# C4 - Gröbner Bases

Goal: provide algorithms that let us perform computations over a polynomial ring.

## 1) Multivariable division algorithm

- Euclidian division: let $f, g \in k[x]$, $g \neq 0$, then there exist a unique couple of elements $q, r \in k[x]$ such that

$$f = q \cdot g + r \quad \text{and} \quad r = 0 \text{ or } \deg(r) < \deg(g).$$

Algorithm:

$q := 0$, $r := f$

while $r \neq 0$ and $LT(g) \mid LT(r)$ then

$$q := q + \frac{LT(r)}{LT(g)}$$

$$r := r - \frac{LT(r)}{LT(g)} \cdot g$$

$p = a_0 x^m + \dots + a_m$, $a_0 \neq 0$, then $LT(p) := a_0 x^m$

Exo: deduce that $k[x]$ is principal: any ideal $I$ is such that $I = (f)$.

- Monomial orders

Def: A monomial order on $R = k[x_1, \dots, x_n]$ is a relation $>$ such that

- $>$ is a total order ($\alpha > \beta$ or $\alpha < \beta$ or $\alpha = \beta$)
- For any $\gamma$, $\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$
- Any nonempty subset has a smallest element.

Notation: $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \dots, \alpha_n)$

Examples:
- Lexicographic order
  $\alpha > \beta$ if the leftmost nonzero entry of $\alpha - \beta$ is positive
- Graded Lex.
  $\alpha > \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the leftmost nonzero entry of $\alpha - \beta$ is positive
- Graded Reverse Lex
  $\alpha > \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta$ is negative.

L

$k[x,y,z]$:

$x >_{lex} yz^2$ and $yz^2 >_{grlex} x$

$x^3y^5z^2 >_{grlex} x^2y^7z$ and $x^2y^7z >_{grevlex} x^3y^5z^2$.

L

- Division

Notation: $k[x_1, \dots, x_n]$ and $>$ a monomial order.

$$f = \sum_{\alpha} c_\alpha x^\alpha.$$

$LT(f) = c_\alpha x^\alpha$ with $\alpha = x^\alpha$ is the biggest mon. such that $c_\alpha \neq 0$.

$LM(f) = x^\alpha$ and $LC(f) = c_\alpha$.

L

Rk: $LT(f \cdot g) = LT(f) \cdot LT(g)$.

**Proposition:** Let $\{f_1, \dots, f_m\}$ be a set of polynomials in $R = k[x_1, \dots, x_n]$, ordered with $>$.

For any $f \in k[x_1, \dots, x_n] = R$ one has

$$f = a_1 f_1 + \dots + a_m f_m + r$$

with $a_i, r \in R$ such that:

- $a_i f_i = 0$ or $LM(f) > LM(a_i f_i)$ $\forall i$
- $r = 0$ or no monomial in $r$ is divisible by any $LM(f_i)$ $\forall i$

$\square$

$r$ is called the remainder of $f$ by $\{f_1 - f_m\}$.

Algorithm/proof:

$a_1 := 0, \dots, a_m := 0$, $r := 0$, $p := f$

While $p \neq 0$ do

  $i := 1$; div := false

  while $i \leq m$ and div = false do

    If $LT(f_i) \mid LT(p)$

    then $a_i := a_i + LT(p)/LT(f_i)$

      $p := p - \left(\frac{LT(p)}{LT(f_i)}\right) \cdot f_i$

      div := true

    else $i := i+1$

  If div = false then $r := r + LT(p)$ and $p := p - LT(p)$.

It turns out that the remainder depends on the order of the family, and moreover $r=0 \Rightarrow f \in (f_1,\dots,f_m)$ but the contrary is not true:

Example: $k[x,y]$ > lex order. $f_1 = xy+1$ $f_2 = y^2-1$
$f = xy^2 - x$

- $F:=\{f_1,f_2\}$ : $f = x^*y^2 - x = y(xy+1) + 0\cdot(y^2-1) + (-x-y)$
- $F:=\{f_2,f_1\}$ $f = xy^2 - x = x(y^2-1) + 0\cdot(xy-1) + 0$

- Grobner bases (G.B.)

Def: A subset $\{g_1,\dots,g_n\}$ of an ideal $I \subset k[x_1,\dots,x_n]$ is a G.B. of $I$ if

$$(LT(g_1),\dots,LT(g_n)) = (LT(I))$$

where $LT(I) = \{ cx^\alpha : \exists f \in I : LT(f) = cx^\alpha \}$.

Corollary: i) Every ideal $I$ has a G.B.
ii) If $\{g_1,\dots,g_n\}$ is a G.B. of $I$ then $(g_1,\dots,g_n) = I$.

Proof: i) exercise (!). — [Cox-Little-O'Shea]
ii) $(g_1,\dots,g_n) \subset I$ is obvious.
Let $f \in I$: $f = \sum_{i=1}^{n} a_i g_i + r$
If $r \neq 0$ then its monomials are not div. by any $LT(g_i)$.
But $r = f - \sum a_i g_i \in I$, so $LT(r) \in (LT(I)) = (LT(g_1),\dots,LT(g_n))$ : contradiction. □

**Proposition** Let $\{g_1, \dots, g_n\}$ be a G.B. of $I$ and $f \in k[x_1, \dots, x_n]$.
Then, there exists a unique $r \in k[x_1, \dots, x_n]$ such that
i) any term in $r$ is not divisible by any $LT(g_i)$
ii) $\exists\, g \in I$ such that $f = g + r$.

In particular, $r$ is the remainder of the division of $f$ by $\{g_1, \dots, g_n\}$ independently of its ordering. (Notation $r = \overline{f}^G$, $G = \{g_1, \dots, g_n\}$.)

**Proof**: The existence of $r$ is the division algorithm.
Let $f = g + r = g' + r'$ two such decompositions.
Then $r - r' = g' - g \in I$.
If $r - r' \neq 0$ then $LT(r - r') \in (LT(I)) = (LT(g_1), \dots, LT(g_n))$
so $\exists\, i$ such that $LT(g_i) \mid LT(r - r')$ : impossible.
(monomial in $r$ or $r'$ or both) □

**Corollary**: If $G = \{g_1, \dots, g_n\}$ is a G.B. of $I$ then
$f \in I \iff$ remainder of $f$ by $\{g_1, \dots, g_n\} = 0$.
i.e. $\overline{f}^G$
└

→ How to characterize Grobner Bases?

- **Syzygy pairs.**

**Def**: Let $f, g \neq 0 \in k[x_1, \dots, x_n]$. Set $LT(f) = cx^\alpha$, $LT(g) = dx^\beta$
and $LCM(x^\alpha, x^\beta) = x^\gamma$ ($\gamma_i = \max(\alpha_i, \beta_i)\ \forall i$)
Then we define

$$S(f,g) := \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

└

**THM**: Let $G=\{g_1,\dots,g_n\}$ and $I=(g_1,\dots,g_n)$ an ideal in $k[x_1,\dots x_n]$.

Then $G$ is a G.B. of $I \iff \overline{S(g_i,g_j)}^{G}=0 \quad \forall i\neq j$.

└

*Proof*: $\Rightarrow$ $S(g_i,g_j)\in I$ (by construction) so they reduce to 0.

$\Leftarrow$ *sketch*: see Cox-Little-O'Shea for details (technical).

Given $f\in I$ one has to show that $LT(f)\in(LT(g_1),\dots,LT(g_n))$.

Since $f\in I$, $f=\sum_{i=1}^{n} a_i g_i$. Then two cases:

Case 1: $LT(f)=LT(a_k g_k)$ for some $k$, and this is finished.

Case 2: there are some cancellations in the leading terms of $a_i g_i$'s.

Each cancellation corresponds to a S-pair and since S-pairs reduce to 0, one can replace them by a new combination of the $g_i$'s.

In this way the total degree of $\sum a_i g_i$ ↘. □.

*Example*: $I=(y-x^2, z-x^3)$. Show that $G=\{y-x^2, z-x^3\}$ is a G.B. for the lex ordering $y>z>x$.

$$S(y-x^3, z-x^3)=\frac{y^3}{y}(y-x^2)-\frac{y^2}{z}(z-x^3)=-zx^2+yx^3$$

And the division: $-zx^2+yx^3=x^3(y-x^2)+(-x^2)(z-x^3)+0$.

□.

## • Buchberger algorithm

Given $I = (f_1, \dots, f_k)$, build a G.B.

**Algorithm:**

INPUT: $G := \{f_1, \dots, f_k\}$

REPEAT

$G' := G$

For each pair $p, q$ in $G'$ do

$S := \overline{S(p,q)}^{G'}$

If $S \neq 0$ then $G := G \cup \{S\}$

UNTIL $G' = G$

**Proof:** • At each step $I = (G)$ because S-pairs $\in I$.

• When the algo stops $G$ is a G.B. by previous THM.

• At each step $G' \subset G$, hence $(LT(G')) \subset (LT(G))$

Now, If $G' \subsetneq G$ then $(LT(G')) \subsetneq (LT(G))$ because a S-pair added is a polynomial $r$ such that $LT(r) \notin (LT(G'))$.

This gives an increasing chain of ideals that must stop!
So $(LT(G')) = (LT(G))$ at some point, hence $G = G'$.

□

Example: Compute a G.B. of $(\underbrace{x^2-y^2}_{f_1}, \underbrace{xy-1}_{f_2})$, lex $x > y$.

- $S(f_1,f_2) = y(x^2-y^2) - x(xy-1) = x-y^3 = f_3$ not reduced by $LT(f_1), LT(f_2)$
- $S(f_1,f_3) = 1(x^2-y^2) - x(x-y^3) = xy^3-y^2$ reduce to zero w.r.t. $f_1,f_2,f_3$

  $S(f_2,f_3) = 1(xy-1) - y(x-y^3) = y^4-1 = f_4$ do not reduce
- final pass, all reduce to zero.

G.B. : $\{ f_1 = x^2-y^2,\ f_2 = xy-1,\ f_3 = x-y^3,\ f_4 = y^4-1 \}$

$f_1$ and $f_2$ seem to be superfluous now.

Minimality:

Lemma: Let $G$ be a G.B of $I$. Let $p \in G$ such that $LT(p) \in (LT(G-\{p\}))$ then $G-\{p\}$ is also a G.B.

Proof: By def $(LT(G)) = (LT(I))$, and by assumption, $(LT(G-\{p\})) = (LT(G))$. ∎

Def: A G.B of $I$ is minimal if

i) $LC(p) = 1 \quad \forall p \in G$

ii) $\forall p \in G,\ LT(p) \notin (LT(G-\{p\}))$.

**Def** A G.B. of $I$ is reduced if

i) $LC(p) = 1 \quad \forall p \in G$

ii) $\forall p \in G$, no ~~more~~ term in $p$ ~~blongs~~ belongs to $(LT(G - \{p\}))$.

**Prop** (Cox-Little-O'Shea) Any ideal has a unique reduced Grobner basis.

## 2. Monomial ideals and applications.

We said that the HP of a finitely generated $R$-mod $M$ can be computed by means of a F.F.R. This is true, but there is a more efficient way to proceed when $M = R/I$.

**Lemma** (Macaulay): $R$ pol. ring and $I$ an homogeneous ideal.

$$H.F\left(\frac{R}{I}, t\right) = HF\left(\frac{R}{(LT(I))}, t\right).$$

**Proof**: $I_i = \langle f_1, \dots, f_j \rangle_K$

One can assume that $in(f_1) > in(f_2) > \dots > in(f_j)$, so $in(f_j)$ are linearly indep.

Assum they do not span $in(I)_i$. Pick $m \in in(I)_i$ not in $\langle in(f_1), \dots, in(f_j) \rangle_K$ ~~which~~ minimal w.r.t. term order. such that $in(m') = m'$ is

$\exists\, g \in I$ such that $in(g) = m'$ ~~$\neq in(m)$~~. $g \in I_i$ and hence is a lin. comb. of $f_1, \dots, f_j$.

$\Rightarrow$ $m'$ must be one of $in(f_j)$, in contradiction with choice of $m'$ minimal.

□

- As a consequence, in order to compute $AP(R/I, i)$, one can compute a G.B. of $I$, say $\{g_1, \dots, g_n\}$ and work with $(LT(I)) = (LT(g_1), \dots, LT(g_n))$

which is a monomial ideal.
It turns out that monomial ideals are nice for computations.

- <u>Lemma</u>: Let $I = (x^{\alpha_1}, \dots, x^{\alpha_j})$ a monomial ideal and $x^\alpha$ a monomial. Then

i) $x^\alpha \in I \iff x^{\alpha_i} \mid x^\alpha$ for some $i$.

ii) $f \in I \iff f$ is a linear combination of monomials that belongs to $I$.

L

<u>Proof</u>: i) $\Leftarrow$ obvious
$\Rightarrow$ $x^\alpha = \sum_i f_j x^{\alpha_j}$ but each term on the right is a multiple of $x^{\alpha_j}$ for some $j$.

ii) same : $f = \sum_i h_j x^{\gamma_j}$ : all monomials belongs to $I$.

L

<u>Lemma</u>: Let $I = (x^{\alpha_1}, \dots, x^{\alpha_j})$ a monomial ideal and $x^\alpha$ a monomial.

Then $$(I : x^\alpha) = \left( \frac{x^{\alpha_1}}{GCD(x^{\alpha_1}, x^\alpha)}, \dots, \frac{x^{\alpha_j}}{GCD(x^{\alpha_j}, x^\alpha)} \right).$$

<u>Proof</u>: $\supseteq$ obvious
$\subseteq$ If $x^\alpha \cdot g \in I$, $g = \sum c_\gamma x^\gamma$, then $x^\alpha \cdot x^\gamma \in I \ \forall \gamma$

i.e $x^{\alpha_i} \mid x^\alpha x^\gamma$ for some $i$ $\Rightarrow$ $\frac{x^{\alpha_i}}{GCD(x^{\alpha_i}, x^\alpha)} \mid \frac{x^\alpha}{GCD(-)} \cdot x^\gamma$

Coprime.

□

• Now one can compute the Hilbert polynomial of a monomial ideal inductively:

Let $I$ be a monomial ideal and $x^\alpha \notin I$, $|\alpha|=d$.

One has the exact sequence

$$0 \to \frac{R(-d)}{(I:x^\alpha)} \xrightarrow{\cdot x^\alpha} \frac{R}{I} \to \frac{R}{(I,x^\alpha)} \to 0$$

which shows that

$$HP\left(\frac{R}{(I,x^\alpha)}, i\right) = HP\left(\frac{R}{I}, i\right) - HP\left(\frac{R}{(I:x^\alpha)}, i-d\right)$$

↑ monomial ideal with $t$ generators

↑ monomial ideals with $t-1$ generators.

↑