C5 – Syzygies, Elimination, Sylvester resultant

1) Computing syzygies of an ideal

- Suppose given an ideal $I = (f_1, \dots, f_m) \subset k[x_1, \dots, x_n] =: R$

For computing the 1st step of a F.F.R. of I one needs to compute the syzygies of I:

$$Syz(I) := \{ (h_1, \dots, h_m) \mid \sum h_i f_i = 0 \} \subset R^m$$

$$0 \to Syz(I) \to R^m \xrightarrow{f_1 \dots f_m} R \to \frac{R}{I} \to 0$$

Actually, what we need is a generating set of $Syz(I) \subset R^m$.

- Let $G = \{ g_1, \dots, g_s \}$ be a G.B. of $I = (g_1, \dots, g_s)$.

$$S(g_i, g_j) = \frac{x^\gamma}{LT(g_i)} g_i - \frac{x^\gamma}{LT(g_j)} g_j \qquad x^\gamma = LCM\left(LM(g_i), LM(g_j)\right)$$

Since G is a G.B. these S-pairs reduce to 0. Hence, by the division algorithm we get:

$$S(g_i, g_j) = \sum_{k=1}^{s} a_{ijk} g_k, \qquad a_{ijk} \text{ polynomials.}$$

Now, set $a_{ij} := a_{ij1} e_1 + \dots + a_{ijs} e_s \in R^s = \bigoplus_{i=1}^{s} R e_i$

and $s_{ij} := \frac{x^\gamma}{LT(g_i)} e_i - \frac{x^\gamma}{LT(g_j)} e_j - a_{ij} \quad \forall i \neq j$

THM (Schreyer): The set $\{s_{ij}, 1 \le i,j \le s\}$ for a generating set of $Syz(I)$ as an R-module.

Proof: See C.-L.-O. (technical).

$\rightsquigarrow$ Buchberger's algorithm, with a slight modification, gives

$$R^N \xrightarrow{\begin{pmatrix} \cdots & \hat{s_{ij}} & \cdots \end{pmatrix}} R^s \xrightarrow{(g_1 \dots g_s)} R \to \frac{R}{I} \to 0$$

To continue this process to get a F.F.R, we need to compute the syzygies of a submodule of R^s, not only a submodule of R (i.e. an ideal).

2) Gröbner basis for modules

Goal: shortly introduce G.B. for submodules $M \subset R^m$ $R = k[x_1 \dots x_n]$

Typical questions: - Given $M \subset R^m$ and $f \in R^m$, determine if $f \in M$.

- Given $\{f_1, \dots, f_s\} \subset R^m$, find a set of generators for the syzygy $Syz(f_1, \dots, f_s) \subset R^s$

Extending Gröbner basis to modules requires three things: define monomial orders, construct a division algo, get a Buchberger-like algorithm.

• Monomial orders.

- a monomial $m \in R^m = \bigoplus_{i=1}^{m} R e_i$ is an elt of the form $x^\alpha e_i$
- Every $f \in R^m$ can be written as $\sum_{i=1}^{\ell} c_i m_i$, $c_i \in k$.

$$\left(f = \begin{pmatrix} 5x \\ 2y \\ x+3z \end{pmatrix} = 5x e_1 + 2y e_2 + x e_3 + 3z e_3 \right)$$

- Let $m = x^\alpha e_i$ and $n = x^\beta e_j$.

$$n \mid m \iff i = j \text{ and } x^\beta \mid x^\alpha$$

and if n/m then $m/n = x^\alpha / x^\beta \in R$.

- $GCD(m,n) = \begin{cases} 0 \text{ if } i \neq j \\ GCD(x^\alpha, x^\beta) \cdot e_i \text{ if } i = j \end{cases}$ $\quad LCM(m,n) = \begin{cases} 0 \text{ if } i \neq j \\ LCM(x^\alpha, x^\beta) e_i \text{ if } i = j \end{cases}$

- An ordering relation $>$ on the monomials of R^m is a monomial ordering if:
  - $>$ is a total order
  - $m, n \in R^m$, $m > n \Rightarrow x^\alpha m > x^\alpha n \quad \forall x^\alpha \in R$
  - $>$ is well-ordering

(very similar to the previous case where $m = 1$).

- We can get monomial orders on R^n by extending monomial order of R as follows:
  First order the entries in a column: $e_1 > e_2 > \cdots > e_m$
  Then, let $>$ be a monomial order on R:
  - TOP-extension: $x^\alpha e_i > x^\beta e_j$ if $x^\alpha > x^\beta$, or if $x^\alpha = x^\beta$ and $i < j$
  - POT-extension: $x^\alpha e_i > x^\beta e_j$ if $i < j$, or if $i = j$ and $x^\alpha > x^\beta$

Now, any $f \in R^m$ is such that $f = \sum_{i=1}^{\ell} c_i m_i$, $m_1 > m_2 > \cdots$
and one can define $LT(f) = c_1 m_1$, $LM(f) = m_1$.

- Division algorithm

Let $\{f_1,\dots,f_s\}$ be a s-tuple of elts in R^m. Then every $f \in R^m$ can be written as

$$f = a_1 f_1 + \dots + a_s f_s + r, \quad a_i \in R, r \in R^m$$

where
- $\langle LM(f) \rangle \not\in \langle LM(a_i f_i) \rangle \ \forall i$
- $r = 0$ or r is a k-linear combination of monomials none of which is divisible by any $LM(f_i)$.

(Same proof as in the case $m=1$).

- Grobner Bases Definition

Let M be a submodule of R^m and $>$ a monomial order.

Let $\langle LT(M) \rangle$ the monomial sub-module generated by the leading terms of all $f \in M$

Def: A finite set $\{g_1,\dots,g_s\} \subset M \subset R^m$ is called a G.B. for M if $\langle LT(M) \rangle = \langle LT(g_1),\dots,LT(g_s) \rangle$.

Proposition: Let $G := \{g_1,\dots,g_s\}$ be a G.B. for a submodule $M \subset R^m$ and let $f \in R^m$:
i) $f \in M \iff$ the remainder of the division by G is 0
ii) G generates M as a module.

Finally G.B. do exist for all submodule of R^m.

Rk: minimal and reduced G.B. can be defined as well.

- S-pairs

Fix a monomial order on R^m and let $f, g \in R^m$.

$$S(f,g) = \frac{m}{LT(f)} f - \frac{m}{LT(g)} g \quad \text{where } m = LCM(LT(f), LT(g)).$$

Example: $f = \begin{pmatrix} xy - x \\ x^3 + y \end{pmatrix}$, $g = \begin{pmatrix} x^2 + 2y^2 \\ x^2 - y^2 \end{pmatrix}$ in $k[x,y]^2$, using POT on $k[x,y]$.

$LT(f) = xy e_1 \quad LT(g) = x^2 e_1 \quad LCM(f,g) = x^2 y e_1$

$S(f,g) = xf - yg = \begin{pmatrix} -x^2 - 2y^3 \\ x^4 - x^2 y + xy + y^3 \end{pmatrix}$.

- Buchberger's criterion and algorithm

THM: A set $G = \{g_1, \dots, g_s\} \subset R^m$ is a G.B. for the module M if it generates iff all S-pairs reduce to zero.

(essentially same proof).

⇒ Same algorithm to build a G.B.

3) Computing F.S.R.

We proceed as in 1) to compute syzygies of a submodule $M \subset R^m$.

Let $G = \{g_1, \dots, g_s\}$ be a G.B. of M. The S-pairs reduce to zero and hence we have

$$S(g_i, g_j) = \sum a_{ijk} g_k$$

which gives a syzygy (as in 1)) denoted by s_{ij}.

Thm (Schreyer) Let $G := \{g_1, \dots, g_s\}$ be a G.B.. The set of S_{ij} syzygies form a G.B. for the syzygy module $\mathrm{Syz}(g_1, \dots, g_s)$.

[See Cox-Little-O'Shea, Chapter 5, Using alg. geom.].

From there, one can compute F.F.R. iteratively. (up to change of basis matrices if one want to keep a specific list of generators instead of a G.B. - see CLO, Chapter 5).

4) Projection and elimination.

Another application of G.B. is solving polynomial systems of equations. The idea is to project down to a lower dimensional space, solve and then lift the solutions. This approach is similar to Gaussian elimination for linear system. It can be done for polynomial systems as follows.

Def: Let $I \subseteq k[x_1, \dots, x_n] = R$ an ideal. The m^{th} elimination ideal ${}_mI$ of I is: ${}_mI = I \cap k[x_{m+1}, \dots, x_n]$.

Geometrically, consider the projection

$$\mathbb{A}^n \xrightarrow{\Pi_m} \mathbb{A}^{n-m}$$

$$(a_1, \dots, a_n) \longrightarrow (a_{m+1}, \dots, a_n)$$

The projection of a variety is not necessarily a variety, but one can consider its closure (Zariski topology).

THM: Assume k is alg. closed field, then

$$\overline{\pi_m(V(I))} = V({}_mI)$$

Proof: $\subseteq$ let $(a_{m+1}, \dots, a_n) \in \pi_m(V(I))$; $\exists\, (a_1 \dots a_n) \in V(I)$: $\pi_m(a_1, \dots, a_n) = (a_{m+1}, \dots, a_n)$

let $f \in {}_m(I)$. Since $f \in I$, $f(a_1, \dots, a_n) = 0$

But $f \in k[x_{m+1}, \dots, x_n]$ so $f(a_{m+1}, \dots, a_n) = 0$
$\quad\quad = f(\pi_m(a_1, \dots, a_n))$

hence $\pi_m(V(I)) \subseteq V({}_m(I))$

$\supseteq$ We show that $I(\pi_m(V(I))) \subseteq I(V({}_mI))$, which gives the result by passing to varieties.

Let $g \in I(\pi_m(V(I))) \subset R = k[x_1, \dots, x_n]$ (seen as a poly. in R).

It vanishes on $V(I)$, so $g^p \in I$, but also $g^p \in k[x_{m+1}, \dots, x_n]$

so $g^p \in {}_mI$, so $g \in \sqrt{{}_mI} = I(V({}_m I))$. $\square$

Now, it remains to compute ${}_mI$.

THM: Let $I \subseteq k[x_1 \dots x_n]$ and let $G = \{g_1, \dots, g_s\}$ be a G.B. for I w.r.t. lex order $x_1 > x_2 > \dots > x_n$. Then

${}_mG := G \cap k[x_{m+1}, \dots, x_n]$ is a G.B. for ${}_mI$.

Proof: It is clear that ${}_mG \subseteq {}_mI$.

Pick $f \in {}_mI$: $f = \sum h_i g_i$ using div. algo. And since we used lex order then all g_i's that appear must be in ${}_mI$.

So ${}_mI = ({}_mG)$. It remains to show that S-pairs reduce to zero, but this is automatic as G is a G.B $\square$

A classical application is to compute equations of the image of a polynomial map. ⇝ M2 file

We will now devise tools for dealing with this question.

More precisely, we consider the implicitization of rational plane curves:

Given a map $\mathbb{P}^1 \longrightarrow \mathbb{P}^2$, $(s:t) \dashrightarrow (f_0 : f_1 : f_2)$ $\left(\mathbb{A}^1 \dashrightarrow \mathbb{A}^2,\ t \to \left(\frac{\tilde{f}_1}{\tilde{f}_0}(t), \frac{\tilde{f}_2}{\tilde{f}_0}(t) \right) \right)$

such that the image is a curve $\mathcal{C}$, compute an implicit equation of $\mathcal{C}$, say $F(x_0, x_1, x_2) = 0$ (of minimal degree).

This pb has a long history. It can be solved via G.B. but this is not satisfactory for many practical applications. More interesting approaches are based on resultant matrices.

4) Sylvester resultant

Let $f = a_0 s^m + \dots + a_m t^m$ and $g = b_0 s^n + \dots + b_n t^n$ be hom. polynomials in $A[s,t]$ (A is a comm. ring). We define

$$Syl_v(f,g) := \begin{pmatrix} a_0 & 0 & \vdots & b_0 & 0 \\ | & \ddots & a_0 & | & \ddots & b_0 \\ a_m & & | & b_n & & | \\ 0 & \ddots & a_m & 0 & \ddots & b_n \end{pmatrix} \begin{matrix} \uparrow \\ m+n \\ \downarrow \end{matrix}, \quad \text{equivalently}$$

$$\underbrace{\quad}_{n} \qquad \underbrace{\quad}_{m}$$

$$\left(s^{m+n-1} \quad s^{m+n-2} t \quad \dots \quad t^{m+n-1} \right) Syl(f,g) = \left(s^{n-1} f \ \dots \ t^{n-1} f \ s^{m-1} g \ \dots \ t^{m-1} g \right).$$

It is called the Sylvester matrix of f, g of degree m, n.

More abstractly, $Syl(f,g)$ is the matrix of the map

$$\left[\begin{array}{ccc} A[s,t](-m) \oplus A[s,t](-n) & \xrightarrow{\Psi} & A[s,t] \\ u \quad\quad v & \longmapsto & uf+vg \end{array}\right]_{m+n-1}$$

in canonical bases.

Def: The Sylvester resultant is defined as

$$\boxed{Res(f,g) := det\left(Syl(f,g)\right) \in A.}$$

Proposition: Assume that A is a domain. TFAE:

i) $Res(f,g) \neq 0$

ii) Ψ is injective

iii) f and g are coprime in $Frac(A)[s,t]$
(which means no common root in $\mathbb{P}^1_{Frac(A)}$).

Moreover, if A is a field then

$$\boxed{corank\left(Syl(f,g)\right) = deg\left(gcd(f,g)\right).}$$

Proof: exercice.

- Coming back to our problem, we have

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^2 \\ (s:t) & \longmapsto & (f_0:f_1:f_2) \end{array}$$

f_i hom. pol. of degree $d \geq 1$; $gcd(f_i)=1$
defining a curve of degree d: $C(x_0,x_1,x_2)$

We have $Res\left(f_1(s,t)-x_1 f_0(s,t),\ f_2(s,t)-x_2 f_0(s,t)\right)$

$$= C(1,x_1,x_2)^{deg(\phi)}.$$

where $deg(\phi)$ is the number of pre-images of a general point a the curve.

Notice that it is clear that $V(Res(-)) = V(C(1, x_1, x_2))$.

Example: circle $\mathbb{P}^1 \to \mathbb{P}^2$

$(s:t) \mapsto (s^2+t^2 : s^2-t^2 : 2st)$ $\quad \left(t \mapsto \frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$

$$(s^2-t^2) - x_1(s^2+t^2) = s^2(1-x_1) + t^2(-1-x_1) = 0$$

$$2st - x_2(s^2+t^2) = s^2(-x_2) + 2st + t^2(-x_2) = 0$$

$$Syl(-,-) = \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cc|cc} \text{s.f} & \text{tf.} & \text{sg} & \text{tg} \end{array} \\ \left(\begin{array}{cc|cc} 1-x_1 & 0 & -x_2 & 0 \\ 0 & 1-x_1 & 2 & -x_2 \\ \hline -1-x_1 & 0 & -x_2 & 2 \\ 0 & -1-x_1 & 0 & -x_2 \end{array}\right) \end{array} \begin{array}{c} s^3 \\ s^2t \\ st^2 \\ t^3 \end{array}$$

$$\det = 4(x_1^2+x_2^2-1).$$

We notice that the size of Syl here is $2d \times 2d$, whereas we expect something of degree d (actually $d = \deg(\mathbb{P}) \cdot \deg(\mathbb{C})$).

It turns out that

$$Res(x_0 f_1 - x_1 f_0, x_0 f_2 - x_2 f_0) = \underbrace{x_0^d}_{\text{hidden extraneous factor}} C(x_0, x_1, x_2)^{\deg(\mathbb{P})}$$