

APPLICATIONS OF GROEBNER BASES WITH EXAMPLES

Shuchao Bi
February, 2009

ABSTRACT. In this write-up, I present some applications of Groebner bases with examples.

1. COMPUTING HOMOGENIZATION (PROJECTIVE CLOSURE)

For a polynomial $f \in S = k[x_1, \dots, x_n]$ of total degree d , define the homogenization $f^h \in k[x_0, x_1, \dots, x_n]$ of f as

$$f^h(x_0, x_1, \dots, x_n) = x_0^d f(x_1/x_0, \dots, x_n/x_0).$$

Similarly, for an ideal I in S , define the homogenization I^h of I in $k[x_0, x_1, \dots, x_n]$ as $I^h := \langle f^h, f \in I \rangle$. It is easy to show that I^h is a homogeneous ideal.

Note, in general, it is not true that $(f_1, \dots, f_t)^h = (f_1^h, \dots, f_t^h)$. For example, let $I = (x_2 - x_1^2, x_3 - x_1x_2)$ be the ideal of the affine twisted cubic. We claim that $I^h \neq (x_2x_0 - x_1^2, x_3x_0 - x_1x_2)$. To prove this, consider the polynomial

$$x_2(x_2 - x_1^2) - x_1(x_3 - x_1x_2) = x_2^2 - x_1x_3 \in I.$$

This polynomial is already homogeneous, so it lies in I^h . If $x_2^2 - x_1x_3 \in (x_2x_0 - x_1^2, x_3x_0 - x_1x_2)$, $x_2^2 - x_1x_3$ will be a k -linear combination of $x_2x_0 - x_1^2$ and $x_3x_0 - x_1x_2$ which is impossible.

However, if we start with a Groebner basis with respect to a graded monomial order, we will get what we expect.

Proposition. If $\{g_1, \dots, g_t\} \subset k[x_1, \dots, x_n]$ is a Groebner basis with respect to a graded monomial order $>$, then $(g_1, \dots, g_t)^h = (g_1^h, \dots, g_t^h)$.

Proof. Define a monomial order $>_h$ in $k[x_0, x_1, \dots, x_n]$ by $x^a x_0^c >_h x^b x_0^d$ iff $x^a > x^b$ or $x^a = x^b$ and $c > d$, where x^a and x^b just involve x_1, \dots, x_n . It is easy to show this actually defines a monomial order. We will prove $\{g_1^h, \dots, g_t^h\}$ is a Groebner basis for $(g_1, \dots, g_t)^h$ with respect to $>_h$, i.e., $LM_{>_h}(g_1^h), \dots, LM_{>_h}(g_t^h)$ generate $in_{>_h}((g_1, \dots, g_t)^h)$.

For any $F \in (g_1, \dots, g_t)^h$, by definition we can write

$$F = A_1 f_1^h + \dots + A_s f_s^h$$

for some $A_i \in k[x_0, x_1, \dots, x_n]$ and $f_i \in I := (g_1, \dots, g_t)$. Let $f := F(1, x_1, \dots, x_n)$ denote the dehomogenization of F with respect to x_0 , then

$$\begin{aligned} f &= F(1, x_1, \dots, x_n) \\ &= A_1(1, x_1, \dots, x_n) f_1^h(1, x_1, \dots, x_n) + \dots + A_s(1, x_1, \dots, x_n) f_s^h(1, x_1, \dots, x_n) \\ &= A_1(1, x_1, \dots, x_n) f_1 + \dots + A_s(1, x_1, \dots, x_n) f_s. \end{aligned}$$

This shows that $f \in I$, also it is easy to see that

$$F = x_0^e f^h$$

for some $e \geq 0$. Thus,

$$LM_{>_h}(F) = x_0^e LM_{>_h}(f^h) = x_0^e LM_{>}(f),$$

where the last equality is by the lemma below. As $\{g_1, \dots, g_t\}$ is a Groebner basis with respect to the graded monomial order $>$, $LM_{>}(f)$ is divisible by some $LM_{>}(g_i) = LM_{>_h}(g_i^h)$ (using the following lemma again), so $LM_{>_h}(F)$ is divisible by some $LM_{>_h}(g_i^h)$ as required. \square

Lemma. If $>$ is a graded monomial order, then for any $f \in k[x_1, \dots, x_n]$, we have $LM_{>}(f) = LM_{>_h}(f^h)$.

Proof. Since $>$ is a graded order, $LM_{>}(f)$ is one of the monomials appearing in the homogeneous component of f of maximal total degree. When we homogenize, this term is unchanged. If $x^a x_0^e$ is any other monomial appearing in f^h , where x^a only involve x_1, \dots, x_n . We have $LM_{>}(f) > x^a$ by the definition of homogenization. Then by the definition of $>_h$, we have $LM_{>}(f) >_h x^a x_0^e$, so $LM_{>}(f) = LM_{>_h}(f^h)$. *square*

Return to our example, $\{x_2 - x_1^2, x_3 - x_1x_2, x_2^2 - x_1x_3\}$ is a Groebner basis respect to the reverse lexicographic order as one can easily check with Buchberger's criterion. So $(x_2 - x_1^2, x_3 - x_1x_2)^h = (x_2x_0 - x_1^2, x_3x_0 - x_1x_2, x_2^2 - x_1x_3)$.

2. COMPUTING ASSOCIATED GRADED RING (TANGENT CONE)

Let $S = k[x_1, x_2, \dots, x_r]$, ideal $I \subset S$ and $R = S/I$. The associated graded ring of R respect to the ideal $m := (x_1, \dots, x_r) + I \subset R$ is

$$gr_I R := R/m \oplus m/m^2 \oplus m^2/m^3 \oplus \dots$$

Geometrically, the associated graded algebra correspondent to the tangent cone. The associated graded algebra is a graded S -module, and

we can define a surjective graded S -module homomorphism φ from S to $gr_I R$ sending 1 to 1. So

$$gr_I R \cong S/I'$$

for some homogeneous ideal $I' = \ker \varphi$. Also it is easy to see that

$$I' = \{f_{min} : f \in I\}$$

where f_{min} denotes the homogeneous component of lowest degree of f . So to compute the associated graded ring, it suffices to compute the ideal I' . As in the previous section, the only subtlety is that when $I = (f_1, \dots, f_t)$, it is not necessary true that $I' = ((f_1)_{min}, \dots, (f_t)_{min})$. For example, let $I = (xy, xz + z(y^2 - z^2)) \subset k[x, y, z]$, we have $yz(y^2 - z^2) = (yz(y^2 - z^2))_{min} = (y(xz + z(y^2 - z^2)) - z(xy))_{min}$ which is not in $((xy)_{min}, (xz + z(y^2 - z^2))_{min}) = (xy, xz)$. Again this difficulty can be overcome by a suitable choice of Groebner basis.

Proposition. For a ideal $I \subset k[x_1, \dots, x_r]$, let $\{G_1, \dots, G_t\}$ be a Groebner basis of the homogenization $I^h \subset k[x_0, x_1, \dots, x_r]$ of I with respect to a monomial order such that among monomials of the same degree, any monomial involving x_0 is greater than any monomials only involving x_1, \dots, x_r . Then $I' = ((g_1)_{min}, \dots, (g_t)_{min})$, where $g_i = G_i(1, x_1, \dots, x_r)$.

Proof. to be done...

Remark. For a ideal I in a polynomial ring, define $I_{max} = \{f_{max} : f \in I\}$ where f_{max} denotes the homogeneous component of highest degree of f . Then a similar result holds, the only difference is that in this case, we want a monomial order such that among monomials of the same degree, any monomial involving x_0 is less than any monomials only involving x_1, \dots, x_r .

Let's return to the example, $I = (xy, xz + z(y^2 - z^2)) \subset k[x, y, z]$. Use graded lexicographic order with $x > y > z$ in $k[x, y, z]$, a Groebner basis is $\{xy, xz + z(y^2 - z^2), x^2z - xz^3\}$. Then apply the proposition of the previous section, $\{xy, xzw + z(y^2 - z^2), x^2zw - xz^3\}$ is a basis of $I^h \subset k[x, y, z, w]$. Use graded lexicographic order with $w > x > y > z$ in $k[x, y, z, w]$, a Groebner basis is for I_h $\{xy, xzw + z(y^2 - z^2), yz(y^2 - z^2)\}$. By the above proposition, $I' = ((xy)_{min}, (xz + z(y^2 - z^2))_{min}, (yz(y^2 - z^2))_{min}) = (xy, xz, yz(y^2 - z^2))$.

Another Example. The associated graded ring of $k[x, y]/(x^2, xy + y^3)$ with respect to $m := (x, y)$ is $k[x, y]/(x^2, xy, xy^3, y^5)$. Details to be

added.

3. COMPUTING SYZYGIES

Let $R = k[x_1, \dots, x_r]$, $G = \{g_1, \dots, g_t\} \subset R^n$ be a Groebner basis. Fix a monomial order $>$ on R^n , for each (i, j) , the S-polynomial vector

$$S_{ij} := \frac{m_{ij}}{LT(g_i)}g_i - \frac{m_{ij}}{LT(g_j)}g_j,$$

where $m_{ij} = \text{LCM}(LT(g_i), LT(g_j))$ is the least common divisor of $LT(g_i)$ and $LT(g_j)$. Note if $LT(g_i)$ and $LT(g_j)$ involve different basis element in R^n , $\text{LCM}(LT(g_i), LT(g_j))$ hence S_{ij} is 0 by convention. Furthermore, as G being a Groebner basis, the remainder of S_{ij} on division by G is 0, and the division algorithm gives an expression

$$S_{ij} = \sum_{k=1}^t a_{ijk}g_k.$$

Set

$$s_{ij} = \frac{m_{ij}}{LT(g_i)}\epsilon_i - \frac{m_{ij}}{LT(g_j)}\epsilon_j - a_{ij1}\epsilon_1 - \dots - a_{ijt}\epsilon_t.$$

These s_{ij} s are obvious syzygies on G , the amazing fact is that they suffice to generate the whole syzygy module of G .

Theorem (Schreyer). With the notation as above, the s_{ij} form a Groebner basis for the syzygy module $\text{Syz}(G) \subset R^t$ of G with respect to the monomial order $>_G$ on R^t defined as follows:

$$\begin{aligned} x^\alpha \epsilon_i >_G x^\beta \epsilon_j \quad \text{if} \quad LT(x^\alpha g_i) > LT(x^\beta g_j) \\ \text{or} \quad LT(x^\alpha g_i) = LT(x^\beta g_j) \quad \text{and} \quad i < j. \end{aligned}$$

Proof. to be done...

For a set F which is not necessarily a Groebner basis, we have the following proposition.

Proposition. Let $F = (f_1, \dots, f_s)$ be an ordered s -tuple, and let $G = (g_1, \dots, g_t)$ be an order Groebner basis for the submodule generated by F with respect to some monomial order $>$. We have matrices A, B with entries in R such that $G = FA$ and $F = GB$. Let s_{ij} be the basis of $\text{Syz}(G)$ given by the above theorem and S_1, \dots, S_s be the columns of $I_s - AB$. Then

$$\text{Syz}(F) = (As_{ij}, S_1, \dots, S_s).$$

Proof. to be done...

Note when you do this calculation by hand, you can always get a Groebner basis $G = f_1, \dots, f_s, g_1, \dots, g_k$ extend the original basis $F = f_1, \dots, f_s$. In this case, the above proposition just means, to get $\text{Syz}(F)$, we only need to substitute g_i in terms of f_j given by the the syzygies defining g_i into other syzygies. We given two examples below, one by hand and in the other example we calculate the Groebner basis on Computer.

Example 1 (By Hand). $F = (g_1, g_2)$ where $g_1 = x^2$ and $g_2 = xy + y^2$. We will first find a Groebner basis with respect to lex order, taking $x > y$. We have $LT(g_1) = x^2$, $LT(g_2) = xy$, the S -polynomial is

$$S_{12} = yg_1 - xg_2 = -xy^2.$$

Divided by F , we get the remainder y^3 and the syzygy

$$s_{12} = y\epsilon_1 - x\epsilon_2 + y\epsilon_2 - \epsilon_3.$$

Set $g_3 = y^3$, we have

$$S_{13} = y^3g_1 - x^2g_3 = 0,$$

so we get a syzygy $s_{13} = y^3\epsilon_1 - x^2\epsilon_3$.

$$S_{23} = y^2g_2 - xg_3 = y^4,$$

subtract yg_3 , we find a remainder 0 and a syzygy

$$s_{23} = y^2\epsilon_2 - (x + y)\epsilon_3.$$

By Buchberger's criterion, $G = (g_1, g_2, g_3)$ is a Groebner basis, apply Schreyer's theorem, $\text{Syz}(G) = \{s_{12}, s_{13}, s_{23}\}$. To get syzygies on g_1 and g_2 , we solve ϵ_3 in s_{12} , get $\epsilon_3 = y\epsilon_1 - x\epsilon_2 + y\epsilon_2$, plug in s_{13} and s_{23} , we finally get $\text{Syz}(F) =$

$$s'_{13} = (y^3 - x^2y)\epsilon_1 + (x^3 - x^2y)\epsilon_2$$

$$s'_{23} = x^2\epsilon_2 - (xy + y^2)\epsilon_1.$$

Example 2 (On Computer). Let $F = (f_1, f_2)$ where $f_1 = xy + x$ and $f_2 = y^2 + 1$. Using lex order with $x > y$, the reduced Groebner basis consists of $g_1 = x$ and $g_2 = y^2 + 1$ according to Singular. Set $G = (g_1, g_2)$, we have

$$G = F \begin{pmatrix} -(y-1)/2 & 0 \\ x/2 & 1 \end{pmatrix} = FA$$

and

$$F = G \begin{pmatrix} y+1 & 0 \\ 0 & 1 \end{pmatrix} = GB.$$

Also it is easy to check that

$$\text{Syz}(G) = s_{12} = \begin{pmatrix} y^2 + 1 \\ -x \end{pmatrix}.$$

Then by the above proposition,

$$\begin{aligned} \text{Syz}(F) &= \{As_{12}, \text{ columns of } I_2 - AB\} = \\ &= \begin{pmatrix} -(y^3 - y^2 + y - 1)/2 \\ (xy^2 - x)/2 \end{pmatrix}, \begin{pmatrix} (y^2 + 1)/2 \\ -(xy + x)/2 \end{pmatrix}. \end{aligned}$$

4. COMPUTING MINIMAL FREE RESOLUTIONS

Push the idea in the previous section further, we get an algorithm to compute a finite free resolution of a given module over a polynomial ring. The resolution produced in this way may not be minimal, but we can do some linear algebra to make this resolution minimal.

More precisely, let $R = k[x_1, \dots, x_r]$ be a polynomial ring, given a submodule $M \subset R^n$. To find a free resolution of M (or equivalently of R^n/M), we first choose a basis (for example a Groebner basis) m_1, \dots, m_{n_1} for M , then we get an exact sequence

$$R^{n_1} \xrightarrow{\varphi_1} M \longrightarrow 0,$$

where φ_1 maps the i -th standard basis of R^{n_1} to m_i . The next step is to compute a basis for the kernel of φ_1 , i.e. the syzygies of m_i s, this can be done using Schreyer's Theorem, then we get an exact sequence

$$R^{n_2} \xrightarrow{\varphi_2} R^{n_1} \xrightarrow{\varphi_1} M \longrightarrow 0,$$

where φ_2 maps the j -th standard basis of R^{n_2} to the j -th generator of the syzygies of m_i s. Continue in this way, we get a free resolution of M .

The only subtlety is that this algorithm might not terminate, and this can actually happen, however if we choose the basis carefully at each step, this process terminates after finite steps as the following theorem shows. Note, the following theorem also provides a computational proof of Hilbert Syzygy Theorem.

Theorem. Let G be a Groebner basis for a submodule $M \subset R^t$ with respect to an arbitrary monomial order $>$, and arrange the elements of G to form an ordered s -tuple $G = (g_1, \dots, g_s)$ so that whenever $\text{LT}(g_i)$ and $\text{LT}(g_j)$ contain the same standard \mathbb{N} -basis vector e_k and $i < j$, then $\text{LM}(g_i)/e_k >_{\text{lex}} \text{LM}(g_j)/e_k$, where $>_{\text{lex}}$ is the lex order on R with $x_1 > \dots > x_n$. If the variables x_1, \dots, x_m do not appear in the leading terms of G , then x_1, \dots, x_{m+1} do not appear in the leading terms of the $s_{ij} \in \text{Syz}(G)$ with respect to the order $>_G$ used in the Schreyer's Theorem in previous section.

To construct a finite free resolution of M , first a Groebner basis as in the preceding theorem, then x_1 does not appear in the leading terms of the first syzygies s_{ij} . Choose a Groebner basis of the first syzygies satisfying the conditions of the theorem, then x_1, x_2 do not appear in the leading terms of the second syzygies. Continue in this way, after $s \leq r$ steps, the s -th syzygy module is generated by scalar vectors, so it is free. We get a finite free resolution of length $s + 1$.

I computed the following 4 examples myself by hand, which took me 5 hours.

Example 1. Three Non-collinear Points in \mathbb{P}^2 . $I = (xy, yz, zx)$ is the ideal of three points $[1, 0, 0]$, $[0, 1, 0]$, and $[0, 0, 1]$ in \mathbb{P}^2 .

Example 2. Three Collinear Points in \mathbb{P}^2 . $I = (z, xy(x - y))$ is the ideal of three points $[1, 0, 0]$, $[0, 1, 0]$, and $[0, 1, 1]$ in \mathbb{P}^2 .

Example 3. Twisted Cubic. $I = (x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2)$.

Example 4. Five General Points in \mathbb{P}^3 . $I = (x_0^2 - x_2x_3, x_0x_1 - x_3^2, x_0x_2 - x_1^2, x_1x_3 - x_2^2, x_0x_3 - x_1x_2)$ is the ideal of five points $[1, t^2, t^4, t]$ in \mathbb{P}^3 where t is a fifth root of 1.

5. IDEAL MEMBERSHIP

Given a polynomial f and an ideal $I \subset k[x_1, \dots, x_r]$, it is natural to ask whether f lies in I or not. In the one variable case, this problem is easy. Every ideal in $k[x]$ is principal, so suppose $I = (g)$, also $k[x]$ is Euclidean, we can use Euclidean algorithm to find the remainder r of f respect to g . Then $f \in I$ iff $r = 0$.

In the multivariate case, we still have a division algorithm, so the question is is the analogue statement true in the multivariate case. The answer is no, because this division algorithm is not good enough in the sense that the remainder is not unique unless we do this respect to a Groebner basis.

Let's see an example, let $I = (x_2 - x_1^2, x_3 - x_1x_2)$ be the ideal of the affine twisted cubic. Consider the polynomial

$$x_2(x_2 - x_1^2) - x_1(x_3 - x_1x_2) = x_2^2 - x_1x_3 \in I.$$

If we apply division algorithm to $x_2^2 - x_1x_3$ with respect to $x_2 - x_1^2$ and $x_3 - x_1x_2$, the remainder is itself $x_2^2 - x_1x_3$. But is the Groebner basis case, everything works fine.

Proposition. If $G = \{g_1, \dots, g_t\}$ is a Groebner basis (with respect to any monomial order), let $I = (g_1, \dots, g_t)$, then $f \in I$ iff the remainder of f respect to G , denoted by \bar{f}^G , is 0.

Proof. " \implies " If $\bar{f}^G \neq 0$, then because \bar{f}^G equals to f - a $k[x_1, \dots, x_n]$ -combination of g_1, \dots, g_t , \bar{f}^G still lies in I . That implies $LT(\bar{f}^G)$ lies in $in(I)$ which is generated by $LM(g_1), \dots, LM(g_t)$. So $LT(\bar{f}^G)$ is divisible by some $LM(g_i)$, that means we can do the division algorithm further which contradicts to the definition of remainder.

" \impliedby " The remainder is zero means f is a $k[x_1, \dots, x_n]$ -combination of g_1, \dots, g_t , so $f \in I$. \square

6. RADICAL MEMBERSHIP

Over a polynomial ring $k[x_1, \dots, x_r]$, the Hilbert Nullstellensatz says that the vanishing ideal of a varieties $V(I)$ is \sqrt{I} . So it becomes important that given a ideal $I = (f_1, \dots, f_t)$ and a polynomial f , we could determine $f \in \sqrt{I}$ or not. This question is answered by the following proposition.

Proposition. Let $I = (f_1, \dots, f_s) \subset k[x_1, \dots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = (f_1, \dots, f_s, 1 - yf) \subset k[x_1, \dots, x_n, y]$.

Proof. to be done...

Explicitly, the radical membership algorithm goes like this: to determine if $f \in (f_1, \dots, f_t) \subset k[x_1, \dots, x_n]$, we compute a reduced Groebner basis of the ideal $(f_1, \dots, f_t, 1 - yf) \subset k[x_1, \dots, x_n, y]$ with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise, $f \notin \sqrt{I}$.

As an example, consider the ideal $I = (xy^2 + 2y^2, x^4 - 2x^2 + 1)$ in $k[x, y]$, and $f = y - x^2 + 1$ lies in \sqrt{I} . Using lex order on $k[x, y, z]$, one checks that the ideal $\tilde{I} = (xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1)) \subset k[x, y, z]$ has reduced Groebner basis $\{1\}$. It follows that $y - x^2 + 1 \in \sqrt{I}$ by the preceding proposition.

7. IDEAL EQUALITY

For ideals $I = (f_1, \dots, f_s)$, $J = (g_1, \dots, g_t) \subset k[x_1, \dots, x_r]$, it is natural to ask whether $I = J$ or not. Of course, we could use ideal membership algorithm to decide whether each $g_i \in I$ and whether each $f_j \in J$, if this is the case, then $I = J$. However, as a consequence of the uniqueness of reduced Groebner basis, we have a more efficient method to do this. Namely, fix a monomial order, compute a reduced Groebner basis for f_1, \dots, f_s and g_1, \dots, g_t respectively. Then the ideals are equal if and only if the Groebner bases are the same.

Proposition. (Uniqueness of reduced Groebner basis) Let I be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Groebner basis.

Proof. to do...

8. ELIMINATION (PROJECTION)

Let ideal $I = (f_1, \dots, f_s) \subset k[x_1, \dots, x_r]$. We want to compute the elimination ideal

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

In general, we don't have $I_l = (\{f_1, \dots, f_s\} \cap k[x_{l+1}, \dots, x_n])$. For example, let $I = (x + y, x - y)$, then it is easy to see $I = (x, y)$ and $I_1 = (y)$. On the other hand, $\{x + y, x - y\} \cap k[y] = \emptyset$. However, as usual, this is the case when we working with a Groebner basis with respect to the lex order such that $x_1 > \dots > x_r$.

Theorem (The Elimination Theorem). Let $I \subset k[x_1, \dots, x_r]$ be an ideal and let G be a Groebner basis of I with respect to lex order where $x_1 > x_2 > \dots > x_r$. Then, for every $0 \leq l \leq n$, the set $G_l = G \cap k[x_{l+1}, \dots, x_r]$ is a Groebner basis of the l -th elimination ideal I_l with respect to lex order $x_{l+1} > \dots > x_r$ on $k[x_{l+1}, \dots, x_r]$.

Proof. to be done...

Example.

9. POLYNOMIAL IMPLICATION (COMPUTING THE IMAGE OF A REGULAR MAP)

10. RATIONAL IMPLICATION (COMPUTING THE IMAGE OF A RATIONAL MAP)

11. PROJECTIVE ELIMINATION

12. COMPUTING IDEAL INTERSECTION

Compute least common divisor of two polynomials and greatest common divisor of two polynomials

13. COMPUTING IDEAL QUOTIENT

14. COMPUTING SATURATION

15. COMPUTING ENVELOPS OF FAMILY OF CURVES

16. COMPUTING AFFINE CLOSURE

HW2 for tropical geometry.

REFERENCES

- D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms.
- D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry.
- D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Chapter 15.
- G. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra.