Let us consider

an infinite, perfect field k, where, if $p := \mathrm{char}(k) \neq 0$, it is possible to extract pth roots,

the algebraic closure k of k,

the polynomial ring $\mathcal{P} := k[X_1, \ldots, X_n]$,

its k-basis $\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}$;

an ideal $\mathsf{I} := (F) := \mathbb{I}(F) := \{\sum_{i=1}^{u} h_i f_i : h_i \in \mathcal{P}\} \subset \mathcal{P}$ given by

a finite basis $F := \{f_1, \ldots, f_u\} \subset \mathcal{P}$,

the algebraic affine variety $\mathcal{Z}(\mathsf{I}) := \{\mathsf{a} \in \mathsf{k}^n : f(\mathsf{a}) = 0,$ for each $f \in F\} \subset \mathsf{k}^n$.

Each polynomial $f \in k[X_1, \ldots, X_n]$ is therefore a unique linear combination

$$f = \sum_{t \in \mathcal{T}} c(f, t) t$$

of the terms $t \in \mathcal{T}$ with coefficients $c(f, t)$ in k; the support

$$\mathrm{supp}(f) := \{t \in \mathcal{T} : c(f, t) \neq 0\}$$

of f being finite, once a term ordering $<$ on $\mathcal{T}$ is fixed, f has a unique representation as an ordered linear combination of terms:

$$f = \sum_{i=1}^{s} c(f, t_i) t_i : c(f, t_i) \in k \setminus 0, t_i \in \mathcal{T}, t_1 > \cdots > t_s;$$

the *maximal term* of f is $\mathbf{T}(f) := t_1$, its *leading coefficient* is $\mathrm{lc}(f) := c(f, t_1)$ and its *maximal monomial* is $\mathbf{M}(f) := c(f, t_1) t_1$.

For any set $F \subset \mathcal{P}$ we denote

- $\mathbf{T}_<\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{T}_<(F) := \{\tau \mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$;
- $\mathbf{N}_<(F) := \mathcal{T} \setminus \mathbf{T}_<(F)$;
- $k[\mathbf{N}_<(F)] := \mathrm{Span}_k(\mathbf{N}_<(F))$

and we will usually omit the dependence on $<$ if there is no ambiguity.

Let us fix any term-ordering $<$ on $\mathcal{T}$ and let us compute a Gröbner basis $G \subset \mathsf{I}$ of I w.r.t. $<$.

Then it holds

- $\mathcal{Z}(\mathsf{I}) = \emptyset \iff 1 \in \mathsf{I} \iff 1 \in G$;
- $\mathcal{Z}(\mathsf{I})$ is infinite iff $\mathbf{N}(\mathsf{I})$ is an infinite dimensional k-vector space iff there exists i such that for each $d \in \mathbb{N} : X_i^d \notin \mathbf{T}(G) = T(\mathsf{I})$;
- $\mathcal{Z}(\mathsf{I})$ is finite iff $\mathbf{N}(\mathsf{I})$ is finite iff for each i there exists $d_i \in \mathbb{N} : X_i^{d_i} \in \mathbf{T}\{G\} \subset \mathbf{T}(\mathsf{I})$; moreover, in this case and under the assumption that I is radical, we have $\#\mathcal{Z}(\mathsf{I}) = \#\mathbf{N}(\mathsf{I})$.

Definition. *Let $\mathcal{P} := k[X_1, \ldots, X_n]$ and let $\mathfrak{f} \subset \mathcal{P}$ be an ideal.*

A subset $\{X_{i_1}, \ldots, X_{i_d}\}$ of d variables for which it holds

$$\mathfrak{f} \cap k[X_{i_1}, \ldots, X_{i_d}] = (0)$$

is called a set of independent variables *for* $\mathfrak{f}$.

If, for each $j \notin \{i_1, \ldots, i_d\}$ it holds

$$\mathfrak{f} \cap k[X_{i_1}, \ldots, X_{i_d}, X_j] \neq (0)$$

$\{X_{i_1}, \ldots, X_{i_d}\}$ *is called a* maximal set of independent variables. □

Lemma (Kredel–Weispfenning)**.** *Let*

$$\mathfrak{f} \subset k[X_1, \ldots, X_n]$$

be an ideal, $<$ be any termordering and $\mathbf{T}_<(\mathfrak{f})$ the corresponding monomial ideal.

If $\{X_{i_1}, \ldots, X_{i_d}\}$ is a set of variables such that $\mathbf{T}_<(\mathfrak{f}) \cap k[X_{i_1}, \ldots, X_{i_d}] = \emptyset$ then $\mathfrak{f} \cap k[X_{i_1}, \ldots, X_{i_d}] = (0)$.

Proof. If exists $f \in \mathfrak{f} \cap k[X_{i_1}, \ldots, X_{i_d}], f \neq 0$, then $\mathbf{T}_<(f) \in \mathbf{T}_<(\mathfrak{f}) \cap k[X_{i_1}, \ldots, X_{i_d}]$. □

Corollary (Kredel–Weispfenning). *Let $\mathfrak{f} \subset k[X_1, \dots, X_n]$ be an ideal, $<$ be any termorderingand $\mathbf{T}_<(\mathfrak{f})$ the corresponding monomial ideal.*

Let $\{X_{i_1}, \dots, X_{i_d}\}$ be a maximal set of independent variables for $\sqrt{\mathbf{T}_<(\mathfrak{f})}$; then

- $\dim(\mathfrak{f}) = d$,
- $\{X_{i_1}, \dots, X_{i_d}\}$ *is a maximal set of independent variables for* $\mathfrak{f}$.

Proof. One has $\dim(\sqrt{\mathbf{T}_<(\mathfrak{f})}) = \dim(\mathbf{T}_<(\mathfrak{f}))$ and $\{X_{i_1}, \dots, X_{i_d}\}$ is a maximal set of independent variables for $\sqrt{\mathbf{T}_<(\mathfrak{f})}$ iff it is a maximal set of independent variables for $\mathbf{T}_<(\sqrt{\mathfrak{f}})$.

Then, by the lemma above, $\{X_{i_1}, \dots, X_{i_d}\}$ is a set of independent variables for $\mathfrak{f}$, and it is also maximal because $\dim(\mathbf{T}_<(\mathfrak{f})) = \dim(\mathfrak{f})$ since they share the same Hilbert polynomial. □

Then, we can re-enumerate and re-label the variables as

$$\{X_1, \dots, X_n\} = \{V_1, \dots, V_d, Z_1, \dots, Z_r\}, \quad \{X_{i_1}, \dots, X_{i_d}\} = \{V_1, \dots, V_d\},$$

so that

$$\mathsf{I} \cap k[V_1, \dots, V_d] = (0)$$

and consider

the field $K := k(V_1, \dots, V_d)$,

its algebraic closure K

the polynomial ring $\mathcal{Q} := K[Z_1, \dots, Z_r]$,

its K-basis $\mathcal{W} := \{Z_1^{a_1} \cdots Z_r^{a_r} : (a_1, \dots, a_r) \in \mathbb{N}^r\}$;

the zero-dimensional ideal $\mathsf{J} := \mathsf{I}^e := \mathsf{I}K[Z_1, \dots, Z_r]$

and the unmixed ideal $\mathsf{J}^c := \mathsf{J} \cap \mathcal{P}$.

Then, if $\mathsf{I} = \cap_{i=1}^{\mathsf{t}} \mathfrak{q}_i$ denotes any irredundant primary representation in $\mathcal{P}$, and we wlog assume that the primaries are ordeded so that, for a suitable value $1 \le \mathsf{r} \le \mathsf{t}$,

$\{X_{i_1}, \dots, X_{i_d}\}$ is a maximal set of independent variables for $\mathfrak{q}_i \iff i \le \mathsf{r}$,

then

$$\mathsf{J} := \mathsf{I}^e = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i^e = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i \mathcal{Q}$$

is an irredundant primary representation in $\mathcal{Q}$ and

$$\mathsf{J} \cap \mathcal{P} =: \mathsf{J}^c = \mathsf{I}^{ec} = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i \subset \mathcal{P}$$

is an irredundant primary representation.

Moreover, the (GTZ, ARGH, CCC)-schemes allow to compute unmixed ideals $\mathfrak{a}_j \subset \mathcal{P}$ giving a decomposition

$$\sqrt{\mathsf{I}} = \sqrt{\mathsf{J}^c} \bigcap \left(\bigcap_j \sqrt{\mathfrak{a}_j} \right).$$

Thus solving the ideal $\mathsf{I} \subset \mathcal{P}$ is reduced, via Gröbner technique, to solving each unmixed (GTZ, ARGH, CCC)-component and solving each such component is reduced to solving the related zero-dimensional extension ideal.

Trinks' Algorithm

Thus we are reduced to consider a zero-dimensional ideal

$$\mathsf{J} \subset \mathcal{Q} := K[Z_1, \dots, Z_r]$$

which we assume to be given via a Gröbner basis $G_\prec$ w.r.t. the lexicographical ordering $\prec$ induced on $\mathcal{W}$ by $Z_1 \prec Z_2 \prec \dots \prec Z_r$:

$$Z_1^{a_1} \dots Z_r^{a_r} \prec Z_1^{b_1} \dots Z_r^{b_r} \iff \text{exists } j : a_j < b_j \text{ and } a_i = b_i \text{ for } i > j.$$

Corollary. *If $\mathsf{I} \subset k[X_1, \dots, X_n]$ is an ideal and G is a Gröbner basis of I w.r.t. the lexicographical ordering$\prec$ then for each $i, 1 \le i \le n$, $G_i := G \cap k[X_1, \dots, X_i]$ is a Gröbner basis of $\mathsf{I} \cap k[X_1, \dots, X_i]$.* □

Then, if we denote, for $i, 1 \le i < r$,

$\mathsf{J}_i := \mathsf{J} \cap K[Z_1, \dots, Z_i]$,

$\pi_i : \mathsf{K}^r \to \mathsf{K}^i$ the canonical projection $\pi_i(a_1, \dots, a_r) = (a_1, \dots, a_i)$,

$G_i := G_\prec \cap K[Z_1, \dots, Z_i]$,

we have, for each i

1. $\mathcal{Z}(\mathsf{J}_i) = \pi_i(\mathcal{Z}(\mathsf{J})) = \{(a_1, \dots, a_i) : (a_1, \dots, a_r) \in \mathcal{Z}(\mathsf{J})\}$,
2. G_i is the reduced lexicographical Gröbner basis of J_i.

In particular, there is a unique polynomial $f(Z_1) \in K[Z_1]$, such that

$$\mathsf{J}_1 = (f) \text{ and } \{f\} = G_\prec \cap K[Z_1].$$

For each $\alpha := (a_1, \dots, a_{i-1}) \in \mathsf{K}^{i-1}$, denote $\Phi_\alpha : K[Z_1, \dots, Z_i] \to \mathsf{K}[T]$ the projection defined by

$$\Phi_\alpha(f) = f(a_1, \dots, a_{i-1}, T) \text{ for each } f \in K[Z_1, \dots, Z_i].$$

Theorem (Trinks)**.** *Let $\alpha := (a_1, \dots, a_{i-1}) \in \mathcal{Z}(\mathsf{J}_{i-1})$ and let $f \in \mathsf{K}[T]$ be a generator of the principal ideal $\Phi_\alpha(\mathsf{J}_i) \subset \mathsf{K}[T]$. Then, for each $b \in \mathsf{K}$*

$$(a_1, \dots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \iff f(b) = 0.$$

Proof. Let $h(Z_1, \dots, Z_i) \in \mathsf{J}_i$ be any polynomial such that

$$f(T) = \Phi_\alpha(h) = h(a_1, \dots, a_{i-1}, T).$$

Then

$$(a_1, \dots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \implies f(b) = h(a_1, \dots, a_{i-1}, b) = 0.$$

Conversely for any $g(Z_1, \dots, Z_i) \in \mathsf{J}_i$, $\Phi_\alpha(g) \in \Phi_\alpha(\mathsf{J}_i)$, so that

$$g(a_1, \dots, a_{i-1}, b) = \Phi_\alpha(g)(b) = 0 \text{ for each } g \in \mathsf{J}_i$$

and $(a_1, \dots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i)$. □

Figure 1: Trinks' Algorithm

$\mathsf{Z} := \textbf{Solve}(F, L)$

where

$F := (f_1, \dots, f_u) \subset \mathcal{Q} := K[Z_1, \dots, Z_r]$,
$L \supset K$ is a field extension of K,
$\mathsf{J} \subset \mathcal{Q}$ is the zero-dimensional ideal generated by F,
$\mathsf{Z} := \{\alpha_1, \dots, \alpha_\mathsf{s}\} = \mathcal{Z}(\mathsf{J}) \cap L^r$.

Compute the reduced lexicographical Gröbner basis G of $(f_1, \dots, f_u)$.

Let $p(Z_1)$ be the unique element in $G \cap K[Z_1]$,

$\mathsf{Z}_1 := \{a \in L : p(a) = 0\}$.

For $i = 2..r$ **do**

$\mathsf{Z}_i := \emptyset$;
For each $(a_1, \dots, a_{i-1}) \in \mathsf{Z}_{i-1}$ **do**
$H := \{g(a_1, \dots, a_{i-1}, Z_i) : g \in G_i \setminus G_{i-1}\}$,
$p := \gcd(H)$,
$\mathsf{Z} := \{a \in L : p(a) = 0\}$,
$\mathsf{Z}_i := \mathsf{Z}_i \cup \{(a_1, \dots, a_{i-1}, a) : a \in \mathsf{Z}\}$.

$\mathsf{Z} := \mathsf{Z}_r$

Gianni–Kalkbrener Algorithm

Remarking that each polynomial $f \in K[Z_1, \dots, Z_i]$ can be uniquely expressed as

$$f = \sum_{j=0}^{D} h_j(Z_1, \dots, Z_{i-1}) Z_i^j, h_D \neq 0,$$

we recall that the degree of f in the variable Z_i is denoted $\deg_{Z_i}(f) := \deg_i(f) := D$, and that $\mathrm{Lp}(f) := h_d$ is named the *leading polynomial* of f, while $Tp(f) = h_0$ the *trailing polynomial* of f. Observe that, for the lexicographical ordering $\prec$, we have $\mathbf{T}(f) = \mathbf{T}(\mathrm{Lp}(f)) Z_i^{\deg_i(f)}$.

We also denote, for each $i, 1 \leq i \leq r$, $\delta \in \mathbb{N}$,

$$G_i := \{g \in G, g \in K[Z_1, \dots, Z_i]\}$$

$$G_{i\delta} := \{g \in G, g \in K[Z_1, \dots, Z_i], \deg_i(g) \leq \delta\}$$

and remark that each $G_{i\delta}$ is a section of both $G_{i\delta+1}$ and G_i and that hold the obvious inclusions

$$G_{11} \subseteq G_{12} \subseteq \dots \subseteq G_1 \subseteq \dots \subseteq G_{i-1} \subseteq \dots \subseteq G_{i\delta} \subseteq G_{i\delta+1} \subseteq \dots \subseteq G_i \subseteq \dots$$

For each $i, 1 \leq i \leq r$, $\delta \in \mathbb{N}$, and each $F \subset \mathcal{Q}$, we denote

$$\mathrm{Lp}_{i\delta}(F) := \{\mathrm{Lp}(g), g \in F \cap K[Z_1, \dots, Z_i], \deg_i(g) \leq \delta\}.$$

Theorem (Gianni—Kalkbrener)**.** *Let $\mathsf{J} \subset \mathcal{Q}$ be an ideal, $\prec$ be the lexicographical ordering induced by $Z_1 \prec \cdots \prec Z_r$.*
Let $G := \{g_1, \dots, g_v\}$ be a Gröbner basis of J w.r.t. $\prec$, enumerated in such a way that

$$\mathbf{T}(g_1) \prec \mathbf{T}(g_2) \prec \dots \prec \mathbf{T}(g_{v-1}) \prec \mathbf{T}(g_v).$$

Then with the notation above:

1. *for each $i, i \leq r$, G_i is a Gröbner basis of J_i;*
2. *for each $i, 1 \leq i \leq r$, $\delta \in \mathbb{N}$, $\mathrm{Lp}_{i\delta}(G)$ is a Gröbner basis of $\mathrm{Lp}_{i\delta}(\mathsf{J})$;*
3. *for each $i, 1 \leq i \leq r$ and each $\alpha := (b_1, \dots, b_{i-1}) \in \mathcal{Z}(\mathsf{J}_{i-1})$, denoting*

   $\Phi_\alpha : \mathcal{Q} \to K[Z_i, \dots, Z_n] \quad f(Z) \to f(\alpha, Z_i, \dots, Z_n)$.
   σ the minimal value such that $\Phi_\alpha(\mathrm{Lp}(g_\sigma)) \neq 0$ and
   j, δ the value such that $g_\sigma \in G_{j\delta}$ so that

   $$g_\sigma = \mathrm{Lp}(g_\sigma) Z_j^{\delta+1} + \dots \in K[Z_1, \dots, Z_j] \setminus K[Z_1, \dots, Z_{j-1}]$$

   it holds

   (a) $j = i$,
   (b) *for each $g \in G_{i-1}, \Phi_\alpha(g) = 0$,*
   (c) *for each $g \in G_{i\delta}, \Phi_\alpha(g) = 0$,*
   (d) $\Phi_\alpha(g_\sigma) = \gcd(\Phi_\alpha(g) : g \in G_i) \in \mathsf{K}[Z_i]$,
   (e) *for each $b \in \mathsf{K}$,*

   $$(b_1, \dots, b_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \iff \Phi_\alpha(g_\sigma)(b) = 0.$$

Figure 2: Trink's Algorithm; Gianni—Kalkbrener improvement

$\mathsf{Z} := \textbf{Solve}(F, L)$

where

$F := (f_1, \dots, f_u) \subset \mathcal{Q} := K[Z_1, \dots, Z_r]$,

$L \supset K$ is a field extension of K,

$\mathsf{J} \subset \mathcal{Q}$ is the zero-dimensional ideal generated by F,

$\mathsf{Z} := \{\alpha_1, \dots, \alpha_\mathsf{s}\} = \mathcal{Z}(\mathsf{J}) \cap L^r$.

Compute the reduced lexicographical Gröbner basis G of $(f_1, \dots, f_u)$.

Sort $G := \{g_1, \dots, g_v\}$ by increasing maximal terms.

$\mathsf{Z}_1 := \{a \in L : g_1(a) = 0\}$,

%% g_1 is the unique element in $G \cap K[Z_1]$.

For $i = 2..r$ **do**

$\mathsf{Z}_i := \emptyset$;

$g := \min(g \in G_i \setminus G_{i-1})$.

For each $(a_1, \dots, a_{i-1}) \in \mathsf{Z}_{i-1}$ **do**

$h := g$,

While $\mathrm{Lp}(h)(a_1, \dots, a_{i-1}) = 0$ **do** $h := \textbf{Next}(h, G)$,

$p := h(a_1, \dots, a_{i-1}, Z_i)$,

%% $p = \gcd(H)$ for $H := \{g(a_1, \dots, a_{i-1}, Z_i) : g \in G_i \setminus G_{i-1}\}$,

$\mathsf{Z} := \{a \in L : p(a) = 0\}$,

$\mathsf{Z}_i := \mathsf{Z}_i \cup \{(a_1, \dots, a_{i-1}, a) : a \in \mathsf{Z}\}$.

$\mathsf{Z} := \mathsf{Z}_r$

Endomorphisms of an Algebra

Let $\mathcal{Q} := K[Z_1, \dots, Z_r]$, $\mathcal{W}$ its monomial K-basis and K the algebraic closure of K. In order to simplify the notation let us wlog assume $K = \mathsf{K}$ to be algebraically closed.

Let $\mathsf{J} \subset \mathcal{Q}$ be a zero-dimensional ideal, $\deg(\mathsf{J}) = s$, and $\mathsf{A} := \mathcal{Q}/\mathsf{J}$ the corresponding quotient algebra, which satisfies $\dim_K(\mathsf{A}) = s$.

For any $f \in \mathcal{Q}$, we will denote $[f] \in \mathsf{A}$ its residue class modulo J and Φ_f the endomorphism $\Phi_f : \mathsf{A} \to \mathsf{A}$ defined by

$$\Phi_f([g]) = [fg] \text{ for each } [g] \in \mathsf{A}.$$

Clearly $\Phi_f = \Phi_h$ iff $[f] = [h]$.

Definition.

1. *A* Gröbner representation *of* J *is the assignment of*
   - *a K-basis* $\mathbf{b} = \{[b_1], \dots, [b_s]\} \subset \mathsf{A}$ *and*
   - *the square matrices* $A_h := \left(a_{ij}^{(h)}\right) = M([Z_h], \mathbf{b})$ *for each* $h, 1 \le h \le s$,
2. *For each* $g \in \mathcal{Q}$ *the* Gröbner description *of g in terms of a Gröbner representation* $(\mathbf{b}, \{A_k\})$ *is the unique (row) vector*

$$\textbf{Rep}(g, \mathbf{b}) := (\gamma(g, b_1, \mathbf{b}), \dots, \gamma(g, b_s, \mathbf{b})) \in K^s$$

which satisfies

$$[g] = \sum_j \gamma(g, b_j, \mathbf{b})[b_j]$$

□

If we fix any K-basis $\mathbf{b} = \{[b_1], \dots, [b_s]\}$ of A so that $\mathsf{A} = \mathrm{Span}_K(\mathbf{b})$, then for each $g \in \mathcal{Q}$, there is a unique (row) vector, the *Gröbner description of* g,

$$\mathbf{Rep}(g,\mathbf{b}) := (\gamma(g,b_1,\mathbf{b}),\dots,\gamma(g,b_s,\mathbf{b})) \in K^s$$

which satisfies

$$[g] = \sum_j \gamma(g,b_j,\mathbf{b})[b_j]$$

and the endomorphism Φ_f is naturally represented by the square matrix

$$M([f],\mathbf{b}) = (\gamma(fb_i,b_j,\mathbf{b})) : \Phi_f(b_i) = [fb_i] = \sum_j \gamma(fb_i,b_j,\mathbf{b})[b_j].$$

An alternative way of representing a zero-dimensional ideal $\mathsf{J} \subset \mathcal{Q}$ and the related quotient algebra A is via its *dual space* (Section 28.1)

$$\mathfrak{L}(\mathsf{J}) := \{\ell \in \mathcal{Q}^* : \ell(g) = 0 \text{ for each } g \in \mathsf{J}\} \subset \mathcal{Q}^*$$

where $\mathcal{Q}^* := \mathrm{Hom}_K(\mathcal{Q},K)$ is the K-vectorspace consisting of all K-linear functionals $\ell : \mathcal{Q} \to K$.

Clearly we have $\dim_K(\mathfrak{L}(\mathsf{J})) = s$ and to each K-basis $\mathbb{L} := \{\lambda_1,\cdots,\lambda_s\}$ of $\mathfrak{L}(\mathsf{J})$ is associated a *Lagrange K-basis* $\mathbf{q} = \{[q_1],\dots,[q_s]\}$ which is *biorthogonal* to $\mathbb{L}$ *id est* $\lambda_i(q_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$

In particular, since, for each i,j,h,

$$\lambda_j(Z_h q_i) = \lambda_j\left(\sum_l a_{il}^{(h)} q_l\right) = \sum_l a_{il}^{(h)} \lambda_j(q_l) = a_{ij}^{(h)},$$

to each basis $\mathbb{L} := \{\lambda_1,\cdots,\lambda_s\}$ of $\mathfrak{L}(\mathsf{J})$ is associated the Gröbner representation

- $\mathbf{q} = \{[q_1],\dots,[q_s]\} \subset \mathsf{A} : \lambda_i(q_j) = \delta_{ij}$ for each i,j,
- $Q_h := (\lambda_j(Z_h q_i))_{ij}$.

Between the two bases $\mathbf{b}$ and $\mathbf{q}$ there are the basis transformations

$$M_{bq} := (\gamma(b_i,q_j,\mathbf{q})) \text{ and } M_{qb} := (\gamma(q_i,b_j,\mathbf{b}))$$

so that, for each i,

$$[b_i] = \sum_j \gamma(b_i,q_j,\mathbf{q})[q_j] \text{ and } [q_i] = \sum_j \gamma(q_i,b_j,\mathbf{b})[b_j];$$

naturally, we have $M_{bq} = M_{qb}^{-1}$, and

$$M([f],\mathbf{b}) = M_{bq} M([f],\mathbf{q}) M_{qb} = M_{bq} M([f],\mathbf{q}) M_{bq}^{-1}$$

so that $M([f],\mathbf{q})$ and $M([f],\mathbf{b})$ are similar and share the same eigenvalues and Jordan normal form.

Toward Auzinger–Stetter's Theorem

With the same notation as in the previous section let us fix

- a Gröbner representation

$$\mathbf{b} = \{[b_1],\dots,[b_s]\} \subset \mathsf{A}, A_h := \left(a_{ij}^{(h)}\right) = M([Z_h],\mathbf{b}), 1 \le h \le r;$$

- a basis $\mathbb{L} := \{\lambda_1,\cdots,\lambda_s\}$ of $\mathfrak{L}(\mathsf{J})$;
- the conjugate Gröbner representation

$$\mathbf{q} = \{[q_1],\dots,[q_s]\} \subset \mathsf{A}, Q_h := (\lambda_j(Z_h q_i))_{ij},$$

  where $\mathbf{q}$ is the Lagrange basis satisfying $\lambda_i(q_j) = \delta_{ij}$ for each i,j,

and let us denote

- $M_{bq} := (\gamma(b_i,q_j,\mathbf{q}))$ and $M_{qb} := (\gamma(q_i,b_j,\mathbf{b}))$ the basis transformation matrices;
- J_h the Jordan normal form matrix for A_h;
- for each $f \in \mathcal{Q}/\mathsf{J} = \mathsf{A}$

$$A_f := M([f],\mathbf{b}) = (\gamma(fb_i,b_j,\mathbf{b})) : \Phi_f(b_i) = [fb_i] = \sum_j \gamma(fb_i,b_j,\mathbf{b})[b_j];$$

- J_f the Jordan normal form matrix for A_f.

Let us also consider the set
$$\mathcal{Z}(\mathsf{J}) := \{\alpha \in K^r : f(\alpha) = 0 \text{ for each } f \in \mathsf{J}\}.$$

Lemma (Auzinger–Stetter)**.** *With the present notation it holds*
$$\gamma(b_i, q_j, \mathbf{q}) = \lambda_j(b_i), 1 \le i, j \le s.$$

Proof. For each $f \in \mathsf{A}$, $\sum_j \gamma(f, q_j, \mathbf{q})[q_j] = f = \sum_j \lambda_j(f)[q_j]$.

The first equality follows from the definition of γ, the second from the property of the Lagrange basis. The claim then follows by the linear independency of $\mathbf{q}$. □

Corollary. *Each i^{th} row of M_{bq} is the vector $(\lambda_1(b_i), \dots, \lambda_s(b_i))$ of the evaluation of the basis element b_i at the functional basis $\mathbb{L}$.*

Each j^{th} column of M_{bq} is the vector $(\lambda_j(b_1), \dots, \lambda_j(b_s))^T$ of the evaluation of the basis $\mathbf{b}$ at the functional λ_j. □

Lemma (Auzinger–Stetter)**.** *For each $\alpha \in \mathcal{Z}(\mathsf{J})$ the vector*
$$(b_1(\alpha), \dots, b_s(\alpha))^T$$
is an eigenvector of the matrix A_f for the eigenvalue $f(\alpha)$.

Proof. For each $i, 1 \le i \le s$, we have $[fb_i] = \Phi_f([b_i]) = \sum_j \gamma(fb_i, b_j, \mathbf{b})[b_j]$ so that $f(\alpha)b_i(\alpha) = \sum_j \gamma(fb_i, b_j, \mathbf{b})b_j(\alpha)$. Thus the claim follows trivially. □

Definition. *A matrix is called* non-derogatory *if, equivalently,*

all its eigenspaces have dimension 1;

its Jordan form has a single Jordan block associated with each eigenvalue. □

Theorem (Auzinger–Stetter)**.** *The set $\{f(\alpha) : \alpha \in \mathcal{Z}(\mathsf{J})\}$ is the set of eigenvalues of A_f. If A_f is non-derogatory, each eigenspace of A_f for $f(\alpha)$ is spanned by $(b_1(\alpha), \dots, b_s(\alpha))^T$.*

Proof. A direct consequence of the Lemmata above. □

Auzinger–Stetter: The Radical case

The relevant aspect of Auzinger–Stetter's Theorem is that while both eigenvalues and eigenvectors of A_f intrinsecally depend on the roots of J their actual values are precise functions of the choice of the matrix A_f and of the basis $\mathbf{b}$; one can therefore expects that for a proper choice of f and $\mathbf{b}$ an eigenvalue computation can allow to deduce the roots of J.

Let us assume that J is radical and see whether the remark above leads to something.

The radicality assumption implies that J has $s = \deg(\mathsf{J})$ different roots in K^r:
$$\mathcal{Z}(\mathsf{J}) = \{\alpha_1, \dots, \alpha_s\} \subset K^r, \quad \alpha_j = (a_1^{(j)}, \dots, a_r^{(j)}).$$

Thus we can wlog identify each functional λ_j with the evaluation at the root α_j:
$$\lambda_j : \mathcal{Q} \to K, p(Z_1, \dots, Z_r) \mapsto \lambda_j(p) = p(a_1^{(j)}, \dots, a_r^{(j)})$$
and $\mathbf{q}$ is the corresponding Lagrange basis.

A matrix A_f is non-derogratory if and only if $f(\alpha_i) \ne f(\alpha_j)$ for each $i \ne j$. Clearly for a generic linear form $Y = \sum_h c_h Z_h$, A_Y is non-derogatory. Thus if we choose a linear form which *separates* $\mathcal{Z}(\mathsf{J})$ *id est* it satisfies the condition

(AS.1) $Y = \sum_h c_h Z_h$ is such that $\beta_i := \sum_h c_h a_h^{(i)} \ne \sum_h c_h a_h^{(j)} =: \beta_j$ for each $i \ne j$

then A_Y is non-derogatory and have s distinct eigenvalues
$$\beta_j := \sum_h c_h a_h^{(j)}, 1 \le j \le s$$
whose associated eigenspaces are generated by
$$(b_1(\alpha_j), \dots, b_s(\alpha_j))^T.$$

In order to deduce the α_js from these eigenvectors, the trick consists in a clever choice of the basis $\mathbf{b}$. The efficient choice is the original one proposed by Auzinger–Stetter: let us denote V the K-vectorspace
$$V := \mathrm{Span}_K\{[1], [Z_1], \dots [Z_r]\}$$
and let $\delta := \dim_K(V) \le s$; then, up to reenumerating the variables, we can wlog assume that

- $V = \mathrm{Span}_K\{[1], [Z_1], \dots [Z_{\delta-1}]\}$
- $\{[1], [Z_1], \dots [Z_{\delta-1}]\}$ is a K-basis of V,
- there are $c_{il} \in K, 0 \le l < \delta \le i \le r$ such that $[Z_i] = c_{i0} + \sum_{l=1}^{\delta-1} c_{il}[Z_l]$.

Moreover, the knowledge of the matrices A_h allows to deduce, by easy linear algebra, both δ and the c_{il}s.
We can therefore choose a basis $\mathbf{b}$ which satisfies the condition

(AS.2) $\mathbf{b} = ([b_1], \dots, [b_s])$ is such that

$$b_1 = 1, b_i = Z_{i-1}, 1 < i \le \delta = \dim_K(V)$$

so that

$$\begin{aligned} V := \mathrm{Span}_K\{[1], [Z_1], \dots [Z_r]\} &= \mathrm{Span}_K\{[1], [Z_1], \dots [Z_{\delta-1}]\} \\ &= \mathrm{Span}_K\{[b_1], \dots, [b_\delta]\}; \end{aligned}$$

thus the eigenvectors corresponding to $\alpha_j = (a_1^{(j)}, \dots, a_r^{(j)})$ are

$$(1, a_1^{(j)}, \dots, a_{\delta-1}^{(j)}, b_{\delta+1}(\alpha_j), \dots, b_s(\alpha_j))^T$$

and the other coordinates of α_j can be deduced from $a_i^{(j)} = c_{i0} + \sum_{l=1}^{\delta-1} c_{il} a_l^{(j)}$.
In conclusion

Theorem (Auzinger–Stetter)**.** *With the present notation and under the assumption that J is radical, then it holds*

1. *each j^{th} column $(b_1(\alpha_j), \dots, b_s(\alpha_j))^T$ of M_{bq} is an eigenvector of each $A_f, f \in \mathcal{Q}$, for the eigenvalue $f(\alpha_j)$;*
2. *for each $f \in \mathcal{Q}$, it holds*
   (a) *the eigenvalues of A_f and A_f^T are $\{f(\alpha_j) : 1 \le j \le s\}$;*
   (b) *the eigenspace of A_f for $\lambda \in K$ is*

$$\mathrm{Span}_K\{(b_1(\alpha_j), \dots, b_s(\alpha_j))^T : f(\alpha_j) = \lambda\};$$

*If, moreover, $Y = \sum_h c_h Z_h$ satisfies condition (**AS.1**) then:*

3. *the j^{th} column $(b_1(\alpha_j), \dots, b_s(\alpha_j))^T$ of M_{bq} is the eigenvector for $\beta_j := \sum_h c_h a_h^{(j)}$ of A_Y;*

*If further $\mathbf{b} = \{[1], [Z_1], \dots [Z_{\delta-1}], [b_{\delta+1}], \cdots, b_s]\}$ satisfies condition (**AS.2**) then:*

4. *denoting $\{(d_{j1}, \dots, d_{js})^T, 1 \le j \le s\}$ the eigenvectors of A_Y and*

$$\alpha_j := \left(d_{j1}^{-1} d_{j2}, \dots, d_{j1}^{-1} d_{j\delta}, c_{\delta 0} + \sum_{l=1}^{\delta-1} c_{\delta l} d_{j1}^{-1} d_{jl}, \dots, c_{n0} + \sum_{l=1}^{\delta-1} c_{nl} d_{j1}^{-1} d_{jl} \right)$$

for each j, then $\mathcal{Z}(\mathsf{J}) = \{\alpha_j, 1 \le j \le s\}$. □

Stetter Algorithm via Grobnerian Technology

A linear form
$$Y := \sum_{h=1}^{r} c_h Z_h$$
is said an *allgemeine coordinate* for the zero-dimensional ideal $\mathsf{J} = \cap_{i=1}^{\mathsf{s}} \mathfrak{q}_i$ iff

(a). there are polynomials $g_i \in K[Y], 0 \le i \le n$, g_0 monic, $\deg(g_i) < \deg(g_0)$, such that
$$G := (g_0(Y), Z_1 - g_1(Y), Z_2 - g_2(Y), \ldots, Z_r - g_r(Y))$$
is the reduced Gröbner basis of the ideal
$$\mathsf{J}^+ := \mathsf{J} + \left(Y - \sum_h c_h Z_h\right) \subset K[Y, Z_1, \ldots, Z_r]$$
w.r.t. the lex ordering induced by $Y < Z_1 < \ldots < Z_r$

and that this condition implies, under the assumption that J is radical, that

(b). $\mathcal{Q}/\mathsf{J} \cong K[Y]/g_0(Y)$

(c). for each $i, 1 \le i \le \mathsf{s}$, $\beta_i := \sum_{h=1}^{r} c_h a_h^{(i)}$ is a root of g_0

(d). $g_0(Y) = \prod_{i=1}^{r}(Y - \beta_i)$;

(e). there are polynomials $h_1(Y), \ldots, h_r(Y) \in K[Y]$, $\deg(h_i) < \deg(g_0)$, such that
$$\mathsf{J}^+ = \mathbb{I}\left(g_0(Y), g_0'(Y)Z_1 - h_1(Y), \ldots, g_0'(Y)Z_r - h_r(Y)\right) \subset K[Y, Z_1, \ldots, Z_r]. \quad (1)$$

(f). for each $\iota, 1 \le \iota \le r$, we have
$$h_\iota(Y) = \sum_{i=1}^{s} a_\iota^{(i)} \prod_{j \ne i} (Y - \beta_j). \quad (2)$$

(g). $a_j^{(i)} = g_j(\beta_i) = \frac{g_0'(\beta_i)}{g_0'(\beta_i)}$ for each $i, 1 \le i \le \mathsf{s}$, and each $j, 1 \le j \le r$,

(h). For each $f \in \mathcal{Q}$, $g_f(Y) := \mathbf{Rem}(f(g_1(Y), \ldots, g_r(Y)), g_0(Y))$ is s.t.
$$f \equiv g_f \bmod \mathsf{J}^+, \deg(g_f) < \deg(g_0).$$

(i). For each $f \in \mathcal{Q}$, $h_f(Y) := \mathbf{Rem}(f(h_1(Y), \ldots, h_r(Y)), g_0(Y)) \in K[Y]$ is s.t.
$$g_0'(Y) f(Z_1, \ldots, Z_r) \equiv g_f \bmod \mathsf{J}^+, \deg(h_f) < \deg(g_0).$$

Moreover, there is a Zarisky open set $\mathbf{U} \subset K^n$ such that $Y := \sum_{h=1}^{r} c_h Z_h$ is an *allgemeine* coordinate for J iff $(c_1, \ldots, c_r) \in \mathbf{U}$.

Since Stetter Algorithm is improved if J is radical and the matrix A_Y is given wrt a linear form Y satisfying condition (**AS.1**), these results can be efficiently — $\mathcal{O}(n^2 s^3)$ — granted by giving an FGLM-like linear algebra version of Gianni's Proposition obtained merging the algorithms by Alonso–Raimondo and Traverso.

We describe here the algorithm under the (useless but simplifer) assumption that J is radical:

1. $\ell := \sum_i a_i Z_i$
2. by linear algebra on the Gröbner descriptions of
$$[1], [\ell], [\ell^2], \dots, [\ell^s]$$
compute the minimal polynomial $g_0[Y] \in K[Y]$ such that
$$g_0(Y) \in \mathsf{J}^+ := \mathsf{J} + \left(Y - \sum_i a_i Z_i\right);$$
3. set $i = r$ and
   (a) verify, by linear algebra on the Gröbner descriptions of $[g_0'(\ell)Z_j], [1], [\ell], [\ell^2], \dots, [\ell^{d-1}]$, whether exists a relation $g_0'(Y)Z_i - h_j(Y) \in \mathsf{J}^+$, $\deg(h_i) < d$;
   (b) if such a relation exists and $i > 1$, set $i := i - 1$ and go to (3.a);
   (c) if such relation does not exist (this necessarily happens iff $\boxed{d := \deg(g_0) < \deg(\mathsf{J})}$ and in this case we have $i > 1$); then
      - set $\ell := \ell + cZ_i, a_i := a_i + c$ and go to (2)
4. if $\boxed{\deg(g_0) = \deg(\mathsf{J})}$, then
   - $\ell := \sum_i a_i Z_i$ is a separating linear form thus satisfyings condition (**AS.1**)
   - $[g_0'(\ell)Z_i] = [h_i(\ell)]$ for $i = 1 \dots, r$.