2.12. Gröbner bases

References:

- Sturmfels: What is a Gröbner basis?
- Cox, Little, O'Shea: Ideals, Varieties, and Algorithms (Chapter 2)

Question

How to determine whether a polynomial h lies in an ideal $I=(f_1,\dots,f_m)\subseteq K[x_1,\dots,x_n]$?

Ex If $n=1$, we can compute $g:=\gcd(f_1,\dots,f_m)$ using the Euclidean algorithm. Then $I=(f_1,\dots,f_m)=(g)$, so $h\in I \Leftrightarrow g\mid h$.

Ex If the polynomials $f_1,\dots,f_m$ have degree ≤ 1, use Gaussian elimination to put the equations into row echelon form.

Def Let $S := S(x_1, \dots, x_n) = \{x_1^{e_1} \cdots x_n^{e_n} \mid e_1, \dots, e_n \geq 0\}$ be the set of monomials in $x_1, \dots, x_n$.

A monomial order is a total order $\leq$ on S such that:

a) $1 \leq M \quad \forall M \in S$

b) If $M \leq N$, then $MU \leq NU \quad \forall U \in S$.

Rmk Some people omit condition a), which ensures that $\leq$ is a well-order: every $\emptyset \neq T \subseteq S$ has a smallest element.

Exe If $n = 1$, there is just one monomial order:

$$1 < x_1 < x_1^2 < x_1^3 < \cdots$$

Exe Lexicographic order

$$x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n}$$

$\iff (a_1, \dots, a_n) < (b_1, \dots, b_n)$ lexicographically

$\iff a_1 = b_1, \dots, a_{i-1} = b_{i-1}, a_i < b_i$ for some $1 \leq i \leq n$.

$$1 < x_2 < x_2^2 < x_2^3 < \cdots < x_1 < x_1 x_2 < x_1 x_2^2 < \cdots < x_1^2 < \cdots$$

Ese Degree lexicographic order

...

$\Leftrightarrow (a_1+\dots+a_n, a_1, \dots, a_n) < (b_1+\dots+b_n, b_1, \dots, b_n)$

lexicographically

$1 < x_2 < x_1 < x_2^2 < x_1x_2 < x_1^2 < x_2^3 < \dots$

Ese Degree reverse lexicographic order

...

$\Leftrightarrow (a_1+\dots+a_n, -a_n, \dots, -a_1) < (b_1+\dots+b_n, -b_n, \dots, -b_1)$

lexicographically

Rmk For $n=2$, deg. lex. = deg. rev. lex.

Def Let $f = \sum_{M \in S} c_M M \in K[x_1, \dots, x_n]$.

A monomial M occurs in f if $c_M \neq 0$.

Let $f \neq 0$.

Its leading monomial (w.r.t. $\leq$) is

$lm(f) := \max\{M \text{ occurring in } f\}$.

Its leading coefficient (w.r.t. $\leq$) is

$lc(f) = c_{lm(f)}$.

Its leading term (w.r.t. $\leq$) is

$lt(f) = lc(f) \cdot lm(f)$.

Rmk $lm(fg) = lm(f) \cdot lm(g)$ for any $f, g \neq 0$.
lt lt lt
lc lc lc

Def A polynomial $f \in K[X_1, \dots, X_n]$ is reduced w.r.t. a subset $G \subseteq K[X_1, \dots, X_n]$ if no monomial M occuring in f is divisible by the leading monomial of any $0 \neq g \in G$.

Ex X^3 is reduced w.r.t. $\{Y, XY+1\}$.

$X^2Y^3 + X^5$ is not reduced w.r.t. $\{X^3+Y\}$ and deg. lex. ordering.
(or any other order!)

Rmk For $f = \sum_M c_M M$, let

$$W(f) = \{ M : c_M \neq 0 \text{ and } lm(g) \mid M \text{ for some } 0 \neq g \in G \}.$$

If $W(f) \neq \emptyset$, let $N^{(1)} = \max(W(f))$, $lm(g) \mid N^{(1)}$, $0 \neq g \in G$.

Consider $f^{(1)} := f - \frac{c_{N^{(1)}} N^{(1)}}{lt(g)} \cdot g$.

Then $M < N^{(1)}$ $\forall M \in W(f^{(1)})$.

Continue this process

$$(f \rightsquigarrow f^{(1)} \rightsquigarrow f^{(2)} \rightsquigarrow \dots)$$
$$\nu(1) > \nu(2) > \nu(3) > \dots$$

Since $\leq$ is a well-order, this process has to terminate with some $f^{(k)}$ which is reduced w.r.t. G.

Def A reduction of f w.r.t. G is a polynomial r which is reduced w.r.t. G and such that

$$r = f - g_1 h_1 - \dots - g_r h_r$$

for some $g_1, \dots, g_r \in G$, $h_1, \dots, h_r \in K[X_1, \dots, X_n]$ with $lm(g_i h_i) \leq lm(f)$.

Rmk $r \equiv f \bmod (G)$.

ideal generated by G

Ex Use lex. order on $K(X,Y)$.

$$f = XY^2 + 1, \qquad G = \{XY+1, Y+1\}$$

$$f^{(1)} = XY^2 + 1 - Y(XY+1) = -Y + 1$$

$$r = f^{(2)} = -Y + 1 + Y + 1 = 2$$

Warning Reductions aren't always unique!

Ex Use lex. order on $\mathbb{F}[x,y]$

$$f = x^2y^2, \qquad G = \{xy^2, x^2y+1\}$$

$$r = f^{(1)} = x^2y^2 - x \cdot xy^2 = 0$$

or $r = f^{(1)} = x^2y^2 - y\cdot(x^2y+1) = -y$

Def A Gröbner basis of an ideal I w.r.t. $\leq$ is a subset $G \subseteq I$ such that

$$lm(I) = \{M : N \mid M \text{ for some } N \in lm(G)\}.$$

Rmk "$\supseteq$" holds for any subset $G \subseteq I$.

Ex I is a Gröbner basis of I.

Ex $\{f\}$ is a Gröbner basis of (f) for any polynomial f.

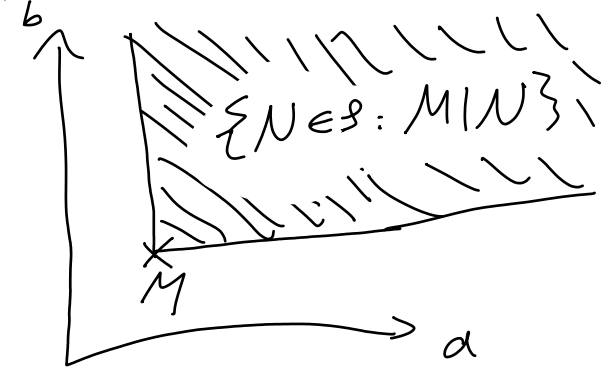
Rmk Let $A \subseteq \mathbb{F}$. A monomial M is divisible by an element of A if and only if it is contained in the ideal (A) generated by the elements of A.

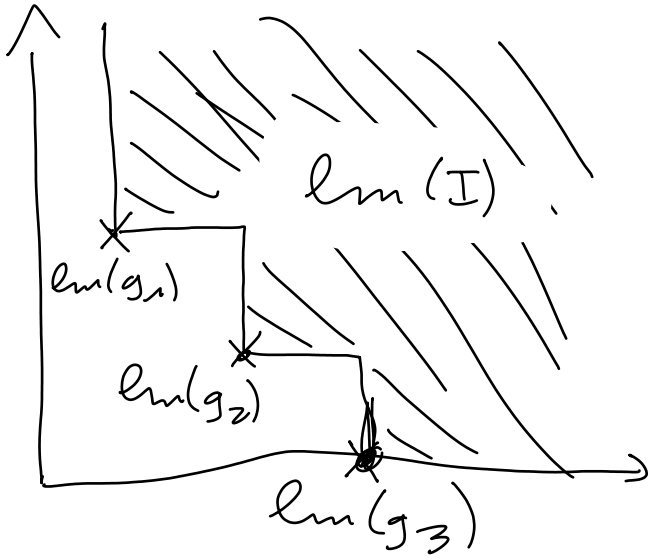
Cor 2.44 Any ideal $I \subseteq K[x_1, \dots, x_n]$ has a finite Gröbner basis.

Pf By Hilbert's Basis Theorem, the ideal $(\mathrm{lm}(I))$ is generated by finitely many elements $\mathrm{lm}(g_1), \dots, \mathrm{lm}(g_r)$ $(0 \neq g_1, \dots, g_r \in I)$.
Take $G = \{g_1, \dots, g_r\}$. □

Picture ($n=2$)

$M = x^a y^b$





Thm 2.45 The monomials $M \notin \mathrm{lm}(I)$ form a basis of the K-vector space

$$K[x_1, \dots, x_n]/I.$$

Pf generators:

consider any $f \in K[x_1, \dots, x_n]$.

Let r be any reduction w.r.t. I.

$\Rightarrow r$ is a linear combination of monomials $M \notin \mathrm{lm}(I)$.

linearly independent:

The leading monomial of any nonzero linear combination f of monomials $M \notin \mathrm{lm}(I)$ is $\mathrm{lm}(f) \notin \mathrm{lm}(I)$.

$\Rightarrow f \notin I$. □

Cor 2.46 $\dim_K(K[x_1, \dots, x_n]/I) = \#(S \setminus \mathrm{lm}(I))$.

Rmk Recall that $\#V(I) \le \dim_K(\dots)$!

Thm 2.47 Reduction w.r.t. a Gröbner basis is always unique.

Pf Let $r_1 \neq r_2$ be reductions of f w.r.t. G.

$\Rightarrow r_1 \equiv r_2 \bmod I$. $\Rightarrow r_1 - r_2 \in I$

$\Rightarrow \mathrm{lm}(r_1 - r_2) \in \mathrm{lm}(I)$.

$\Rightarrow r_1$ or r_2 isn't reduced w.r.t. G! ↯ □

Cor 2.48 Let G be a "Gröbner basis of I. Then, $f \in I$ if and only if its reduction w.r.t. G is 0.

Pf Any reduction $r \equiv f \bmod I$ is a linear combination of monomials $M \notin \mathrm{lm}(I)$. Then, $r \in I$ if and only if $r = 0$. □

Cor 2.49 Any "Gröbner basis G of I generates I.

Pf

If $f \in I$, then $0 = r \equiv f \bmod (G)$, so $f \in (G)$.
($0 = r$ since $f \in I$)

□

Thm 2.50 (Buchberger's criterion)

A set G is a Gröbner basis for $I := (G)$ if and only if for all $0 \neq f, g \in G$, some/every reduction of

$$S(f,g) = \frac{M}{\mathrm{lt}(f)} \cdot f - \frac{M}{\mathrm{lt}(g)} \cdot g \text{ w.r.t. to } G$$

is 0, where $M = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.

Note: $\mathrm{lt}\left(\frac{M}{\mathrm{lt}(f)} \cdot f\right) = M = \mathrm{lt}\left(\frac{M}{\mathrm{lt}(g)} \cdot g\right)$,

so the leading terms cancel.