, x_j) = x_i^2 + x_ix_j + x_j^2$

and define the ideal

$$I = \left\langle \{v(x_j) \mid j = 1, \dots, 8\} \cup \{a(x_i, x_j) \mid x_i \text{ adjacent to } x_j\} \right\rangle$$

Then the graph has a 3-colouring if and only if $\mathbb{V}(I) \neq$. We can compute a Gröbner basis G for I, given by

$$\begin{aligned}
g_1 &= x_1 - x_7 \\
g_2 &= x_2 + x_7 + x_8 \\
g_3 &= x_3 - x_7 \\
g_4 &= x_4 - x_8 \\
g_5 &= x_5 + x_7 + x_8 \\
g_6 &= x_6 - x_8 \\
g_7 &= x_7^2 + x_7x_8 + x_8^2 \\
g_8 &= x^8 - 1
\end{aligned}$$

Then $\mathrm{red}_G(1) = 1$, and in fact the Gröbner basis gives us all possible 3-colourings of the graph, so we can see that in this case, the colouring is unique up to permutation of the colours.

8 Chicken nuggets

Now suppose we wanted to find a solution over $\mathbb{N}$ to

$$6a_6 + 9a_9 + 20a_{20} = 123$$

Consider the ideal

$$I = (y_6 - x^6, y_9 - x^9, y_{20} - x^{20}) \trianglelefteq k[x, y_6, y_9, y_{20}]$$

We can compute a Gröbner basis for I, and we get

$$\begin{aligned}
g_1 &= y_9^{20} - y_{20}^9 \\
g_2 &= y_{20}^6y_6 - y_9^{14} \\
g_3 &= y_6y_9^6 - y_{20}^3 \\
g_4 &= y_{20}^3y_6^2 - y_9^8 \\
g_5 &= y_6^3 - y_9^2 \\
g_6 &= xy_{20} - y_6^2y_9 \\
g_7 &= xy_9^5 - y_{20}^2y_6 \\
g_8 &= xy_6^2y_9^3 - y_{20}^2 \\
g_9 &= x^2y_9^2 - y_{20} \\
g_{10} &= x^3y_9 - y_6^2 \\
g_{11} &= x^3y_6 - y_9 \\
g_{12} &= x^6 - y_6
\end{aligned}$$

Then $\mathrm{red}_G(x^{123}) = y_{20}^3y_9^7$. So $a_6 = 0, a_9 = 7, a_{20} = 3$ is a solution. We can also try other values. For example, $\mathrm{red}_G(x^{41}) = y_{20}y_6^2y_9$, $\mathrm{red}_G(x^{42}) = y^6y_9^4$. On the other hand, $\mathrm{red}_G(x^{43}) = xy_6y_9^4$.