Computational Algebra

6. Minimal and reduced Gröbner bases

Def: a Gröbner basis $G = \{g_1, \dots, g_s\}$ is called minimal if

i. $LC_\leq(g_i) = 1 \quad \forall i$

ii. for all $i \neq j$, $LT_\leq(g_i)$ does not divide $LT_\leq(g_j)$

Lemma: if $G = \{g_1, \dots, g_s\}$ is a Gröbner basis and $LT_\leq(g_i)$ divides $LT_\leq(g_j)$, then $\hat{G} := \{g_1, \dots, \hat{g}_j, \dots, g_s\}$ is also a Gröbner basis

Proof: this follows from the definition of Gröbner basis.

Prop: let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis; perform the following:

- remove every g_j such that there exists g_i with $LT_\leq(g_i)$ dividing $LT_\leq(g_j)$
- divide each remaining polynomial in G by its leading coefficient

Proof: by the previous lemma the first operation preserves the property of being a Gröbner basis of the same ideal; then the result follows from the definition of minimal Gröbner basis.

Prop: if $G = \{g_1, \dots, g_s\}$ and $F = \{f_1, \dots, f_r\}$ are minimal Gröbner bases of the same ideal and with respect the same term order, then

$s = r$ and after a possible relabelling, $LT_{\leq}(f_i) = LT(g_i)$ $\forall i$

Proof: since $f_1 \in I$, where $I = (f_1, \ldots, f_r) = (g_1, \ldots, g_s)$, then there exists $i \in \{1, \ldots, s\}$ such that $LT_{\leq}(g_i)$ divides $LT_{\leq}(f_1)$; after a possible relabelling, we may assume that $i = 1$; now, $g_1 \in I$, so there exists $j \in \{1, \ldots, r\}$ such that $LT_{\leq}(f_j)$ divides $LT_{\leq}(g_1)$, but then $LT_{\leq}(f_j)$ divides $LT_{\leq}(f_1)$ and the only possibility then because of minimality is that $j = 1$, thus $LT_{\leq}(f_1) = LT_{\leq}(g_1)$; now we repeat this process and this leads to the conclusion.

Unfortunately, minimal Gröbner bases are not unique; to achieve uniqueness, one needs to impose more conditions.

Def: a Gröbner basis $G = \{g_1, \ldots, g_s\}$ is called <u>reduced</u> if for all $i \in \{1, \ldots, s\}$ we have that $LC_{\leq}(g_i) = 1$ and g_i is reduced with respect to $G \setminus \{g_i\}$ (this means that no term in the support of g_i is divisible by $LT_{\leq}(g_j)$ for some $i \neq j$).

Prop: given a Gröbner basis $G = \{g_1, \ldots, g_s\}$ that is minimal, the following process yields a reduced Gröbner basis; consider

$g_1 \xrightarrow{H_1} h_1$ where h_1 is reduced w.r.t. $H_1 := \{g_2, \ldots, g_s\}$

$g_2 \xrightarrow{H_2} h_2$ where h_2 is reduced w.r.t. $H_2 := \{h_1, g_3, \ldots, g_s\}$

$\vdots$

$\vdots$

$g_s \xrightarrow{H_s} h_s$ where h_s is reduced w.r.t. $H_s := \{h_1, \dots, h_{s-1}\}$

Proof: since G is a minimal Gröbner basis, we have $LT_\leq(h_i) = LT_\leq(g_i)$ for every $i \in \{1, \dots, s\}$; hence $H := \{h_1, \dots, h_s\}$ is also a Gröbner basis for (G), and it is a minimal one; now, since what matters in being reduced is having monomials that are divisible by some leading terms, and since the leading terms are preserved by the construction, then the procedure yields a reduced Gröbner basis for (G).

Theorem: (Buchberger) once a term order is fixed, every non-zero ideal $I \subseteq k[x_1, \dots, x_n]$ has a unique reduced Gröbner basis with respect to that term order.

Proof: so far, we proved that every non-zero ideal admits a reduced Gröbner basis; now suppose that $G = \{g_1, \dots, g_s\}$ and $H = \{h_1, \dots, h_r\}$ are both reduced Gröbner bases for an ideal, say $I \subseteq k[x_1, \dots, x_n]$; since they are in particular minimal, we have that $r = s$ and we can assume that

$$LT_\leq(g_i) = LT_\leq(h_i) \quad \forall i \in \{1, \dots, s\}$$

now suppose that for some $i \in \{1, \dots, s\}$, we have $g_i \neq h_i$

then $g_i - h_i \in I$ and this is a non-zero polynomial, so there exists $j \in \{1, \dots, s\}$ such that $LT_{\leq}(g_j)$ divides $LT_{\leq}(g_i - h_i)$; by construction $LT_{\leq}(g_i - h_i) < LT_{\leq}(g_i)$, so it must be $j \neq i$; then $LT_{\leq}(g_j)$ $\left(= LT_{\leq}(h_j)\right)$ divides some term of g_i or h_i, and this contradicts the hypothesis that G and H are reduced.

So our program of providing an adequate multivariate counterpart to univariate polynomial division has come to an end. What we obtained is that to each non-zero ideal in the polynomial ring we can associate, once we fix a term order, a unique object that can be effectively computed from a given finite system of generators of the ideal and that provides a solution for multivariate division.

The next goal is to explore the possibilities that this new tool offers us.