I. Duality


- 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
\( \mathcal{P} := k[X_1, \ldots, X_n], \)

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

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

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

\( \mathfrak{N}(\mathfrak{l}) := \{t_1, \ldots, t_r\}, \)

\( \mathfrak{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P} \) the set triangular to \( \mathbb{L} \), obtained via Möller’s Algorithm;

\[
\begin{pmatrix}
q^{(h)}_{ij}
\end{pmatrix} \in k^{r^2}, 1 \leq k \leq r \text{ be the matrices defined by}
\]

\[
X_h q_i = \sum_j q^{(h)}_{ij} q_j \text{ mod } \mathfrak{l},
\]

\( \Lambda := \{\lambda_1, \ldots, \lambda_r\} \) be the set biorthogonal to \( \mathfrak{q} \), which can be trivially deduced by Gaussian reduction

Then

\[
X_h \lambda_j = \sum_{i=1}^{r} q^{(h)}_{ij} \lambda_i, \forall i, j, h.
\]
\( \mathcal{P} := k[X_1, \ldots, X_n] \);

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

\( m := (X_1, \ldots, X_n) \) be the maximal at the origin;

\( I \subset \mathcal{P} \) an ideal;

the \( m \)-closuse of \( I \) is the ideal \( \bigcap_d I + m^d \);

\( I \) is \( m \)-closed iff \( I = \bigcap_d I + m^d \);

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

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

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

\( f := \sum_{t \in \mathcal{T}} a_t t \in \mathcal{P} \) 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 \textit{stable} if \( \lambda \in \Lambda \implies X_i \cdot \lambda \in \Lambda \) i.e. \( \Lambda \) is a \( \mathcal{P} \)-module.
Clealy $\mathcal{P}^* \cong k[[\mathcal{M}]]$; however in order to have reasonable duality we must restrict ourselves to $\text{Span}_k(\mathcal{M}) \cong k[\mathcal{M}]$.

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

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

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

$$\mathcal{M}(P) := \mathcal{L}(P) \cap \text{Span}_k(\mathcal{M})$$

$$= \{\ell \in \text{Span}_k(\mathcal{M}) : \ell(f) = 0, \forall f \in P\}.$$

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

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

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

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

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

$$\dim_k(\Lambda) = \deg(\mathcal{I}(\Lambda)).$$
II. Macaulay Bases


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

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

so that  

\[
t - \sum_{\tau \in \mathbb{N}_< (I)} \gamma(t, \tau, \prec) \tau \in \mathcal{I},
\]

\[
t < \tau \implies \gamma(t, \tau, \prec) = 0.
\]

Define, for each \(\tau \in \mathbb{N}_< (\mathcal{I})\),

\[
\ell(\tau) := M(\tau) + \sum_{t \in T_<(\mathcal{I})} \gamma(t, \tau, \prec) M(t) \in k[[\mathcal{M}]].
\]

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

To obtain this we must choose as \(<\) a \textit{standard} ordering i.e. such that

- \(X_i < 1, \forall i,\)
- for each infinite decreasing sequence in \(T\)
  \[
  \tau_1 > \tau_2 > \cdots \tau_\nu > \cdots
  \]
  and each \(\tau \in T\) there is \(\nu : \tau > \tau_\nu\).

In this setting the generalization of the notion of Gröbner basis is called Hironoka/standard basis and deals with \textit{series} instead of polynomials.

The choice of this setting is natural, since a Hironaka basis of an ideal \(\mathcal{I}\) returns its \(m\)-closure.
Let $<$ be a standard ordering on $\mathcal{T}$ and let $I \subset \mathcal{P}$ an $m$-closed ideal. Denote

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

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

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

Then

$$\mathcal{M}(l) = \text{Span}_k \{\ell(\tau), \tau \in \mathbb{N}_<(l)\}.$$ 

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

There is an algorithm which, given a finite basis (not necessarily Gröbner/standard) of an $m$-primary ideal $l$, computes its Macaulay Basis.

Such algorithm becomes an infinite procedure which, given a finite basis of an ideal $l \subset m$, returns the infinite Macaulay Basis of its $m$-closure.
III. Cerlienco–Mureddu Correspondence

- Cerlienco, L., Mureddu, M. Algoritmi combinatori per l’interpolazione polinomiale in dimensione \( \geq 2 \). *Preprint* (1990)


**Problem 1** Given a finite set of points,

\[ \{a_1, \ldots, a_s\} \subset k^n, \quad a_i := (a_{i1}, \ldots, a_{in}), \]

*to compute* \( N_<(l) \) *w.r.t. the lexicographical ordering* \( < \) *induced by* \( X_1 < \cdots < X_n \) *where*

\[ l := \{f \in \mathcal{P} : f(a_i) = 0, 1 \leq i \leq s\}. \]
Cerlienco–Mureddu Algorithm, to each ordered finite set of points

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

associates

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

which satisfies

**Theorem 1** \( N(I) = N(X) \) 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 \( X' := \{a_1, \ldots, a_{s-1}\} \), and the corresponding order ideal \( N' := N(X') \) and bijection \( \Phi' := \Phi(X') \).

If \( s = 1 \) the only possible solution is \( N = \{1\}, \Phi(a_1) = 1 \).
$$\mathcal{T}[1,m] := \mathcal{T} \cap k[X_1, \ldots, X_m] = \{X_1^{a_1} \cdots X_m^{a_m} : (a_1, \ldots, a_m) \in \mathbb{N}^m\},$$

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

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

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

With this notation, let us set

$$m := \max (j : \exists i < s : \pi_j(a_i) = \pi_j(a_s));$$

$$d := \#\{a_i, i < s : \pi_m(a_i) = \pi_m(a_s)\};$$

$$W := \{a_i : \Phi'(a_i) = \tau_i X_m^{d+1}, \tau_i \in \mathcal{T}[1,m]\} \cup \{a_s\};$$

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

$$\tau := \Phi(Z)(\pi_m(a_s));$$

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

where $\mathbb{N}(Z)$ 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

- $\mathbb{N} := \mathbb{N}' \cup \{t_s\},$

- $\Phi(a_i) := \begin{cases} \Phi'(a_i) & i < s \\ t_s & i = s \end{cases}$
\( a_1 := (0, 0, 1), \)
\[
\Phi(a_1) := t_1 := 1;
\]
\( a_2 := (0, 1, -2), m = 1, \)
\[
d = 1, W = \{(0, 1)\}, \tau = 1, \quad \Phi(a_2) := t_2 := X_2, \]
\( a_3 := (2, 0, 2), m = 0, \)
\[
d = 1, W = \{(2, 0)\}, \tau = 1, \quad \Phi(a_3) := t_3 := X_1, \]
\( a_4 := (0, 2, -2), m = 1, \)
\[
d = 2, W = \{(0, 2)\}, \tau = 1, \quad \Phi(a_4) := t_4 := X_2^2, \]
\( a_5 := (1, 0, 3), m = 0, \)
\[
d = 2, W = \{(1, 0)\}, \tau = 1, \quad \Phi(a_5) := t_5 := X_2^2, \]
\( a_6 := (1, 1, 3), m = 1, \)
\[
d = 1, W = \{(0, 1), (1, 1)\}, \tau = X_1, \quad \Phi(a_6) := t_6 := X_1 X_2. \]
\( a_7 := (1, 1, 1), m = 2, \)
\( d = 1, W = \{(1, 1, 1)\}, \tau = 1, \)
\( \Phi(a_7) := t_7 := X_3. \)

\( a_8 := (2, 0, 1), m = 2, \)
\( d = 1, W = \{(1, 1, 1), (2, 0, 1)\}, \tau = X_1, \)
\( \Phi(a_8) := t_8 := X_1X_3, \)

\( a_9 := (2, 0, 0), m = 2, \)
\( d = 2, W = \{(2, 0, 0)\}, \tau = 1, \)
\( \Phi(a_9) := t_9 := X_3^2, \)

\[
\begin{array}{c|ccc}
(0, 2, -2) & (0, 1, -2) & (1, 1, 3) \\
(0, 0, 1) & (2, 0, 2) & (1, 0, 3) \\
\end{array}
\]

A combinatorial reformulation which

– builds a tree on the basis of the point coordinates,

– combinatorially recombines the tree,

– reeds on this tree the monomial structure.

It returns $\mathcal{N}$ but not $\Phi$; more important: it is *not* iterative.


Extends Cerlienco–Mureddu Algorithm to multiple points described via Macaulay Bases
IV. Macaulay’s Algorithm


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

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

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

an \( m \)-closed ideal \( I, \)

the finite corner set \( \mathcal{C}_<(I) := \{\omega_1, \ldots, \omega_s\}, \)

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

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

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

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]

\[ \cdots \]
$m = (X_1, \ldots, X_n) \subset P := k[X_1, \ldots, X_n], \n$
$T := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}, \n$
a standard-ordering $<$ on $T, \n$
an $m$-closed ideal $I, \n$
the finite corner set $C_{<}(I) := \{\omega_1, \ldots, \omega_s\}, \n$
the (not-necessarily finite) set $N_{<}(I), \n$
the Macaulay basis $\{\ell(\tau) : \tau \in N_{<}(I)\}, \n$
$\Lambda := \text{Span}_k\{\ell(\tau) : \tau \in N_{<}(I)\} \subset \text{Span}_k(M); \n$
$\forall j, 1 \leq j \leq s, \Lambda_j := \text{Span}_k\{v \cdot \ell(\omega_j) : v \in T\}. \n$
$\forall j, 1 \leq j \leq s, q_j := I(\Lambda_j). \n$

Let $J \subset \{1, \ldots, s\}$ be the set such that $\{q_j : j \in J\}$ is the set of the minimal elements of $\{q_j : 1 \leq j \leq s\}$ and remark that $q_i \subset q_j \iff \Lambda_i \supset \Lambda_j.$

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

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

we have

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

$$\ell(\omega_j) \notin \Lambda'_j = M(q_j : m),$$

$q' \supset q_j \implies M(q') \subseteq \Lambda'_j.$
\( m = (X_1, \ldots, X_n) \subset \mathcal{P} := k[X_1, \ldots, X_n], \)
\( \mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}, \)
a standard-ordering \(<\) on \( \mathcal{T}, \)
an \( m \)-closed ideal \( I, \)
the finite corner set \( C_<(l) := \{\omega_1, \ldots, \omega_s\}, \)
the (not-necessarily finite) set \( \mathbb{N}_<(l), \)
the Macaulay basis \( \{\ell(\tau) : \tau \in \mathbb{N}_<(l)\}, \)
\( \Lambda := \text{Span}_k\{\ell(\tau) : \tau \in \mathbb{N}_<(l)\} \subset \text{Span}_k(\mathbb{M}); \)
\( \forall j, 1 \leq j \leq s, \Lambda_j := \text{Span}_k\{v \cdot \ell(\omega_j) : v \in \mathcal{T}\}. \)
\( \forall j, 1 \leq j \leq s, q_j := I(\Lambda_j). \)

Let \( J \subset \{1, \ldots, s\} \) be the set such that \( \{q_j : j \in J\} \) is the set of the minimal elements of \( \{q_j : 1 \leq j \leq s\} \) and remark that \( q_i \subset q_j \iff \Lambda_i \supset \Lambda_j. \)

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

1. each \( \Lambda_j \) is a finite-dim. stable vectorspace;
2. each \( q_j \) is an \( m \)-primary ideal,
3. is reduced
4. and irreducible.
5. \( I := \cap_{j \in J} q_j \) is a reduced representation of \( I. \)
V. Reduced Irreducible Decomposition


- 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 AAECC* To appear
• (Lasker-Noether) In a noetherian ring $R$, every ideal $a \subset R$ is a finite intersection of irreducible ideals.

• (Noether) A representation $a = \bigcap_{j=1}^{r} i_j$ of an ideal $a$ in a noetherian ring $R$ as intersection of finitely many irreducible ideals is called a reduced representation if
  - $\forall j \in \{1, \ldots, r\}$, $i_j \not\supset \bigcap_{h=1}^{r} i_h$ and
  - there is no irreducible ideal $i_j' \supset i_j$ such that

$$a = \left( \bigcap_{h=1}^{r} i_h \right) \cap i_j'.$$

• (Noether) In a noetherian ring $R$, each ideal $a = \bigcap_{i=1}^{r} q_i \ a \subset R$ has a reduced representation as intersection of finitely many irreducible ideals.

• A primary component $q_j$ of an ideal $a$ contained in a noetherian ring $R$, is called reduced if there is no primary ideal $q_j' \supset q_j$ such that

$$a = \left( \bigcap_{i=1}^{r} q_i \right) \cap q_j'.$$

• 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 
\[ q' := I + m^\rho \] is an $m$-primary component of $I$;

\[ I = \mathcal{C}_1 \] an irredundant primary representation

of $I$ with $\sqrt{q_1} = m$;

\[ b := I : m^\infty = \mathcal{C}_2 \]

is a reduced representation of $b$;

\[ q_1 := \mathcal{C}_3 \] a reduced representation of $q_1$ which

is wlog ordered so that $q_i \supset b \iff i > t$;

\[ q := \mathcal{C}_4 \].

Then

1. $q$ is a reduced $m$-primary component of $I$,
2. $q := \mathcal{C}_5$ is a reduced representation of $q$,
3. $I = \mathcal{C}_6$ is a reduced representation of $I$.

\[ I := (X^2, XY), \]
\[ \Lambda := \text{Span}_k\{M(1), M(X)\} \cup \{M(Y^i), i \in \mathbb{N}\}; \]
\[ \rho = 2, \]
\[ \mathcal{M}(I + m^2) = \{M(1), M(X), M(Y)\}, \]
\[ \omega_1 := X, \Lambda_1 = \{M(1), M(X)\}, q_1 = (X^2, Y), \]
\[ \omega_2 := Y, \Lambda_2 = \{M(1), M(Y)\}, q_2 = (X, Y^2), \]
\[ I : m^\infty = (X) \subset (X, Y^2), \]
\[ (X^2, XY) = (X) \cap (X^2, Y). \]
\[ l := (X^2, XY), \]
\[ \Lambda = \text{Span}_k \{ M(1), M(X) \} \cup \{ M(Y^i), i \in \mathbb{N} \}; \]
\[ \rho = 2, \]
\[ \mathcal{M}(l + m^2) = \{ M(1), M(X), M(Y) \}, \]
\[ \omega_1 := X, \Lambda_1 = \{ M(1), M(X) \}, q_1 = (X^2, Y), \]
\[ \omega_2 := Y, \Lambda_2 = \{ M(1), M(Y) \}, q_2 = (X, Y^2), \]
\[ l : m^\infty = (X) \subset (X, Y^2), \]
\[ (X^2, XY) = (X) \cap (X^2, Y). \]

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

\[ \rho = 2, \]
\[ \mathcal{M}(l + m^2) = \{ M(1), M(X) - aM(Y), M(Y) \}, \]
\[ \omega_1 := X, \Lambda_1 = \{ M(1), M(X) - aM(Y) \}, q_1 = (X^2, Y + aX), \]
\[ \omega_2 := Y, \Lambda_2 = \{ M(1), M(Y) \}, q_2 = (X, Y^2), \]
\[ l : m^\infty = (X) \subset (X, Y^2), \]
\[ (X^2, XY) = (X) \cap (X^2, Y + aX). \]
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 $\prec$ be the lex. ordering induced by $X_1 \prec X_2$.

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

$$T(f_0) < T(f_1) < \cdots < T(f_k).$$

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 $i$;

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

$H_{i+1} \in (G_1 \cdots G_i, \ldots, H_j G_{j+1} \cdots G_i, \ldots, H_{i-1} G_i, H_i), \forall i$. 
VII. Axis-of-Evil Theorem


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

\[ I = \bigcap q_i \subset P, \sqrt{q_i} = (X_1 - a_{i1}, \ldots, X_n - a_{in}) \]

in terms of a Macaulay representation, i.e. of its roots \((a_{i1}, \ldots, a_{in})\) and of the Macaulay basis of each \(q_i\).

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 22\(^{th}\) letter \(W\) in order to perform german gematria.
Let $I \subset \mathcal{P}$ be a zero-dimensional radical ideal;

$Z := \{a_1, \ldots, a_s\} \subset k^n$ its roots;

$N := N(I)$;

$G_{<}(I) := \{t_1, \ldots, t_r\}, t_1 < t_2 < \ldots < t_r$, $t_i := X_1^{d(i)} \cdots X_n^{d(i)}$ the minimal basis of its associated monomial ideal $T_{<}(I)$;

$G := \{f_1, \ldots, f_r\}, T(f_i) = t_i \forall i$, 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
  
  $F_{m\delta i} := N(Z_{m\delta i}) \subset T \cap k[X_1, \ldots, X_{m-1}]$

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

Moreover, setting

$\nu$ the maximal value such that $d^{(i)}_\nu \neq 0, d^{(i)}_m = 0, m > \nu$ so that $f_i \in k[X_1, \ldots, X_\nu] \setminus k[X_1, \ldots, X_{\nu-1}]$,

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

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