21-610 4 October 2021

Buchberger's criterion:

$$G \text{ Gröbner} \iff S(g_i, g_j) \bmod G = 0 \quad \forall g_i, g_j \in G$$

Pf: .... $f \in (G)$

$$f = \underbrace{\sum_{LM(a_i g_i) = \alpha} LT(a_i) g_i}_{\Sigma_1} + \underbrace{\sum_{LM(a_i g_i) = \alpha} (a_i - LT(a_i)) g_i}_{\Sigma_2} + \underbrace{\sum_{LM(a_i g_i) < \alpha} a_i g_i}_{\Sigma_3}$$

Using lemma, rewrite Σ_1 as a sum of sum of $S(LT(a_i)g_i, LT(a_j)g_j)$

$$\Sigma_1 = \sum_{i,j} \underbrace{B_{ij}\, S(LT(a_i)g_i, LT(a_j)g_j)}_{\text{each summand } LM < \alpha}$$

Using the division algorithm

$S(g_i, g_j)$ as a linear combination $\sum_k h_{kij}\, g_k$ of polynomials g_k in G whose $LM(h_{kij}\, g_k) \leq LM(g_i, g_j)$

and remainder is 0 (by the assumption on G).

$$q_{ij} = S(LT(a_i)g_i, LT(a_j)g_j) = x^{\beta_{ij}} S(g_i, g_j)$$

for some $\beta_{ij} \geq 0$

So q_{ij} can also be written as a linear combination of g_k's with the same property

$$\begin{array}{cccc} LM = \alpha & < \alpha & & < \alpha \end{array}$$

$$f = \Sigma_1 + \Sigma_2 + \Sigma_3$$

$$= \Sigma_1' + \Sigma_2 + \Sigma_3$$

and use induction as long as $LM(f) < x^\alpha$

Case $LM(f) = x^\alpha = \max\{LM(h_i g_i) : i = 1, \dots, m\}$

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

Goal: $LM(f) \in (LM(g_1), \dots, LM(g_m))$

$LM(f)$ appears on the right, say in $h_j g_j$, and by definition of α

$$x^\alpha \le LM(h_j g_j) \le x^\alpha$$

so, $LM(f) = LM(h_j) LM(g_j)$

$$\Longrightarrow LM(f) \in (LM(g_j)) \subseteq (LM(g_1), \dots, LM(g_m)) \quad \blacksquare$$

Finding a Gröbner basis:

Input $B \subset F[x_1, \dots, x_n]$

Output: Gröbner basis for (B).

1) $G = B$

2) While $\exists\, i,j$ s.t. $S(g_i, g_j) \bmod G \neq 0$

add $S(g_i, g_j)$ to G.

3) Output G.

$S(g_i, g_j) \in (g_i, g_j) \Rightarrow G \subset (B)$ By induction on # of steps

Consider a step of the algorithm:

$$h = S(g_i, g_j) \bmod G \qquad \in (B)$$

Every term of h, and in particular $LT(h)$, is not divisible by any $LT(g_i)$ $g_i \in G$.

$$\Longleftrightarrow \quad h \notin (LT(g_1), \ldots, LT(g_m))$$

So $(LT(g_1), \ldots, LT(g_m), LT(h))$ strictly contains

By the ascending chain condition, this must stop.

Let $I \subset F[x_1,\dots,x_n]$

Def: j'th elimination ideal of I is

$$I_j \stackrel{def}{=} I \cap F[x_{j+1},\dots,x_n]$$

Note I_j is an ideal in $F[x_{j+1},\dots,x_n]$.

Prop: Consider lexicographical ordering on $F[x_1,\dots,x_n]$

let G be a Gröbner basis for I.

Then $G_j = G \cap F[x_{j+1},\dots,x_n]$ is a Gröbner basis for I_j.

Pf: Note that $G_j \subseteq I_j$.

WTS $LT(I_j) \subseteq (LT(g))_{g \in G_j}$

Say, $f \in I_j$ and WTS $LT(f) \in (LT(g))_{g \in G_j}$

Since G is Gröbner (using the division algorithm)

$$f = \sum_{g_i \notin G_j} h_i g_i(x_1, \dots, x_n) + \sum_{g_i \in G_j} h_i g_i(x_{j+1}, \dots, x_n)$$

Recall that for g_i to appear in this sum

$LT(g_i)$ must divide $LT(f')$

for some intermediate f' in the algorithm

By induction on the # of steps in the division $LT(f')$ is not divisible by $LT(g_i)$ $\forall g_i \notin G_j$.

In fact $f' \in F[x_{j+1}, \dots, x_n]$

Step: $f' \in F[x_{j+1}, \dots, x_n]$ at a start of division step

some g_i s.t. $LM(g_i) \in F[x_{j+1}, \dots, x_n]$ $\overset{\text{lex}}{\Longrightarrow}$ $g_i \in F[x_{j+1}, \dots]$

Replace f' by $f' - \dfrac{LT(f')}{LM(g_i)} g_i \in F[x_{j+1}, \dots, x_n]$. $\square$

Modules (linear algebra).

Def: Let R be a ring with 1.

An left R-module is an abelian M together with an action of R on M, i.e. a function $R \times M \to M$ denoted by rm for $r \in R$, $m \in M$

s.t.

- $(r_1 + r_2)m = r_1 m + r_2 m$
- $(r_1 r_2)m = r_1(r_2 m)$
- $r(m_1 + m_2) = rm_1 + rm_2$
- $1m = m$ $\quad [\cancel{rm = 0\ \forall m}]$

$$\overset{R}{\overset{\Downarrow}{0}} + \overset{R}{\overset{\Downarrow}{0}}$$

$$(0+0)m = 0m$$
$$\|$$
$$0m + 0m$$

Since M is abelian group $\Rightarrow$ $\overset{R}{\overset{\Downarrow}{0}} m = \overset{M}{\overset{\Downarrow}{0}}$.

Ex: If R is a field,

the R-module $=$ R-vector space