Computational Algebra

7. First applications of Gröbner bases

Gröbner bases allow us to solve several problems:

(i) given $f \in k[x_1, \dots, x_n]$, determine whether $f \in I$, where I is an ideal given by a finite set of generators; if $f \in I$ and $I = (f_1, \dots, f_r)$, find $h_1, \dots, h_r$ such that $f = h_1 f_1 + \dots + h_r f_r$.

(ii) determine whether two ideals $I, J \subseteq k[x_1, \dots, x_n]$ are equal

(iii) find "nice" representatives for elements in $k[x_1, \dots, x_n]/I$

(iv) find a k-vector basis for $k[x_1, \dots, x_n]/I$

(v) determine the multiplication table of $k[x_1, \dots, x_n]/I$

(vi) find inverses in $k[x_1, \dots, x_n]/I$ when they exist.

In fact, determining whether a polynomial f belongs to an ideal I can be done by computing a Gröbner basis for I and then reducing f w.r.t. this Gröbner basis: the polynomial belongs to the ideal if and only if the remainder is zero. Moreover, by adapting the multivariate division and Buchberger's algorithm, we can keep track of reductions so that, if we start from a system of generators $(f_1, \dots, f_r)$ for I,

and we compute a Gröbner basis $G = \{g_1, \dots g_s\}$, then we can also output matrices A and B with polynomial entries such that

$$\begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix} = A \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}$$

In this way, whenever $f \in I$, i.e., $f \xrightarrow{G} 0$, we can keep track of the reductions to express f as a linear combination with polynomial coefficients of $g_1, \dots g_s$ and then use the matrix B to obtain f as a combination of $f_1, \dots f_r$. This solves task (i)

Determining whether two polynomial ideals are equal can be reduced to computing their reduced Gröbner bases with respect to the same term order and then checking if they are the same as a set. This solves task (ii)

Tasks (iii), (iv), and (v) are solved once we remember that the remainder of a polynomial with respect to a Gröbner basis is reduced and unique, and that a k-basis for the quotient by an ideal is given by all the terms that are reduced with respect to the Gröbner basis.

Computing whether a class $[f]$ in $k[x_1, \dots, x_n]/I$ (and $f \in k[x_1 \dots x_n]$) is invertible and finding its inverse can be done as follows: invertibility of $[f]$ is equivalent to $I + (f) = (1)$, hence one can check whether the reduced Gröbner basis of $I + (f)$ is $\{1\}$; if this is the case, then one can effectively write

$$1 = f_1 g_1 + \dots + f_r g_r + fg$$

with $I = (f_1, \dots f_r)$, and then $[g]$ is the inverse of $[f]$ in the quotient $k[x_1, \dots, x_r]/I$.

The next set of applications will come once we see how Gröbner bases can solve the problem of <u>elimination</u> of <u>variables</u>. This means the following: we are given an ideal I in a polynomial ring with two sets of variables, namely $I \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$, and we want to compute

$$I \cap k[y_1, \dots y_m]$$

namely, we want to eliminate the variables $x_1, \dots, x_n$.

<u>Def</u>: Suppose we are given a term order $\leq_x$ on $k[x_1, \dots, x_n]$ and a term order $\leq_y$ on $k[y_1, \dots, y_m]$; we then define the following order relation on the terms of $k[y_1, \dots y_m, x_1, \dots, x_n]$: if X_1, X_2 are terms in the x-coordinates and Y_1, Y_2 are terms in the y-coor-

dinates, then we say:

$$X_1 Y_1 \preccurlyeq X_2 Y_2 \quad \text{if and only if}$$

$$X_1 \prec_x X_2 \quad \text{or} \quad \left(X_1 = X_2 \text{ and } Y_1 \preccurlyeq_y Y_2 \right)$$

and we say that this is an elimination order with the x-variables larger than the y-variables.

Lemma: the elimination order is a term order.

Lemma: if $Y \in \mathbb{T}(y_1, \dots, y_m)$ is a term only in the y-variables and $Z \in \mathbb{T}(y_1, \dots y_m, x_1, \dots x_n)$ is a term in the x and y-variables where one of the x-variables appears with positive power, then $Y \prec Z$ in the elimination order defined above.

Proof: if we write Y and Z in the form

$$Y = X_1 Y_1, \quad Z = X_2 Y_2, \quad X_i \in \mathbb{T}(x_1, \dots, x_n), \quad Y_i \in \mathbb{T}(y_1, \dots, y_m)$$

then we see that $X_1 = 1$, while X_2 is a term which is different from 1 by construction; therefore we have $X_1 \prec X_2$, and so by definition $Y \prec Z$

The main result in elimination theory with Gröbner bases is the following:

Theorem: let $I \subset k[y_1, \dots, y_m, x_1, \dots, x_n]$ be a non-zero ideal, let $\preccurlyeq$ be an elimination term order with the x-variables larger than the y-

variables; let G be a Gröbner basis for I with respect to $<$;

then $G \cap k[y_1, \dots, y_m]$ is a Gröbner basis for $I \cap k[y_1, \dots, y_m]$.

Proof: we have that $G \cap k[y_1, \dots, y_m] \subseteq I \cap k[y_1, \dots, y_m]$; let us consider a polynomial $f \in I \cap k[y_1, \dots, y_m]$, with $f \neq 0$; since G is a Gröbner basis for I, then there exists $g \in G$ such that $LT_<(g)$ divides $LT_<(f)$; since $LT_<(f)$ is only in the y-variables, the same must happen for $LT_<(g)$; because of the previous lemma, then, no monomial in g may have positive powers of the x-coordinates, so $g \in k[y_1, \dots, y_m]$; hence $g \in G \cap k[y_1, \dots, y_m]$ and this shows that $G \cap k[y_1, \dots, y_m]$ is a Gröbner basis for $I \cap k[y_1, \dots, y_m]$.

Def, an ideal of the form $I \cap k[y_1, \dots, y_m]$ for $I \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$ is called an <u>elimination ideal</u>.

With this tool at hand, we can compute intersections of ideals, kernels of polynomial maps and whether polynomials are in the image of a polynomial map. Let us begin with intersections.

Prop, let $I, J \subseteq k[x_1, \dots, x_n]$ be ideals, let w be a new variable and let $K := w \cdot I + (1-w) J \subseteq k[x_1, \dots, x_n, w]$; then

$$I \cap J = K \cap k[x_1, \dots, x_n]$$

Proof: if $f \in I \cap J$, then $f = wf + (1-w)f \in K \cap k[x_1, \dots, x_n]$; let

now $f \in K$, namely there exist $g_1, \dots g_s \in I$, $h_1, \dots h_r \in J$ and $\lambda_1, \dots \lambda_s, \mu_1, \dots \mu_r \in k[x_1, \dots x_n, \omega]$ such that

$$f = \omega \sum_{i=1}^{s} \lambda_i g_i + (1-\omega) \sum_{j=1}^{r} \mu_j h_j$$

now, since we want to show the statement, let us suppose that $f \in K \cap k[x_1, \dots x_n]$; then by setting $\omega = 0$ or $\omega = 1$ in the previous expression we obtain $f \in I$ and $f \in J$, respectively.

Hence elimination gives us a way to compute intersections of ideals.

The next situation we want to deal with is the one of polynomial maps. Namely, we suppose we are given a k-algebra homomorphism

$$\varphi : k[y_1, \dots, y_m] \longrightarrow k[x_1, \dots, x_n]$$

i.e. a ring homomorphism which is also a k-vector space homomorphism, so in particular $\varphi|_k = id_k$. By the universal property of the ring of polynomials, the map φ is uniquely identified once we fix the images $f_i := \varphi(y_i)$ of the variables of the domain. We want:

(i) a Gröbner basis for $\ker \varphi$

(ii) an algorithm that decides whether a polynomial is in the image of φ

(iii) an algorithm that decides whether φ is surjective.

Lemma: let R be a commutative ring, let $a_1, \dots, a_n, b_1, \dots, b_n \in R$; then $a_1 \cdots a_n - b_1 \cdots b_n \in (a_1 - b_1, \dots, a_n - b_n)$.

Proof: the statement follows by induction on n; for $n=1$, it is immediately true; now, suppose that the statement holds for $n-1$, and write

$$a_1 \cdot \ldots \cdot a_n - b_1 \cdot \ldots \cdot b_n = a_1 \left(a_2 \cdot \ldots \cdot a_n - b_2 \cdots b_n \right) + b_2 \cdots b_n \left(a_1 - b_1 \right)$$

Theorem: let $\varphi : k[y_1, \ldots, y_m] \longrightarrow k[x_1, \ldots, x_n]$ be a k-algebra homomorphism; for all $i \in \{1, \ldots, m\}$, let $f_i := \varphi(y_i)$; set

$$K := (y_1 - f_1, \ldots, y_m - f_m) \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$$

then we have

$$\ker \varphi = K \cap k[y_1, \ldots, y_m]$$

Proof: "$\supseteq$" let $g \in K \cap k[y_1, \ldots, y_m]$, we have to show that $\varphi(g) = 0$

by assumption we know that

$$g = \sum_{i=1}^{m} (y_i - f_i) h_i$$

where $h_i \in k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ for all i; now, $\varphi(g)$ is $g(f_1, \ldots, f_m)$, which is hence zero.

"$\subseteq$" suppose that $g \in \ker \varphi$; then $g(f_1, \ldots, f_m) = 0$; if we write

$$g = \sum_{\alpha \in \mathbb{N}^m} c_\alpha \, y_1^{\alpha_1} \cdots y_m^{\alpha_m}$$

then

$$g = g - g(f_1, \ldots, f_m) = \sum_{\alpha \in \mathbb{N}^m} c_\alpha \left(y_1^{\alpha_1} \cdots y_m^{\alpha_m} - f_1^{\alpha_1} \cdots f_m^{\alpha_m} \right)$$

and by the previous lemma, the latter belongs to K.

Recall that, given a polynomial f and a Gröbner basis G of an ideal, we denote by $N_G(f)$ the normal remainder of f with respect to G, namely the unique element h such that $f \xrightarrow{G} h$ and h is reduced with respect to G.

Exercise: let $f, g \in k[x_1, \dots, x_n]$ and let $I \subseteq k[x_1, \dots, x_n]$ be an ideal; let G be a Gröbner basis for I; then $f \equiv g \mod I$ if and only if $N_G(f) = N_G(g)$.

Theorem: let $\varphi : k[y_1, \dots, y_m] \longrightarrow k[x_1, \dots, x_n]$ be a homomorphism of k-algebras with $\varphi(y_i) = f_i \ \forall i \in \{1, \dots, m\}$; let

$$K := (y_1 - f_1, \dots, y_m - f_m) \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$$

let G be a Gröbner basis of K with respect to an elimination order where the x are larger than the y; let $f \in k[x_1, \dots, x_n]$; then f is in the image of φ if and only if there exists $h \in k[y_1, \dots, y_m]$ such that $f \xrightarrow{G} h$; in this case we have

$$f = \varphi(h) = h(f_1, \dots, f_m)$$

Proof: "$\Leftarrow$" suppose that $f \in \mathrm{im}(\varphi)$, then $f = g(f_1, \dots, f_m)$ for some $g \in k[y_1, \dots, y_m]$; we consider $f - g \in k[y_1, \dots, y_m, x_1, \dots, x_n]$ as we argued before we have that $f - g \in K$, hence by the previous exercise $N_G(f) = N_G(g)$, which means that

$f \xrightarrow{G} N_G(f) = N_G(g)$ and $g \xrightarrow{G} N_G(f) = N_G(g)$

let $h := N_G(f) = N_G(g)$; since $g \in k[y_1, \dots y_m]$, the polynomial g can only be reduced by elements in G that have all terms in the y-coordinates; hence $h \in k[y_1, \dots, y_m]$; moreover, since $K = \ker \varphi$, we have $g = h + u$ with $u \in K$, and $f = \varphi(g)$ so $f = \varphi(h + u) = \varphi(h)$

"$\Rightarrow$" suppose that $f \xrightarrow{G} h$ with $h \in k[y_1, \dots, y_m]$, then $f - h \in K$, so we can write

$$f - h = \sum_{i=1}^{m} g_i (y_i - f_i)$$

hence we see that $f - h(y_1, \dots, y_m) = 0$, so $f = \varphi(h)$.

Corollary: with the same notation, $f \in \text{im}(\varphi)$ if and only if $N_G(f) \in k[y_1, \dots y_m]$.

Corollary: with the same notation, and supposing furthermore that G is the reduced Gröbner basis of K, then φ is surjective if and only if for each $i \in \{1, \dots n\}$ there exists $g_i \in G$ such that $g_i = x_i - h_i$ for $h_i \in k[y_1, \dots y_m]$; in this case $x_i = h_i(f_1, \dots, f_m)$

Proof: "$\Rightarrow$" let us suppose that φ is surjective, then by the previous theorem $x_1 \xrightarrow{G} h_1'$ (let us suppose that $x_1 \leq x_2 \leq \dots \leq x_n$, otherwise, we re-label the variables) with $h_1' \in k[y_1, \dots y_m]$; this means that $x_1 - h_1' \in K$, so there exists $g_1 \in G$ such that

$$LT_{\leq}(g_1) \text{ divides } LT_{\leq}(x_1 - h_1') = x_1$$

this forces $g_1 = x_1 - h_1$ with $h_1 \in k[y_1, \dots, y_m]$; now we can do the same with x_2, obtaining $h_2' \in k[y_1, \dots y_m]$ and $g_2 \in G$ such that $LT_{\leq}(g_2)$ divides $LT_{\leq}(x_2 - h_2') = x_2$, so $g_2 = x_2 - h_2$, where h_2 is a polynomial in x_1 and $y_1, \dots y_m$; however, since $LT_{\leq}(g_1) = x_1$ and G is a reduced Gröbner basis, then h_2 can only be in $y_1, \dots y_m$! now we repeat the same argument

"$\Leftarrow$" Suppose now that $x_i - h_i \in G$ for all $i \in \{1, \dots, n\}$ with $h_i \in k[y_1, \dots y_m]$; then $x_i \xrightarrow{G} h_i$ and since h_i is only in the y-variables, then $x_i = \varphi(h_i)$, which means that φ is surjective.

By setting up the constructions properly, one can adapt the results above in order to solve the analogous problems for homomorphisms of k-algebras of finite type:

$$\varphi : k[y_1, \dots y_m]/J \longrightarrow k[x_1, \dots x_n]/I.$$