A minimal amount of Gröbner bases

$R = \mathbb{C}[x_1, \dots, x_n]$

Def. A monomial ordering of is a total ordering, $>$, of the monomials of R such that

1) $x^a > x^b \implies x^c x^a > x^c x^b \quad \forall$ monomials x^c

2) $1 = x^{\vec{0}}$ is the smallest monomial.

Example

1. Lex $\quad x^a > x^b$ if the left-most nonzero entry of $a-b$ is positive. ← More of the earlier (more expensive) variables.

$$x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1.$$

2. Deglex $x^a > x^b$ if $\sum a_i > \sum b_i$ or if $\sum a_i > \sum b_i$ and $x^a >_{lex} x^b$.

$$x^2 > xy > xz > y^2 > yz > z^2 > x > y > z > 1.$$

3. Degrevlex (or grlex – for graded reverse lexicographic)
$x^a > x^b$ if $\sum a_i > \sum b_i$ or if $\sum a_i > \sum b_i$ and the right-most entry of $a-b$ is negative.

Fewer of the later (less expensive variables)

$$x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1.$$

From now on, fix a monomial ordering on R.

Def. A term is a monomial times a constant: αx^a with $\alpha \in \mathbb{C}$.

If $\alpha, \beta \neq 0$, say $\alpha x^a > \beta x^b$ if $x^a > x^b$. The initial term of $f \in R$, denoted $in(f)$ is the largest term of f. (Take $in(0) = 0$)

If $I \subseteq R$ is an ideal, then the initial ideal of I is the monomial ideal

$$in(I) = \langle in(f) : f \in I \rangle.$$

Thm. (Macaulay) Let $I \subseteq R$ be an ideal. A $\mathbb{C}$-vector space basis for R/I is the set of monomials not in $in(I)$.

Division Algorithms

one variable

Thm. For $f, g \in \mathbb{C}[x]$, $\exists!$ $q, r \in \mathbb{C}[x]$ with $\deg r < \deg g$ such that

$$f = qg + r.$$

Example

$$
\begin{array}{r|l}
 & 2x^2 + x - 2 \\
\hline
x^2+1 & 2x^4 + x^3 + 1 \\
 & 2x^4 + 2x^2 \\
\hline
 & x^3 - 2x^2 + 1 \\
 & x^3 + x \\
\hline
 & -2x^2 - x + 1 \\
 & -2x^2 - 2 \\
\hline
 & -x + 3
\end{array}
$$

$$\underbrace{2x^4+x^3+1}_{f} = (\underbrace{2x^2+x-2}_{q})(\underbrace{x^2+1}_{g}) + (\underbrace{-x+3}_{r})$$

Cor. (1) $f(\alpha) = 0$ iff $(x-\alpha) \mid f$

(2) $\mathbb{C}[x]$ is a PID

(3) $f \in (g)$ iff the remainder of f upon division by g is 0.

several variables

Division algorithm $f, g_1, \dots, g_k \in R$. $\exists\, q_1, \dots, q_k, r$ s.t.

$$f = q_1 g_1 + \cdots + q_k g_k + r$$

where ...

No term of r is divisible by any $in(g_i)$ and $in(f) \geq in(q_i g_i)$ $\forall i$.

Here's how: Start with f. Find the largest term αx^a divisible by some $in(g_i)$. Replace f by $f - \frac{\alpha x^a}{in(g_i)} g_i$ to get rid of αx^a in f. Repeat.

Example $f = x^3 + 2xy^2 - y^3 + x$, $g_1 = xy + 1$, $g_2 = x^2 + y$ (Use deglex.)

$$
\begin{array}{l}
\underline{\quad xg_2 + 2yg_1 - g_1 \quad} \\
x^3 + 2xy^2 - y^3 + x \\
\underline{x^3 + xy} \\
2xy^2 - y^3 - xy + x \\
\underline{2xy^2 + 2y} \\
-y^3 - xy + x - 2y \\
\underline{\quad -xy - 1} \\
x - 2y + 1
\end{array}
$$

$$x^3 + 2xy^2 - y^3 + x = (2y-1)g_1 + xg_2 + (x - 2y + 1).$$

Depressing example $\quad f = x^2 + y, \quad g_1 = x^2, \quad g_2 = x^2 + y$

$$f = g_1 + y \quad \text{or} \quad f = g_2 + 0$$

The remainder is not unique! It depends on the ordering of the g_i.

The division algorithm does not solve the ideal membership problem:

$$f \in \langle x^2, x^2 + y \rangle.$$