Lecture LIX : Detecting Gröbner Bases (Buchberger's Criterion)

§59.1 Summary :

Let K be a field, $n \geq 1$ and set $R = K[x_1, \dots, x_n]$

- $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $\quad \underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$
- $f = \sum_{\substack{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \\ \text{finite}}} c(\underline{\alpha})\, \underline{x}^{\underline{\alpha}}$ a typical polynomial in R
- $\leq$ = a monomial order (ie total order on $\{ \underline{x}^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \}$ st
  - $\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}} \Rightarrow \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}} \quad \forall\, \underline{\gamma} \in \mathbb{Z}_{\geq 0}^n$
  - $\leq$ is a well-order ($\Leftrightarrow 1 \leq \underline{x}^{\underline{\alpha}} \quad \forall\, \underline{\alpha}$)

Ex: $\leq = <_{lex}$ with $x_1 > x_2 > \cdots > x_n$.

- **Multivariate Division Algorithm :**

  Fixed data : $G = \{g_1, \dots, g_m\} \subset R$ a set, $<$

  Input : $f \in R$

  Output : $q_1, \dots, q_m \in R$, $r \in R$ st $f = q_1 g_1 + \cdots + q_m g_m + r$ where
  - $r = 0$ or $r \neq 0$ & no monomial of r is divisible by any $LT(g_i)$.
  - $\forall i \quad LT(f) \geq LT(q_i g_i)$ whenever $q_i g_i \neq 0$

  (Use $LT(g_1), \dots, LT(g_m)$ to do the division)

- $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of I (wrt $<$) if, and only if,

  $g_1, \dots, g_m \in I$ and $LT(I) = (LT(g_1), \dots, LT(g_m))$

  $\| \quad (LT(f) : f \in I)$

Facts about GB:

(1) Every ideal has a Gröbner basis

(2) If $\{g_1, \dots, g_m\}$ is a GB of I, then :

$f \in I \Leftrightarrow$ the remainder from the division algorithm is 0.

Q1: How to build a GB?

Q2: How to test if a finite set is a GB without computing $LT(I)$?

A : Buchberger's Algorithm!

§59.2 Buchberger's Theorem:

Notation: • given $G = \{g_1, \dots, g_m\} \subseteq R$, we will write $f \equiv 0 \bmod G$ if the multivariate division algorithm outputs remainder $r = 0$.

• Given $f_1, f_2 \in R$, we let M be the monic least common multiple of $LT(f_1)$ and $LT(f_2)$. More precisely:

$$LT(f_1) = \underline{x}^{\underline{\alpha}}, \quad LT(f_2) = x^{\beta} \Rightarrow M = x_1^{\max\{\alpha_1, \beta_1\}} \cdots x_n^{\max\{\alpha_n, \beta_n\}}$$

• If $LT(f) = x^{\underline{\alpha}}$ then $L(f) = c_{(\alpha)} x^{\underline{\alpha}}$ $\quad c(\alpha)$ = coefficient of $x^{\underline{\alpha}}$ in f.

Definition: Given $f_1, f_2 \in R \setminus \{0\}$, the **S-polynomial** between f_1 and f_2 is

$$S(f_1, f_2) = \frac{M}{L(f_1)} f_1 - \frac{M}{L(f_2)} f_2$$

Note: The construction produces a polynomial that is either 0 or whose LT is $< M$.

Theorem (Buchberger) Let $I = (g_1, \dots, g_m) \subseteq R$ be an ideal. Then:

$G = \{g_1, \dots, g_m\}$ is a Gröbner basis of $I \iff \forall i, j: S(g_i, g_j) \equiv 0 \bmod G$.

Before we discuss the proof, let us look at an example:

Example: $R = K[x, y]$, $\leq$ = lexicographic order with $x > y$.

$I = (f_1, f_2)$ where $f_1 = \underline{x^3 y} - x y^2 + 1$

$f_2 = \underline{x^2 y^2} - y^3 - 1$ (we underline the leading terms)

$G_0 = \{f_1, f_2\}$ $\quad M = x_1^3 y^2$

$$S(f_1, f_2) = \frac{x_1^3 y^2}{x^3 y} f_1 - \frac{x_1^3 y^2}{x_2^2 y^2} f_2 = y f_1 - x f_2 = y + x \equiv x + y \bmod G$$

$\Rightarrow \{f_1, f_2\}$ is not a GB by Buchberger's Theorem.

We need to prove both implications of Buchberger's Criterion. We will need the following technical result that will be used for ($\Rightarrow$)

Lemma: Assume $f_1, \dots, f_m \in K[x_1, \dots x_n]$ are non-zero polynomials with the same Leading monomial and pick $a_1, \dots, a_m \in K$ s.t. $h = a_1 f_1 + \cdots + a_m f_m$ has $LT(h) < LT(f_i)$

Then, $\exists\, b_2, \dots, b_m \in K$ s.t. $h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i)$.

Proof: Let $\alpha \in \mathbb{Z}^n_{\geq 0}$ and $c_1, \dots, c_m \in K$ s.t. $LT(f_i) = c_i x^\alpha \quad \forall i$

Write $f_i = c_i f_i'$ where $c_i \in K$, f_i' is monic with $LT(f_i') = x^\alpha$.

Then $h = \sum_{i=1}^m a_i c_i f_i' = a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \cdots$

$\cdots + (a_1 c_1 + a_2 c_2 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') + (a_1 c_1 + \cdots + a_m c_m) f_m'$.

By construction, $S(f_{i-1}, f_i) = \frac{1}{c_{i-1}} f_{i-1} - \frac{1}{c_i} f_i = f_{i-1}' - f_i'$.

Since h & all $(f_{i-1}' - f_i')$ have $LT < x^\alpha$ we must have $a_1 c_1 + \cdots + a_m c_m = 0$ because the only term in (RHS) with a monomial x^α is $(a_1 c_1 + \cdots + a_m c_m) f_m'$. Then, writing $b_j = \sum_{i=1}^{j-1} a_i c_i \quad \forall j = 2, \dots, m$ we get $h = \sum_{j=2}^m b_j S(f_{j-1}, f_j)$ as we wanted. □

Proof of Buchberger's Theorem:

($\Rightarrow$) $\forall i,j$: $S(g_i, g_j) \in I$. So the Membership Test ensures $S(g_i, g_j) \equiv 0 \bmod G$.

($\Leftarrow$) To show G is a GB we must confirm $LT(I) = (LT(g_1), \dots, LT(g_m))$

Pick any $f \in I \setminus \{0\}$. Since $I = (g_1, \dots, g_m)$, we can find $h_1, \dots, h_m \in R$ with

$$f = \sum_{i=1}^m h_i g_i$$

The presentation is not unique. Choose one where $\max\{LT(h_i g_i) : h_i g_i \neq 0\}$ is minimal (such choice exists because $<$ well-orders $\mathbb{Z}^n_{\geq 0}$). Let this monomial be $\underline{x}^\alpha$. (since $f \neq 0$, the max will not be taken over an empty-set).

By construction $LT(f) \leq \underline{x}^\alpha$

Our goal: Show $LT(f) = \underline{x}^\alpha$ ($\Rightarrow$ we get $x^\alpha \in (LT(g_1), \dots, LT(g_m))$)

Write $A := \{i : LT(h_i g_i) = x^\alpha\}$

Up to relabeling, we assume $A = \{1, \dots, s\}$

We treat 2 cases:

CASE 1: Assume $LT(f) = \underline{x}^\alpha$.

This means $LT\left(\sum_{i=1}^s LT(h_i) g_i\right) = c x^\alpha$ for some c, so no cancellation of leading terms occurs. In particular, $LT(f) = \sum_{i=1}^s LT(h_i) LT(g_i) \in (LT(g_1), \dots, LT(g_m))$

CASE 2: Assume $LT(f) < x^\alpha$.

We write $$f = \sum_{\substack{i \\ LT(h_i g_i) = x^\alpha}} h_i g_i + \sum_{\substack{i \\ LT(h_i g_i) < x^\alpha \\ \text{or } h_i g_i = 0}} h_i g_i$$

$$= \sum_{LT(h_i g_i) = x^\alpha} L(h_i) g_i + \underbrace{\sum_{LT(h_i g_i) = x^\alpha} (h_i - L(h_i)) g_i + \sum_{\substack{i \\ LT(h_i g_i) < x^\alpha \\ \text{or } h_i g_i = 0}} h_i g_i}_{\text{all monomials here are } < x^\alpha} \qquad (*)$$

Then, by construction, the monomial x^α must not be present in the (RHS) of (*). This means that it has to be cancelled using only terms in the first summand. In particular $\exists\, i \neq j$ with $LT(h_i g_i)$ and $LT(h_j g_j)$ agree with x^α up to a constant.

Write $LT(h_r) = a_r \underline{x}^{\beta(r)}$ where $a_r \in K$ for $r = 1, \dots, s$

- Our objective is to rewrite the first summand to be of the form $\sum_{r=1}^{m} h'_r g_r$ with $LT(h'_r g_r) < x^\alpha$. This will say our choice of x^α was not minimal, leading to a contradiction, and thus ending CASE 2.

Note $LT(x^{\beta(r-1)} g_{r-1})$ and $LT(x^{\beta(r)} g_r)$ agree with x^α up to a multiplicative constant.

By Lemma §59.2 applied to $\sum_{r=1}^{s} a_r (\underline{x}^{\beta(r)} g_r)$, we can rewrite this term as

$$\sum_{LT(h_r g_r) = x^\alpha} L(h_r) g_r = \sum_{r=2}^{s} b_r S(x^{\beta(r-1)} g_{r-1}, x^{\beta(r)} g_r) \qquad (**)$$

Claim: $S(x^{\beta(r-1)} g_{r-1}, x^{\beta(r)} g_r) = \sum_{j=1}^{m'} f_j^{(r)} g_j$ with $LT(f_j^{(r)} g_j) < x^\alpha$.

Pf/ Write $x^{\gamma_{r-1,r}}$ to be the monic least common multiple of $LT(g_{r-1})$ & $LT(g_r)$.

Then: $x^{\alpha - \beta_{r-1,r}} S(g_{r-1}, g_r) = S(x^{\beta(i-1)} g_{i-1}, x^{\beta(i)} g_i)$ because

$$x^{\alpha - \beta_{r-1,r}} S(g_{r-1}, g_r) = x^{\alpha - \beta_{r-1,r}} \left(\frac{x^{\beta_{r-1,r}}}{L(g_{r-1})} g_{r-1} - \frac{x^{\beta_{r-1,r}}}{L(g_r)} g_r \right) =$$

$$= \frac{x^\alpha}{L(g_{r-1})} g_{r-1} - \frac{x^\alpha}{L(g_r)} g_r = \frac{x^\alpha}{L(x^{\beta(r-1)} g_{r-1})} (x^{\beta(r-1)} g_r) - \frac{x^\alpha}{L(x^{\beta(r)} g_r)} x^{\beta(r)} g_r$$

$= S\left(x^{\beta(r-1)} g_{r-1}, x^{\beta(r)} g_r\right)$ because $x^\alpha = \text{mmic lcm}\left(LT\left(x^{\beta(r-1)} g_r\right), LT\left(x^{\beta(r)} g_r\right)\right)$

By definition, $LT(S(g_{r-1}, g_r)) < x^{\beta_{r-1,r}}$ so $LT\left(x^{\alpha-\beta_{r-1}} S(g_{r-1}, g_r)\right) < x^\alpha$

Since $S(g_{r-1}, g_r) \equiv 0 \mod G$ by assumption, we can find $q_1^{(r)}, \dots, q_m^{(r)} \in R$ such that $S(g_{r-1}, g_r) = \sum_{j=1}^m q_j^{(r)} g_j$ and $LT(q_j^{(r)} g_j) \leq LT(S(g_{r-1}, g_r)) < x^{\beta_{r-1,r}}$ if $q_j^{(r)} g_j \neq 0$.

Then, $S\left(x^{\beta(r-1)} g_{r-1}, x^{\beta(r)} g_r\right) = \sum_{j=1}^m \underbrace{\left(x^{\alpha-\beta_{r-1,r}}\right) q_j^{(r)}}_{= \tilde{q}_j^{(r)}} g_j$ with $LT(\tilde{q}_j^{(r)} g_j) < x^\alpha \ \forall r, j$ if $\tilde{q}_j^{(r)} g_j \neq 0$.

As a consequence of the claim and (**), the (RHS) of (*) can be rewritten as $\sum_{i=1}^m h_i' g_i$ where $LT(h_i' g_i) < x^\alpha \ \forall i$ with $h_i' g_i \neq 0$. Contradiction!

Since we have $LT(f) \in (LT(g_1), \dots, LT(g_m)) \ \forall f \in I \setminus \{0\}$, we get

$$LT(I) \subseteq (LT(g_1), \dots, LT(g_m)) \subseteq LT(I)$$

so equality holds, as we wanted. □