REVISTA INVESTIGACIÓN OPERACIONAL VOL. 27, No. 1, 75-98, 2006

CERLIENCO-MUREDDU CORRESPONDENCE AND LAZARD STRUCTURAL THEOREM

Maria Grazia Marinari*[1] and Teo Mora**[2]
*DIMA, Università di Genova
**DIMA and DISI, Università di Genova

ABSTRACT
This paper is devoted to characterize the shape of polynomial equation systems (viewed as polynomial ideals) with finitely many solutions (counting their multiplicities) and the dual structure of the quotient algebra. Our characterization links both the techniques for solving polynomial systems (Gianni–Kalkbrener Theorem) and the inverse interpolation problem (Möller Algorithm).
Key words: polynomial equations, duality, combinatorial description.

MSC 14L40

RESUMEN
Este trabajo se dedica a caracterizar la forma de sistemas de ecuaciones polinomiales (miradas como ideales polinomiales) con un número finito de soluciones (contando su multiplicidad) y la estructura dual del álgebra cociente. Nuestra caracterización conecta ambas técnicas para resolver sistemas polinomiales (Teorema de Gianni–Kalkbrener) y el problema de interpolación inversa (Algoritmo de Möller).

1 INTRODUCTION

In 1927 Macaulay [Macaulay (1927)] gave a construction which, to each monomial ideal

$\mathbf{J} \subset k[X_1, . . . ,X_n] =: \mathbf{P}$,

associates a set **X** of distinct points in k^n such that, using modern lingo, the monomial ideal associated to each degree-compatible Gröbner basis of the radical ideal

$\mathbf{I} := \mathbf{I}(\mathbf{X}) := \{f \in k[X_1, . . . ,X_n] : f(a_1, . . . , a_n) = 0, \text{ for each } (a_1, . . . , a_n) \in \mathbf{X}\}$

is the given monomial ideal **J**, i.e. $\mathbf{J} = \mathbf{T}(\mathbf{I})$; moreover Macaulay explicitly stated a direct correspondence between the points of **X** and the monomials $\tau \notin \mathbf{J}$ forming the "Gröbner sous-éscalier" **N**(**I**).

In 1981 Möller [Möller- Buchberger (1982)] introduced Duality in Computer Algebra proposing an algorithm – essentially a multivariate version of Newton Interpolation –which, for each finite set of (distinct) points $\mathbf{X} \subset k^n$, computes the Gröbner basis and the "Gröbner sous-éscalier" of **I** := **I**(**X**). Möller's Algorithm was later refined and generalized [Faugère et. al. (1993), Marinari et. al. (1993)] to any finite set of functionals $\mathbf{L} \subset \mathbf{P}^* := \mathrm{Hom}_k(\mathbf{P}, k)$ such that

$P(\mathbf{L}) := \{f \in \mathbf{P} : \lambda(f) = 0, \text{ for each } \lambda \in \mathbf{L}\}$

[1] marinari@dima.unige.it
[2] theomora@disi.unige.it

is an ideal, computing the Gröbner-basis and sous-éscalier of **N**(P(**L**)).

In 1985 Lazard [Lazard (1985)] characterized the Gröbner-basis of any ideal **I** $\subset k[X_1, X_2]$ thus also refining Macaulay's result. Lazard's result was then subsumed by Gianni-Kalkbrener Theorem [Gianni (1987), Kalkbrener (1987)] describing the lexicographical reduced Gröbner-basis of any zero-dimensional ideal in **P**.

In 1990 Cerlienco–Mureddu [Cerlienco-Mureddu (1990)] gave an algorithm which, for each finite set of distinct points **X** $\subset k^n$, computes the Gröbner sous-éscalier **N**(**I**) of **I**:= I(**X**) and a direct correspondence between **X** and **N**(**I**).

Recently, [Marinari - Mora (2003)] merged Lazard's result, Cerlienco–Mureddu Algorithm and Möller Algorithm in order to give an enhanced Lazard Structural Theorem for a zero-dimensional radical ideal.

Finding out later that Cerlienco and Mureddu [Cerlienco-Mureddu (1990)] had extended (in 1995) their results to cover any zero-dimensional ideal whose primary components are translations of monomial primary ideals at the origin (CeMu-ideal), [Marinari - Mora (2004)] generalized the Enhanced Lazard Structural Theorem to CeMu-ideals, strongly improving its factorization results.

The aim of this paper is to extend to all zero-dimensional ideals both Cerlienco –Mureddu Algorithm and the Enhanced Lazard Structural Theorem; as we will see, the factorization results don't hold in the general setting.

We are therefore able to describe the structure of the lexicographical Gröbner basis of any zero dimensional ideal **I** $\subset k[X_1, . . . ,X_n]$ in terms of its Macaulay Representation (i.e. the set of the inverse systems at each root of **I**).

In particular, denoting < the lexicographical ordering induced by $X_1 < . . .<X_n$ an easy combinatorial algorithm returns the "Gröbner sous-éscalier" **N**(**I**) of **I**, thus allowing to deduce the minimal basis

$\{t_1, . . . , t_r\}, t_1 < t_2 < . . . < t_r$

of its associated monomial ideal **T**(**I**) and (by interpolation) the unique reduced lexicographical Gröbner basis

G := $\{f_1, . . . , f_r\}$, **T**$(f_i) = t_i$ for each i.

Moreover, for a CeMu-ideal, a variation of Cerlienco–Mureddu algorithm allows to deduce a canonical "linear" factorization of each element of such Gröbner basis in the following sense: for each $t_i := X_1^{d_1} \cdots X_n^{d_n}$, $1 \le l \le r$, a combinatorial algorithm and interpolation allow to deduce polynomials

$\gamma_{m\delta i} = X_m - g_{m\delta i} (X_1, . . . ,X_{m-1})$

for each i, m, δ, $1 \le i \le r$, $1 \le m \le n$, $1 \le \delta \le d_m$ satisfying

$f_i = \Pi_m \Pi_\delta \gamma_{m\delta i}$ (mod $(f_1, . . . , f_{i-1})$) for each i.

At least in the radical ideal case, this combinatorial description subsumes Gianni–Kalkbrener Theorem as a corollary and gives a combinatorial justification of their algorithm.

2 NOTATION

Let **P** := $k[X_1, . . . ,X_n]$, **m** = $(X_1, . . . ,X_n)$ the maximal ideal at the origin, **T** := $\{X_1^{a_1} \cdots X_n^{a_n} : (a_1,...,a_n) \in \mathbb{N}^n\}$, < the lexicographical ordering on **T** induced by $X_1 < \cdots < X_n$.

The algebraic closure of k is denoted $\bar{k}$ and for each zero-dimensional ideal **I** $\subset$ **P**, Z(**I**) := {**a** $\in \bar{k}^n$: f(a) = 0, $\forall$f $\in$ **I**} $\subset \bar{k}^n$; for any $\alpha = (b_1, \ldots, b_d) \subset \bar{k}^d$, Φ_α is the projection Φ_α: **P** $\rightarrow \bar{k}[X_{d+1}, \ldots, X_n]$ defined by

$\Phi_\alpha(f) = f(b_1, \ldots, b_d, X_{d+1}, \ldots, X_n)\ \forall f \in k[X_1, \ldots, X_n]$.

Each element f $\in$ **P** can be uniquely expressed either as

$$f = \sum_{i=0}^{\deg(f)} g_i X_n^i \in k[X_1, \ldots, X_{n-1}][X_n]$$

$g_i \in k[X_1, \ldots, X_{n-1}]$, $g_{\deg(f)} \neq 0$, or as a linear combination

$$f = \sum_{t \in T} c(f,t)t = \sum_{i=1}^{s} c(f,t_i)t_i$$

$c(f, t_i) \neq 0$, $t_i \in$ **T** , $t_1 > \cdots > t_s$ of terms t $\in$ **T** with coefficients c(f, t) $\in$ k; and we will denote Lp(f) := $g_{\deg(f)}$ the *leading polynomial* of f, T(f) := t_1 its *maximal term*, lc(f) := c(f, t_1) its *leading coefficient.*

For each subset G $\subset$ **P**, **T**{G} := {**T**(g) : g $\in$ G} and **T**(G) := {τ**T**(g) : $\tau \in$ **T** , g $\in$ G} is the monomial ideal it generates. For each ideal **I** $\subset$ **P**, **G**(**I**) is the *minimal basis* of the monomial ideal **T**(**I**) = **T**{I},

N(**I**) := **T** \ **T**(**I**) and

B(**I**) := {X_ht : 1 $\leq$ h $\leq$ n, t $\in$ **N**(**I**)} \ **N**(**I**) = **T**(**I**) $\cap$ ({1} $\cup$ {X_ht : 1 $\leq$ h $\leq$ n, t $\in$ **N**(**I**)}),

we set k[**N**(**I**)] := Span_k(**N**(**I**)).

For each f $\in$ **P**, there is [Buchberger (1965), (1970) and Buchberger–Loos (1982)] a unique *canonical form*

g := Can(f, **I**) = $\sum_{t \in \mathbf{N}(\mathbf{I})} \gamma(f, t, <)t \in$ k[**N**(**I**)]

such that f - g $\in$ **I**. A *Gröbner basis* [Buchberger (1965), (1970)] of **I** is any set G $\subset$ **I** such that **T**(G) = **T**{**I**}, i.e. **T**{G} generates the monomial ideal **T**(**I**) = **T**{**I**}; the *reduced Gröbner basis* [Buchberger (1965), (1970)] of **I** is the set **G**(**I**) := {τ - Can(τ, **I**) : $\tau \in$ **G**(**I**)}; the *border basis* [Marinari et.al (1993)] of **I** is the set $\mathcal{B}$(**I**) := {τ - Can(τ, **I**) : $\tau \in$ **B**(**I**)}.

Two sets L := {$l_1, \ldots, l_s$} $\subset$ **P*** := Hom_k(**P**, k), and **q** = {$q_1, \ldots, q_s$} $\subset$ **P** are triangular if $l_i(q_j)$ = 0, for each i < j.

Denoting, for each k-vector subspace **L** $\subset$ **P***,

P(**L**) := {g $\in$ **P** : l(g) = 0, for each $l \in$ **L**}

and, for each k-vector subspace P $\subset$ **P**,

L(P) := {$l \in$ **P*** : l(g) = 0, for each g $\in$ P},

we recall [Macaulay (1927, 1913), Marinari et.al (1996), Alonso et.al (2000), Mora (2005)] that the mutually inverse maps L(·) and P(·) give a biunivocal, inclusion reversing, correspondence between the set of the zero-dimensional ideals P $\subset$ **P** and the set of 'certain' finite k-dimensional **P**-modules **L** $\subset$ **P***.

3 MACAULAY FRAMEWORK

For each $\tau \in \mathbf{T}$, letting

$M(\tau) := c(f, \tau)$, for each $f = \sum_{t \in \mathbf{T}} c(f, t)t \in \mathbf{P}$

one has a morphism $M(\tau) : \mathbf{P} \to k$; letting $\mathbf{M} := \{M(\tau) : \tau \in \mathbf{T}\}$, $\mathrm{Span}_k(\mathbf{M}) \subset \mathbf{P}^*$ is the set of the *Noetherian equations* [Macaulay (1927, 1913), Mora (2005)] of **P**.

For each element

$l = \sum_i c_i M(\tau_i) \in \mathrm{Span}_k(\mathbf{M}) : c_i \in k \setminus \{0\}, \tau_i \in T, \tau_1 < \tau_2 < \cdots < \tau_i < \cdots$

$\mathbf{T}_<(l) := \tau_1$ is the *leading term* of l, $\mathrm{ord}(l) := \min_i(\deg(\tau_i))$ is the *order* (or *under-degree*) of l, $\deg(l) := \max_i(\deg(\tau_i))$ is the *degree* of l.

For a subset $\Lambda \subset \mathrm{Span}_k(\mathbf{M})$, we set

$\mathbf{T}_<\{\Lambda\} := \{\mathbf{T}_<(l), l \in \Lambda\}$, $\mathbf{N}_<(\Lambda) := \mathbf{T} \setminus \mathbf{T}_<\{\Lambda\}$.

For each $j = 1, \ldots, n$, $\sigma_j := \sigma_{X_j} : \mathrm{Span}_k(\mathbf{M}) \to \mathrm{Span}_k(\mathbf{M})$ is the linear map such that

$$\sigma_{X_j}(M(\tau)) = \begin{cases} M(w) & if \quad \tau = X_j w \\ 0 & if \quad X_j \nmid \tau \end{cases} \qquad \forall \tau \in T;$$

since, for each i, j, $\sigma_{X_i X_j} := \sigma_{X_i} \sigma_{X_j}$, a linear map $\sigma_t : \mathrm{Span}_k(\mathbf{M}) \to \mathrm{Span}_k(\mathbf{M})$ is inductively defined for each $t \in \mathbf{M}$ by $\sigma_{X_i t} := \sigma_{X_i} \sigma_t$ so that for each $\tau, w \in \mathbf{T}$ we have

$$\sigma_\tau(M(w)) = \begin{cases} M(v) & if \quad w = \tau v \\ 0 & if \quad \tau \nmid w \end{cases}$$

for each $f := \sum_{\tau \in \mathbf{T}} c(f, \tau)\tau \in \mathbf{P}$, $\sigma_f : \mathrm{Span}_k(\mathbf{M}) \to \mathrm{Span}_k(\mathbf{M})$ is defined as

$$\sigma_f(l) = \sum_{\tau \in T} c(f, \tau) \sigma_\tau(l) \qquad for\ each\ l \in Span_k(M).$$

A vector subspace $\Lambda \subset \mathrm{Span}_k(\mathbf{M})$ is called *stable* if for each $l \in \Lambda$ and each $f \in \mathbf{P}$, $\sigma_f(l) \in \Lambda$.

Proposition 3.1 For any $f, g \in \mathbf{P}$ and $w \in \mathbf{T}$ it holds

$$M(w)(fg) = \sum_{\substack{v \in T \\ v\tau = w}} M(v)(f)M(\tau)(g)$$

Proof: For
$f = \sum_{v \in \mathbf{T}} c(f, v)v = \sum_{v \in \mathbf{T}} M(v)(f)v$,
$g = \sum_{\tau \in \mathbf{T}} c(g, \tau)\tau = \sum_{\tau \in \mathbf{T}} M(\tau)(g)\tau$,
$fg = \sum_{u \in \mathbf{T}} c(fg, u)u = \sum_{u \in \mathbf{T}} M(u)(fg)u$
and, for each $w \in \mathbf{T}$, we have

$$M(w)(fg) = c(fg, w) = \sum_{\substack{v \in T \\ v\tau = w}} c(f, v)c(g, \tau) = \sum_{\substack{v \in T \\ v\tau = w}} M(v)(f)M(\tau)(g).$$

Denoting, for each k-vector subspace $\Lambda \subset \mathrm{Span}_k(\mathbf{M})$,

$\mathbf{I}(\Lambda) := \{f \in \mathbf{P} : l(f) = 0, \text{ for each } l \in \Lambda\}$

and, for each k-vector subspace P $\subset$ **P**,

M(P) := {$l \in$ Span$_k$(**M**) : l(f) = 0, for each f $\in$ P},

we recall [Macaulay (1913), (1916), Marinari et. al (1993), Mora (2005)] that the mutually inverse maps I(·) and M(·) give a biunivocal, inclusion reversing, correspondence between the set of the **m**-closed ideals **I** $\subset$ **P** and the set of the stable k-vector subspaces $\Lambda \subset$ Span$_k$(**M**), **m**-primary ideals being dual to finite-dimensional stable spaces and we remark that, for each **m**-closed ideal **I** $\subset$ **P**, M(**I**) consists of all the Noetherian equations of **I.**

A basis {$l_1, l_2, \ldots, l_i, \ldots$} of a stable vector subspace $\Lambda \subset$ Spank(**M**) is called the *Macaulay basis* [Macaulay (1913), Mora (2005)] of Λ w.r.t. < if

- $\mathbf{T}_<\{\Lambda\}$:= {$\mathbf{T}_<(l_i)$} $\subset$ **T** is an order ideal[3];
- $l_i := M(T_<(l_i)) + \sum_{v \in N_<(\Lambda)} \xi(v, T_<(l_i)) M(v)$, for suitable $\xi(v, \mathbf{T}_<(l_i)) \in$ k and for each i.

If we set $l(\tau) := M(\tau)+\sum_{t\in T(I)}\gamma(t,\tau,\mathbf{N(I)})M(t) \in$ Span$_k$(**M**), for each **m**-closed ideal **I** $\subset$ **P** and each $\tau \in$ **N**(**I**), then **I** can be characterized [Macaulay (1913), (1916), Marinari et. al (1993), Mora (2005)] by the unique *Macaulay basis* {$l(\tau)$: $\tau \in$ **N**(**I**)} of M(**I**).

Therefore, each zero-dimensional ideal **I** $\subset$ **P** can be considered as *given* if we know the set **Z** := Z(**I**) and, for each **a** $\in$ **Z**, the Macaulay basis of the corresponding primary component of **I**.

For each **a** $\in$ **Z** := Z(**I**), **a** := ($a_1, \ldots, a_n$), denote:

- $\lambda_{\mathbf{a}}$: **P** $\rightarrow$ **P** the translation $\lambda_{\mathbf{a}}(X_i)=X_i+a_i$
- $\mathbf{m_a} = (X_1 - a_1, \ldots, X_n - a_n)$,
- $\mathbf{q_a}$ the $\mathbf{m_a}$-primary component of **I**,
- $\Lambda_{\mathbf{a}}$:= M($\lambda_{\mathbf{a}}(\mathbf{q_a})$) $\subset$ Span$_k$(**M**),
- $l_{v\mathbf{a}}$, $\forall$v $\in$ $\mathbf{N}_<(\lambda_{\mathbf{a}}(\mathbf{q_a}))$, the Macaulay equation $l_{v\mathbf{a}}$:= l(v) so that
- {$l_{v\mathbf{a}}$: v $\in$ $\mathbf{N}_<(\lambda_{\mathbf{a}}(\mathbf{q_a}))$} is the Macaulay basis of $\Lambda_{\mathbf{a}}$.

Setting s := $\sum_{\mathbf{a}\in\mathbf{Z}}$ deg($\mathbf{q}_a$) and

L := {$\lambda_1, \ldots, \lambda_s$} := { $l_{v\mathbf{a}}\lambda_{\mathbf{a}}$: v $\in$ $N_<(\lambda_{\mathbf{a}}(\mathbf{q_a}))$, **a** $\in$ **Z**},

we know that Span$_k$(**L**) = L(**I**) and **I** = P(Span$_k$(**L**)); moreover, w.l.o.g. we can assume **L** to be ordered so that, for each σ,

$\mathbf{I}_\sigma$ = **P**(Span$_k$\{$\lambda_1, \ldots, \lambda_\sigma$\})

is an ideal [[Macaulay (1913), (1916), Möller (1993), Mora (2005)] .

We also set

X := {$x_1, \ldots, x_s$} := {(**a**, v) : v $\in$ $\mathbf{N}_<(\mathbf{q_a})$, **a** $\in$ **Z**}

enumerated so that x_j = (**a**, v) $\Leftrightarrow$ $\lambda_j = l_{v\mathbf{a}}\lambda_{\mathbf{a}}$ and $\forall$j, $1 \le j \le s$, we set M(λ_j) := M(v)$\lambda_{\mathbf{a}}$ where $\lambda_j = l_{v\mathbf{a}}\lambda_{\mathbf{a}}$.

Under the following equivalent assumptions:

[3] A subset **N** $\subset$ **T** is called an *order ideal* if it satisfies st $\in$ **N** $\Rightarrow$ t $\in$ **N**, for each s, t $\in$ **T** .

• $\lambda = M(\lambda)$ for each $\lambda \in$ **L**,
• $l_{va} = M(v)$, for each $\lambda = l_{va}\lambda_{\mathbf{a}} \in$ **L**,
• each $\lambda_{\mathbf{a}}(\mathbf{q}_{\mathbf{a}})$ is a monomial ideal,

Cerlienco–Mureddu Algorithm [Cerlienco-Mureddu-(1990), (1995)] associates to each couple of sets **L** and **X** as above, an order ideal **N** := **N**(**L**) and a bijection $\Phi := \Phi(\mathbf{L}) : \mathbf{L} \to \mathbf{N}$, which, as we will proof later, satisfies

$\mathbf{N}_<(\mathbf{L}) = \mathbf{N}(P(Span_k(\mathbf{L})))$

for the lexicographical ordering induced by $X_1 < \cdots < X_n$.

Definition 3.2 The ordered sets **L**(**I**) := **L** and **X**(**I**) := **X** are called, respectively, *a Macaulay representation* and a *CeMu-skeleton* of **I** := **P**(**L**); each $\lambda = l_{va}\lambda_a \in$ **L** is called a *CeMu-functional* and each x = (a, v) ∈ **X** a *CeMu-card.*

Moreover, if $\forall\lambda = l_{va}\lambda_{\mathbf{a}} \in$ **L**, $\lambda = \mathbf{M}(\lambda) = \mathbf{M}(v)\lambda_{\mathbf{a}}$, then **I** is called a *CeMu-ideal,* **X** its *CeMu-scheme,* and each x = (**a**, v) ∈ **X** a *CeMu-condition.*

We need also to consider, for each m < n, the sets

$\mathbf{T}[1,m] := \mathbf{T} \cap k[X_1, \ldots, X_m] = \{X_1^{a_1} \cdots X_m^{a_m} : (a_1, \ldots, a_m) \in \mathbb{N}^m\}$,
$\mathbf{M}[1,m] := \{M(\tau) : \tau \in \mathbf{T}[1,m]\}$

and the projection

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

which we freely use to denote also the projections

$\pi_m : \mathbf{T} \approx \mathbb{N}^n \longrightarrow \mathbb{N}^m \approx \mathbf{T}[1,m]$, $\pi_m(X_1^{a_1} \cdots X_n^{a_n}) = X_1^{a_1} \cdots X_m^{a_m}$,
$\pi_m : \mathbf{M} \longrightarrow \mathbf{M}[1,m]$, $\pi_m(\mathbf{M}(\tau)) = \mathbf{M}(\pi_m(\tau))$,

and $\pi_m : k^n \times \mathbf{T} \to k^m \times \mathbf{T}[1,m]$, $\pi_m(\mathbf{a}, \tau) = (\pi_m(\mathbf{a}), \pi_m(\tau))$.

Recalling Macaulay's notation [Macaulay (1913), (1916)] for Noether equations as members of $k[X_1^{-1}, \ldots, X_n^{-1}]$, we remark that for each Noetherian equation

$l(\tau) := M(\tau) + \sum_{t \in \mathbf{T}(\mathbf{I})} \gamma(t, \tau, \mathbf{N}(\mathbf{I}))M(t) = \tau^{-1} + \sum_{t \in \mathbf{T}(\mathbf{I})} \gamma(t, \tau, \mathbf{N}(\mathbf{I}))t^{-1}$,

$\tau = X_1^{d_1} \cdots X_n^{d_n}$ there are unique polynomials
$f_i(X_1^{-1}, \ldots, X_i^{-1}) \in k[X_1^{-1}, \ldots, X_i^{-1}]$

so that

$$l(\tau) := \Big(\Big(\cdots (1 + X_1^{-1} f_1(X_1^{-1}))X_1^{-d_1} + X_2^{-1} f_2(X_1^{-1}, X_2^{-1})\Big)X_2^{-d_2} \cdots + X_{n-1}^{-1} f_{n-1}(X_1^{-1}, \ldots, X_{n-1}^{-1}))X_{n-1}^{-d_{n-1}} + X_n^{-1} f_n(X_1^{-1}, \ldots, X_n^{-1}))X_n^{-d_n}$$

and we set

$$\pi_m l(\tau) := (\cdots(1 + X_1^{-1} f_1(X_1^{-1})X_1^{-d_1} + \cdots\cdots + X_{m-1}^{-1} f_{m-1}(X_1^{-1}, \ldots, X_{m-1}^{-1})X_{m-1}^{-d_{m-1}} + X_m^{-1} f_m(X_1^{-1}, \ldots, X_m^{-1}) = \sigma_{X_m^{d_m}, \ldots, X_n^{d_n}}(l(\tau))(X_1^{-1}, \ldots, X_m^{-1},) \ldots,)) \in k[X_1^{-1}, \ldots, X_m^{-1}]$$

Finally, for a CeMu-functional $\lambda = l_{va}\lambda_{\mathbf{a}}$ we set

$\pi_m(\lambda) := \pi_m\pi_m\,(l_{va}\lambda_a) := \pi_m(l_{va})\lambda_{\pi_l}\,(a).$

4 LAZARD, GIANNI–KALKBRENER AND CERLIENCO–MUREDDU RESULTS

Theorem 4.1 (**Lazard Structural Theorem**) [Lazard (1985)]
Let **P** := $k[X_1,X_2]$, < the lexicographical ordering induced by $X_1 < X_2$, $\mathbf{I} \subset \mathbf{P}$ an ideal and $\{f_0, f_1, \ldots, f_k\}$ a Gröbner basis of **I**, ordered so that

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

Then

$f_0 = PG_1 \cdots G_{k+1}$,
$f_j = PH_jG_{j+1} \cdots G_{k+1},\ 1 \le j < k$,
$f_k = PH_kG_{k+1}$,

where

- P is the primitive part of $f_0 \in k[X_1][X_2]$;
- $G_i \in k[X_1],\ 1 \le i \le k + 1$;
- $H_i \in k[X_1][X_2]$ is a monic polynomial of degree d(i), for each i;
- $d(1) < d(2) < \cdots < d(k)$;
- $H_{i+1} \in (G_1 \cdots G_i, H_1G_2 \cdots G_i, \ldots, H_jG_{j+1} \cdots G_i, \ldots, H_{i-1}G_i, H_i),\ \forall i$.

Theorem 4.2 (**Gianni—Kalkbrener**) [Gianni (1987), Kalkbrener (1987)] Let $\mathbf{I} \subset \mathbf{P} := k[X_1,\ldots,X_n]$, be an ideal, < the lexicographical ordering induced by $X_1 < \cdots < X_n$ and $G := \{g_1, \ldots, g_s\}$ a Gröbner basis of **I** w.r.t. <, enumerated in such a way that

$\mathbf{T}(g_1) < \mathbf{T}(g_2) < \ldots < \mathbf{T}(g_{s-1}) < \mathbf{T}(g_s)$.

For each d, $1 \le d \le n$, $\delta \in \mathbb{N}$, set

$G_d := G \cap k[X_1, \ldots, X_d]$,
$G_{d\delta} := \{g \in G,\ g \in k[X_1, \ldots, X_d],\ deg_i(g) \le \delta\}$

and remark that
$G_{11} \subseteq G_{12} \subseteq \ldots \subseteq G_1 \subseteq \ldots \subseteq G_{d-1} \subseteq \ldots \subseteq G_{d\delta} \subseteq G_{d\delta+1} \subseteq \ldots \subseteq G_d \subseteq \ldots$,
each $G_{d\delta}$ is a section of both $G_{d\delta+1}$ and G_d.

Each G_d and $Lp_{d\delta}(G) := \{Lp(g),\ g \in G_{d\delta}\}$ are Gröbner bases w.r.t. < of, respectively, $\mathbf{I}_d := \mathbf{I} \cap k[X_1, \ldots, X_d]$ and $Lp_{d\delta}(\mathbf{I}) := \{Lp(g),\ g \in \mathbf{I}_d,\ deg(g) \le \delta\}$.

Moreover, for each d, $1 \le d \le n$ and each $\alpha := (b_1, \ldots, b_d) \in Z(\mathbf{I}_d)$,
denoting σ the minimal value such that $\Phi_\alpha(Lp(g_\sigma)) \ne 0$ and j, δ the values such that

$g_\sigma = Lp(g_\sigma)X_j^{\delta+1} + \cdots \in k[X_1, \ldots, X_j] \setminus k[X_1, \ldots, X_{j-1}]$

it holds
- j = d+1,
- for each $g \in G_d$, $\Phi_\alpha(g) = 0$,
- for each $g \in G_{d+1\delta}$, $\Phi_\alpha(g) = 0$,
- $\Phi_\alpha(g_\sigma) = \gcd(\Phi_\alpha(g) : g \in G_{d+1}) \in k[X_{d+1}]$,
- for each $b \in k$, $(b_1, \ldots, b_d, b) \in Z(\mathbf{I}_{d+1}) \Leftrightarrow \Phi_\alpha(g_\sigma)(b) = 0$.

Algorithm 4.3 (**Cerlienco–Mureddu**) [Cerlienco-Mureddu-(1990), (1995)] Given a Macaulay representation **L** consisting of CeMu-functionals, and a CeMu-skeleton **X** of an unknown zero-dimensional CeMu-ideal $\mathbf{I} \subset \mathbf{P}$, determine it by assigning an order ideal **N** := **N**(**L**) and a bijection
$\Phi := \Phi(\mathbf{L}) : \mathbf{L} \to \mathbf{N}$ satisfying

$\mathbf{N}_<(\mathbf{L}) = \mathbf{N}(P(\mathrm{Span}_k(\mathbf{L})))$

for the lexicographical ordering induced by $X_1 < \cdots < X_n$.

The algorithm is inductive on s = #(**L**), the only possible solution for s = 1 being **N** = {1}, $\Phi(\lambda_1) = 1$.

Let then $\mathbf{L}' := \{\lambda_1, \ldots, \lambda_{s-1}\}$, $\mathbf{N}' := \mathbf{N}(\mathbf{L}')$, $\Phi' := \Phi(\mathbf{L}')$, and set

$m := \max (j : \exists i < s : \pi_j(\lambda_i) = \pi_j(\lambda_s))$,
$d := \#\{\lambda_i,\ i < s : \pi_m(\lambda_i) = \pi_m(\lambda_s),\ \Phi'(\lambda_i) \in \mathbf{T}[1,m+1]\}$,
$\mathbf{W} := \{\lambda_i : \Phi'(\lambda_i) = w_i X_{m+1}^d,\ w_i \in \mathbf{T}[1,m]\} \cup \{\lambda_s\}$,
$\mathbf{V} := \pi_m(\mathbf{W})$,
$w := \Phi(\mathbf{V})(\pi_m(\lambda_s))$,
$t_s := w X_{m+1}^d$,

where **N**(**V**) and Φ(**V**) are the result of applying the present algorithm to **V**, which can be inductively done since $\#(\mathbf{V}) \le s - 1$. We then define

$\mathbf{N} := \mathbf{N}' \cup \{t_s\}$ and $\Phi(\lambda_i) := \begin{cases} \Phi'(\lambda_i) & i < s \\ t_s & i = s \end{cases}$

5 CERLIENCO–MUREDDU CORRESPONDENCE

Let
$\mathbf{L} := \{\lambda_1, \ldots, \lambda_s\}$, $X := \{x_1, \ldots, x_s\} \subset k^n \times \mathbf{T}$,
$x_i = (\mathbf{a}_i, v_i)$, $\mathbf{a}_i := (a_{i1}, \ldots, a_{in})$, $v_i = \prod_{l=1}^{n} X_l^{\alpha_{il}}$
be the Macaulay representation and the CeMu-skeleton of an unknown zero-dimensional ideal $\mathbf{I} \subset \mathbf{P}$. Our aim is to generalize Cerlienco–Mureddu Algorithm removing the assumption **I** a CeMu-ideal.

The algorithm is inductive on s = #(**X**), the only possible solution for s = 1 being **N** = {1}, $\Phi(x_1) = 1$.
Let us therefore consider $\mathbf{L}' := \{\lambda_1, \ldots, \lambda_{s-1}\}$, the corresponding order ideal $\mathbf{N}' := \mathbf{N}(\mathbf{L}')$ and the bijection $\Phi' := \Phi'(\mathbf{L}')$.

Let us also denote, $\forall \nu,\ 1 \le \nu < n,\ \delta \in \mathbb{N}$,

$Y_{\nu\delta} := \mathrm{Span}_k\{\pi_\nu(\lambda) : \lambda \in L', \text{ exists } w \in \mathbf{T}[1, \nu] : \Phi'(\lambda) = w X_{\nu+1}^{\delta}\}$.

If $P(\mathrm{Span}_k(\mathbf{L}))$ is radical, by abuse of notation, we simply identify each $x_i = (\mathbf{a}_i, 1)$ and the corresponding $\lambda_i = \lambda_{a_i}$ with a_i. With this notation, we set

$m := \max (j : \pi_j(\lambda_s) \in \mathrm{Span}_k(\pi_j(\mathbf{L}')))$,
$d := \min\{\delta : \pi_m(\lambda_s) \notin Y_{m\delta}\}$,
$\mathbf{W} := \{\pi_m(\lambda) : \Phi'(\lambda) = w X_{m+1}^d,\ w \in \mathbf{T}[1,m]\} \cup \{\pi_m(\lambda_s)\}$

$w := \Phi(\mathbf{W})(\pi_m(\lambda_s))$,
$t_s := w X_{m+1}^{d}$

where **N**(**W**) and Φ(**W**) result by applying the present algorithm to **W**, which can be inductively done since #(**W**) ≤ s - 1. We then define

$\mathbf{N} := \mathbf{N}' \cup \{t_s\}$ and $\Phi(\lambda_i) := \begin{cases} \Phi'(\lambda_i) & i < s \\ t_s & i = s \end{cases}$

Let

$\mathbf{L} := \{\lambda_1, \ldots, \lambda_{1s}\}$, $\mathbf{X} := \{x_1, \ldots, x_s\} \subset k^n \times T$,

$x_i = (\mathbf{a}_i, v_i)$, $\mathbf{a}_i := (a_{i1}, \ldots, a_{in})$, $v_i = \prod_{l=1}^{n} X_l^{\alpha_{il}}$

be the Macaulay representation and the CeMu-skeleton of a zero-dimensional ideal **I** ⊂ **P** and let **N** := **N**(**L**), Φ := Φ(**L**) be the result of Cerlienco–Mureddu Correspondence. Then

Lemma 5.1 If $\mathbf{Y} = \{\lambda_1, \ldots, \lambda_r\} \subset \mathbf{L}$ is an initial segment of **L** then

- **Y** is a CeMu-skeleton,
- **N**(**Y**) ⊂ **N**(**L**),
- for each $j \le r < s$, $\Phi(\mathbf{Y})(\lambda_j) = \Phi(\mathbf{L})(\lambda_j)$.

Remark 5.2 Let us remark that, by construction, we will have

$P(\mathrm{Span}_k(\pi_v(\mathbf{L})')) = \mathbf{Y}_{v0} \supset \mathbf{Y}_{v1} \supset \cdots \supset \mathbf{Y}_{v\delta} \supset \mathbf{Y}_{v\delta+1} \supset \cdots$;
$\mathbf{I} \cap k[X_1, \ldots, X_v] = P(\mathrm{Span}_k(\pi_v(\mathbf{L}'))) = P(\mathbf{Y}_{v0}) \cdots \subset P(\mathbf{Y}_{v\delta}) \subset \mathbf{P}(\mathbf{Y}_{v\delta+1}) \subset \cdots$.

The result is essentially a specialization of Kalkbrener's Theorem [Kalkbrener (1997)].

6 LAZARD STRUCTURAL THEOREM

Let

$\mathbf{L} := \{\lambda_1, \ldots, \lambda_s\}$, $\mathbf{X} := \{x_1, \ldots, x_s\} \subset k^n \times \mathbf{T}$,

$x_i = (\mathbf{a}_i, v_i)$, $\mathbf{a}_i := (a_{i1}, \ldots, a_{in})$, $v_i = \prod_{l=1}^{n} X_l^{\alpha_{il}}$

be the Macaulay representation and the CeMu-skeleton of a zero-dimensional ideal **I** ⊂ **P** and let **N** := **N**(**L**), Φ := Φ(**L**) be the result of Cerlienco–Mureddu Correspondence. Then

Fact 6.1 It holds

(A) **N** := **N**(**I**).

Since **N** is an order ideal, ***T*** := **T** \ **N** is a monomial ideal whose minimal basis **G** := $\{t_1, \ldots, t_r\}$ will be ordered so that $t_1 < t_2 < \ldots < t_r$.

Denoting further

$\mathbf{B} := (\{1\} \cup \{X_i\tau : \tau \in \mathbf{N}\}) \setminus \mathbf{N}$

we obviously obtain

Corollary 6.2 It holds

(B) **G**(**I**) = **G** = $\{t_1, \ldots, t_r\}$, $t_1 < t_2 < \ldots < t_r$;

(C) **B**(**I**) = **B**.

Let us extend the ordering of **L** to **N** = $\{\tau_1, \dots, \tau_r\}$ enumerating it so that $\tau_\sigma = \Phi(\lambda_\sigma)$, for each σ and let us denote the ordering of **L** and **N** by $\prec$ so that
for each α, β, $\tau_\alpha \prec \tau_\beta$, $\lambda_\alpha \prec \lambda_\beta$, $\Leftrightarrow \alpha < \beta$.

Denote for each $\tau \in$ **N**

- **L**$(\tau) := \{\lambda \in$ **L** $: \lambda \prec \Phi^{-1}(\tau)\} = \{\lambda \in$ **L** $: \Phi(\lambda) \prec \tau\}$,
- $X(\tau) := \{x_j : \lambda_j \in$ **L**$(\tau)\}$,
- **I**(**L**(τ)) := P(Span$_k$(**L**(τ))),

and, for each $\tau \in$ **N** $\cup$ **B**

- **N**$(\tau) := \{w \in$ **N** $: w \prec \tau\}$,

so that

Corollary 6.3 It holds

(D) For each $\tau \in$ **N** there is a unique polynomial

$$f_\tau := \tau - \sum_{w \in N(\tau)} c(f_\tau, w) w$$

such that $\lambda(f_\tau) = 0$, for each $\lambda \in$ **L**(τ).

(E) For each $\tau \in$ **G** there is a unique polynomial

$$f_\tau := \tau - \sum_{w \in N(\tau)} c(f_\tau, w) w$$

such that $\lambda(f_\tau) = 0$, for each $\lambda \in$ L.

Proof: Since #**L**(τ) = #**X**(τ) = #**N**(τ) and #**L** = #**X** = #**N**, f_τ can be computed by interpolation.

In the same mood, but interpolation is not sufficient to prove it, we can state

Fact 6.4 It holds

(F) For each $\tau \in$ **B** there is a polynomial

$$f_\tau := \tau - \sum_{w \in N(\tau)} c(f_\tau, w) w$$

$\lambda(f_\tau) = 0$, for each $\lambda \in$ **L**.

Corollary 6.5 It holds:

(G) The reduced Gröbner-basis of **I** is

G(**I**) := $\{f_\tau : \tau \in$ **G**$\}$;

moreover, for each $\tau \in$ **N**, **T**$(f_\tau) = \tau$.

(H) The border basis of **I** is

B(**I**) := $\{f_\tau : \tau \in$ **B**$\}$;

Proof: For each $\tau \in \mathbf{G} \cup \mathbf{B}$, τ is the only term in f_τ which is not a member of $\mathbf{N}$ so that $\mathbf{T}(f_\tau) = \tau$. For any $\tau \in \mathbf{N}$, $\mathbf{T}(f_\tau) = \tau$ because Cerlienco–Mureddu Correspondence grants $\tau \in \mathbf{G}(\mathbf{I}(\mathbf{L}(\tau)))$ and $\mathbf{N}(\mathbf{I}(\mathbf{L}(\tau))) = \mathbf{N}(\tau)$.

Fact 6.6 It holds:

(I) For each ν, $1 \le \nu < n$,

let j_ν be the value such that $t_{j_\nu} < X_{\nu+1} \le t_{j_{\nu+1}}$; then $\{f_{t_1}, \ldots, f_{t_{j_\nu}}\}$ is a minimal Gröbner basis of $P(\mathrm{Span}_k(\pi_\nu(\mathbf{L})))$ and of $\mathbf{I} \cap k[X_1, \ldots, X_\nu]$; for each $\delta \in \mathrm{IN}$, let $j(\nu\delta)$ be the value such that $t_{j(\nu\delta)} < X_{\nu+1}^{\delta} \le t_{j(\nu\delta)+1}$; then $\{\mathrm{Lp}(f_{t_1}), \ldots, \mathrm{Lp}(f_{t_{j\nu\delta}})\}$ is a Gröbner basis of $\mathbf{I}(\mathbf{Y}_{\nu\delta})$;

(L) for each j, $1 \le j \le s$, $\lambda_j(f_{\tau_j}) \ne 0$ so that $\mathbf{L}$ and $\{\lambda_j(f_{\tau_j})^{-1} f_{\tau_j}, 1 \le j \le s\}$ are triangular.

7 INTERMEZZO: FACTORIZATION RESULTS

Let us now restrict ourselves to a CeMu-ideal, assuming that

$\mathbf{L} := \{\lambda_1, \ldots, \lambda_{1s}\}$, $X := \{x_1, \ldots, x_s\} \subset k^n \times \mathbf{T}$,

$x_i = (\mathbf{a}_i, v_i)$, $\mathbf{a}_i := (a_{i1}, \ldots, a_{in})$, $v_i = \prod_{l=1}^{n} X_l^{\alpha_{il}}$

are the Macaulay representation and the CeMu-scheme of a CeMu-ideal $\mathbf{I}$, so that, for each i,

$\lambda_i = M(\lambda) = M(v_i)\lambda_{a_i}$, for each i, $1 \le i \le s$.

Under this assumption, for any term

$\tau := X_1^{d_1} \cdots X_n^{d_n} \in \mathbf{T} \setminus \mathbf{N}(\mathbf{L})$

such that $\mathbf{N} \cup \{\tau\}$ is an order ideal, we define, for each m, $1 \le m \le n$:

$\mathbf{N}_m(\tau) := \mathbf{N}_m(\mathbf{L}, \tau) := \{w \in \mathbf{T}[1,m] : \tau > wX_{m+1}^{d_{m+1}} \cdots X_n^{d_n} \in \mathbf{N}\}$,
$A_m(\tau) := A_m(\mathbf{L}, \tau) := \{\Phi^{-1}(wX_{m+1}^{d_{m+1}} \cdots X_n^{d_n}) : w \in \mathbf{N}_m(\tau)\} \subset \mathbf{L}$,
$B_m(\tau) := B_m(\mathbf{L}, \tau) := \pi_m(A_m(\tau)) \subset (k[X_1, \ldots, X_m])^*$,
$C_m(\tau) := C_m(\mathbf{L}, \tau) := \{\pi_m(\lambda) \in B_m(\tau) : \pi_{m-1}(\lambda) \notin B_{m-1}(\tau)\}$,
$\mathbf{L}_m(\tau) := L_m(\mathbf{L}, \tau) := \{\lambda \in \mathbf{L} : \{\pi_m(\lambda) \in C_m(\tau)\} \subset \mathbf{L}$;
$D_m(\tau) := D_m(\mathbf{L}, \tau) := \{x_i \in \mathbf{X} : \{\pi_m(\lambda_i) \in C_m(\tau)\} \subset k^m \times \mathbf{T}[1,m]$;
$M_m(\tau) := M_m(\mathbf{L}, \tau) := \{w \in \mathbf{T}[1,m] : w < X_m^{d_m}, wX_{m+1}^{d_{m+1}} \cdots X_n^{d_n} \in \mathbf{N}\}$,
$M_m(\tau) := \{w \in M_m(\tau) : w$ □ $\tau\}$,

where, with slight abuse of notation, we have

$\mathbf{N}_n(\tau) := \{w \in \mathbf{T} : w < \tau\}$, $A_n(\tau) := \{\lambda : \Phi(\lambda) < \tau\}$, $C_1(\tau) := B_1(\tau)$.

Lemma 7.1 With the notation above, it holds

1. $\#(B_m(\tau)) = \#(A_m(\tau)) = \#(\mathbf{N}_m(\tau))$;

2. Cerlienco–Mureddu Correspondence associates to $B_m(\tau)$ the order ideal

$\mathbf{N}(B_m(\tau)) = \mathbf{N}_m(\tau)$

and the bijection $\Phi(B_m(\tau))$ defined by

$\Phi(B_m(\tau))(\pi_m(x)) X_{m+1}^{d_{m+1}} \cdots X_n^{d_n}) = \Phi(x)$, for each $x \in A_m$;

3. $\#(L_m(\tau)) = \#(C_m(\tau)) \le \#(M_m(\tau))$;

4. under Cerlienco–Mureddu Correspondence one has

$N(C_m(\tau)) \subset \{w \in \mathbf{T}[1,m] : w < X_m^{d_m}\}$;

5. $L = \cup_m L_m(\tau)$.

Proof:

1. is trivial;

2. Cerlienco–Mureddu Algorithm when applied to the ordered set **L** associates each element $\lambda \in A_m(\tau)$ to the term

$\Phi(\lambda) = \Phi(\pi_m(A_m(\tau)))(\pi_m(\lambda)) X_{m+1}^{d_{m+1}} \cdots X_n^{d_n})$;

3. in order to obtain $M_m(\tau)$ one has to remove from $N_m(\tau)$ the subset

$\{w X_m^{d_m} \in N_m(\tau) : w \in \mathbf{T}[1,m-1]\} = \{ w X_m^{d_m} : w \in \mathbf{N}_{m-1}(\tau)\}$

while for each $w \in N_{m-1}(\tau)$ there are $d_m + 1$ CeMu-conditions $y = (\mathbf{a}, v) \in k^m \times \mathbf{T}[1,m]$ for which

$M(v)\lambda_a \in B_m(\tau)$ and $\Phi(B_{m-1}(\tau))(\pi_{m-1}(l_{va}\lambda_a) = w$.

4. In order that there is $w \in \mathbf{N}(C_m(\tau))$ such that $w \ge X_m^{d_m}$, Cerlienco–Mureddu Algorithm requires that $\exists$ at least d_m+1 CeMu-conditions $X_i, \ldots, X_{d_m}, X_i = (\mathbf{a}_i, v_i)$, $0 \le i \le d_m$ such that

$\pi_m(X_0) = \cdots = \pi_m(X_i) = \cdots = \pi_m(X_{d_m})$,

so that $\pi_{m-1}(M(v_i)\lambda_{ai}) \in B_{m-1}(\tau)$

5. If $\lambda \in \mathbf{L}$ is such that $\Phi(\lambda) < \tau$, then there is a minimal value $m \le n$ for which $\lambda \in A_m(\tau)$, $\pi_m(\lambda) \in B_m(\tau)$, $\pi_m(\lambda) \in C_m(\tau)$, $\lambda \in L_m(\tau)$.

If $\lambda \in L$ is such that $\Phi(\lambda) = X_1^{e_1} \cdots X_n^{e_n} > \tau$, there is $m \le n$ such that $e_m > d_m$, while $e_i = d_i$, for each $i > m$; this implies that there is $l \in A_m(\tau)$ such that $\pi_m(l) = \pi_m(\lambda)$ so that $\lambda \in D_m(\tau)$.

As for (D-E) linear interpolation is all one needs to prove

Proposition 7.2 With the same notation as in Lemma 7.1, it holds

(V) for each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in \mathbf{G}$, and each m, $1 \le m \le n$, there are polynomials $g_{m\tau} := X_m^{d_m} + \sum_{w \in M_m(\tau)} c(g_{m\tau}, w)w$
such that $\lambda(g_{m\tau}) = 0$, for each $\lambda \in L_m(\tau)$;

(T) for each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **N** and each m, $1 \le m \le n$, there are polynomials

$$g_{m\tau} := X_m^{d_m} + \sum_{w \in M_m(\tau)} c(g_{m\tau}, w)w$$

such that $\lambda(g_{m\tau}) = 0$, for each $\lambda \in L_m(\tau)$, λ □ $\Phi^{-1}(\tau)$;

Proof:

(V) Since $\#(C_m(\tau)) \leq \#(M_m(\tau))$, we can evaluate each $c(g_{m\tau}, w)$ by interpolation, so that $l(g_{m\tau}) = 0$, $\forall l \in C_m(\tau)$ and $\lambda(g_{m\tau}) = \pi_m(\lambda)(g_{m\tau})$, $\forall \lambda \in L_m(\tau)$.

.

(T) One has just to apply (V) to the set $X(\tau)$.

For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in \mathbf{N}$ let us denote $\nu := \nu(\tau) \leq n$ the value such that $d_\nu \neq 0$ while $d_\mu = 0$ for each $\mu > \nu$ so that $\tau \in T[1, \nu]$, $g_{m\tau} = 1$ for $m > \nu$, and, denoting

$$h_\tau = \prod_{m=1}^{n} g_{m\tau} \in k[X_1, \ldots, X_{\nu-1}][X_\nu],$$

$$l_\tau = \prod_{m=1}^{\nu(\tau)-1} g_{m\tau} \in k[X_1, \ldots, X_{\nu-1}],$$

$$p_\tau = g_{\nu\tau} \in k[X_1, \ldots, X_{\nu-1}][X_\nu]$$

it holds

$h_\tau = l_\tau p_\tau = l_\tau X_\nu^{d_\nu} + \cdots$

so that $l_\tau \in k[X_1, \ldots, X_{\nu-1}]$ is the leading polynomial and the content of h_τ while the monic polynomial p_τ is the primitive component of h_τ .

Therefore we have[4]

Corollary 7.3 With the notation above, under the assumption **I** radical ideal, it holds

(W) for each $\tau := X_1^{d_1} \cdots X_\nu^{d_\nu} \in \mathbf{N}$, there are

$l_i \in k[X_1, \ldots, X_{\nu-1}]$

and a monic polynomial

$$p_\tau := X_\nu^{d_\nu} + \sum_{w \in M_\nu(\tau)} c(p_\tau, w)w \in k[X_1, \ldots, X_{\nu-1}][X_\nu]$$

so that $h_\tau := l_\tau p_\tau$ are such that

- $T(h_\tau) = \tau$,
- $Lp(h_\tau) = l_\tau$,
- $l_\tau(\pi_{\nu-1}(\mathbf{a})) = 0$, for all $\mathbf{a} \in \mathbf{X}(\tau)$,
- $p_\tau(\mathbf{a}) = 0$, for each $\mathbf{a} \in D_\nu(\tau)$,
- $h_\tau(\mathbf{a}) = 0$, for each $\mathbf{a} \in \mathbf{X}$ such that $\mathbf{a}$ □ $\Phi^{-1}(\tau)$.

(X) for each i, $1 \leq i \leq r$ there are

$l_i \in k[X_1, \ldots, X_{\nu-1}]$

[4] This justifies why we need to require that **I** is radical: in this restricted setting, each functional λ_i is evaluation at a point and distributes with product

and a monic polynomial

$$p_i := X_\nu^{d_\nu} + \sum_{w \in M_\nu(t_i)} c(p_i, w) w \in k[X_1, \ldots, X_{\nu-1}][X_\nu]$$

so that $h_i := l_i p_i$ are such that

- $\mathbf{T}(h_i) = t_i = X_1^{d_1} \cdots X_\nu^{d_\nu} \in \mathbf{G} \cap \mathbf{T}[1, \nu]$,
- $Lp(h_i) = l_i$,
- $l_i(\pi_{\nu-1}(\mathbf{a})) = 0$, for each $a \in \bigcup_{m=1}^{\nu-1} D_m(t_i)$,
- $p_i(\mathbf{a}) = 0$, for each $\mathbf{a} \in D_\nu(t_i)$,
- $h_i(\mathbf{a}) = 0$, for each $\mathbf{a} \in \mathbf{X}$.

While $\#(C_m(\tau)) \leq \#(M_m(\tau))$, in general equality does not hold and the polynomials $g_{m\tau}$ are not unique. However, uniqueness can be forced via Cerlienco–Mureddu Corespondence in such a way that the result does not require the assumption **I** radical ideal.

We begin by remarking that

$\#(C_1(\tau)) = \#(M_1(\tau))$, for each $\tau := X_1^{d_1} \cdots X_n^{d_n}$,

so that $g_{1\tau}$ is actually unique. We can therefore set $\gamma_{1\tau} := g_{1\tau}$ and compute inductively, for m, $1 < m \leq n$,

$\zeta_{m\tau} := \prod_{\nu=1}^{m-1} \gamma_{\nu\tau}$,

$Q_m(\tau) := \{M(w)\lambda_a : w \in \mathbf{T}[1, m-1], a \in Z := \mathbf{Z}(\mathbf{I}), M(w)\lambda_a(\zeta_{m\tau}) \neq 0\}$,

$P_m(\tau) := \{M(\pi_m(\frac{v_i}{w}))\lambda_{a_i} : M(v_i)\lambda_{a_i} \in L_m(\tau), M(w)\lambda_{a_i} \in Q_m(\tau)\}$,

$R_m(\tau) := \{(\pi_m(\mathbf{a}_i), \pi_m(\frac{v_i}{w})) : M(\pi_m(\frac{v_i}{w}))\lambda_{a_i} \in P_m(\tau)\}$,

$E_m(\tau) := \mathbf{N}(R_m(\tau))$,

$S_m(\tau) := \{(\pi_m(a_i), \pi_m(\frac{v_i}{w})) \in R_m(\tau) : (\mathbf{a}_i, v_i) \,\square\, \Phi^{-1}(\tau)\}$,

$F_m(\tau) := \mathbf{N}(S_m(\tau))$

This decomposition can be further refined if, for each $\tau := X_1^{d_1} \cdots X_n^{d_n}$, and each $\nu \leq n$, we iteratively compute, for decreasing $\delta \leq d_\nu$,

$Y_{\nu\delta}(\tau) := \{\pi_\nu(x) : \exists w \in \mathbf{T}[1, \nu] : \Phi(x) = w X_{\nu+1}^{\delta}, x \in P_{\nu\delta+1}(\tau)\}$,
$\mathbf{E}_{\nu\delta}(\tau) := N(Y_{\nu\delta}(\tau))$,
$P_{\nu\delta}(\tau) := \{M(\pi_\nu(\frac{v_i}{w}))\lambda_{a_i} : M(v_i)\lambda_{a_i} \in L_\nu(\tau), M(w)\lambda_{a_i} \in Y_{\nu\delta}(\tau)\}$,
$S_{\nu\delta}(\tau) := \{\pi_\nu(x) \in Y_{\nu\delta}(\tau) : x \,\square\, \Phi^{-1}(\tau)\}$,
$F_m(\tau) := \mathbf{N}(S_m(\tau))$.

with initial value $P_{\nu d_n+1}(\tau) := P_{\nu-1} := P_{\nu-1\,2}$.

We then obtain:

Corollary 7.4 [Marinari - Mora (2004)] It holds

(M) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **N** and each m, $1 \le m \le n$, there are unique polynomials

$$\gamma_{m\tau} := X_m^{d_m} + \sum_{w \in F_m(\tau)} c(\gamma_{m\tau}, w)w$$

and

$$\gamma_{m\delta\tau} := X_m + \sum_{w \in F_{m\delta}(\tau)} c(\gamma_{m\tau}, w)w, \qquad 1 \le \delta \le d_m$$

such that

- $\pi_m(\lambda)(\gamma_{m\delta\tau}) = 0$, for each $\lambda \in Y_{v\delta}(\tau)$, $\lambda \square \Phi^{-1}(\tau)$;
- $\pi_m(\lambda)(\gamma_{m\tau}) = 0$, for each $\lambda \in L_m(\tau)$, $\lambda \square \Phi^{-1}(\tau)$;
- $\gamma_{m\tau} = \Pi_\delta \gamma_{m\delta\tau}$.

(N) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **G**, and each m, $1 \le m \le n$, there are unique polynomials

$$\gamma_{m\tau} := X_m^{d_m} + \sum_{w \in E_m(\tau)} c(\gamma_{m\tau}, w)w$$

and

$$\gamma_{m\delta\tau} := X_m + \sum_{w \in E_{m\delta}(\tau)} c(\gamma_{m\tau}, w)w, \qquad 1 \le \delta \le d_m$$

such that

- $\pi_m(\lambda)(\gamma_{m\delta\tau}) = 0$, for each $\lambda \in \mathbf{Y}_{m\delta}(\tau)$,
- $\pi_m(\lambda)(\gamma_{m\tau}) = 0$, for each $\lambda \in \mathbf{L}_m(\tau)$,
- $\gamma_{m\tau} = \Pi_\delta \gamma_{m\delta\tau}$;

(O) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **N**, there are

$L_\tau \in k[X_1, \dots, X_{v-1}]$

and a unique monic polynomial

$$P_\tau := X_v^{d_v} + \sum_{w \in F_v(\tau)} c(P_\tau, w)w \in k[X_1, \dots, X_{v-1}][X_v]$$

so that $H_\tau := L_\tau P_\tau$ are such that

- $\mathbf{T}(H_\tau) = \tau$, $Lp(H_\tau) = L_\tau$,
- $\pi_{v-1}(\lambda)(L_\tau) = 0$, for each $\lambda \in L(\tau)$,
- $\pi_v(\lambda)(P_\tau) = 0$, for each $\lambda \in L_v(\tau)$,
- $\pi_v(\lambda)(H_\tau) = 0$, for each $\lambda \in \mathbf{L} : \lambda \square \Phi^{-1}(\tau)$.

(P) For each i, $1 \le i \le r$ there are

$L_i \in k[X_1, \dots, X_{v-1}]$

and a unique monic polynomial

$$P_i := X_v^{d_v} + \sum_{w \in E_v(t_i)} c(P_i, w)w \in k[X_1, \dots, X_{v-1}][X_v]$$

so that $H_i := L_i P_i$ are such that

- $\mathbf{T}(H_i) = t_i = X_1^{d_1} \cdots X_v^{d_v} \in \mathbf{G} \cap T[1,v]$, $Lp(H_i) = L_i$,
- $\pi_{v-1}(\lambda)(L_i) = 0$, for each $\lambda \in \bigcup_{m=1}^{v-1} L_m(t_i)$,
- $\pi_v(\lambda)(P_i) = 0$, for each $\lambda \in L_v(t_i)$,

• $\pi_\nu(\lambda)(H_i) = 0$, for each $\lambda \in$ **L**.

Proof: The only non trivial statements, i.e. the vanishing of $\pi_{\nu-1}(\lambda)(L_i)$ and $\pi_\nu(\lambda)(H_i)$ are an elementary consequence of Leibniz Formula (Proposition 3.1).

Fact 7.5 It holds

(Q) L_i , P_i , H_i, $1 \le i \le r$ satisfy $\{H_1, \dots, H_r\}$ is a minimal Gröbner basis of **I**, for each ν, $1 \le \nu < n$, $\{H_1, \dots, H_{j_\nu}\}$ is a minimal Gröbner basis of **I** $\cap$ k$[X_1, \dots, X_\nu]$ and of **I**(π_ν(**X**)); for each ν, $1 \le \nu < n$, $\{L_1, \dots, L_{j_{\nu\delta}}\}$ is a Gröbner basis of **I**($\mathbf{Y}_{\nu\delta}$)).

Clearly, if **I** is radical similar statements hold for $\{h_1, \dots, h_r\}$, $\{l_1, \dots, l_{j_{\nu\delta}}\}$ and $\{h_1, \dots, h_{j_\nu}\}$.

Remark 7.6 Among the three bases

$\{f_1, \dots, f_r\}$, $\{h_1, \dots, h_r\}$ and $\{H_1, \dots, H_r\}$

only the first one is reduced. On the other side, for each i, we have

T(f_i) = **T**(h_i) = **T**$(H_i) = t_i$.

Therefore we have

• $f_1 = h_1 = H_1$ and
• $f_i - h_i \in (h_1, \dots, h_{i-1})$, $f_i - H_i \in (H_1, \dots, H_{i-1})$ for each i, $1 < i \le r$,

whence

• $f_i \in (h_1, \dots, h_i)$, $f_i \in (H_1, \dots, H_i)$ for each i, $1 < i \le r$

Fact 7.7 It holds

(R) For each i, $2 \le i \le r$, $P_i \in (H_1, \dots, H_i) : L_i$.
(S) For each j, $1 \le j \le s$, $\lambda_j(H_{\tau_j}) \ne 0$; **L** and $\{\lambda_j(H_{\tau_j})^{-1} H_{\tau_j}, 1 \le j \le s\}$ are triangular.

Corollary 7.8 Moreover, if **I** is radical

(Z) l_i, p_i, h_i, $1 \le i \le r$ satisfy
$\{h_1, \dots, h_r\}$ is a minimal Gröbner basis of **I**;
for each ν, $1 \le \nu < n$, $\{h_1, \dots, h_{j_\nu}\}$ is a minimal Gröbner basis of P(Span$_k$(π_ν(**L**)))
and **I** $\cap$ k$[X_1, \dots, X_\nu]$;
for each ν, $1 \le \nu < n$, $\{l_1, \dots, l_{j_{\nu\delta}}\}$ is a Gröbner basis of **I**($\mathbf{Y}_{\nu\delta}$);
for each i, $2 \le$ **I** $\le r$, $p_i \in \{h_1, \dots, h_i\} : l_i$;
for each j, $1 \le j \le s$, $\lambda_j(h_{\tau_j}) \ne 0$;
L is triangular to $\{\lambda_j(h_{\tau_j})^{-1} h_{\tau_j}, 1 \le j \le s\}$.

Figure 1: Möller Algorithm for Macaulay representation

(**N**, **q**, **B**, *B*) := Möller(**L**)

where

L = $\{l_1, \dots, l_s\}$ is a Macauly representation of a zero-dimensional ideal **I**,
N := **N**(**I**),
q = $\{q_1, \dots, q_s\}$ is triangular to L,

B := **B**(**I**),

$B := B(\mathbf{I})$.

r := 1, **B** := ∅;

$t_1 := 1$, **N** := $\{t_1\}$, $q_1 := t_1$, **q** := $\{q_1\}$,

For h = 1..n **do**

  $t := X_h$, $b_t := X_h - a_{h_1}$, **B** := **B** ∪ {t}

While $r \leq s$ **do**

  Let t := $\min_<\{t \in$ **B** : $\lambda_{r+1}(b_t) \neq 0\}$

  r := r + 1, **B** := **B** \ {t},

  $t_r := t$, **N** := **N** ∪ $\{t_r\}$, $q_r := \lambda_r(b_t)^{-1} b_t$, **q** := **q** ∪ $\{q_r\}$,

  For each τ ∈ **B** **do** $b_\tau := b_\tau - \lambda_r(b_\tau) q_r$,

  For h = 1..n **do**

    If $X_h t_r \notin$ **B** **then**

      $t := X_h t_r$,

      $f := X_h b_{t_r} - \sum_{\substack{\tau \in N \\ X_h \tau \in B}} c(b_{t_r}, \tau) b_{X_h \tau}$

    B := **B** ∪ $\{X_h t_r, h = 1..n\}$

N, **q**, $\{b_\tau : \tau \in$ **B**$\}$

---

8 PROOF

In order to complete the proof all we need is to directly apply Möller Algorithm [Möller-Buchberger (1982), Faugère et. al. (1993), Alonso et. al. (2003) Marinari et. al. (1993), Mora (2005)] (a simplified version of it in our context being presented in Figure 1).

The proof is by induction, we begin with

Lemma 8.1 If #**L** = 1 conditions (A), (F), (I), (L), (Q), (R), (S) hold.

Proof: When we have a single point $(a_1, \ldots, a_n) \in k^n$, we have

- **N** = {1},
- **B** = **G** = $\{X_1, \ldots, X_n\}$,
- $f_1 = 1$,
- $f_{X_i} = X_i - a_i$, for each i,

and the properties are obviously satisfied.

Thus having a starting point for induction, let us assume we have a Macaulay representation and the corresponding CeMu-skeleton

L := $\{\lambda_1, \ldots, \lambda_s\}$, **X** := $\{x_1, \ldots, x_s\} \subset k^n \times$ **T** ,

$\mathbf{x}_i = (\mathbf{a}_i, v_i)$, $\mathbf{a}_i := (a_{i1}, \ldots, a_{in})$, $v_i = \prod_{l=1}^{n} X_l^{\alpha_{il}}$

of a zero-dimensional **I**, and let us denote

X' := $\{x_1, \ldots, x_{s-1}\}$, **L**' := $\{\lambda_1, \ldots, \lambda_{s-1}\}$ and **I'** := P(Span$_k$(**L**'),

for which we assume conditions (A-L) hold. If moreover **I** (and thus **I'**) is a CeMu-ideal, we also assume that conditions (M-S) hold for **I'**.

In particular:

Φ' := **N'**→ **L'** is Cerlienco–Mureddu Correspondence,
G' := **G**(**I'**) = $\{w_1, . . . , w_r\}$, $w_1 < w_2 < . . . < w_r$,
B' := **B**(**I'**),
f'_w, $w \in$ **B'**, are the polynomials whose existence is implied by (F),
$F_i := f'_{w_i}$, are the polynomials whose existence is implied by (E), so that $\{F_i : 1 \le i \le r\}$ is the reduced Gröbner basis of **I'**,
L'_i, P'_i, H'_i are the polynomials whose existence is implied by (P).

Setting

$\mathcal{I} := \min_< \{j, 1 \le j \le r : \lambda_s(F_j) \neq 0\}$,

then it holds

Lemma 8.2 If **L'** satisfies conditions (A-L) then

$\Phi(\mathbf{L})(\lambda_s) = w_{\mathcal{I}}$.

Proof: Let $w_{\mathcal{I}} = X_1^{d_1} \cdots X_n^{d_n}$ and let m + 1 := max(i : $d_i \neq 0$), so that

$F_{\mathcal{I}} \in k[X_1 \cdots X_{m+1}]$.

Since, by (I), for each ν

$\mathbf{I'} \cap k[X_1 \cdots X_\nu] = P(\mathrm{Span}_k(\pi_\nu(\mathbf{L'})))$,

and

$F_j \in k[X_1 \cdots X_\nu]$, $\nu \le m \Rightarrow j < \mathcal{I}$

we deduce that

$\pi_\nu(\lambda_s)(F_j) = \lambda_s(F_j) = 0$, for each $F_j \in k[X_1 \cdots X_\nu]$, $\nu \le m$, while $\pi_{m+1}(\lambda_s)(F_{\mathcal{I}}) = \lambda_s(F_{\mathcal{I}}) \neq 0$.

This allows to deduce that

$m = \max (j : \pi_j(\lambda_s) \in \mathrm{Span}_k(\pi_j((\mathbf{L'})))$.

Therefore $\pi_{m+1}(\lambda_s) \notin \mathrm{Span}_k(\pi_{m+1}((\mathbf{L'}))$; also

$d_m = \min\{\delta : \pi_m(\lambda_s) \notin \mathbf{Y}_{m\delta}\}$;

in fact, for each $\delta < d_m$, since

$\mathbf{T}(F_j) = w_j < X_m^{\delta} \cdots X_m^{d_m} \Rightarrow j < \mathcal{I}$,

and $\pi_m(\lambda_s)(F_j) = 0$, (I) allows to deduce that $\pi_m(\lambda_s) \in Y_{m\delta}$ and $\pi_m(\lambda_s) \notin Y_{m d_m}$

As a consequence we consider

W := $\{\pi_m(\lambda) : \Phi'(\lambda) = w X_{m+1}^{d_m}, w \in \mathbf{T}[1, \nu]\} \cup \{\pi_m(\lambda_s)\}$;

in this setting Cerlienco–Mureddu Correspondence gives a relation between each point $\pi_m(\mathbf{x}_i)$ and the corresponding term τ_i.

Moreover, since the argument is on the cardinality of the Macaulay representation and #(**W**) < #(**L**), we directly deduce that the ideal $\mathbf{P}(\pi_m(\mathbf{W}))$ has $\{Lp(f_{t_1}), \ldots, Lp(f_{t_{j(md_m)}})\}$ as Gröbner basis. Also

$\pi_m(\lambda_s)(Lp(f_{t_j})) = 0$, for each $j < I$ while $\pi_m(\lambda_s)(Lp(f_{t_I})) \neq 0$.

so that the same argument grants that Cerlienco–Mureddu Correspondence returns $\Phi(\pi_m(\lambda_s)) = X_1^{d_1} \cdots X_m^{d_m}$.

As a consequence, applying Möller Algorithm to $\mathbf{L} = \mathbf{L}' \cup \{\lambda_s\}$ we get

$q_s := c^{-1}F_I$, with $c = \lambda_s(F_I)$;
$\mathbf{N} := \mathbf{N}' \cup \{w_I\}$;
$\mathbf{B} := \mathbf{B}' \setminus \{w_I\} \cup \{X_i w_I,\ 1 \le i \le n\}$;
$f_\tau := f'_\tau - \lambda_s(f'_\tau)q_s$ for each $\tau \in \mathbf{B}' \setminus \{w_I\}$, $\tau > w_I$ and
$f_\tau := f'_\tau$, for each $\tau \in \mathbf{B}' \setminus \{w_I\}$, $\tau < w_I$ since $\lambda_s(f'_\tau) = 0$;

for each $\tau := X_i w_I \notin \mathbf{B}'$

$$f_\tau := (X_i - a_{is})F_I - \sum_{X_i w \in B'} c(F_I, w) f_{X_i w}$$

where

$$F_I := w_I + \sum_{w \in N'} c(F_I, w) w$$

Corollary 8.3 If **L**' satisfies conditions (A-L) then **L** satisfies conditions
(A), (F), (I), (L), (Q), (R), (S).
Proof:
(A) and (F) are obvious;

(I) and (Q) are a direct consequence of the application of Cerlienco–Mureddu Algorithm to $P(\pi_m(\mathbf{W}))$;

(L) $\lambda_s(f_{\omega_I}) \neq 0$ for construction;

(R) on the basis of Remark 7.6 we know that $F_I \in (H'_1, \ldots, H'_I)$; also all we need to prove is that, for each i,

$H_i \in (H_1, \ldots, H_{i-1}) = \{H_j, \mathbf{T}(H_j) < \mathbf{T}(H_i)\}$.

Therefore

• if $\mathbf{T}(H_i) = t_i \in \mathbf{G}'$, $i < I$, we have
$H_i = H'_i \in (H'_1, \ldots, H'_{i-1}) = (H_1, \ldots, H_{i-1})$;
• if $\mathbf{T}(H_i) = t_I \in \mathbf{G}'$, $i > I$, we have
$H_i = H'_i - aF_I \in (H'_1, \ldots, H'_{i-1}) = (H_1, \ldots, H_{i-1})$;

so that, also $(H'_1, \ldots, H'_i) = (H_1, \ldots, H_i)$.

• Finally, for $\tau = X_i t_I$ we have $L_\tau = L'_I$, and

$L_\tau P_\tau = H_\tau \equiv f_\tau \equiv (X_i - a_{is})F_{\mathcal{I}} \equiv (X_i - a_{is})L'_{\mathcal{I}}P'_{\mathcal{I}} \equiv 0$ modulo $(H'_1, \dots, H'_{\mathcal{I}}) = (H_1, \dots, H_{\mathcal{I}})$;

The same argument proofs the claim for $\{h_1, \dots, h_r\}$.

(S) $\lambda_s(H_{w_I}) \neq 0$ and $\lambda_s(h_{w_I}) \neq 0$ because both $H_{w_I} - f_{w_I}$ and $h_{w_I} - f_{w_I}$ have a representation in terms of $\{F_i, i < \mathcal{I}\}$ and $\lambda_s(F_i) = 0$, for each $i < \mathcal{I}$.

In conclusion we have:

Theorem 8.4 For a zero-dimensional ideal **I**, given by a Macaulay representation **L**, using the same notation as above, it holds

(A) **N** := **N**(I).
(B) **G**(**I**) = **G** = $\{t_1, \dots, t_r\}$, $t_1 < t_2 < \dots < t_r$.
(C) **B**(**I**) = **B**.
(D) For each $\tau \in$ **N** there is a unique polynomial

$$f_\tau := \tau - \sum_{w \in N(\tau)} c(f_\tau, w) w$$

such that $\lambda(f_\tau) = 0$, for each $\lambda \in$ **L**(τ).

(E) For each $\tau \in$ **G** there is a unique polynomial

$$f_\tau := \tau - \sum_{w \in N} c(f_\tau, w) w$$

such that $\lambda(f_\tau) = 0$, for each $\lambda \in$ **L**.

(F) For each $\tau \in$ **B** there is a polynomial

$$f_\tau := \tau - \sum_{w \in N(\tau)} c(f_\tau, w) w$$

such that $\lambda(f_\tau) = 0$, for each $\lambda \in$ **L**.

(G) The reduced Gröbner basis of **I** is

G(I) := $\{f_\tau : \tau \in$ **G**$\}$,

moreover, for each $\tau \in$ **N**, **T**$(f_\tau) = \tau$.

(H) The border basis of **I** is

B(**I**) := $\{ f_\tau : \tau \in$ **B**$\}$.

(I) For each ν, $1 \leq \nu < n$,

let j_ν be the value such that $t_{j_\nu} < X_{\nu+1} \leq t_{j_{\nu+1}}$; then $\{f_{t_1}, \dots, f_{t_{j_\nu}}\}$ is a minimal Gröbner basis of $P(\mathrm{Span}_k(\pi_\nu(\mathbf{L})))$ and of $\mathbf{I} \cap k[X_1, \dots, X_\nu]$; for each $\delta \in \mathbb{N}$, let $j(\nu\delta)$ be the value such that $t_{j(\nu\delta)} < X^\delta_{\nu+1} \leq t_{j(\nu\delta)+1}$; then $\{Lp(f_{t_1}), \dots, Lp(f_{t_{j\nu\delta}})\}$ is a Gröbner basis of $\mathbf{I}(\mathbf{Y}_{\nu\delta})$.

(L) For each j, $1 \leq j \leq s$, $\lambda_j(f_{\tau_j}) \neq 0$ so that **L** and $\{\lambda_j(f_{\tau_j})^{-1} f_{\tau_j}\ 1 \leq j \leq s\}$ are triangular.

If **I** is a CeMu-ideal:

(M) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **N**, and each m, $1 \leq m \leq n$, there are unique polynomials

$$\gamma_{m\tau} := X_m^{d_m} + \sum_{w \in F_m(\tau)} c(\gamma_{m\tau}, w) w$$

and

$$\gamma_{m\delta\tau} := X_m + \sum_{w \in F_{m\delta}(\tau)} c(\gamma_{m\tau}, w) w \qquad 1 \leq \delta \leq d_m$$

such that

- $\pi_m(\lambda)(\gamma_{m\delta\tau}) = 0$, for each $\lambda \in Y_{\nu\delta}(\tau)$, $\lambda \square \Phi^{-1}(\tau)$;
- $\pi_m(\lambda)(\gamma_{m\tau}) = 0$, for each $\lambda \in L_m(\tau)$, $\lambda \square \Phi^{-1}(\tau)$;
- $\gamma_{m\tau} = \Pi_\delta \gamma_{m\delta\tau}$.

(N) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **G**, and each m, $1 \leq m \leq n$, there are unique polynomials

$$\gamma_{m\tau} := X_m^{d_m} + \sum_{w \in E_m(\tau)} c(\gamma_{m\tau}, w) w$$

and

$$\gamma_{m\delta\tau} := X_m + \sum_{w \in E_{m\delta}(\tau)} c(\gamma_{m\tau}, w) w \qquad 1 \leq \delta \leq d_m$$

such that

- $\pi_m(\lambda)(\gamma_{m\delta\tau}) = 0$, for each $\lambda \in Y_{m\delta}(\tau)$,
- $\pi_m(\lambda)(\gamma_{m\tau}) = 0$, for each $\lambda \in L_m(\tau)$,
- $\gamma_{m\tau} = \Pi_\delta \gamma_{m\delta\tau}$.

(O) For each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in$ **N**, there are

$L_\tau \in k[X_1, \ldots, X_{\nu-1}]$

and a unique monic polynomial

$$P_\tau := X_\nu^{d_\nu} + \sum_{w \in F_\nu(\tau)} c(P_\tau, w) w \in [X_1, \ldots, X_{\nu-1}][X_\nu]$$

so that $H_\tau := L_\tau P_\tau$ are such that

- **T**$(H_\tau) = \tau$, $Lp(H_\tau) = L_\tau$,
- $\pi_{\nu-1}(\lambda)(L_\tau) = 0$, for each $\lambda \in$ **L**(τ),
- $\pi_\nu(\lambda)(P_\tau) = 0$, for each $\lambda \in$ **L**$_\nu(\tau)$,
- $\pi_\nu(\lambda)(H_\tau) = 0$, for each $\lambda \in$ **L** : $\lambda \square \Phi^{-1}(\tau)$.

(P) For each i, $1 \leq$ **I** $\leq r$ there are

$L_i \in k[X_1, \ldots, X_{\nu-1}]$

and a unique monic polynomial

$$P_i := X_\nu^{d_\nu} + \sum_{w \in E_\nu(t_i)} c(P_i, w) w \in [X_1, \ldots, X_{\nu-1}][X_\nu]$$

so that $H_i := L_i P_i$ are such that

- **T**$(H_i) = t_i = X_1^{d_1} \cdots X_\nu^{d_\nu} \in$ **G** $\cap$ **T**$[1, \nu]$, $Lp(H_i) = L_i$,
- $\pi_{\nu-1}(\lambda)(L_i) = 0$, for each $\lambda \in \bigcup_{m=1}^{\nu-1}$ **L**$_m(t_i)$,
- $\pi_\nu(\lambda)(P_i) = 0$, for each $\lambda \in$ **L**$_\nu(t_i)$,
- $\pi_\nu(\lambda)(H_i) = 0$, for each $\lambda \in$ **L**.

(Q) L_i, P_i, H_i, $1 \le i \le r$ satisfy

$\{H_1, . . . , H_r\}$ is a minimal Gröbner basis of **I**,
for each ν, $1 \le \nu < n$, $\{H_1, . . . , H_{j\nu}\}$ is a minimal Gröbner basis of
$\mathbf{I} \cap k[X_1, . . . , X_\nu]$ and $\mathbf{I}(\pi_\nu(\mathbf{X}))$;

for each ν, $1 \le \nu < n$, $\{L_1, . . . , L_{j\nu\delta})\}$ is a Gröbner basis of $\mathbf{I}(\mathbf{Y}_{\nu\delta})$.

(R) For each i, $2 \le I \le r$, $P_i \in (H_1, . . . , H_i) : L_i$.

(S) For each j, $1 \le j \le s$, $\lambda_j(H_{\tau_j}) \neq 0$; **L** and $\{\lambda_j(H_{\tau_j})^{-1} H_{\tau_j}, 1 \le j \le s\}$ are triangular.

(T) for each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in \mathbf{N}$ and each m, $1 \le m \le n$, there are polynomials

$$g_{m\tau} := X_m^{d_m} + \sum_{w \in M_m(\tau)} c(g_{m\tau}, w) w$$

such that $\lambda(g_{m\tau}) = 0$, for each $\lambda \in \mathbf{L}_m(\tau)$, λ □ $\Phi^{-1}(\tau)$.

(V) for each $\tau := X_1^{d_1} \cdots X_n^{d_n} \in \mathbf{G}$ and each m, $1 \le m \le n$, there are polynomials

$$g_{m\tau} := X_m^{d_m} + \sum_{w \in M_m(\tau)} c(g_{m\tau}, w) w$$

such that $\lambda(g_{m\tau}) = 0$, for each $\lambda \in \mathbf{L}_m(\tau)$.

Moreover, if **I** is radical:

(W) for each $\tau := X_1^{d_1} \cdots X_\nu^{d_\nu} \in \mathbf{N}$, there are

$l_\tau \in k[X_1, . . . , X_{\nu-1}]$

and a monic polynomial

$$p_\tau := X_\nu^{d_\nu} + \sum_{w \in M_\nu(\tau)} c(p_\tau, w) w \in k[X_1, ..., X_{\nu-1}][X_\nu]$$

so that $h_\tau := l_\tau p_\tau$ are such that

- $T(h_\tau) = \tau$,
- $Lp(h_\tau) = l_\tau$,
- $l_\tau(\pi_{\nu-1}(a)) = 0$, for all $a \in X(\tau)$,
- $p_\tau(a) = 0$, for each $a \in D_\nu(\tau)$,
- $h_\tau(\mathbf{a}) = 0$, for each $\mathbf{a} \in \mathbf{X}$ such that $\mathbf{a}$ □ $\Phi^{-1}(\tau)$.

(X) for each i, $1 \le i \le r$ there are

$l_i \in k[X_1, . . . , X_{\nu-1}]$

and a monic polynomial

$$p_i := X_\nu^{d_\nu} + \sum_{w \in M_\nu(t_i)} c(p_i, w) w \in k[X_1, ..., X_{\nu-1}][X_\nu]$$

so that $h_i := l_i p_i$ are such that

- $\mathbf{T}(h_i) = t_i = X_1^{d_1} \cdots X_\nu^{d_\nu} \in \mathbf{G} \cap \mathbf{T}[1,\nu]$,
- $Lp(h_i) = l_i$,

- $l_i(\pi_{v-1}(\mathbf{a})) = 0$, for each $\mathbf{a} \in \bigcup_{m=1}^{v-1} D_m(t_i)$,
- $p_i(\mathbf{a}) = 0$, for each $\mathbf{a} \in D_v(t_i)$,
- $h_i(\mathbf{a}) = 0$, for each $\mathbf{a} \in X$.

(Z) l_i, p_i, h_i, $1 \le i \le r$ satisfy

$\{h_1, \ldots, h_r\}$ is a minimal Gröbner basis of **I**;

for each v, $1 \le v < n$, $\{h_1, \ldots, h_{j_v}\}$ is a minimal Gröbner basis of $P(\mathrm{Span}_k(\pi_v(\mathbf{L})))$ and $\mathbf{I} \cap k[X_1, \ldots, X_v]$;

for each v, $1 \le v < n$, $\{l_1, \ldots, l_{j_{v\delta}}\}$ is a Gröbner basis of $\mathbf{I}(\mathbf{Y}_{v\delta})$;

for each i, $2 \le i < r$, $p_i \in \{h_1, \ldots, h_i\} : l_i$;

for each j, $1 \le j \le s$, $\lambda_j(h_{\tau_j}) \ne 0$;

L is triangular to $\{\lambda_j(h_{\tau_j})^{-1} h_{\tau_j}, 1 \le j \le s\}$.

REFERENCES

Alonso, M. E., M.G. Marinari, T. Mora (2003) The Big Mother of All the Dualities, I: Möller Algorithm**, Comm**. **Alg**. 31

Buchberger B., (1965) Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, **Ph. D.Thesis,** Innsbruck

Buchberger B., (1970), Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem, **Aeq. Math**. 4, 374–383

Buchberger B., Loos R. (1982), Algebraic Simplification. In **Computer Algebra.Symbolic and Algebraic Computation,** 11–44. (Buchberger B., Collins G.E., Loos R., Eds.), Springer, Berlin.

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

Cerlienco L., Mureddu M. (1995), From algebraic sets to monomial linear bases by means of combinatorial algorithms, **Discrete Math**. 139, 73–87.

Faugère J.C., Gianni P., Lazard D. and Mora T. (1993), Efficient Computation of Zero--dimensional Gröbner Bases by Change of Ordering. **J. Symb. Comp**. 16, 329–344.

Gianni P., (1987), Properties of GröbnerBases under Specialization, **L. N. Comp. Sci**. 378, 293-297.

Kalkbrener, M. (1987), Solving Systems of Algebraic Equations by Using Gröbner Bases, **L. N. Comp. Sci**. 378, 282–292.

Kalkbrener M., (1997) On the stability of Gröbner Bases under specialization, **J. Symb. Comp.** 24, 51–58.

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

Macaulay F. S., (1927), Some Properties of Enumeration in the Theory of Modular Systems, **Proc. London Math. Soc**. 26, 531–555

Macaulay F. S. (1913), On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers, **Math. Ann**. 74, 66–121.

Macaulay F. S. (1916), **The Algebraic Theory of Modular Systems**, Cambridge Univ. Press., Cambridge.

Marinari M.G., Möller H.M., Mora T. (1993), Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. **AAECC** 4 , 103–145.

Marinari M.G., Möller H.M., Mora T. (1996), On multiplicities in Polynomial System Solving, **Trans. AMS**, 348 , 3283–3321.

Marinari M.G., Mora T. (2003) A remark on a remark by Macaulay or Enhancing Lazard Structural Theorem, **Bull. Iranian Math. Soc**., 29, 1-45.

Marinari M.G., Mora T. (2004), Some Comments on Cerlienco–Mureddu Algorithm and Enhanced Lazard Structural Theorem **Rejected by ISSAC-2004**

Möller H.M. (1993), Systems of Algebraic Equations Solved by Means of Endomorphisms, **L. N. Comp. Sci**. 673 , 43–56.

Möller H.M., Buchberger B. (1982), The construction of Multivariate Polynomials with Preassigned Zeros, **L. N. Comp. Sci**. 144, 24–31.

Mora T.(2005) **Solving Polynomial Equation Systems II**, Cambridge Univ. Press..