

I. Duality

- Macaulay F. S., On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers, *Math. Ann.* **74** (1913), 66–121;
- Macaulay F. S. , *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press (1916);
- Gröbner W., *Moderne Algebraische Geometrie*, Springer (1949);
- Möller H.M., Systems of Algebraic Equations Solved by Means of Endomorphisms, *L. N. Comp. Sci.* **673** (1993), 43–56, Springer;
- Marinari M.G., Möller H.M., On multiplicities in Polynomial System Solvin. *Trans. AMS*, **348** (1996), 3283–3321;
- Alonso M.E., Marinari M.G., The big Mother of all Dualities 2: Macaulay Bases, *J AAECC*
To appear

$$\mathcal{P} := k[X_1, \dots, X_n],$$

$\mathbb{L} := \{\ell_1, \dots, \ell_r\} \subset \mathcal{P}^*$ be a linearly independent set of k -linear functionals such that

$L := \text{Span}_k(\mathbb{L})$ is a \mathcal{P} -module so that

$I := \mathfrak{P}(L)$ is a zero-dimensional ideal;

$$\mathbf{N}(I) := \{t_1, \dots, t_r\},$$

$\mathbf{q} := \{q_1, \dots, q_r\} \subset \mathcal{P}$ the set triangular to \mathbb{L} , obtained via Möller's Algorithm;

$\left(q_{ij}^{(h)} \right) \in k^{r^2}$, $1 \leq h \leq r$ be the matrices defined by

$$X_h q_i = \sum_j q_{ij}^{(h)} q_j \text{ mod } I,$$

$\Lambda := \{\lambda_1, \dots, \lambda_r\}$ be the set biorthogonal to \mathbf{q} , which can be trivially deduced by Gaussian reduction

Then

$$X_h \lambda_j = \sum_{i=1}^r q_{ij}^{(h)} \lambda_i, \forall i, j, h.$$

$\mathcal{P} := k[X_1, \dots, X_n]$;

$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\}$;

$\mathfrak{m} := (X_1, \dots, X_n)$ be the maximal at the origin;

$I \subset \mathcal{P}$ an ideal;

the \mathfrak{m} -*closure* of I is the ideal $\bigcap_d I + \mathfrak{m}^d$;

I is \mathfrak{m} -*closed* iff $I = \bigcap_d I + \mathfrak{m}^d$;

For each $\tau \in \mathcal{T}$, denote $M(\tau) : \mathcal{P} \rightarrow k$ the morphism defined by

$$M(\tau)(f) = c(f, \tau), \forall f = \sum_{t \in \mathcal{T}} c(f, t)t \in \mathcal{P}.$$

Denoting $\mathbb{M} := \{M(\tau) : \tau \in \mathcal{T}\}$ for all

$$f := \sum_{t \in \mathcal{T}} a_t t \in \mathcal{P} \text{ and } \ell := \sum_{\tau \in \mathcal{T}} c_\tau M(\tau) \in k[[\mathbb{M}]] \cong \mathcal{P}^*$$

it holds $\ell(f) = \sum_{t \in \mathcal{T}} a_t c_t$.

$$\forall \tau \in \mathcal{T}, X_i \cdot M(\tau) = \begin{cases} M(\frac{\tau}{X_i}) & \text{if } X_i \mid \tau \\ 0 & \text{if } X_i \nmid \tau \end{cases}$$

A k -vector subspace $\Lambda \subset \text{Span}_k(\mathbb{M})$ is called *stable* if $\lambda \in \Lambda \implies X_i \cdot \lambda \in \Lambda$ i.e. Λ is a \mathcal{P} -module.

Clearly $\mathcal{P}^* \cong k[[\mathbb{M}]]$; however in order to have reasonable duality we must restrict ourselves to $\text{Span}_k(\mathbb{M}) \cong k[\mathbb{M}]$.

For each k -vector subspace $\Lambda \subset \text{Span}_k(\mathbb{M})$ denote

$$\mathfrak{I}(\Lambda) := \mathfrak{P}(\Lambda) = \{f \in \mathcal{P} : \ell(f) = 0, \forall \ell \in \Lambda\}$$

and for each k -vector subspace $P \subset \mathcal{P}$ denote

$$\begin{aligned} \mathfrak{M}(P) &:= \mathfrak{L}(P) \cap \text{Span}_K(\mathbb{M}) \\ &= \{\ell \in \text{Span}_K(\mathbb{M}) : \ell(f) = 0, \forall f \in P\}. \end{aligned}$$

The mutually inverse maps $\mathfrak{I}(\cdot)$ and $\mathfrak{M}(\cdot)$ give a biunivocal, inclusion reversing, correspondence between the set of the \mathfrak{m} -closed ideals $I \subset \mathcal{P}$ and the set of the stable k -vector subspaces $\Lambda \subset \text{Span}_k(\mathbb{M})$.

They are the restriction of, respectively, $\mathfrak{P}(\cdot)$ to \mathfrak{m} -closed ideals $I \subset \mathcal{P}$, and $\mathfrak{L}(\cdot)$ to stable k -vector subspaces $\Lambda \subset \text{Span}_k(\mathbb{M})$.

Moreover, for any \mathfrak{m} -primary ideal $\mathfrak{q} \subset \mathcal{P}$, $\mathfrak{M}(\mathfrak{q})$ is finite k -dimensional and we have

$$\text{deg}(\mathfrak{q}) = \dim_K(\mathfrak{M}(\mathfrak{q}));$$

conversely for any finite k -dim. stable k -vector subspace $\Lambda \subset \text{Span}_K(\mathbb{M})$, $\mathfrak{I}(\Lambda)$ is an \mathfrak{m} -primary ideal and we have

$$\dim_k(\Lambda) = \text{deg}(\mathfrak{I}(\Lambda)).$$

II. Macaulay Bases

- Macaulay F. S., On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers, *Math. Ann.* **74** (1913), 66–121;
- Macaulay F. S. , *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press (1916);
- Gröbner W., *Moderne Algebraische Geometrie*, Springer (1949);
- Möller H.M., Systems of Algebraic Equations Solved by Means of Endomorphisms, *L. N. Comp. Sci.* **673** (1993), 43–56, Springer;
- Marinari M.G., Möller H.M., On multiplicities in Polynomial System Solvin. *Trans. AMS*, **348** (1996), 3283–3321;
- Alonso M.E., Marinari M.G., The big Mother of all Dualities 2: Macaulay Bases, *J AAECC*
To appear

Let $<$ be a semigroup ordering on \mathcal{T} and $I \subset \mathcal{P}$ an m -closed ideal.

$$\text{Can}(t, I, <) =: \sum_{\tau \in \mathbf{N}_{<}(I)} \gamma(t, \tau, <) \tau \in k[[\mathbf{N}_{<}(I)]] \subset k[[X_1, \dots, X_n]]$$

so that

$$t - \sum_{\tau \in \mathbf{N}_{<}(I)} \gamma(t, \tau, <) \tau \in I,$$

$$t < \tau \implies \gamma(t, \tau, <) = 0.$$

Define, for each $\tau \in \mathbf{N}_{<}(I)$,

$$\ell(\tau) := M(\tau) + \sum_{t \in \mathbf{T}_{<}(I)} \gamma(t, \tau, <) M(t) \in k[[\mathbb{M}]].$$

Remark that $\ell(\tau) \in \mathfrak{M}(I)$ requires $\ell(\tau) \in k[[\mathbb{M}]]$ which holds iff $\{t : \gamma(t, \tau, <) \neq 0\}$ is finite and is granted if $\{t : t > \tau\}$ is finite.

To obtain this we must choose as $<$ a *standard ordering* i.e. such that

- $X_i < 1, \forall i,$
- for each infinite decreasing sequence in \mathcal{T}

$$\tau_1 > \tau_2 > \dots \tau_\nu > \dots$$

and each $\tau \in \mathcal{T}$ there is $\nu : \tau > \tau_\nu$.

In this setting the generalization of the notion of Gröbner basis is called Hironaka/standard basis and deals with *series* instead of polynomials.

The choice of this setting is natural, since a Hironaka basis of an ideal I returns its m -closure.

Let $<$ be a standard ordering on \mathcal{T} and let $I \subset \mathcal{P}$ an \mathfrak{m} -closed ideal. Denote

$$\text{Can}(t, I, <) =: \sum_{\tau \in \mathbf{N}_{<}(I)} \gamma(t, \tau, <) \tau \in k[[\mathbf{N}_{<}(I)]]$$

and, for each $\tau \in \mathbf{N}_{<}(I)$,

$$\ell(\tau) := M(\tau) + \sum_{t \in \mathbf{T}_{<}(I)} \gamma(t, \tau, <) M(t) \in k[\mathbb{M}].$$

Then

$$\mathfrak{M}(I) = \text{Span}_k \{ \ell(\tau), \tau \in \mathbf{N}_{<}(I) \}.$$

The set $\{ \ell(\tau), \tau \in \mathbf{N}_{<}(I) \}$ is called the *Macaulay Basis* of I .

There is an algorithm which, given a finite basis (not necessarily Gröbner/standard) of an \mathfrak{m} -primary ideal I , computes its Macaulay Basis.

Such algorithm becomes an infinite procedure which, given a finite basis of an ideal $I \subset \mathfrak{m}$, returns the infinite Macaulay Basis of its \mathfrak{m} -closure.

III. Cerlienco–Mureddu Correspondence

- Cerlienco, L, Mureddu, M. Algoritmi combinatori per l'interpolazione polinomiale in dimensione ≥ 2 . *Preprint* (1990)
- Cerlienco L., Mureddu M., From algebraic sets to monomial linear bases by means of combinatorial algorithms *Discrete Math.*, **139** (1995), 73–87.
- Cerlienco L., Mureddu M., Multivariate Interpolation and Standard Bases for Macaulay Modules, *J. Algebra* **251** (2002), 686–726

Problem 1 *Given a finite set of points,*

$$\{a_1, \dots, a_s\} \subset k^n, \quad a_i := (a_{i1}, \dots, a_{in}),$$

to compute $\mathbf{N}_{<}(\mathbf{l})$ w.r.t. the lexicographical ordering $<$ induced by $X_1 < \dots < X_n$ where

$$\mathbf{l} := \{f \in \mathcal{P} : f(a_i) = 0, 1 \leq i \leq s\}.$$

Cerlienco–Mureddu Algorithm, to each *ordered* finite set of points

$$X := \{a_1, \dots, a_s\} \subset k^n, \quad a_i := (a_{i1}, \dots, a_{in}),$$

associates

- an order ideal $\mathbf{N} := \mathbf{N}(X)$ and
- a bijection $\Phi := \Phi(X) : X \mapsto \mathbf{N}$

which satisfies

Theorem 1 $\mathbf{N}(I) = \mathbf{N}(X)$ holds for each finite set of points $X \subset k^n$.

Since they do so by induction on $s = \#(X)$ let us consider the subset $X' := \{a_1, \dots, a_{s-1}\}$, and the corresponding order ideal $\mathbf{N}' := \mathbf{N}(X')$ and bijection $\Phi' := \Phi(X')$.

If $s = 1$ the only possible solution is $\mathbf{N} = \{1\}$, $\Phi(a_1) = 1$.

$$\begin{aligned}\mathcal{T}[1, m] &:= \mathcal{T} \cap k[X_1, \dots, X_m] \\ &= \{X_1^{a_1} \cdots X_m^{a_m} : (a_1, \dots, a_m) \in \mathbb{N}^m\},\end{aligned}$$

$$\pi_m : k^n \mapsto k^m, \quad \pi_m(x_1, \dots, x_n) = (x_1, \dots, x_m),$$

$$\pi_m : \mathcal{T} \cong \mathbb{N}^n \mapsto \mathbb{N}^m \cong \mathcal{T}[1, m],$$

$$\pi_m(X_1^{a_1} \cdots X_n^{a_n}) = X_1^{a_1} \cdots X_m^{a_m}.$$

With this notation, let us set

$$m := \max(j : \exists i < s : \pi_j(\mathbf{a}_i) = \pi_j(\mathbf{a}_s));$$

$$d := \#\{\mathbf{a}_i, i < s : \pi_m(\mathbf{a}_i) = \pi_m(\mathbf{a}_s)\};$$

$$W := \{\mathbf{a}_i : \Phi'(\mathbf{a}_i) = \tau_i X_{m+1}^d, \tau_i \in \mathcal{T}[1, m]\} \cup \{\mathbf{a}_s\};$$

$$Z := \pi_m(W);$$

$$\tau := \Phi(Z)(\pi_m(\mathbf{a}_s));$$

$$t_s := \tau X_{m+1}^d;$$

where $\mathbf{N}(Z)$ and $\Phi(Z)$ are the result of the application of the present algorithm to Z , which can be inductively applied since $\#(Z) \leq s - 1$.

We then define

- $\mathbf{N} := \mathbf{N}' \cup \{t_s\}$,
- $\Phi(\mathbf{a}_i) := \begin{cases} \Phi'(\mathbf{a}_i) & i < s \\ t_s & i = s \end{cases}$

$$a_1 := (0, 0, 1),$$

$$\Phi(a_1) := t_1 := 1;$$

$$a_2 := (0, 1, -2), m = 1,$$

$$d = 1, W = \{(0, 1)\}, \tau = 1,$$

$$\Phi(a_2) := t_2 := X_2,$$

$$a_3 := (2, 0, 2), m = 0,$$

$$d = 1, W = \{(2, 0)\}, \tau = 1,$$

$$\Phi(a_3) := t_3 := X_1,$$

$$a_4 := (0, 2, -2), m = 1,$$

$$d = 2, W = \{(0, 2)\}, \tau = 1,$$

$$\Phi(a_4) := t_4 := X_2^2,$$

$$a_5 := (1, 0, 3), m = 0,$$

$$d = 2, W = \{(1, 0)\}, \tau = 1,$$

$$\Phi(a_5) := t_5 := X_1^2,$$

$$a_6 := (1, 1, 3), m = 1,$$

$$d = 1, W = \{(0, 1), (1, 1)\}, \tau = X_1,$$

$$\Phi(a_6) := t_6 := X_1 X_2.$$

$(0, 2, -2)$		
$(0, 1, -2)$	$(1, 1, 3)$	
$(0, 0, 1)$	$(2, 0, 2)$	$(1, 0, 3)$

$$a_7 := (1, 1, 1), m = 2,$$

$$d = 1, W = \{(1, 1, 1)\}, \tau = 1,$$

$$\Phi(a_7) := t_7 := X_3.$$

$$a_8 := (2, 0, 1), m = 2,$$

$$d = 1, W = \{(1, 1, 1), (2, 0, 1)\}, \tau = X_1,$$

$$\Phi(a_8) := t_8 := X_1 X_3,$$

$$a_9 := (2, 0, 0), m = 2,$$

$$d = 2, W = \{(2, 0, 0)\}, \tau = 1,$$

$$\Phi(a_9) := t_9 := X_3^2,$$

$(0, 2, -2)$		
$(0, 1, -2)$	$(1, 1, 3)$	
$(0, 0, 1)$	$(2, 0, 2)$	$(1, 0, 3)$

- Gao S., Rodrigues V.M., Stroomer J., Gröbner basis structure of finite sets of points *Preprint* (2003)

A combinatorial reformulation which

- builds a tree on the basis of the point coordinates,
- combinatorially recombines the tree,
- reads on this tree the monomial structure.

It returns \mathbf{N} but not Φ ; more important: it is *not* iterative.

- Marinari M.G., Cerlienco–Mureddu Correspondence and Lazard Structural Theorem. *Investigaciones Matemáticas* (2006). To appear.

Extends Cerlienco–Mureddu Algorithm to multiple points described via Macaulay Bases

IV. Macaulay's Algorithm

- Macaulay F. S., On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers, *Math. Ann.* **74** (1913), 66–121;
- Macaulay F. S. , *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press (1916);
- Gröbner W., *Moderne Algebraische Geometrie*, Springer (1949);
- Alonso M.E., Marinari M.G., The big Mother of all Dualities 2: Macaulay Bases, *J AAECC*
To appear

$\mathfrak{m} = (X_1, \dots, X_n) \subset \mathcal{P} := k[X_1, \dots, X_n]$,

$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\}$,

a standard-ordering $<$ on \mathcal{T} ,

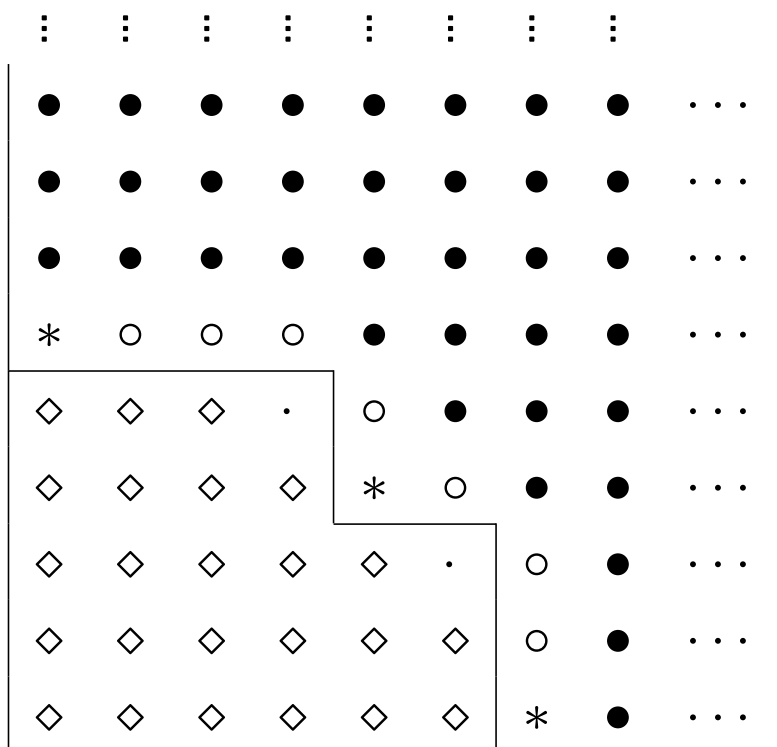
an \mathfrak{m} -closed ideal I ,

the finite corner set $C_{<}(I) := \{\omega_1, \dots, \omega_s\}$,

the (not-necessarily finite) set $N_{<}(I)$,

the Macaulay basis $\{\ell(\tau) : \tau \in N_{<}(I)\}$,

the k -vectorspace $\Lambda \subset \text{Span}_k(\mathbb{M})$ generated by it.



$\mathfrak{m} = (X_1, \dots, X_n) \subset \mathcal{P} := k[X_1, \dots, X_n],$

$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\},$

a standard-ordering $<$ on $\mathcal{T},$

an \mathfrak{m} -closed ideal $I,$

the finite corner set $\mathbf{C}_{<}(I) := \{\omega_1, \dots, \omega_s\},$

the (not-necessarily finite) set $\mathbf{N}_{<}(I),$

the Macaulay basis $\{\ell(\tau) : \tau \in \mathbf{N}_{<}(I)\},$

$\Lambda := \text{Span}_k\{\ell(\tau) : \tau \in \mathbf{N}_{<}(I)\} \subset \text{Span}_k(\mathbb{M});$

$\forall j, 1 \leq j \leq s, \Lambda_j := \text{Span}_k\{v \cdot \ell(\omega_j) : v \in \mathcal{T}\}.$

$\forall j, 1 \leq j \leq s, \mathfrak{q}_j := \mathfrak{I}(\Lambda_j).$

Let $J \subset \{1, \dots, s\}$ be the set such that $\{\mathfrak{q}_j : j \in J\}$ is the set of the minimal elements of $\{\mathfrak{q}_j : 1 \leq j \leq s\}$ and remark that $\mathfrak{q}_i \subset \mathfrak{q}_j \iff \Lambda_i \supset \Lambda_j.$

Lemma 1 (Macaulay) *With the notation above, for each $j,$ denoting*

$$\Lambda'_j := \text{Span}_K\{v \cdot \ell(\omega_j) : v \in \mathcal{T} \cap \mathfrak{m}\}$$

we have

$$\dim_K(\Lambda'_j) = \dim_K(\Lambda_j) - 1,$$

$$\ell(\omega_j) \notin \Lambda'_j = \mathfrak{M}(\mathfrak{q}_j : \mathfrak{m}),$$

$$\mathfrak{q}' \supset \mathfrak{q}_j \implies \mathfrak{M}(\mathfrak{q}') \subseteq \Lambda'_j.$$

$\mathfrak{m} = (X_1, \dots, X_n) \subset \mathcal{P} := k[X_1, \dots, X_n],$

$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\},$

a standard-ordering $<$ on $\mathcal{T},$

an \mathfrak{m} -closed ideal $I,$

the finite corner set $\mathbf{C}_{<}(I) := \{\omega_1, \dots, \omega_s\},$

the (not-necessarily finite) set $\mathbf{N}_{<}(I),$

the Macaulay basis $\{\ell(\tau) : \tau \in \mathbf{N}_{<}(I)\},$

$\Lambda := \text{Span}_k\{\ell(\tau) : \tau \in \mathbf{N}_{<}(I)\} \subset \text{Span}_k(\mathbb{M});$

$\forall j, 1 \leq j \leq s, \Lambda_j := \text{Span}_k\{v \cdot \ell(\omega_j) : v \in \mathcal{T}\}.$

$\forall j, 1 \leq j \leq s, \mathfrak{q}_j := \mathfrak{I}(\Lambda_j).$

Let $J \subset \{1, \dots, s\}$ be the set such that $\{\mathfrak{q}_j : j \in J\}$ is the set of the minimal elements of $\{\mathfrak{q}_j : 1 \leq j \leq s\}$ and remark that $\mathfrak{q}_i \subset \mathfrak{q}_j \iff \Lambda_i \supset \Lambda_j.$

Theorem 2 (Gröbner) *If I is \mathfrak{m} -primary, then:*

1. *each Λ_j is a finite-dim. stable vectorspace;*
2. *each \mathfrak{q}_j is an \mathfrak{m} -primary ideal,*
3. *is reduced*
4. *and irreducible.*
5. *$I := \bigcap_{j \in J} \mathfrak{q}_j$ is a reduced representation of $I.$*

V. Reduced Irreducible Decomposition

- Noether Noether E. Idealtheorie in Ringbereichen, *Math. Annalen*, **83** (1921), 25–66.
- Macaulay F. S., On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers, *Math. Ann.* **74** (1913), 66–121;
- Macaulay F. S. , *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press (1916);
- Gröbner W., *Moderne Algebraische Geometrie*, Springer (1949);
- Renschuch. B, *Elementare und praktische Idealtheorie*, Deutscher Verlag der Wissenschaften (1976);
- Alonso M.E., Marinari M.G., The big Mother of all Dualities 2: Macaulay Bases, *J AAEECC*
To appear

- (Lasker-Noether) In a noetherian ring R , every ideal $\mathfrak{a} \subset R$ is a finite intersection of irreducible ideals.
- (Noether) A representation $\mathfrak{a} = \bigcap_{j=1}^r \mathfrak{i}_j$ of an ideal \mathfrak{a} in a noetherian ring R as intersection of finitely many irreducible ideals is called a *reduced representation* if
 - $\forall j \in \{1, \dots, r\}, \mathfrak{i}_j \not\supset \bigcap_{\substack{h=1 \\ j \neq h}}^r \mathfrak{i}_h$ and
 - there is no irreducible ideal $\mathfrak{i}_j' \supset \mathfrak{i}_j$ such that

$$\mathfrak{a} = \left(\bigcap_{\substack{h=1 \\ j \neq h}}^r \mathfrak{i}_h \right) \cap \mathfrak{i}_j'.$$
- (Noether) In a noetherian ring R , each ideal $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{q}_i$ $\mathfrak{a} \subset R$ has a reduced representation as intersection of finitely many irreducible ideals.
- A primary component \mathfrak{q}_j of an ideal \mathfrak{a} contained in a noetherian ring R , is called *reduced* if there is no primary ideal $\mathfrak{q}_j' \supset \mathfrak{q}_j$ such that

$$\mathfrak{a} = \left(\bigcap_{\substack{i=1 \\ j \neq i}}^r \mathfrak{q}_i \right) \cap \mathfrak{q}_j'.$$
- In an irredundant primary decomposition of an ideal of a noetherian ring, each primary component can be chosen to be reduced.

The decomposition

$$(X^2, XY) = (X) \cap (X^2, XY, Y^\lambda), \forall \lambda \in \mathbb{N}, \lambda \geq 1,$$

where $\sqrt{(X^2, XY, Y^\lambda)} = (X, Y) \supset (X)$, shows that embedded components are not unique; however,

$$(X^2, XY, Y) = (X^2, Y) \supseteq (X^2, XY, Y^\lambda), \forall \lambda > 1,$$

shows that (X^2, Y) is a reduced embedded irreducible component and that

$$(X^2, XY) = (X) \cap (X^2, Y)$$

is a reduced representation.

The decompositions

$$(X^2, XY) = (X) \cap (X^2, Y + aX), \forall a \in \mathbb{Q},$$

where $\sqrt{(X^2, Y + aX)} = (X, Y) \supset (X)$ and, clearly, each $(X^2, Y + aX)$ is reduced, show that also reduced representations are not unique; remark that, setting $a = 0$, we find again the previous one $(X^2, XY) = (X) \cap (X^2, Y)$.

If I is not m -primary, let

$\rho := \max\{\deg(\omega_j) + 1 : \omega_j \in C(I)\}$ so that

$\mathfrak{q}' := I + m^\rho$ is an m -primary component of I ;

$I = \bigcap_{i=1}^r \mathfrak{q}_i$ an irredundant primary representation
of I with $\sqrt{\mathfrak{q}_1} = m$;

$\mathfrak{b} := I : m^\infty = \bigcap_{i=2}^r \mathfrak{q}_i$;

$\mathfrak{b} = \bigcap_{i=1}^u \mathfrak{Q}_i$, a reduced representation of \mathfrak{b} ;

$\mathfrak{q}_1 := \bigcap_{j=1}^s \mathfrak{q}_j$ a reduced representation of \mathfrak{q}_1 which
is wlog ordered so that $\mathfrak{q}_i \supset \mathfrak{b} \iff i > t$;

$\mathfrak{q} := \bigcap_{j=1}^t \mathfrak{q}_j$.

Then

1. \mathfrak{q} is a reduced m -primary component of I ,
2. $\mathfrak{q} := \bigcap_{j=1}^t \mathfrak{q}_j$ is a reduced representation of \mathfrak{q} ,
3. $I = \bigcap_{i=1}^u \mathfrak{Q}_i \cap \bigcap_{j=1}^t \mathfrak{q}_j$ is a reduced representation
of I .

$I := (X^2, XY),$

$\Lambda = \text{Span}_k\{M(1), M(X)\} \cup \{M(Y^i), i \in \mathbb{N}\};$

$\rho = 2,$

$\mathfrak{M}(I + m^2) = \{M(1), M(X), M(Y)\},$

$\omega_1 := X, \Lambda_1 = \{M(1), M(X)\}, \mathfrak{q}_1 = (X^2, Y),$

$\omega_2 := Y, \Lambda_2 = \{M(1), M(Y)\}, \mathfrak{q}_2 = (X, Y^2),$

$I : m^\infty = (X) \subset (X, Y^2),$

$(X^2, XY) = (X) \cap (X^2, Y).$

$$l := (X^2, XY),$$

$$\Lambda = \text{Span}_k\{M(1), M(X)\} \cup \{M(Y^i), i \in \mathbb{N}\};$$

$$\rho = 2,$$

$$\mathfrak{M}(l + \mathfrak{m}^2) = \{M(1), M(X), M(Y)\},$$

$$\omega_1 := X, \Lambda_1 = \{M(1), M(X)\}, \mathfrak{q}_1 = (X^2, Y),$$

$$\omega_2 := Y, \Lambda_2 = \{M(1), M(Y)\}, \mathfrak{q}_2 = (X, Y^2),$$

$$l : \mathfrak{m}^\infty = (X) \subset (X, Y^2),$$

$$(X^2, XY) = (X) \cap (X^2, Y).$$

Both the reduced representation and the notion of Macaulay basis strongly depend on the choice of a frame of coordinates.

In fact, considering, for each $a \in \mathbb{Q}, a \neq 0$,

$$\Lambda = \text{Span}_k\{M(1), M(X) - aM(Y)\} \cup \{M(Y^i), i \in \mathbb{N}\},$$

we obtain

$$\rho = 2,$$

$$\mathfrak{M}(l + \mathfrak{m}^2) = \{M(1), M(X) - aM(Y), M(Y)\},$$

$$\omega_1 := X, \Lambda_1 = \{M(1), M(X) - aM(Y)\}, \mathfrak{q}_1 = (X^2, Y + aX),$$

$$\omega_2 := Y, \Lambda_2 = \{M(1), M(Y)\}, \mathfrak{q}_2 = (X, Y^2),$$

$$l : \mathfrak{m}^\infty = (X) \subset (X, Y^2),$$

$$(X^2, XY) = (X) \cap (X^2, Y + aX).$$

VI. Lazard Structural Theorem

- Lazard D., Ideal Basis and Primary Decomposition: Case of two variables *J. Symb. Comp.* **1** (1985) 261–270

Theorem 3 Let $\mathcal{P} := k[X_1, X_2]$ and let $<$ be the lex. ordering induced by $X_1 < X_2$.

Let $I \subset \mathcal{P}$ be an ideal and let $\{f_0, f_1, \dots, f_k\}$ be a Gröbner basis of I ordered so that

$$\mathbf{T}(f_0) < \mathbf{T}(f_1) < \dots < \mathbf{T}(f_k).$$

Then

- $f_0 = PG_1 \cdots G_{k+1}$,
- $f_j = PH_j G_{j+1} \cdots G_{k+1}$, $1 \leq j < k$,
- $f_k = PH_k G_{k+1}$,

where

P is the primitive part of $f_0 \in k[X_1][X_2]$;

$G_i \in k[X_1]$, $1 \leq i \leq k + 1$;

$H_i \in k[X_1][X_2]$ is a monic polynomial of degree $d(i)$, for each i ;

$d(1) < d(2) < \dots < d(k)$;

$H_{i+1} \in (G_1 \cdots G_i, \dots, H_j G_{j+1} \cdots G_i, \dots, H_{i-1} G_i, H_i), \forall i$.

VII. Axis-of-Evil Theorem

- Marinari M.G., Mora T., A remark on a remark by Macaulay or Enhancing Lazard Structural Theorem. *Bull. of the Iranian Math. Soc.*, **29** (2003), 103–145;
- Marinari M.G., Mora T.
Some Comments on Cerlienco–Mureddu Algorithm and Enhanced Lazard Structural Theorem. Rejected by ISSAC-2004 (2004)
- Marinari M.G., Mora T.
Cerlienco–Mureddu Correspondence and Lazard Structural Theorem.
Investigaciones Matemáticas (2006). To appear.

Description of the combinatorial structure [Gröbner and border basis, linear and Gröbner representation] of a 0-dimensional ideal

$$I = \cap \mathfrak{q}_i \subset \mathcal{P}, \sqrt{\mathfrak{q}_i} = (X_1 - a_{i1}, \dots, X_n - a_{in})$$

in terms of a **Macaulay representation**, i.e. of its roots (a_{i1}, \dots, a_{in}) and of the Macaulay basis of each \mathfrak{q}_i .

It is summarized into 22* statements.

The description is "algorithmical" in terms of elementary combinatorial tools and linear interpolation.

It extends Cerlienco–Mureddu Correspondence and Lazard's Structural Theorem.

The proof is essentially a direct application of Möller's Algorithm.

*in honour of Trythemius, the founder of cryptography (*Steganographia* [1500], *Polygraphia* [1508]) which introduced in German the 22th letter **W** in order to perform German gematria.

Let

$I \subset \mathcal{P}$ be a zero-dimensional radical ideal;

$Z := \{\mathbf{a}_1, \dots, \mathbf{a}_s\} \subset k^n$ its roots;

$\mathbf{N} := \mathbf{N}(I)$;

$\mathbf{G}_{<}(I) := \{t_1, \dots, t_r\}, t_1 < t_2 < \dots < t_r, t_i := X_1^{d_1^{(i)}} \dots X_n^{d_n^{(i)}}$ the minimal basis of its associated monomial ideal $\mathbf{T}_{<}(I)$;

$G := \{f_1, \dots, f_r\}, \mathbf{T}(f_i) = t_i \forall i$, the unique reduced lexicographical Gröbner basis of I .

There is a combinatorial algorithm which, given Z , returns sets of points

$$Z_{m\delta i} \subset k^m, \forall m, \delta, i : 1 \leq i \leq r, 1 \leq m \leq n, 1 \leq \delta \leq d_m^{(i)},$$

thus allowing to compute

- by means of Cerlienco–Mureddu Algorithm the corresponding order ideal

$$F_{m\delta i} := \mathbf{N}(Z_{m\delta i}) \subset \mathcal{T} \cap k[X_1, \dots, X_{m-1}]$$

- and, by interpolation* unique polynomials

$$\gamma_{m\delta i} := X_m - \sum_{\omega \in F_{m\delta i}} c_\omega \omega$$

which satisfy the relation

$$f_i = \prod_m \prod_\delta \gamma_{m\delta i} \pmod{(f_1, \dots, f_{i-1})} \forall i.$$

Moreover, setting

ν the maximal value such that $d_\nu^{(i)} \neq 0, d_m^{(i)} = 0, m > \nu$ so that $f_i \in k[X_1, \dots, X_\nu] \setminus k[X_1, \dots, X_{\nu-1}]$,

$$L_i := \prod_{m=1}^{\nu-1} \prod_\delta \gamma_{m\delta i} \text{ and}$$

$$P_i := \prod_\delta \gamma_{\nu\delta i}$$

we have $f_i = L_i P_i$ where L_i is the *leading polynomial* of f_i .

$$* X_m(\mathbf{a}) = \sum_{\omega \in F_{m\delta i}} c_\omega \omega(\mathbf{a}), \mathbf{a} \in Z_{m\delta i}.$$