The method of Gröbner Bases

- We write monomial in $x_1, \ldots, x_n$ as
$$x^\alpha = x_1^{a_1} \cdots x_n^{a_n},$$
so that $\alpha = (a_1, \ldots, a_n) \in Z^n_{\geq 0}$ is the vector of exponents.

- A *monomial order* is any total order $>$ on monomials in $k[x_1, \cdots, x_n]$ with the following two properties:
  1. (Well-Ordering) $>$ is a well-ordering on the set of monomials, i.e., any nonempty subset of monomials has a least element under $>$.
  2. (Compatibility) If $x^\alpha > x^\beta$, then $x^\alpha x^\gamma > x^\beta x^\gamma$ for any monomial x^γ.

- The *lexicographic* order (lex for short) is defined by
$$x_1^{a_1} \cdots x_n^{a_n} >_{lex} x_1^{b_1} \cdots x_n^{b_n} \iff a_1 > b_1, \text{ or } a_1 = b_1 \text{ and } a_2 > b_2, \text{ etc.}$$

- The *graded reverse lexicographic*(grevlex) is defined by
$$x_1^{a_1} \cdots x_n^{a_n} >_{grevlex} x_1^{b_1} \cdots x_n^{b_n} \iff \begin{array}{l} a_1 + \cdots + a_n > b_1 + \cdots + b_n, \text{ or else} \\ a_1 + \cdots + a_n = b_1 + \cdots + b_n \text{ and either} \\ a_n < b_n, \text{ or } a_n = b_n \text{ and } a_{n-1} < b_{n-1}, \text{ etc.} \end{array}$$

- If we write $f \in k[x_1, \ldots, x_n]$ as
$$f = \sum_\alpha c_\alpha x^\alpha, \ c_\alpha \in k,$$
then a *term* of f is $c_\alpha x^\alpha$ for $c_\alpha \neq 0$, and the *leading term* of f is
$$\mathrm{LT}(f) = \max_>\{c_\alpha x^\alpha | c_\alpha \neq 0\},$$
where $\max_>$ mean the maximum with respect to $>$. The leading term is sometimes called the *initial term* and a monomial order is often called a *term order*.

- We assume that a monomial order $>$ on $k[x_1, \ldots, x_n]$ is given, an expression of the form

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where the "remainder" r should satisfy

  1. no term of r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$;
  2. $\mathrm{LT}(f) \geq \mathrm{LT}(q_i f_i), \quad 1 \leq i \leq s.$

- Given a monomial order $>$ and an ideal $I \subset k[x_1, \ldots, x_n]$, we say that $\{g_1, \ldots, g_t\} \subset I$ is a Gröbner **basis** of I if

$$< \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) > = < \mathrm{LT}(I) > .$$

- **Proposition 1.** *If $g_1, \ldots, g_t$ is a* Gröbner *basis for I and $f \in k[x_1, \ldots, x_n]$, then $f \in I$ if and only if the remainder of f on division by $g_1, \ldots, g_t$ is zero.*

- **Proposition 2.** *If $g_1, \ldots, g_t$ is a* Gröbner *basis for I and $f \in k[x_1, \ldots, x_n]$, then f can be written uniquely in the form*

$$f = g + r$$

where $g \in I$ and no term of r is divisible by any $\mathrm{LT}(g_i)$.

- The *S-polynomial* of $f_1, f_2 \in k[x_1, \ldots, x_n]$ is defined to be

$$S(f_1, f_2) = \frac{x^\gamma}{\mathrm{LT}(f_1)} f_1 - \frac{x^\gamma}{\mathrm{LT}(f_2)} f_2,$$

where $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))$ and $\mathrm{LM}(f_i)$ is the *leading monomial* of f_i (the leading term with the coefficient removed).

- **Buchberger's Criterion.** *A basis $\{g_1, \ldots, g_t\} \subset I$ is a* Gröbner *basis of I if and only if for all $i < j$, we have*

$$\overline{S(g_i, g_j)}^G = 0.$$

Here, $\overline{S(g_i, g_j)}^G$ denotes the remainder of $S(g_i, g_j)$ on division by G.

- **Buchberger's Algorithm.** *Given* $\{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$, *consider the algorithm which starts with* $F = \{f_1, \ldots, f_s\}$ *and then repeats the two steps*
  - *(Compute Step) Compute* $\overline{S(f_i, f_j)}^F$ *for all* $f_i, f_j \in F$ *with* $i < j$.
  - *(Augment Step) Augment* F *by adding the nonzero* $\overline{S(f_i, f_j)}^F$ *until the Compute Step gives only zero remainders. This algorithm always terminates and the final value of* F *is a* Gröbner *basis of* $< f_1, \ldots, f_s >$.