Gröbner Bases and their applications in the theory of algebraic equations, geometry and graph theory

Alexander Levin

The Catholic University of America
Washington, D. C. 20064

SEMINAR IN FUNCTIONAL ANALYSIS AND RELATED AREAS

January 25, 2023

Let K be a field and $R = K[x_1, \ldots, x_n]$ a ring of polynomials in n variables $x_1, \ldots, x_n$ over K.

By a **monomial** in R we mean a power product $t = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ with $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ ($\mathbb{N} = \{0, 1, 2, \ldots\}$).

The integer $\deg t = \sum_{i=1}^{n} \alpha_i$ is called the **degree** of t. The set of all monomials will be denoted by T.

Every element of R is a linear combination of monomials. Say, if $R = K[x_1, x_2, x_3]$, then an element

$f = 4x_1^3x_2^5x_3 - 5x_1^2x_2x_3^4 + x_1x_2^3 + 7$ is a linear combination of the monomials

$t_1 = x_1^3x_2^5x_3$, $t_2 = x_1^2x_2x_3^4$, $t_3 = x_1x_2^3$, and $t_4 = 1$ with coefficients $4, 5, 1$,and 7, respectively.

A monomial with a coefficient will be called a *term*. Say, f has terms $4x_1^3x_2^5x_3$, $-5x_1^2x_2x_3^4$, $x_1x_2^3$, and 7.

By a **monomial ordering** we mean any total ordering $\leq$ on T such that

(I) $x^\alpha > 1$ for any $x^\alpha \in T$, $x^\alpha \neq 1$.

(Recall that $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$. The total ordering of a set T is a relation $\leq$ on T such that (i) $t \leq t$ for any $t \in T$; (ii) if $t \leq t'$ and $t' \leq t$, then $t = t'$; (iii) if $t \leq t'$ and $t' \leq t''$, then $t \leq t''$ $(t, t', t'' \in T)$, and (iv) whenever $t, t' \in T$, one has either $t \leq t'$ or $t' \leq t$. If $t \leq t'$ and $t \neq t'$, we write $t < t'$ or $t' > t$.)

(II) If $x^\alpha < x^\beta$, then $x^\alpha x^\gamma < x^\beta x^\gamma$ for any $x^\gamma \in T$.

It can be shown that any monomial ordering of T is a well-ordering, that is, every non-empty subset of T has the smallest element.

We define the **lexicographic order** $<_{lex}$ on T with $x_1 > x_2 > \cdots > x_n$ as follows: if $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$, then $x^\alpha <_{lex} x^\beta$ if and only if the first coordinates α_i and β_i from the left, which are different, satisfy $\alpha_i < \beta_i$. (As usual, we write $t \leq_{lex} t'$ if $t <_{lex} t'$ or $t = t'$ where $t, t' \in T$).

For example, $x_1 x_2^3 x_3^4 <_{lex} x_1^2 x_2 x_3^3 <_{lex} x_1^2 x_2^2$

We define the **graded lexicographic order** (also called a **degree lexicographic order**) $<_{grlex}$ on T with $x_1 > x_2 > \cdots > x_n$ as follows:

$x^\alpha <_{grlex} x^\beta$ if and only if either

$\deg x^\alpha = \sum_{i=1}^{n} \alpha_i \leq \deg x^\beta = \sum_{i=1}^{n} \beta_i$ or $\deg x^\alpha = \deg x^\beta$ and $x^\alpha <_{lex} x^\beta$.

For example, $x_1 x_2^3 x_3^4 >_{grlex} x_1^2 x_2 x_3^3 >_{grlex} x_1^2 x_2^2 >_{grlex} x_1 x_2^2 x_3$.

Division Algorithm

If $n = 1$, $f(x), g(x) \in K[x]$, and $g(x) \neq 0$, then there exist unique polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) such that

$$f(x) = q(x)g(x) + r(x) \quad \text{and either} \quad r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

$q(x)$ and $r(x)$ are called the quotient and remainder of the division, respectively.

For example, let $f = x^3 - 2x^2 + 2x + 8$ and $g = 2x^2 + 3x + 1$. Dividing f by g we proceed as follows.

$$
\begin{array}{r|l}
 & \frac{1}{2}x - \frac{7}{4} \\
\hline
2x^2+3x+1 & x^3 - 2x^2 + 2x + 8 \\
 & -x^3 + \frac{3}{2}x^2 + \frac{1}{2}x \\
\hline
 & -\frac{7}{2}x^2 + \frac{3}{2}x + 8 \\
 & -\left(-\frac{7}{2}x^2 - \frac{21}{4}x - \frac{7}{4}\right) \\
\hline
 & \frac{27}{4}x + \frac{39}{4}
\end{array}
$$

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

$q(x)$ $\qquad$ $r(x)$

We first multiplied g by $\frac{1}{2}x$ and subtracted the resulted product from f in order to cancel the "leading term" x^3 in f and obtain $h = -\frac{7}{2}x^2 + \frac{3}{2}x + 8$. Such an operation is called a **reduction** of f by g; we write $f \xrightarrow{g} h$.

If $f \in K[x_1, \ldots, x_n]$ $(n \geq 1)$, then f has a unique (up to the order of the terms in the sum) "standard" representation as

$$f = a_1 t_1 + \cdots + a_r t_r$$

where $t_i \in T = \{x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{N}\}$, $0 \neq a_i \in K$ $(i = 1, \ldots, r)$, and $t_i \neq t_j$ whenever $i \neq j$.

If $<$ is a fixed monomial order on T, we define the **leading monomial** of f, written as $\mathrm{lm}(f)$, to be the greatest monomial of f (with respect to $<$). The coefficient of $\mathrm{lm}(f)$ is called the **leading coefficient** of f; it is denoted by $\mathrm{lc}(f)$. The term $\mathrm{lc}(f)\,\mathrm{lm}(f)$ is said to be the **leading term** of f; it is denoted by $\mathrm{lt}(f)$.

Clearly, for any two polynomials f and g, $\mathrm{lm}(fg) = \mathrm{lm}(f)\,\mathrm{lm}(g)$ and $\mathrm{lm}(f+g) \leq \max\{\mathrm{lm}(f), \mathrm{lm}(g)\}$ with equality if and only if the leading terms of f and g do not cancel in the sum.

If $t_1 = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ and $t_2 = x_1^{\beta_1} \dots x_n^{\beta_n}$ are two monomials, we say that t_1 divides t_2 and write $t_1 | t_2$ is there exists a monomial t' such that $t_2 = t_1 t'$. Then we write $t' = \frac{t_2}{t_1}$. If $u_1 = at_1$ and $u_2 = bt_2$ are terms ($a, b \in K$), we say that u_1 divides u_2 and write $u_1 | u_2$ if $t_1 | t_2$. Then $\frac{u_2}{u_1} = \frac{b}{a}\frac{t_2}{t_1}$

Given $f, g, h \in K[x_1, \dots, x_n]$ with $g \neq 0$, we say that f **reduces to** h **modulo** g **in one step** and write $f \xrightarrow{g} h$ if and only if $\mathrm{lt}(g)$ divides some nonzero term u that appears in f and $h = f - \frac{u}{\mathrm{lt}(g)} g$.

Given $f, g \in K[x_1, \ldots, x_n]$ and a set of nonzero polynomials $G \subseteq K[x_1, \ldots, x_n]$, we say that f **reduces to** h **modulo** G and write $f \xrightarrow{G} h$ if there exist elements $g_1, \ldots, g_k \in F$ and $h_1, \ldots, h_{k-1} \in K[x_1, \ldots, x_n]$ such that
$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2 \xrightarrow{g_3} \ldots \xrightarrow{g_{k-1}} h_{k-1} \xrightarrow{g_k} h$.

A polynomial r is called **reduced** with respect to a set of nonzero polynomials $G = \{g_1, \ldots, g_s\}$ if either $r = 0$ or no term in r is divisible by any $lt(g_i)$ $(i = 1, \ldots, s)$. In other words, r cannot be reduced modulo G.

Theorem 1

(Division Algorithm) With the above notation and a fixed monomial order $<$, let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $K[x_1, \ldots, x_n]$. Then every polynomial $f \in K[x_1, \ldots, x_n]$ can be written as

$$f = q_1 f_1 + \cdots + q_s f_s + r \tag{1}$$

where $q_i, r \in K[x_1, \ldots, x_n]$ and either $r = 0$ or r is a K-linear combination of monomials none of which is divisible by any $\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)$ and $\mathrm{lm}(q_i f_i) \leq \mathrm{lm}(f)$ for $i = 1, \ldots, s$.

PROOF. In order to prove the theorem, one should just notice that the following algorithm terminates and produces an equality of the form (4) whose entries satisfy the conditions of the theorem.

Input: $f, f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, with $f_i \neq 0\,(i = 1, \ldots, s)$
Output: $q_1, \ldots, q_s, r \in K[x_1, \ldots, x_n]$ such that
$f = q_1 f_1 + \cdots + q_s f_s + r$ and r is reduced with respect to $\{f_1, \ldots, f_s\}$ and $\mathrm{lm}(q_i f_i) \leq \mathrm{lm}(f)$ for $i = 1, \ldots, s$.
Initialization: $q_1 := 0, \ldots, q_s := 0, r := 0$, h:=f
While $h \neq 0$ **Do**
IF there exists i such that $\mathrm{lm}(f_i) | \mathrm{lm}(h)$ **THEN**
choose i least such that $\mathrm{lm}(f_i) | \mathrm{lm}(h)$
$q_i := q_i + \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)}$
$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)} f_i$
ELSE
$r := r + \mathrm{lt}(h)$
$h := h - \mathrm{lt}(h)$ □

Example 1

Let $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$ be polynomials in $K[x, y]$ where we fix a lexicographic order $<$ with $y < x$.
The division of f by (f_1, f_2) produces

$f \xrightarrow{f_1} h_1 = x^2y + xy^2 + y^2 - x(xy - 1) = xy^2 + x + y^2 \xrightarrow{f_1} h_2 = xy^2 + x + y^2 - y(xy - 1) = x + y^2 + y \xrightarrow{f_1} r = h_2 - f_2 = x + y + 1$. Thus,

$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$, so $f = q_1 f_1 + q_2 f_2 + r$ with $q_1 = x + y$, $q_2 = 1$, $r = x + y + 1$.

On the other hand, the division of f by (f_2, f_1) gives

$f \xrightarrow{f_2} h_1 = x^2y + xy^2 + y^2 - x(y^2 - 1) = x^2y + x + y^2 \xrightarrow{f_2} h_2 = x^2y + x + y^2 - (y^2 - 1) = x^2y + x + 1$
$\xrightarrow{f_1} r = x^2y + x + 1 - x(xy - 1) = 2x + 1$.

Thus, $x^2y + xy^2 + y^2 = (x + 1)(y^2 - 1) + x(xy - 1) + 2x + 1$, that is, $f = q_2' f_2 + q_1' f_1 + r'$ where $q_1' = x$, $q_2' = x + 1$, and $r' = 2x + 1$.

Gröbner Bases

Let I be an ideal of $K[x_1, \ldots, x_n]$. It means that I is a set of polynomials such that if $f, g \in I$, then $f + g \in I$, $-f \in I$, and $hf \in I$ for any $h \in K[x_1, \ldots, x_n]$.
For example, if $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, then the set of all linear combinations $h_1 f_1 + \cdots + h_k f_k$ with $h_1, \ldots, h_k \in K[x_1, \ldots, x_n]$ is an ideal. We say that this is an ideal generated by the set $\{f_1, \ldots, f_k\}$ and denote this ideal by $\langle f_1, \ldots, f_k \rangle$.

An ideal I in $K[x_1, \ldots, x_n]$ is called a **monomial ideal** if it is generated by a set of monomials.Such an ideal can be always generated by a finite set of monomials; this is a consequence of the following statement.

Proposition 1 (Dickson's Lemma)

Every set of monomials X in $K[x_1, \ldots, x_n]$ contains a finite subset $Y \subseteq X$ such that every monomial in X is a multiple of some monomial in Y.

Definition 2

Let $K[x_1, \ldots, x_n]$ be a ring of polynomials in n variables $x_1, \ldots, x_n$ over a field K, and let a monomial order $<$ on the set of all monomials of $K[x_1, \ldots, x_n]$ be fixed. Let I be an ideal of $K[x_1, \ldots, x_n]$. A finite subset $G = \{g_1, \ldots, g_s\}$ of I is called a **Gröbner basis** (or a **standard basis**) for the ideal I if for every nonzero polynomial $f \in I$, there exists some $g_i \in G$ such that $\mathrm{lm}(g_i)$ divides $\mathrm{lm}(f)$.

A finite set $G \subseteq K[x_1, \ldots, x_n]$ is called a Gröbner basis if it is a Gröbner basis of the ideal $\langle G \rangle$.

Note that if G is a Gröbner basis of an ideal I and $G \subseteq H \subseteq I$, then H is also a Gröbner basis of I.

Theorem 3

Let I be an ideal of $K[x_1, \ldots, x_n]$. The following statements are equivalent for a set of polynomials $G = \{g_1, \ldots, g_s\} \subseteq I$.

(i) *G is a Gröbner basis for I.*

(ii) *$f \in I$ if and only if $f \xrightarrow{G} 0$.*

(iii) *The remainder on the division of and element $f \in K[x_1, \ldots, x_n]$ by $g_1, \ldots, g_s$ does not depend on the order of reductions by elements of the set $\{g_1, \ldots, g_s\}$.*

(iv) *$f \in I$ if and only if f can be expressed as $f = \sum_{i=1}^{s} h_i g_i$ with*

$\mathrm{lm}(f) = \max_{1 \leq i \leq s}(\mathrm{lm}(h_i)\,\mathrm{lm}(g_i))$.

(v) $\langle \{\mathrm{lm}(f) \mid f \in I\} \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle$.

Let f and g be two non-zero polynomials in $K[x_1, \ldots, x_n]$ and et L denote the least common multiple of $lm(f)$ and $lm(g)$.

(Recall that the least common multiple of two monomials $t_1 = x_1^{i_1} \ldots x_n^{i_n}$ and $t_2 = x_1^{j_1} \ldots x_n^{j_n}$, denoted by $\mathrm{lcm}(t_1, t_2)$, is the monomial $x_1^{\max\{i_1, j_1\}} \ldots x_n^{\max\{i_n, j_n\}}$.)

Then the polynomial

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

is called the *S-polynomial of f and g*.

The following theorem gives the theoretical foundation for computing Gröbner bases.

Theorem 4 (B. Buchberger, 1964)

With the above notation, let $G = \{g_1, \ldots, g_s\}$ *be set of nonzero polynomials in* $K[x_1, \ldots, x_n]$*. Then* G *is a Gröbner basis of the ideal* $I = (g_1, \ldots, g_s)$ *if and only if*

$$S(g_i, g_j) \xrightarrow{G} 0$$

for all $g_i, g_j \in G$, $i \neq j$.

Example 2

Let $f_1 = xy - x$, $f_2 = x^2 - y \in \mathbb{Q}[x, y]$ with $<_{grlex}$ with $x < y$. Let $I = \langle f_1, f_2 \rangle$. In order to construct a Gröbner basis of I, consider

$$S(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{F} y^2 - y.$$

Since $f_3 = y^2 - x^2$ is reduced with respect to $F == \{f_1, f_2\}$, we adjoin f_3 to F and obtain a new set $F' = \{f_1, f_2, f_3\} \subseteq I$.

Now

$$S(f_1, f_2) \xrightarrow{F'} 0,\ S(f_1, f_3) = yf_1 - xf_3 = 0 \text{ and}$$

$$S(f_2, f_3) = y^2 f_2 - x^2 f_3 = -y^3 + x^2 y \xrightarrow{F'} x^2 y - y^2 \xrightarrow{F'} 0.$$

Therefore, $F' = \{f_1, f_2, f_3\}$ is a Gröbner basis of I.

A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is called **minimal** if for all i, $\mathrm{lc}(g_i) = 1$ and for all $i \neq j$, $\mathrm{lm}(g_i)$ does not divide $\mathrm{lm}(g_j)$.

Let $G = \{g_1, \ldots, g_s\}$ be any Gröbner basis. Let us eliminate all g_i for which there exists $j \neq i$ such that $\mathrm{lm}(g_j)$ divides $\mathrm{lm}(g_i)$ and divide each remaining g_i by $\mathrm{lc}(g_i)$. It is clear that the remaining system of elements is a minimal Gröbner basis. It follows that *every ideal in a polynomial ring has a minimal Gröbner basis*.

Proposition 2

If $F = \{f_1, \ldots, f_s\}$ and $G = \{g_1, \ldots, g_t\}$ are two minimal Gröbner bases of an ideal I of $K[x_1, \ldots, x_n]$, then $s = t$ and after renumbering, if necessary, $\mathrm{lm}(f_i) = \mathrm{lm}(g_i)$ for all $i = 1, \ldots, s$.

A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is called a **reduced Gröbner basis** if, for all i, $\mathrm{lc}(g_i) = 1$ and g_i is reduced with respect to $G \setminus \{g_i\}$. That is, for all i, no nonzero monomial in g_i is divisible by any $\mathrm{lm}(g_j)$ for any $j \neq i$.
Clearly, a reduced Gröbner basis is minimal.

Proposition 3

Let $G = \{g_1, \ldots, g_t\}$ be a minimal Gröbner basis of an ideal I in a polynomial ring. Consider the following reduction process:

$g_1 \xrightarrow{H_1} h_1$ *where* h_1 *is reduced with respect to* $H_1 = \{g_2, \ldots, g_t\}$;

$g_2 \xrightarrow{H_2} h_2$ *where* h_2 *is reduced with respect to* $H_2 = \{h_1, g_3 \ldots, g_t\}$;

$g_3 \xrightarrow{H_3} h_3$ *where* h_3 *is reduced with respect to* $H_3 = \{h_1, h_2, g_4 \ldots, g_t\}$;

$\ldots$

$g_t \xrightarrow{H_t} h_t$ *where* h_t *is reduced with respect to* $H_t = \{h_1, h_2, \ldots, h_{t-1}\}$.

Then $H = \{h_1, h_2, \ldots, h_t\}$ *is a reduced Gröbner basis of* I.

Example 3

Let $I = \langle f_1, f_2, f_3 \rangle$ be an ideal of $\mathbb{Q}[x, y, z]$ generated by $f_1 = y^2 + yx + x^2$, $f_2 = y + x$, and $f_3 = y$.

Let us consider the lexicographic monomial order with $y > x$. Then $S(f_1, f_2) = x^2$ is reduced with respect to $\{f_1, f_2, f_3\}$.

Set $f_4 = x^2$. It is easy to check that $S(f_1, f_3) \xrightarrow{\{f_1, f_2, f_3, f_4\}} 0$ and $S(f_2, f_3) = x$ is reduced with respect to $\{f_1, f_2, f_3, f_4\}$.

Setting $f_5 = x$ and considering $S(f_i, f_j)$ $(1 \leq i < j \leq 5)$ we obtain that $\{f_1, f_2, f_3, f_4, \}$ is a Gröbner basis of I. Now we can remove f_1, f_2, f_4 and obtain a minimal Gröbner basis $G_1 = \{f_3 = y,\ f_5 = x\}$ of I.

We can also drop f_1, f_3, f_4 and obtain a minimal Gröbner basis $G_2 = \{f_2 = y + x,\ f_5 = x\}$.

(We see that minimal Gröbner bases are not unique.) G_1 is a reduced Gröbner basis of I, and it can be obtained from G_2 by the procedure described in the last Proposition.

Let I be and ideal in $K[x_1, \ldots, x_n]$. Then $V(I)$ will denote the set of all points $(a_1, \ldots, a_n)$ with entries in K such that $f(a_1, \ldots, a_n) = 0$. ($V(I)$ is called a **variety** of the ideal I.)

Furthermore, we set $\sqrt{I} = \{f \in K[x_1, \ldots, x_n] \mid f^k \in I \text{ for some } k \in \mathbb{N}, k > 0\}$. It is easy to show that $\sqrt{I}$ is an ideal of $K[x_1, \ldots, x_n]$; it is called the **radical** of I.

Theorem 5 (Hilbert Nullstellensatz)

If the field K is algebraically closed (say, $K = \mathbb{C}$), then a polynomial $f(x_1, \ldots, x_n)$ vanishes at any point $(a_1, \ldots, a_n) \in V(I)$ (I is an ideal of $K[x_1, \ldots, x_n]$) if and only if $f \in \sqrt{I}$.

Recall that a field K is said to be algebraically closed if every polynomial in one variable with coefficients in K has a root in K. Say, the field of real numbers $\mathbb{R}$ is not algebraically closed, since the polynomial with real coefficients $f(x) = x^2 + 1$ has no root in $\mathbb{R}$.

Even if K is not algebraically closed, the statement of the Hilbert Nullstellensatz if the coordinates of points in $V(I)$ are considered in the algebraic closure of K.

Hilbert Nullstellensatz implies that if a field K is algebraically closed and I an ideal of $K[x_1, \ldots, x_n]$, then $V(I) = \emptyset$ if and only if $I = K[x_1, \ldots, x_n]$, that is, $1 \in I$ ("Weak Nullstellensatz").

Considering an ideal I generated by some polynomials $f_1, \ldots, f_s$ ($f_i = f_1(x_1, \ldots, x_n)$), we see that the system of algebraic equations $f_1 = 0, \ldots, f_s = 0$ has no solutions in K if and only if $1 \in I = \langle f_1, \ldots, f_s \rangle$, that is, the (unique) reduced Gröbner basis G is $\{1\}$.

Hilbert Nullstellensatz also shows that an algebraic equation $f = 0$ is a consequence of a system of algebraic equations $f_1 = 0, \ldots, f_s = 0$ ($f, f_i \in K[x_1, \ldots, x_n]$) if and only if $f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$, that is, $f^k \in \langle f_1, \ldots, f_s \rangle$ for some positive integer k. The following theorem reduces the question of membership in $\sqrt{I}$ (I is an ideal in $K[x_1, \ldots, x_n]$ to a question of membership in an ideal of the ring $K[x_1, \ldots, x_n, y]$ where y is a new variable.

Theorem 6

Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in $K[x_1, \ldots, x_n]$. Then $f \in \sqrt{I}$ if and only if $1 \in \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq K[x_1, \ldots, x_n, y]$

Thus, an algebraic equation $f = 0$ is a consequence of a system of algebraic equations $f_1 = 0, \ldots, f_s = 0$ if and only if $1 \in G$ where G is a reduced Gröbner basis of the ideal $\langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq K[x_1, \ldots, x_n, y]$.

Applications of Gröbner Bases

The Ideal Membership Problem

If we combine Gröbner bases with the division algorithm, we get the following **ideal membership algorithm**: given an ideal $I = \langle f_1, \ldots, f_s \rangle$, we can decide whether a given polynomial f lies in I as follows. First, using a Gröbner basis algorithm, find a Gröbner basis $G = \{g_1, \ldots, g_t\}$ for I. Then use the fact that

$$f \in I \text{ if and only if } f \xrightarrow{G} 0.$$

Example 1. Let $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \in \mathbb{C}[x, y, z]$, and use the grlex order. Let $f = -4x^2y^2z^2 + y^6 + 3z^5$ We want to know if $f \in I$.

The generating set given is not a Gröbner basis of I because $\langle \mathrm{lm}(I) \rangle$ also contains polynomials such as $\mathrm{lm}(S(f_1, f_2)) = \mathrm{lm}(-x^2y^2 + z^3) = -x^2y^2$ that are not in the ideal $\langle \mathrm{lm}(f_1), \mathrm{lm}(f_2) \rangle = \langle xz, x^3 \rangle$. Hence, we begin by computing a Gröbner basis for I. Using a computer algebra system, we find a Gröbner basis

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Note that this is a reduced Gröbner basis.

We may now test polynomials for membership in I. For example, dividing f above by G, we find

$$f = (-4xy^2z - 4y^4) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (-3) \cdot f_5 + 0.$$

Since the remainder is zero, we have $f \in I$.

For another example, consider $f = xy - 5z^2 + x$. Even without completely computing the remainder on division by G, we can see from the form of the elements in G that $f \notin I$. The reason is that $\mathrm{lm}(f) = xy$ is clearly not in the ideal $\langle \mathrm{lm}(G) \rangle = \langle xz, x^3, x^2y^2, xy^4, y^6 \rangle$. Hence, $f \xrightarrow{G} / \rightarrow 0$, so that $f \notin I$.

This last observation illustrates the way the properties of an ideal are revealed by the form of the elements of a Gröbner basis.

Example 2. We will solve the system of equations

$$\begin{aligned} x^2+y+z&=1,\\ x+y^2+z&=1,\\ x+y+z^2&=1. \end{aligned} \tag{1}$$

If we let I be the ideal

$$I=\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle, \tag{2}$$

then a Gröbner basis for I with respect to lex order is given by the four polynomials

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

It follows that equations (1) and (3) have the same solutions. However, since

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2+2z-1)$$

involves only z, we see that the possible z's are 0, 1, and $-1 \pm \sqrt{2}$. Substituting these values into $g_2 = y^2 - y - z^2 + z = 0$ and $g_3 = 2yz^2 + z^4 - z^2 = 0$, we can determine the possible y's, and then finally $g_1 = x + y + z^2 - 1 = 0$ gives the corresponding x's. In this way, one can check that equations (1) have exactly five solutions:

$$(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1),$$
$$(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),$$
$$(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Example 3. Consider the system of polynomial equations obtained by applying Lagrange multipliers to find the minimum and maximum values of $x^3 + 2xyz - z^2$ subject to the constraint $x^2 + y^2 + z^2 = 1$:

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0, \\ 2xz - 2y\lambda &= 0, \\ 2xy - 2z - 2z\lambda &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0. \end{aligned}$$

We begin by computing a Gröbner basis for the ideal in $\mathbb{R}[x, y, z, \lambda]$ generated by the left-hand sides of the four equations, using the lex order with $\lambda > x > y > z$. We find a Gröbner basis:

$$\begin{aligned} &\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ &x^2 + y^2 + z^2 - 1, \\ &xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ &xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ &y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ &y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ &yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ &z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{aligned} \tag{2}$$

We see that the last polynomial depends only on the variable z. We have "eliminated" the other variables in the process of finding the Gröbner basis.

(Miraculously) the equation obtained by setting this polynomial equal to zero has the roots

$$z = 0,\ \pm 1,\ \pm 2/3,\ \pm\sqrt{11}/8\sqrt{2}.$$

If we set z equal to each of these values in turn, the remaining equations can then be solved for y, x (and λ, though its values are essentially irrelevant for our purposes). We obtain the following solutions:

$$\begin{aligned}
&z = 0; \quad y = 0; \quad x = \pm 1,\\
&z = 0; \quad y = \pm 1; \quad x = 0,\\
&z = \pm 1; \quad y = 0; \quad x = 0,\\
&z = 2/3; \quad y = 1/3; \quad x = -2/3,\\
&z = -2/3; \quad y = -1/3; \quad x = -2/3,\\
&z = \sqrt{11}/8\sqrt{2}; \quad y = -3\sqrt{11}/8\sqrt{2}; \quad x = -3/8,\\
&z = -\sqrt{11}/8\sqrt{2}; \quad y = 3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.
\end{aligned}$$

From here, it is easy to determine the minimum and maximum values.

Let us apply the technique of Gröbner bases to solve a well-known problem in graph theory: determining whether a given graph can be 3-colored.

Let us first state the problem precisely. We are given a graph $\mathcal{G}$ with n vertices with at most one edge between any two vertices. We want to color the vertices in such a way that only 3 colors are used, and no two vertices connected by an edge are colored the same way. If $\mathcal{G}$ can be colored in this fashion, then $\mathcal{G}$ is called *3-colorable*. This can be seen to be the same as the 3-color problem for a map: the vertices represent the regions to be colored, and two vertices are connected by an edge if the two corresponding regions are adjacent.

First, we let $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ be a cube root of unity (i.e. $\xi^3 = 1$). We represent the 3-colors by $1, \xi, \xi^2$, the 3 distinct cube roots of unity. Now, we let $x_1, \ldots, x_n$ be variables representing the distinct vertices of the graph $\mathcal{G}$. Each vertex is to be assigned one of the 3 colors $1, \xi, \xi^2$. This can be represented by the following n equations

$$x_i^3 - 1 = 0, \ 1 \leq i \leq n. \tag{1}$$

Also, if the vertices x_i and x_j are connected by an edge, they need to have a different color. Since $x_i^3 = x_j^3$, we have $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Therefore x_i and x_j will have different colors if and only if

$$x_i^2 + x_i x_j + x_j^2 = 0. \tag{2}$$

Let I be the ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by the polynomials in Equation (1) and for each pair of vertices x_i, x_j which are connected by an edge by the polynomials in Equation (2). We will consider the variety $V(I)$ contained in $\mathbb{C}^n$, that is, a solution set of the ideal I.

THEOREM. *The graph $\mathcal{G}$ is 3-colorable if and only if $V(I) \neq \emptyset$.*

We can use Gröbner bases to determine if $V(I) = \emptyset$. We first compute a reduced Gröbner basis for I. If $1 \in G$, then $V(I) = \emptyset$ and otherwise $V(I) \neq \emptyset$ (it follows from Hilbert Nullstellensötz).

EXAMPLE Consider the graph $\mathcal{G}$ of Figure 1.

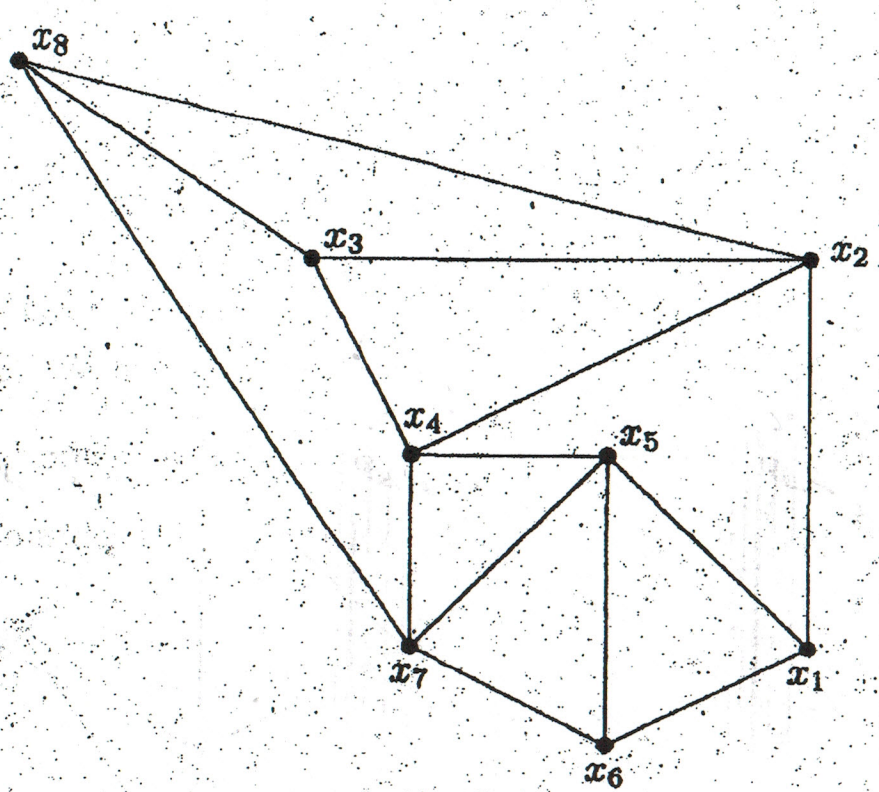


FIGURE 1. The graph $\mathcal{G}$

The polynomials corresponding to $\mathcal{G}$ are:

$$x_i^3 - 1, \text{ for } i = 1, \ldots, 8$$

and

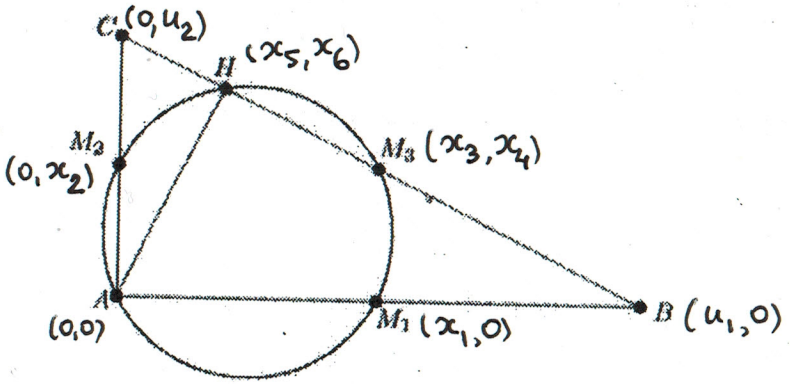
$$x_i^2 + x_i x_j + x_j^2, \text{ for the pairs } (i,j) \in \{(1,2),(1,5),(1,6),(2,3),(2,4),$$
$$(2,8),(3,4),(3,8),(4,5),(4,7),(5,6),(5,7),(6,7),(7,8)\}.$$

We compute a Gröbner basis G for the ideal I corresponding to the above polynomials. Using the lex term ordering with $x_1 > x_2 > \cdots > x_8$, we obtain

$$G = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8,$$
$$x_6 - x_8, x_7^2 + x_7 x_8 + x_8^2, x_8^3 - 1\}.$$

Since $1 \notin G$, we have that $V(I) \neq \emptyset$, and hence, by the Theorem, $\mathcal{G}$ is 3-colorable. We can use the Gröbner basis G to give an explicit coloring, since the system of equations represented by G turns out to be easy to solve. Let us assume that the 3 colors we are using are blue, red, and green. We must first choose a color for x_8, say red, since the only polynomial in one variable in G is $x_8^3 - 1$. We then must choose a different color for x_7, say blue, because of the polynomial $x_7^2 + x_7 x_8 + x_8^2 \in G$. Then we have that x_1 and x_3 must be blue because of the polynomials $x_1 - x_7, x_3 - x_7 \in G$, and x_4, x_6 must be red because of the polynomials $x_4 - x_8$, $x_6 - x_8 \in G$. Finally x_2 and x_5 have the same color, which is a different color from the colors assigned to x_7 and x_8, so x_2 and x_5 are green; this is because the polynomials $x_2 + x_7 + x_8$, and $x_5 + x_7 + x_8$ are in G.

Gröbner bases in geometry theorem proving



Theorem (The Circle Theorem of Appolonius)
Consider a right triangle spanned by A, B, and C, with the right angle at A. The midpoints of the three sides of the triangle, and the foot of the altitude drawn from A to the edge $\vec{BC}$, all lie on one circle.

The coordinates of the triangle are as follows: we place A at $(0,0)$, B at $(u_1,0)$, and C at $(0,u_2)$, where u_1 and u_2 are arbitrary. The three midpoints at the sides M_1, M_2, and M_3 have their coordinates respectively at $(x_1,0)$, $(0,x_2)$, and (x_3,x_4). Expressing that M_1 is the midpoint of the edge spanned by A and B imposes the condition $h_1 = 2x_1 - u_1 = 0$. The second condition $h_2 = 2x_2 - u_2 = 0$ is imposed by stating that M_2 is the midpoint of the edge spanned by A and C. For M_3 we have two conditions: $h_3 = 2x_3 - u_1 = 0$ and $h4 = 2x_4 - u_2 = 0$.

For the foot of the altitude H we choose coordinates (x_5, x_6). Then we formulate two hypotheses. First: $h_5 = x_5u_1 - x_6u_2 = 0$ expresses that the line segment AH is perpendicular to the edge BC. Second: $h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0$ means that the points B, H, and C are collinear. To formulate these conditions we use the slopes defined by the segments.

Finally, we consider the statement that the three midpoints and H lie on a circle by saying that the circle through the three midpoints must also contain H. Let (x_7, x_8) be the coordinates of the center O of the circle. We have two more conditions: $M_1O = M_2O$ and $M_1 = M_3O$, given respectively by $h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0$ and $h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$.

The eight hypothesis form the following system

$$f(\mathbf{u}, \mathbf{x}) = \begin{cases} 2x_1 - u_1 = 0 \\ 2x_2 - u_2 = 0 \\ 2x_3 - u_3 = 0 \\ 2x_4 - u_4 = 0 \\ x_5u_1 - x_6u_2 = 0 \\ x_5u_2 + x_6u_1 - u_1u_2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0 \end{cases}$$

With respect to these eight hypotheses, the conclusion must then be that $HO = M_1O$, expressed by

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

The theorem is true if g belongs to the ideal spanned by the polynomials of the hypotheses.

Thanks!