4. Gröbner Bases

4.1. Introduction: From Gauss to Gröbner — From linear to polynomial equations

When we have to solve a system of linear equations, we apply the elimination procedure of Gauss and transform the system into a triangular one. From this triangular form we can immediately read off the solutions:

$$\begin{array}{rcl} 2x-y-z &=& 0 \\ x+2y-2z &=& 1 \\ x-y+2z &=& 2 \end{array} \quad \Longrightarrow \quad \begin{array}{rcl} x+2y-2z &=& 1 \\ y-5z &=& -4 \\ z &=& 1 \end{array}$$

A similar process can be applied in adapted form to systems of non-linear polynomial (algebraic) equations:

$$\begin{array}{r} 2x^4-3x^2y+y^4-2y^3+y^2=0 \\ 4x^3-3xy=0 \\ 4y^3-3x^2-6y^2+2y=0 \end{array} \quad \Longrightarrow \quad \begin{array}{r} 3x^2+2y^2-2y=0 \\ xy=0 \\ x^3=0 \end{array}$$

A representation such as the one on the right hand side is called a Gröbner basis (of the ideal generated by the equations).

We discuss the method of Gröbner bases, and an application of the method to the inverse kinematic problem in robotics.

Linear equations — elimination method of Gauss

For a system of linear equations we order the variables, e.g. $x > y > z$, and then successively eliminate higher variables from equations, i.e. eliminate under the diagonal. In this way the system is transformed to triangular form, from which we can read off the solution:

$$\begin{array}{rcl} 2x-y-z &=& 0 \\ x+2y-2z &=& 1 \\ x-y+2z &=& 2 \end{array} \quad \Longrightarrow \quad \begin{array}{rcl} x+2y-2z &=& 1 \\ y-5z &=& -4 \\ z &=& 1 \end{array}$$

So the solution is: $x = 1, y = 1, z = 1$

Univariate equations — Euclidean algorithm

We want to determine the common solutions of 2 polynomial equations in 1 variable:

$$f(x) = g(x) = 0.$$

The common solutions are the solutions of the greatest common divisor (gcd).

We compute the remainder of $f(x)$ on division by $g(x)$, i.e. $\mathrm{rem}(f, g) = h(x)$, and replace the pair (f, g) by (g, h). This leaves the greatest common divisor (gcd) unchanged:

$$\begin{array}{rrl} r_0 = & f = & x^4 + x^3 - x - 1 \\ r_1 = & g = & x^4 + x^2 - 2 \\ r_2 = & \mathrm{rest}(r_0, r_1) = & x^3 - x^2 - x + 1 \\ r_3 = & \mathrm{rest}(r_1, r_2) = & 3x^2 - 3 \\ r_4 = & \mathrm{rest}(r_2, r_3) = & 0 \end{array}$$

So $\gcd(f, g) = x^2 - 1$

The common solutions of $f(x) = g(x) = 0$ are the zeros of $\gcd(f, g)$, so $x = \pm 1$.

Multivariate non-linear equations — Gröbner bases

We consider systems of polynomial (algebraic) equations in several variables $x_1, \ldots, x_n$:

$$\begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0, \\ & & \vdots \\ f_m(x_1, \ldots, x_n) & = & 0. \end{array}$$

The collection of all linear combinations

$$\sum_{i=1}^{m} g_i \cdot f_i, \qquad \text{for } g_i \text{polynomials}$$

is called the **ideal** generated by $F = \{f_1, \ldots, f_m\}$. F is called a basis for this ideal. It is easy to see that the common solutions of F are the same as the common solutions of all the polynomials in the ideal generated by F.

We order the terms in these polynomials, for instance lexicographically:

$$1 < x < x^2 < \ldots < y < xy < x^2y < \ldots < y^2 < \ldots$$

or degree-lexicographically:

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < \ldots$$

so every polynomial $f(x_1, \ldots, x_n) \neq 0$ has a "leading power product" $\mathrm{lpp}(f)$ with a "leading coefficient" $\mathrm{lc}(f)$

Now we reduce higher terms in these polynomials. Let f, g, h be polynomials:

We say that f can be reduced to g modulo h,

$$f \longrightarrow_h g,$$

iff a multiple of the leading term of h, of the form $c \cdot t \cdot lpp(h)$, occurs in f, and

$$g = f - c \cdot t \cdot h.$$

Example: polynomials in $\mathbb{Q}[x, y]$, lexicographical term ordering with $x < y$:

$$2x^2y^2 + x^7y - 4 \quad \longrightarrow_{x^3y+y+x} \quad 2x^2y^2 - x^4y - x^5 - 4$$

This reduction is not unique, in general. We want to make it unique. In particular, we get non-uniqueness of reduction by reducing the least common multiple (lcm) of the leading power products of two polynomials in the basis $F = \{f_1, \ldots, f_m\}$:

$$g_i \longleftarrow_{f_i} \mathrm{lcm}(\mathrm{lpp(f_i)}, \mathrm{lpp(f_j)}) \longrightarrow_{\mathrm{f_j}} \mathrm{g_j}$$

Then $g_i - g_j$ is in the ideal generated by F, and it should be reducible to 0 if we would have uniqueness of reduction. These polynomials play an important role in the theory of Gröbner bases. For $f_i, f_j \in F$ we define:

$$\begin{aligned} \mathrm{spol}(f_i, f_j) &= g_i - g_j \quad \text{(as above)} \\ &= \tfrac{1}{\mathrm{lc(f_i)}} \cdot \tfrac{\mathrm{lcm(lpp(f_i),lpp(f_j))}}{\mathrm{lpp(f_i)}} \cdot f_i - \tfrac{1}{\mathrm{lc(f_j)}} \cdot \tfrac{\mathrm{lcm(lpp(f_i),lpp(f_j))}}{\mathrm{lpp(f_j)}} \cdot f_j \end{aligned}$$

$\mathrm{spol(f_i, f_j)}$ is called the **S-polynomial** of f_i, f_j.

For instance, for

$$f_i = 2x^2y^2 + x^7y - 4, \quad f_j = x^3y + y + x$$

we have

$$\mathrm{spol(f_i, f_j) = -y^2 + \frac{1}{2}x^8y - xy - 2x}$$

Definition: A (finite) set of polynomials $G = \{g_1, \ldots, g_n\}$ is a **Gröbner basis** (for the ideal generated by G) iff the reduction modulo the polynomials in G (in possibly several finitely many steps) is unique.

The following theorem makes the notion of Gröbner bases constructive.

Theorem: (Buchberger 1965): *A (finite) set of polynomials $G = \{g_1, \ldots, g_n\}$ is a Gröbner basis (for the ideal generated by G) iff all S-polynomials of G can be reduced to 0 modulo the polynomials in G (in possibly several finitely many steps).*

This leads to the following algorithm for constructing Gröbner bases.

Gröbner basis algorithm
For transforming a set of polynomials F into a Gröbner basis, we consider all S-polynomials, reduce them, and add the reduction result to the basis (if it is non-zero). We proceed in the same way with the enlarged basis, until all the S-polynomials are dealt with.
At the end of this process we interreduce the basis and eliminate 0 from the basis.

This process always terminates and upon termination yields a Gröbner basis for the input ideal. Obviously this process does not change the set of solutions, since the ideal remains unchanged. From a Gröbner basis (w.r.t. a lexicographic term ordering) we can "read off" the solutions of the system.

Example: We compute a Gröbner basis for the system of equations (actually for the polynomials on the left hand sides)

$$f_1(x, y) = f_2(x, y) = 0,$$

where

$$f_1 = x^2y^2 + y - 1, \quad f_2 = x^2y + x.$$

We order the terms lexicographically with $x < y$.
$\mathrm{spol(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3}$ is irreducible, so $G := \{f_1, f_2, f_3\}$.
$\mathrm{spol(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4}$, so $G := \{f_1, f_2, f_3, f_4\}$.
$\mathrm{spol(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5}$, so $G := \{f_1, \ldots, f_5\}$.
All the other S–polynomials reduce to 0, so we get the Gröbner basis

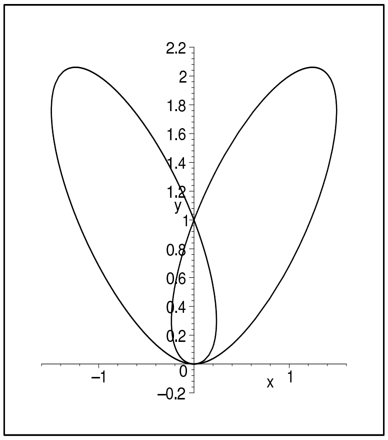
$$G = \{x^2y^2 + y - 1, x^2y + x, -xy + y - 1, y - 1, -x\}.$$

Obviously the only solution of these equations is

$$(x, y) = (0, 1). \qquad \Box$$

Example: Let us determine the singular points on an algebraic curve, namely the tacnode curve defined as the set of zeros of

$$f(x, y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4.$$



The singular points are those for which no unique tangent is defined. This means that both the defining polynomial and also its partial derivatives have to vanish at a singular point (as can be seen from Taylor expansion). So we want to solve the system of equations

$$\begin{aligned} f(x, y) &= 0 \\ \frac{\partial f}{\partial x}(x, y) &= 0 \\ \frac{\partial f}{\partial y}(x, y) &= 0 \end{aligned}$$

We use Maple 9.5 to transform these polynomials into a Gröbner basis:

```
> with(Groebner):
> f := 2*x^4-3*x^2*y+y^2-2*y^3+y^4;
```

$$f := 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

```
> gbasis({f,diff(f,x),diff(f,y)},plex(y,x));
```

$$[x^3, \; x\,y, \; 2y^2 - 2y + 3x^2]$$

From this basis transformation

$$\begin{array}{rcr} 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 & & 2y^2 - 2y + 3x^2 \\ 4x^3 - 3xy & \Longrightarrow_{\text{GB.Alg.}} & xy \\ 4y^3 - 3x^2 - 6y^2 + 2y & & x^3 \end{array}$$

we read off the singularities: $(0, 0)$ and $(0, 1)$. $\Box$