Gröbner Bases

Jesse Vogel

1 Introduction

Consider the ring of polynomials $R = k[x_1, \ldots, x_n]$ over some field k. Given polynomials $f_1, \ldots, f_s$ the ideal generated by these polynomials is

$$I = (f_1, \ldots, f_s) = \Big\{ a_1 f_1 + \cdots + a_s f_s : a_i \in R \Big\}.$$

For example, take the ideal $I = (f, g)$ generated by $f = x^2 y$ and $g = xy^2 - z$ in $k[x, y, z]$. One can ask whether or not xz belongs to I. After a bit of puzzling, we see that we can cancel the leading terms of f and g to find that

$$xz = yf - xg.$$

Next, one can ask: does z^2 belong to I? Again the answer is positive, as can be seen from

$$z^2 = y^3 f - (xy^2 + z)g,$$

but it is not clear how to find such an expression. What if we cannot find such a linear combination? What if we have many indeterminates and many polynomials, and doing these computations by hand is infeasible. How do we know *for sure* whether or not a polynomial belongs to I?

> **The Ideal Membership Problem**: Given an ideal $I = (f_1, \ldots, f_s) \subset R$ and a polynomial $f \in R$, does $f \in I$? And if so, find an expression of the form
>
> $$f = a_1 f_1 + \cdots + a_s f_s.$$

2 Monomial orders

The way we will solve this problem is by trying to reduce a polynomial f modulo the generators $f_1, \ldots, f_s$. This is easy to do for polynomials in one variable, using polynomial division: dividing f by g means finding q and r such that

$$f = qg + r \qquad \text{with } \deg(r) < \deg(g).$$

However, for multivariate polynomials this is not so clear. For example, take $f = xy$ and $g = x + y$, then

$$xy = y \cdot (x + y) - y^2, \qquad xy = x \cdot (x + y) - x^2, \qquad xy = 0 \cdot (x + y) + xy,$$

but in no case can we get the degree of the remainder below $\deg(x + y) = 1$. Hence, we need another way to compare polynomials, different from simply comparing their degrees.

Definition 1. A *monomial* in R is any term of the form $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i \in \mathbb{N}$.

Definition 2. A *monomial order* on R is a total order $<$ on the set of monomials, such that

- $X < Y \implies XZ < YZ$ for any monomial Z,
- $1 < X$ for any monomial $X \neq 1$.

Example 3. The *lexicographical order* is the monomial order defined by

$$X^\alpha < X^\beta \iff \begin{cases} \text{the first coordinates } \alpha_i \text{ and } \beta_i \text{ which} \\ \text{are different satisfy } \alpha_i < \beta_i \end{cases}$$

In particular, for $k[x, y]$ this gives $1 < y < y^2 < y^3 < \cdots < x < xy < xy^2 < \cdots < x^2 < \cdots$

Example 4. The *degree lexicographical order* is the monomial order defined by

$$X^\alpha < X^\beta \iff \begin{cases} \deg(X^\alpha) < \deg(X^\beta), \\ \text{with lex order as tiebreaker} \end{cases}$$

In particular, for $k[x, y]$ this gives $1 < y < x < y^2 < xy < x^2 < y^3 < xy^2 < x^2y < x^3 < \cdots$

Example 5. The *degree reverse lexicographical order* is defined as

$$X^\alpha < X^\beta \iff \begin{cases} \deg(X^\alpha) < \deg(X^\beta), \text{ and as tiebreaker:} \\ \text{use reverse lex order, invert the result} \end{cases}$$

In particular, for $k[x, y, z]$ this gives $z^2 < yz < y^2 < xz < xy < x^2$.

Definition 6. Fix a monomial order on $k[x_1, \ldots, x_n]$. Given any non-zero polynomial $f \in k[x_1, \ldots, x_n]$, write

$$f = c_1 X^{\alpha_1} + \cdots c_r X^{\alpha_r}$$

with $c_i \neq 0$ and such that $X^{\alpha_1} > \cdots > X^{\alpha_r}$. Then we define

- $\mathrm{LM}(f) = X^{\alpha_1}$, the *leading monomial* of f,
- $\mathrm{LC}(f) = c_1$, the *leading coefficient* of f,
- $\mathrm{LT}(f) = c_1 X^{\alpha_1}$, the *leading term* of f.

Example 7. Consider the degree lexicographical order. For $f = 2y^3 + x^2 + 7$ we find

$$\mathrm{LM}(f) = y^3, \qquad \mathrm{LC}(f) = 2, \qquad \mathrm{LT}(f) = 2y^3.$$

By default, we will just use degree lexicographical order.

3 Polynomial reduction

Definition 8. Given polynomials $f, g, h \in R$ with $g \neq 0$, we say that f *reduces to* h *modulo* g *in one step*, written

$$f \xrightarrow{g} h$$

if $\mathrm{LM}(g)$ divides a non-zero term X of f and $h = f - \frac{X}{\mathrm{LT}(g)} g$. Note that this subtracts the term X from f and replaces it by terms which are strictly smaller than X.

Example 9.

$$xy \xrightarrow{x+y} -y^2 \qquad \text{(subtracted } y \cdot (x+y)\text{)}$$

$$x^2y + 7y^3 \xrightarrow{y^2+2x} x^2y - 14xy \qquad \text{(subtracted } y \cdot (y^2+2x)\text{)}$$

Definition 10. Given polynomials $f, h \in R$ and a set $G = \{g_1, \ldots, g_s\} \subset R$ of non-zero polynomials, we say that f *reduces to* h *modulo* G, denoted

$$f \xrightarrow{G} h,$$

if there exists a sequence of indices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1}$ such that

$$f \xrightarrow{g_{i_1}} h_1 \xrightarrow{g_{i_2}} h_2 \xrightarrow{g_{i_3}} \cdots \xrightarrow{g_{i_{t-1}}} h_{t-1} \xrightarrow{g_{i_t}} h.$$

Example 11. Let $G = \{g_1, g_2\}$ with $g_1 = xy - y$ and $g_2 = y^2 - x$. Then $xy^2 \xrightarrow{F} x$ since

$$xy^2 \xrightarrow{g_1} y^2 \xrightarrow{g_2} x.$$

Definition 12. A polynomial f is called *reduced w.r.t.* G if it cannot be reduced modulo G. That is, no term of f is divisible by any one of the $\mathrm{LM}(g_i)$.

This allows multivariate division! Given a polynomial f, there are polynomials q_i and r such that

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

such that r is reduced w.r.t. G.

Now we cannot always expect such a decomposition to be unique, but we would like to have a unique remainder. In particular, if $f \in I = (f_1, \ldots, f_s)$ we would like the remainder to be always zero.

The constant polynomial 1 cannot be reduced modulo $F = \{x^2, x^2+1\}$, but it definitely lives in the ideal $(x^2, x^2+1) = (1)$. Hence, these generators are probably not good generators in some sense.

4 Gröbner bases

Definition 13. A set of non-zero polynomials $G = \{g_1, \ldots, g_s\}$ is called a *Gröber basis* for the ideal $I = (g_1, \ldots, g_s)$ if for all non-zero $f \in I$, we have that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$ for some $g_i \in G$.

In other words, G is a Gröbner basis for I if there are no non-zero polynomials in I which are reduced with respect to G. Note that it is not clear from the definition that such bases actually exist or are unique.

Proposition 14. *G is a Gröbner basis if and only if for all $f \in R$ the remainder of reduction of f by G is unique.*

Proof. We only proof the 'only if' part. Let G be a Gröbner basis, and suppose $f \xrightarrow{G} r_1$ and $f \xrightarrow{G} r_2$, with r_1 and r_2 reduced w.r.t. G. Since $f - r_1$ and $f - r_2$ are both in I, so is $r_1 - r_2$. But $r_1 - r_2$ is reduced, so $r_1 - r_2 = 0$. □

5 Buchberger's algorithm

Recall that $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for $I = (g_1, \ldots, g_s)$ if and only if for all $f \in I$, there exists some $g_i \in G$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$. So a difficulty arises with elements $f \in I$ whose leading monomial $\mathrm{LM}(f)$ is not divisible by any $\mathrm{LM}(g_i)$. However, note that we can always write

$$f = \sum_{i=1}^{s} a_i g_i,$$

so the problem occurs when the largest of the $\mathrm{LM}(a_i g_i) = \mathrm{LM}(a_i)\,\mathrm{LM}(g_i)$ cancel. The simplest case of such is the following.

Definition 15. Given non-zero $f, g \in R$, the *S-polynomial* of f and g is

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

where $L = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

Example 16. Let $f = 2xy - y$ and $g = y^2 - x$. Then $L = \mathrm{lcm}(xy, y^2) = y^2 x$ and

$$S(f,g) = \tfrac{1}{2} y f - x g = x^2 - \tfrac{1}{2} y^2.$$

The S-polynomial may also be viewed in another way. Namely, in the division of f by $f_1, \ldots, f_s$, it may happen that some term X appearing in f is divisible by both $\mathrm{LM}(f_i)$ and $\mathrm{LM}(f_j)$ for $i \neq j$, and hence divisible by $L = \mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$. If we reduce f using f_i, we get the polynomial $h_1 = f - \frac{X}{\mathrm{LT}(f_i)} f_i$, and if we reduce using f_j, we get $h_2 = f - \frac{X}{\mathrm{LT}(f_j)} f_j$. The ambiguity lies in

$$h_2 - h_1 = \frac{X}{\mathrm{LT}(f_i)} f_i - \frac{X}{\mathrm{LT}(f_j)} f_j = \frac{X}{L} S(f_i, f_j).$$

Hence, for such ambiguities to disappear, we want these S-polynomials to be in our Gröbner basis!

Theorem 17 (Buchberger)**.** *A set of non-zero polynomials $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for $I = (g_1, \ldots, g_s)$ if and only if for all $i \neq j$,*

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

Proof. Omitted, see [1, Theorem 1.7.4]. □

This theorem gives an algorithm to compute a Gröbner basis. One simply checks if all S-polynomials reduce to zero, and if not, we add the remainder of that S-polynomial to the basis. This way, all S-polynomials will reduce to zero by force.

Algorithm 18 (Buchberger's Algorithm)**.**

> **Input**: a set $F = \{f_1, \ldots, f_s\}$ of non-zero polynomials.
> **Output**: a Gröbner basis G for the ideal $I = (f_1, \ldots, f_s)$.

(1) Start with $G := F$. Let $A = \{(f_i, f_j) : i < j\}$ be the set of all pairs whose S-polynomial needs to be checked.

(2) As long as $A \neq \varnothing$, take a pair (f, g) out of A, and compute the S-polynomial $S(f, g)$.

(3) If the reduction $S(f, g) \xrightarrow{G} r$ is non-zero, then add r to G, and also add the pairs (g, r) to A for all $g \in G$.

Remark 19. To see why this algorithm terminates, look at the *initial ideal* of the set G, which is generated by the leading monomials of the elements of G,

$$\mathrm{in}(G) = (\mathrm{LM}(g) : g \in G).$$

This ideal strictly grows as more elements are added to G, but this process must stop because R is noetherian.

Example 20. Let I be the ideal generated by $f_1 = xy - y$ and $f_2 = y^2 - x$. We want to use the algorithm to compute a Gröbner basis for $I = (f_1, f_2)$. As in an earlier example, we computed

$$S(f_1, f_2) = x^2 - y^2 \xrightarrow{f_2} x^2 - x =: f_3.$$

Then we compute

$$S(f_1, f_3) = 0$$

and

$$S(f_2, f_3) = -x^3 + xy^2 \xrightarrow{f_3} xy^2 - x \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0.$$

So $\{f_1, f_2, f_3\}$ is a Gröbner basis for I.

6 Uniqueness of Gröbner bases

Definition 21. A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is *minimal* if $\mathrm{LC}(g_i) = 1$ for all i, and $\mathrm{LM}(g_i)$ does not divide $\mathrm{LM}(g_j)$ for $i \neq j$.

To obtain a minimal Gröbner basis from a Gröbner basis, simply make each g_i monic, and remove all g_i whose $\mathrm{LM}(g_i)$ are divisible by some other $\mathrm{LM}(g_j)$.

Lemma 22. *If $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for I, and $\mathrm{LM}(g_2)$ divides $\mathrm{LM}(g_1)$, then $\{g_2, \ldots, g_s\}$ is a Gröbner basis for I as well.*

Proof. Clearly, if for a polynomial $f \in I$ the leading monomial $\mathrm{LM}(f)$ is divisible by $\mathrm{LM}(g_1)$, then it is divisible by $\mathrm{LM}(g_2)$ as well, so we can omit g_1. □

Still, minimal Gröbner bases are not unique, but we are getting closer.

Proposition 23. *If $G = \{g_1, \ldots, g_s\}$ and $H = \{h_1, \ldots, h_t\}$ are minimal Gröbner bases for I, then $s = t$ and after renumbering if necessary, $\mathrm{LM}(g_i) = \mathrm{LM}(h_i)$.*

Proof. Since g_1 is in I, and H is a Gröbner basis, $\mathrm{LM}(h_i)$ divides $\mathrm{LM}(g_1)$ for some i. After renumbering if necessary, we can assume $i = 1$. Now since G is a Gröbner basis, $\mathrm{LM}(g_j)$ divides $\mathrm{LM}(h_1)$ for some j. Hence $\mathrm{LM}(g_j) | \mathrm{LM}(g_1)$ and thus $j = 1$ as G is minimal, and hence $\mathrm{LM}(g_1) = \mathrm{LM}(h_1)$. Similarly for g_2, some $\mathrm{LM}(h_i)$ divides $\mathrm{LM}(g_2)$, and we cannot have $i = 1$ since $\mathrm{LM}(h_1) = \mathrm{LM}(g_1)$, so we can assume $i = 2$. Then $\mathrm{LM}(g_j)$ divides $\mathrm{LM}(h_2)$, which must be $j = 2$, so $\mathrm{LM}(g_2) = \mathrm{LM}(h_2)$. Continue inductively. □

Definition 24. A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is called *reduced* if it is minimal, and moreover each $g_i \in G$ is reduced w.r.t. $G \setminus \{g_i\}$.

To construct a reduced Gröbner basis from a minimal Gröbner basis, simply replace each g_i with its reduction w.r.t. the other g_j.

Theorem 25 (Buchberger)**.** *Fix a monomial order. Then every non-zero ideal I has a unique reduced Gröbner basis.*

Proof. If G and H are both reduced Gröbner bases, we have already seen that $\mathrm{LM}(g_i) = \mathrm{LM}(h_i)$ for all i, possibly after renumbering. If $g_i \neq h_i$ for some i, then $g_i - h_i \in I$ implies that $\mathrm{LM}(h_j)$ divides $\mathrm{LM}(g_i - h_i)$ for some j. We must have $j \neq i$ as $\mathrm{LM}(g_i - h_i) < \mathrm{LM}(h_i)$. But then $\mathrm{LM}(h_j) = \mathrm{LM}(g_j)$ divides a term of g_i or h_i, which contradicts the fact that G and H are reduced. Hence $g_i = h_i$. □

7 Applications

Ideal membership. Let $I = (f_1, \ldots, f_s)$ be an ideal in R, and suppose we want to determine whether some $f \in R$ is contained in I. This can be done by computing a Gröbner basis for I, and checking if $f \xrightarrow{G} 0$. By keeping track of which linear combinations of f_i make up the g_i, one can recover an expression $f = a_1 f_1 + \cdots + a_s f_s$ whenever $f \in I$.

Ideal equality. One can check whether two ideals $I, J \subset R$ are equal, by checking whether they have the same reduced Gröbner basis.

Coset representatives. Given an ideal $I \subset R$, one can define canonical representatives for any $f \in R/I$. To do so, let G be a Gröbner basis for I, and define the *normal form* of $f \in R$ to be the reduction $N_G(f)$ of f w.r.t. G. Then $f \equiv g \mod I$ if and only if $N_G(f) = N_G(g)$ by Proposition 14.

Moreover, this gives a canonical basis for the k-vector space R/I. Namely, one can take

$$\big\{\text{monomials } X^\alpha \text{ not divisible by any } \mathrm{LM}(g_i)\big\}.$$

Computing inverses in quotient. Using the above basis for R/I, we can easily write down a multiplication table w.r.t. the basis. Then computing inverses in R/I is simply a matter of linear algebra. Note that this does require the k-basis to be finite!

Radical membership. Let $I = (f_1, \ldots, f_s) \subset R$ be an ideal, and suppose we want to determine whether $f \in \sqrt{I}$. We claim it is equivalent to check whether $1 \in \tilde{I}$ for the ideal $\tilde{I} =$

$(f_1, \ldots, f_s, 1 - wf) \subset k[x_1, \ldots, x_n, w]$, which can be done using a Gröbner basis for $\tilde{I}$. Indeed, by Hilbert's nullstellensatz, we have that

$$\begin{aligned} f \in \sqrt{I} &\iff f \text{ vanishes whenever } f_1, \ldots, f_s \text{ vanish} \\ &\iff f_1 = \ldots = f_s = 1 - wf = 0 \text{ has no solution (over an algebraic closure } \overline{k}) \\ &\iff 1 \in (f_1, \ldots, f_s, 1 - wf) = \tilde{I}. \end{aligned}$$

In particular, we can also determine whether two ideals I and J have the same radical. Namely, $\sqrt{I} = \sqrt{J}$ if and only if $I \subset \sqrt{J}$ and $J \subset \sqrt{I}$. However, actually computing the radical is not so easy.

Solvability of equations. Suppose k is algebraically closed. Then a system of equations $f_1, \ldots, f_s \in R$ has a solution if and only if $I = (f_1, \ldots, f_s)$ does not contain 1.

Furthermore, we have finitely many solutions if and only if the ideal is *zero-dimensional* if and only if for each i there is an $m \in \mathbb{N}$ such that $(x_i)^m \in \mathrm{LM}(G)$.

Computing kernels and images. Let $\phi : k[y_1, \ldots, y_m] \to k[x_1, \ldots, x_n]$ be a ring morphism. Such a map is uniquely determined by the images $f_i = \phi(y_i)$. To compute the kernel $\ker \phi$, we use the following theorem.

Theorem 26 ([1, Theorem 2.4.2])**.** *Let* $K = (y_1 - f_1, \ldots, y_m - f_m) \subset k[y_1, \ldots, y_m, x_1, \ldots, x_n]$. *Then* $\ker \phi = K \cap k[y_1, \ldots, y_m]$.

Now compute a Gröbner basis G for K with respect to a monomial order of $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ for which the x_i are greater than the y_i. Then the polynomials in G which are independent of the x_i form Gröbner basis for $\ker \phi$.

In order to determine whether some $f \in k[x_1, \ldots, x_n]$ lies in the image of ϕ, we use the following theorem.

Theorem 27 ([1, Theorem 2.4.4])**.** *Let* $K = (y_1 - f_1, \ldots, y_m - f_m) \subset k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ *with reduced Gröbner basis* G, *w.r.t. the above-mentioned monomial order. Then* $f \in k[x_1, \ldots, x_n]$ *lies in the image of* ϕ *if and only if* $f \xrightarrow{G} h$ *for some* $h \in k[y_1, \ldots, y_m]$. *Moreover, if this is the case,* $f = \phi(h)$.

8 Gröbner bases for modules

Consider the free R-module R^m with the natural basis $e_1, \ldots, e_m$.

Definition 28. A *monomial* in R^m is any term of the form Xe_i, for some $1 \leq i \leq m$ and monomial X in R. We say that Xe_i *divides* Ye_j if $i = j$ and X divides Y, in which case we write $Xe_i/Ye_j = X/Y$.

Definition 29. A *monomial order* on R^m is a total order $<$ on the monomials of R^m such that

- $Xe_i < ZXe_i$ for all monomials Xe_i of R^m and monomials $Z \neq 1$ of R,

- if $Xe_i < Ye_j$, then $ZXe_i < ZYe_j$ for all monomials Z of R.

Example 30. Given a monomial order on R, there are two natural monomial orders on R^m. The monomial order *TOP* (*term over position*) is given by

$$Xe_i < Ye_j \iff \begin{cases} X < Y \text{ or} \\ X = Y \text{ and } i < j, \end{cases}$$

and the monomial order *POT* (*position over term*) is given by

$$Xe_i < Ye_j \iff \begin{cases} i < j \text{ or} \\ i = j \text{ and } X < Y. \end{cases}$$

Now, given a monomial order on R^m, the theory previous sections carries over very naturally.

- One can define LM, LC and LT analogous to Definition 6.
- One can define notions of reduction $f \xrightarrow{g} h$ and $f \xrightarrow{F} h$ for $f, g, h \in R^m$ and $F \subset R^m$, analogous to Definition 8 and Definition 10.
- One can define the notion of a (minimal/reduced) Gröbner basis for submodules $M \subset R^m$.
- One can define the least common multiple of monomials of R^m as

$$\operatorname{lcm}(Xe_i, Ye_j) = \begin{cases} \operatorname{lcm}(X, Y) & \text{if } i = j, \\ 0 & \text{else.} \end{cases}$$

- One can define the S-polynomial of two non-zero $f, g \in R^m$ as

$$S(f, g) = \frac{L}{\operatorname{LT}(f)} f - \frac{L}{\operatorname{LT}(g)} g \quad \text{with} \quad L = \operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g)).$$

- One has an analogue of Buchberger's algorithm for submodules $M \subset R^m$.
- Similarly, every non-zero submodule $M \subset R^m$ has a unique reduced Gröbner basis.

9 Syzygy modules

Let $\phi : R^s \to R^m$ be an R-module morphism. Note that the map ϕ is completely determined by the images $f_i = \phi(e_i) \in R^m$ of the basis vectors for $1 \leq i \leq s$.

Definition 31. A *syzygy* of ϕ is a vector $(r_1, \ldots, r_s) \in R^s$ such that

$$r_1 f_1 + \cdots r_s f_s = 0,$$

that is, an element of the kernel of ϕ. The submodule $\operatorname{Syz}(\phi) = \ker(\phi) \subset R^s$ of all syzygies of ϕ is called the *syzygy module* of ϕ.

Now suppose that $G = \{f_1, \ldots, f_s\}$ is a Gröbner basis for the image of ϕ. Observe that the S-polynomials $S(f_i, f_j)$ yields syzygies of ϕ. Namely, as $S(f_i, f_j) \xrightarrow{G} 0$, we can write

$$S(f_i, f_j) = \frac{L}{\mathrm{LT}(f_i)} f_i - \frac{L}{\mathrm{LT}(f_j)} f_j = \sum_{\ell=1}^{s} a_\ell g_\ell \quad (\text{with } L = \mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j)))$$

for some $a_\ell \in R$. This gives the syzygy

$$\left(a_1, a_2, \ldots, a_{i-1}, a_i - \frac{L}{\mathrm{LT}(f_i)}, a_{i+1}, \ldots, a_{j-1}, a_j + \frac{L}{\mathrm{LT}(f_j)}, a_{j+1}, \ldots, a_s\right) \in \mathrm{Syz}(\phi).$$

In fact, we have $a_i = a_j = 0$ since $\mathrm{LT}(S(f_i, f_j))$ must be smaller than both $\mathrm{LT}(f_i)$ and $\mathrm{LT}(f_j)$.

The following theorem states that the syzygies of ϕ obtained this way generate all of syzygies of ϕ.

Theorem 32 (Schreyer's Theorem [2, Theorem 15.10])**.** *Suppose that $G = \{f_1, \ldots, f_s\}$ forms a Gröbner basis for the image of ϕ, then*

$$\left\{\frac{L}{\mathrm{LT}(f_i)} e_i - \frac{L}{\mathrm{LT}(f_j)} e_j : 1 \le i < j \le s\right\} \quad (\text{with } L = \mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j)))$$

generates the syzygy module $\mathrm{Syz}(\phi)$*. Moreover, this set forms a Gröbner basis of* $\mathrm{Syz}(\phi)$ *with respect to the monomial order on R^s given by*

$$Xe_i < Ye_j \iff \begin{cases} \mathrm{LM}(Xf_i) < \mathrm{LM}(Yf_j) \text{ or} \\ \mathrm{LM}(Xf_i) = \mathrm{LM}(Yf_j) \text{ and } i < j. \end{cases}$$

Remark 33. Note that Schreyer's theorem directly gives an algorithm to compute a free resolutions for a given finitely generated R-module M.

$$\cdots \to R^{\oplus m_i} \xrightarrow{\varphi_i} R^{\oplus m_{i-1}} \xrightarrow{\varphi_{i-1}} \cdots \xrightarrow{\varphi_2} R^{\oplus m_1} \xrightarrow{\varphi_1} R^{\oplus m_0} \xrightarrow{\varphi_0} M \to 0$$

Indeed, let $\varphi_0 : R^{\oplus m_0} \to M$ be a surjection such that the $\varphi_0(e_i)$ form a Gröbner basis for M. Then a generating set for $\ker(\varphi_0)$ is given by Schreyer's theorem. Applying Buchberger's algorithm gives a Gröbner basis for $\ker(\varphi_0)$, which determines $\varphi_1 : R^{\oplus m_1} \to R^{\oplus m_0}$. This process can be continued inductively, and by Hilbert's syzygy theorem, this process must terminate.

Remark 34. The algorithm presented in the above remark to construct free resolutions of R-modules M is good, but not super efficient. For a more efficient approach, look into Schreyer resolutions.

References

[1] W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* American Mathematical Soc., 1994.

[2] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1995.