The Abdus Salam International Centre for Theoretical Physics

United Nations Educational, Scientific and Cultural Organization

IAEA International Atomic Energy Agency

1958-13

Summary School and Conference Mathematics, Algorithms and Proofs

11 - 29 August 2008

A Survey on Combinatorial Duality Approach to Zero-dimensional Ideals.

Teo Mora
DIMA and DISI, Università di Genova, Italy

theomora@dima.unige.it

A Survey on Combinatorial Duality Approach to Zero-dimensional Ideals

Teo Mora
DIMA and DISI, Università di Genova
theomora@dima.unige.it

May 30, 2008

1 Gröbner Technology

k denotes an arbitrary field, $\overline{k}$ denotes its algebraic closure and k_q denotes a finite field of size q (so q is implicitly understood to be a power of a prime) and $\mathcal{P} := k[X] := k[x_1, \ldots, x_n]$ the polynomial ring over the field k.

For any ideal $\mathsf{I} \subset \mathcal{P}$ and any extension field E of k, let $\mathcal{V}_E(\mathsf{I})$ be the rational points of I over E. We also write $\mathcal{V}(\mathsf{I}) = \mathcal{V}_{\overline{k}}(\mathsf{I})$.

Let $\mathcal{T}$ be the set of terms in $\mathcal{P}$, *id est*

$$\mathcal{T} := \{x_1^{a_1} \cdots x_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\},$$

which is a multiplicative version of the additive semigroup $\mathbb{N}^n$, the relation between these notations being obvious: given

$$\alpha := (a_1, \ldots, a_n), \quad \beta := (b_1, \ldots, b_n), \quad \gamma := (c_1, \ldots, c_n)$$

and the terms

$$\tau_a := X^\alpha = x_1^{a_1} \cdots x_n^{a_n}, \quad \tau_b := X^\beta = x_1^{b_1} \cdots x_n^{b_n}, \quad \tau_c := X^\gamma = x_1^{c_1} \cdots x_n^{c_n},$$

we have

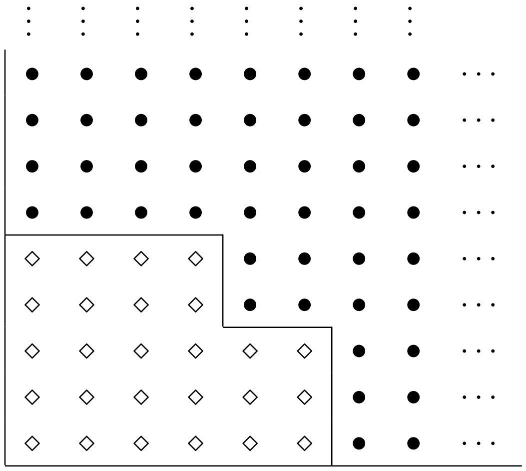
$$\begin{array}{rcccc} \tau_a \cdot \tau_b = \tau_c & \iff & a_i + b_i = c_i \text{ for each } i & \iff & \alpha + \beta = \gamma \\ \tau_a \mid \tau_b & \iff & a_i \leq b_i \text{ for each } i & \iff & \alpha \leq_P \beta \end{array}$$

where $<_P$ is the natural partial ordering over $\mathbb{N}^n$.

The assignement of a finite set of terms

$$G := \{\tau_1, \ldots, \tau_\nu\} \subset \mathcal{T}, \tau_i = x_1^{a_1^{(i)}} \cdots x_n^{a_n^{(i)}}$$

Figure 1:



— or, equivalently of a finite set of integer vectors

$$\{a^{(1)}, \ldots, a^{(\nu)}\} \subset \mathbb{N}^n, a^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)}) \in \mathbb{N}^n,$$

defines a partition of $\mathcal{T}$ (resp. $\mathbb{N}^n$) in two parts (see Figure 1 where $G := \left\{x_1^7, x_1^5 x_2^3, x_2^5\right\} \subset \mathcal{T}$):

- $T := \{\tau\tau_i : \tau \in \mathcal{T}, 1 \le i \le \nu\} \cong \{\alpha + a^{(i)} : \alpha \in \mathbb{N}^n, 1 \le i \le \nu\} =: \Sigma$ which is a *semigroup ideal*, *id est* a subset $T \subset \mathcal{T}($ resp. $\Sigma \subset \mathbb{N}^n)$ such that

$$\tau \in T, t \in \mathcal{T} \implies t\tau \in T, \text{ resp. } a \in \Sigma, b \in \mathbb{N}^n, a \le_P b \implies b \in \Sigma;$$

$\diamond$ $N := \mathcal{T} \setminus T \cong \mathbb{N}^n \setminus \Sigma =: \Delta$ which is an *order ideal*, *id est* a subset $N \subset \mathcal{T}$ (resp. $\Delta \subset \mathbb{N}^n$) such that

$$\tau \in N, t \in \mathcal{T}, t \mid \tau \implies t \in N, \text{ resp. } a \in \Delta, b \in \mathbb{N}^n, a \ge_P b \implies b \in \Delta.$$

Remark that the assignement of

- a finite monomial set $G \subset \mathcal{T}$,
- a semigroup ideal $T \subset \mathcal{T}$,
- an order ideal $N \subset \mathcal{T}$

uniquely characterize the other data: in fact

- N and T are related by their being complementary in $\mathcal{T}$,
- each semigroup ideal $T \subset \mathcal{T}$ has a unique minimal basis $G \subset T$ such that $T := \{\tau\tau_i : \tau \in \mathcal{T}, \tau_i \in G\}$; the fact, whose proof is quite involved, that G is finite is known as Dickson's Lemma but actually was already proved by Gordan [28].

We recall that the well-orderings on $\mathcal{T}$ which are a *semigroup ordering*, *id est* satysfy

$$\tau_1 < \tau_2 \implies \tau\tau_1 < \tau\tau_2 \text{ for each } \tau, \tau_1, \tau_2 \in \mathcal{T}$$

are called *term orderings*, even if the old-fashioned notion of *admissible ordering* can still be found somewhere.

For a free-module $\mathcal{P}^m$, $m \in \mathbb{N}$, denote $\{\mathbf{e}_1, \dots, \mathbf{e}_m\}$ its canonical basis,

$$\begin{aligned} \mathcal{T}^{(m)} &= \{t\mathbf{e}_i, t \in \mathcal{T}, 1 \le i \le m\} = \\ &= \{x_1^{a_1} \cdots x_n^{a_n}\mathbf{e}_i, (a_1, \dots, a_n) \in \mathbb{N}^n, 1 \le i \le m\} \end{aligned}$$

its monomial k-basis and $\prec$ a well-ordering on $\mathcal{T}^{(m)}$ which is compatible with the term-ordering $<$ on $\mathcal{T}$, that is, satisfying

$$t_1 \le t_2, \tau_1 \preceq \tau_2 \implies t_1\tau_1 \preceq t_2\tau_2$$

for each $t_1, t_2 \in \mathcal{T}, \tau_1, \tau_2 \in \mathcal{T}^{(m)}$.

Note that $\mathcal{T}^{(1)} = \mathcal{T}$.

For each $f = \sum_{\tau \in \mathcal{T}^{(m)}} \mathsf{c}(f, \tau)\tau \in \mathcal{P}^m$, its *support* is

$$\mathrm{supp}(f) := \{\tau \in \mathcal{T}^{(m)} : \mathsf{c}(f, \tau) \ne 0\},$$

its *leading term* is the term $\mathbf{T}_\prec(f) := \max_\prec(\mathrm{supp}(f))$, its *leading coefficient* is $\mathrm{lc}_\prec(f) := \mathsf{c}(f, \mathbf{T}_\prec(f))$ and its *leading monomial* is $\mathbf{M}_\prec(f) := \mathrm{lc}_\prec(f)\mathbf{T}_\prec(f)$.

When $\prec$ is understood we will drop the subscript, as in $\mathbf{T}(f) = \mathbf{T}_\prec(f)$.

For any set $F \subset \mathcal{P}^m$, write

- $\mathbf{T}\{F\} := \mathbf{T}_\prec\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{M}\{F\} := \mathbf{M}_\prec\{F\} := \{\mathbf{M}(f) : f \in F\}$;
- $\mathbf{T}(F) := \mathbf{T}_\prec(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$, a *monomial module*[1];
- $\mathbf{N}(F) := \mathbf{N}_\prec(F) := \mathcal{T}^{(m)} \setminus \mathbf{T}_\prec(F)$, an *order module*[2];
- $\mathbb{I}(F) = \langle F \rangle$ the module generated by F.

Remark that, if $m = 1$, the assignment of $\mathbf{T}\{F\}$ gives the partition $\mathcal{T} = \mathbf{T}(F) \sqcup \mathbf{N}(F)$ discussed above, that the related semigroup ideal $\mathbf{T}(F)$ is also denoted $\Sigma(F)$ while the related order ideal $\mathbf{N}(F)$ is also denoted $\Delta(F)$ and labelled Δ-*set* or *footprint*. When F is the Gröbner basis of the module $\mathbb{I}(F)$ it generates, $\mathbf{N}(F)$ is called the *Gröbner éscalier*[25] of $\mathbb{I}(F)$.

We can now however induce a finer partition of $\mathcal{T}^{(m)}$ in terms of a module $\mathsf{M} \subset \mathcal{P}^m$ and a term-ordering $\prec$, by defining (see Figure 2 where again $\mathsf{M} = \mathbb{I}(x_1^7, x_1^5x_2^3, x_2^5) \subset \mathcal{P}$)

$\diamond$ $\mathbf{N}_\prec(\mathsf{M}) = \mathcal{T}^{(m)} \setminus \mathbf{T}_<(\mathsf{M})$ its *Gröbner éscalier*;

[1] *Id est* a subset $T \subset \mathcal{T}^{(m)}$ such that $\tau \in T, t \in \mathcal{T} \implies t\tau \in T$.

[2] *Id est* a subset $T \subset \mathcal{T}^{(m)}$ such that $t\tau \in T, t \in \mathcal{T} \implies \tau \in T$.

$\circ$ $\mathbf{B}_\prec(\mathsf{M}) := \{x_h\tau : 1 \leq h \leq n, \tau \in \mathbf{N}_\prec(\mathsf{M})\} \setminus \mathbf{N}_\prec(\mathsf{M})$, its *border set*;

$\bullet$ $\mathbf{J}_\prec(\mathsf{M}) := \mathbf{T}_\prec(\mathsf{M}) \setminus \mathbf{B}_\prec(\mathsf{M})$,

$*$ $\mathbf{G}_\prec(\mathsf{M}) \subset \mathbf{B}_\prec(\mathsf{M})$ the unique minimal basis of $\mathbf{T}_\prec(\mathsf{M})$,

$\cdot$ $\mathbf{C}_\prec(\mathsf{M}) := \{\tau \in \mathbf{N}_\prec(\mathsf{M}) : x_h\tau \in \mathbf{T}_\prec(\mathsf{M}), \forall h\}$ its *corner set.*

Under this notation, the following properties are trivially satisfied:

Lemma 1 *It holds*

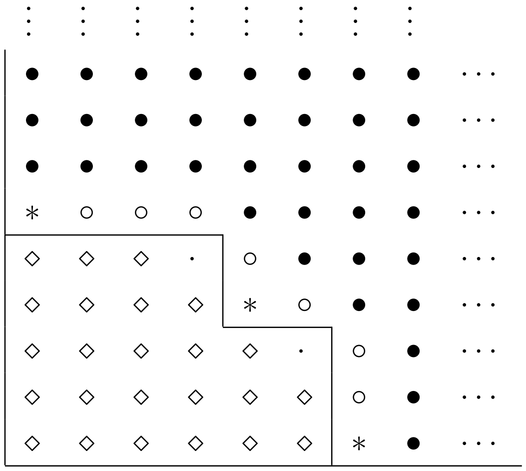
1. $\mathbf{T}_\prec(\mathsf{M}) = \{\tau \in \mathcal{T} : \exists g \in \mathsf{M} : \mathbf{T}_\prec(g) = \tau\}$;
2. $\mathbf{J}_\prec(\mathsf{M}) = \left\{\tau \in \mathbf{T}_\prec(\mathsf{M}) : x_i \mid \tau \implies \frac{\tau}{x_i} \in \mathbf{T}_\prec(\mathsf{M})\right\}$;
3. $\mathbf{B}_\prec(\mathsf{M}) = \left\{\tau \in \mathbf{T}_\prec(\mathsf{M}) : \exists x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})\right\}$;
4. $\mathbf{G}_\prec(\mathsf{M}) = \left\{\tau \in \mathbf{T}_\prec(\mathsf{M}) : \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})\right\}$;
5. $\mathbf{C}_\prec(\mathsf{M}) = \{\tau \in \mathbf{N}_\prec(\mathsf{M}) : \forall i, x_i\tau \in \mathbf{B}_\prec(\mathsf{M})\}$;
6. $\mathbf{N}_\prec(\mathsf{M}) = \{\tau \in \mathcal{T} : \nexists g \in \mathsf{M} : \mathbf{T}_\prec(g) = \tau\}$;
7. $\mathbf{C}_\prec(\mathsf{M}) \cup \mathbf{T}_\prec(\mathsf{M})$ *is a monomial module;*
8. $\mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{G}_\prec(\mathsf{M})$ *and* $\mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{B}_\prec(\mathsf{M})$ *are order modules.*
9. $\tau \in \mathbf{J}_\prec(\mathsf{M}) \iff \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{T}_\prec(\mathsf{M})$;
10. $\tau \in \mathbf{B}_\prec(\mathsf{M}) \setminus \mathbf{G}_\prec(\mathsf{M}) \iff \exists h, H : \frac{\tau}{x_h} \in \mathbf{N}_\prec(\mathsf{M}), \frac{\tau}{x_H} \in \mathbf{B}_\prec(\mathsf{M}) \subset \mathbf{T}_\prec(\mathsf{M})$;
11. $\tau \in \mathbf{B}_\prec(\mathsf{M}) \setminus \mathbf{G}_\prec(\mathsf{M}) \implies \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{B}_\prec(\mathsf{M})$;
12. $\tau \in \mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{G}_\prec(\mathsf{M}) \iff \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})$;
13. $\tau \in \mathbf{T}_\prec(\mathsf{M}) \cup \mathbf{C}_\prec(\mathsf{M}) \iff \forall i, x_i\tau \in \mathbf{T}_\prec(\mathsf{M})$;
14. $\tau \in \mathbf{N}_\prec(\mathsf{M}) \setminus \mathbf{C}_\prec(\mathsf{M}) \iff \exists h : x_h\tau \in \mathbf{N}_\prec(\mathsf{M})$. $\square$

Lemma 2 *Let* N *be a finitely generated* $\mathcal{P}$*-module,* $\Phi : \mathcal{P}^m \mapsto \mathsf{N}$ *be any surjective morphism and set* $\mathsf{M} := \ker(\Phi)$*. Then*

1. $\mathcal{P}^m \cong \mathsf{M} \oplus \mathrm{Span}_k(\mathbf{N}(\mathsf{M}))$;
2. $\mathsf{N} \cong \mathrm{Span}_k(\mathbf{N}(\mathsf{M}))$;
3. *for each* $f \in \mathcal{P}^m$*, there is a unique* $g := \mathrm{Can}(f, \mathsf{M}, \prec) \in \mathrm{Span}_k(\mathbf{N}(\mathsf{M}))$ *such that* $f - g \in \mathsf{M}$.

   Such g *is called the* canonical form *of* f *w.r.t.* M *and satisfies also:*

Figure 2:



(a) $\mathrm{Can}(f_1, \mathsf{M}, \prec) = \mathrm{Can}(f_2, \mathsf{M}, \prec) \iff f_1 - f_2 \in \mathsf{M}$;

(b) $\mathrm{Can}(f, \mathsf{M}, \prec) = 0 \iff f \in \mathsf{M}$. $\square$

Definition 3 *Let* N *be a finitely generated* $\mathcal{P}$*-module,* $\Phi : \mathcal{P}^m \mapsto \mathsf{N}$ *be any surjective morphism and set* $\mathsf{M} := \ker(\Phi)$.

Let $G \subset \mathsf{M}$, $f, h, f_1, f_2 \in \mathcal{P}^m$. *Then*

1. G *will be called a* Gröbner basis *of* M *if*

$$\mathbf{T}(G) = \mathbf{T}(\mathsf{M}),$$

that is, $\mathbf{T}\{G\} := \{\mathbf{T}(g) : g \in G\}$ *generates* $\mathbf{T}(\mathsf{M}) = \mathbf{T}\{\mathsf{M}\}$.

2. *For each* $f_1, f_2 \in \mathcal{P}^m$ *such that*

$$\mathbf{T}(f_1) = t_1\mathbf{e}_{i_1}, \mathbf{T}(f_2) = t_2\mathbf{e}_{i_2},$$

the S-polynomial of f_1 and f_2 *exists only if* $\mathbf{e}_{i_1} = \mathbf{e}_{i_2} := \epsilon$, *in which case it is*

$$S(f_1, f_2) := \mathrm{lc}(f_2)^{-1}\frac{\delta(f_1, f_2)}{t_2}f_2 - \mathrm{lc}(f_1)^{-1}\frac{\delta(f_1, f_2)}{t_1}f_1,$$

where $\delta := \delta(f_1, f_2) := \mathrm{lcm}(t_1, t_2)$*;* $\delta\epsilon$ *is called the* formal term *of* $S(f_1, f_2)$.

3. f *has a* Gröbner representation $\sum_{i=1}^{\mu} p_i g_i$ *in terms of* G *if* [3]

$$f = \sum_{i=1}^{\mu} p_i g_i, p_i \in \mathcal{P}, g_i \in G, \mathbf{T}(p_i)\mathbf{T}(g_i) \preceq \mathbf{T}(f), \text{ for each } i.$$

[3] note that here, unilike in (4), we are not assuming $i \neq j \implies \mathbf{T}(p_i)\mathbf{T}(g_i) \neq \mathbf{T}(p_j)\mathbf{T}(g_j)$; moreover both here, in (4) and in (5) a same element of G can repeatedly appear.

4. *f has the* (strong) Gröbner representation $\sum_{i=1}^{\mu} c_i t_i g_i$ *in terms of G if*

$$f = \sum_{i=1}^{\mu} c_i t_i g_i, c_i \in k \setminus \{0\}, t_i \in \mathcal{T}, g_i \in G,$$

with $\mathbf{T}(f) = t_1\mathbf{T}(g_1) \succ \cdots \succ t_i\mathbf{T}(g_i) \succ \cdots$.

5. *f has the* weak Gröbner representation $\sum_{i=1}^{\mu} c_i t_i g_i$ *in terms of G if*

$$f = \sum_{i=1}^{\mu} c_i t_i g_i, c_i \in k \setminus \{0\}, t_i \in \mathcal{T}, g_i \in G,$$

with $\mathbf{T}(f) = t_1\mathbf{T}(g_1) \succeq \cdots \succeq t_i\mathbf{T}(g_i) \succeq \cdots$.

6. *For any $f_1, f_2 \in \mathcal{P}^m$, whose S-polynomial exists and has $\delta\epsilon$ as formal term, we say that $S(f_1, f_2)$ has a* quasi-Gröbner representation *in terms of G if it can be written as $S(g, f) = \sum_{k=1}^{\mu} p_k g_k$, with $p_k \in \mathcal{P}, g_k \in G$* and $\mathbf{T}(p_k)\mathbf{T}(g_k) \prec \delta\epsilon$ for each k.

7. $h := \mathrm{NF}_{\prec}(f, G)$ *is called a* normal form *of f w.r.t. G, if*

   - *$f - h \in \mathbb{I}(G)$ has a strong Gröbner representation in terms of G and*
   - $h \neq 0 \implies \mathbf{T}(h) \notin \mathbf{T}(G)$.

8. *The* reduced Gröbner basis *of* M *wrt $\prec$ is the set*

$$\{\tau - \mathrm{Can}(\tau, \mathsf{M}, \prec) : \tau \in \mathbf{G}_{\prec}(\mathsf{M})\}.$$

9. *The* border basis *of* M *w.r.t. $\prec$ is the set*

$$\{\tau - \mathrm{Can}(\tau, \mathsf{M}, \prec) : \tau \in \mathbf{B}_{\prec}(\mathsf{M})\}.$$

10. *A* Gröbner representation *of* M *is the assignment of*

    - *a linearly independent set $\mathbf{q} = \{q_1, \ldots, q_s\}$ ($q_1 = 1$), where $s = \#(\mathbf{N}(\mathsf{M}))$, such that $\mathcal{P}^m/\mathsf{M} = \mathrm{Span}_k(\mathbf{q})$,*
    - *the set*
    $$\mathcal{M} = \mathcal{M}(\mathbf{q}) := \left\{ \left(a_{lj}^{(h)}\right) \in k^{s^2}, 1 \leq h \leq n \right\}$$
    of the $s \times s$ square matrices $\left(a_{lj}^{(h)}\right)$ defined by the equalities
    $$x_h q_l = \sum_j a_{lj}^{(h)} q_j, \forall l, j, h, 1 \leq l, j \leq s, 1 \leq h \leq n$$
    in $\mathcal{P}^m/\mathsf{M} = \mathrm{Span}_k(\mathbf{q})$.

11. *For each* $f \in \mathcal{P}$ *the* Gröbner description *of* f *in terms of a Gröbner representation* $(\mathbf{q}, \mathcal{M})$ *is the unique vector*

$$\mathbf{Rep}(f, \mathbf{q}) := (\gamma(f, q_1, \mathbf{q}), \dots, \gamma(f, q_s, \mathbf{q})) \in k^s$$

such that $f - \sum_j \gamma(f, q_j, \mathbf{q}) q_j \in \mathsf{M}$.

12. *The* linear representation *of* M *w.r.t.* $\prec$ *is the Gröbner representation* $(\mathbf{N}_\prec(\mathsf{M}), \mathcal{M}(\mathbf{N}_\prec(\mathsf{M})))$ *where* $\mathbf{q} = \mathbf{N}_\prec(\mathsf{M})$. □

With these definitions, if $\mathbf{N}_\prec(\mathsf{M}) = \{\tau_1, \dots, \tau_s\}$, *the Gröbner description*

$$\mathbf{Rep}(f, \mathbf{N}_\prec(\mathsf{M})) := (\gamma(f, \tau_1, \mathbf{N}_\prec(\mathsf{M})), \dots, \gamma(f, \tau_s, \mathbf{N}_\prec(\mathsf{M})))$$

of f *in terms of the linear representation of* M *w.r.t.* $\prec$ is a convoluted synonym of the notion of the canonical form

$$\mathrm{Can}(f, \mathsf{M}, \prec) = \sum_{j=1}^{s} \gamma(f, \tau_j, \prec)\tau_j = \sum_{j=1}^{s} \gamma(f, \tau_j, \mathbf{N}_\prec(\mathsf{M}))\tau_j$$

of f in terms of $\prec$.

2 Duality (1)

Denote $\mathcal{P}^* := \mathrm{Hom}_k(\mathcal{P}, k)$ the k-vector space of all k-linear functionals $\ell : \mathcal{P} \mapsto k$ and remark that it holds $f \in \mathcal{P}, \ell \in \mathcal{P}^* \implies \ell(f) = \sum_{\tau \in \mathcal{T}} \mathsf{c}(f, \tau)\ell(\tau)$ and that $\mathcal{P}^*$ is made a $\mathcal{P}$-module defining $\ell \cdot f \in \mathcal{P}^*$, for each $\ell \in \mathcal{P}^*, f \in \mathcal{P}$, as

$$(\ell \cdot f)(g) := \ell(fg) \text{ for each } g \in \mathcal{P}.$$

Two sets $\mathbb{L} = \{\ell_1, \dots, \ell_r\} \subset \mathcal{P}^*$ and $\mathbf{q} = \{q_1, \dots, q_s\} \subset \mathcal{P}$ are said to be

- *triangular* if $r = s$, $\ell_i(q_j) = 0$, for each $i < j$ and $\ell_j(q_j) \neq 0$, for each j;
- *biorthogonal* if $r = s$ and $\ell_i(q_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$

For each k-vector subspace $L \subset \mathcal{P}^*$, let

$$\mathfrak{P}(L) := \{g \in \mathcal{P} : \ell(g) = 0, \forall \ell \in L\}$$

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

$$\mathfrak{L}(P) := \{\ell \in \mathcal{P}^* : \ell(g) = 0, \forall g \in P\}.$$

Lemma 4 *For each k-vector subspaces $P, P_1, P_2 \subset \mathcal{P}$ and each k-vector subspaces $L, L_1, L_2 \subset \mathcal{P}^*$ it holds*

1. *if P is an ideal then $\mathfrak{L}(P)$ is a $\mathcal{P}$-module;*

2. *if L is a $\mathcal{P}$-module then $\mathfrak{P}(L)$ is an ideal.*

3. $P_1 \subset P_2 \implies \mathfrak{L}(P_1) \supset \mathfrak{L}(P_2)$;

4. $L_1 \subset L_2 \implies \mathfrak{P}(L_1) \supset \mathfrak{P}(L_2)$;

5. $\mathfrak{L}(P_1 \cap P_2) \supset \mathfrak{L}(P_1) + \mathfrak{L}(P_2)$;

6. $\mathfrak{P}(L_1 \cap L_2) \supset \mathfrak{P}(L_1) + \mathfrak{P}(L_2)$;

7. $\mathfrak{L}(P_1 + P_2) = \mathfrak{L}(P_1) \cap \mathfrak{L}(P_2)$;

8. $\mathfrak{P}(L_1 + L_2) = \mathfrak{P}(L_1) \cap \mathfrak{P}(L_2)$.

9. $P = \mathfrak{P}\mathfrak{L}(P)$.

10. $L \subset \mathfrak{L}\mathfrak{P}(L)$;

11. $\dim_k(L) < \infty \implies L = \mathfrak{L}\mathfrak{P}(L)$. □

Id est $\mathfrak{P}$ and $\mathfrak{L}$ define a duality between finite dimensional $\mathcal{P}$-modules of functionals and zero-dimensional ideals.

3 Möller's Algorithm

Let $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ be a (not necessarily linearly independent) set of k-linear functionals such that $L := \mathrm{Span}_k(\mathbb{L})$ is a $\mathcal{P}$-module, and let us denote, for each $f \in \mathcal{P}$, $v(f, \mathbb{L}) := (\ell_1(f), \ldots, \ell_s(f)) \in k^s$. Since $\dim_k(L) < \infty$ then $\mathsf{I} := \mathfrak{P}(L)$ is a zero-dimensional ideal and

$$\#(\mathbf{N}(\mathsf{I})) = \deg(\mathsf{I}) = \dim_k(L) =: r \leq s;$$

therefore, denoting

$$\mathbf{N}(\mathsf{I}) = \{t_1, \ldots, t_r\}, \quad 1 = t_1 < \ldots < t_i < t_{i+1} < \ldots < t_r,$$

we can consider the $s \times r$ matrix $\ell_i(t_j)$ whose columns are the vectors $v(t_j, \mathbb{L})$ and are linearly independent, since any relation $\sum_j c_j v(t_j, \mathbb{L}) = 0$ would imply

$$\ell_i(\sum_j c_j t_j) = \sum_j c_j \ell_i(t_j) = 0 \text{ and } \sum_j c_j t_j \in \mathfrak{P}(L) = \mathsf{I}$$

contradicting the definition of $\mathbf{N}(\mathsf{I})$.

The matrix $\ell_i(t_j)$ has rank $r \leq s$ and it is possible to extract an ordered subset $\Lambda := \{\lambda_1, \ldots, \lambda_r\} \subset \mathbb{L}$, satisfying $\mathrm{Span}_k\{\Lambda\} = \mathrm{Span}_k\{\mathbb{L}\}$ and to renumber the terms in $\mathbf{N}(\mathsf{I})$ in such a way that each principal minor $\lambda_i(t_j), 1 \leq i, j \leq \sigma \leq r$ is invertible. Therefore, if we consider a set

$$\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$$

which is triangular w.r.t. $\mathbb{L}$, and (a_{ij}) denotes the invertible matrix such that $q_i = \sum_{j=1}^{r} a_{ij} t_j, \forall i \leq r$, then for each $\sigma \leq r$

- $\{q_1, \ldots, q_\sigma\}$ and $\{\lambda_1, \ldots, \lambda_\sigma\}$ are triangular;
- $\mathrm{Span}_k\{t_1, \ldots, t_\sigma\} = \mathrm{Span}_k\{q_1, \ldots, q_\sigma\}$;
- (a_{ij}) is lower triangular.

If we now further assume that

1. $\dim_k(L) = r = s$ and
2. each subvectorspace $L_\sigma := \mathrm{Span}_k(\{\ell_1, \ldots, \ell_\sigma\})$ is a $\mathcal{P}$-module

so that each $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$ is a zero-dimensional ideal and there is a chain

$$\mathsf{I}_1 \supset \mathsf{I}_2 \supset \cdots \supset \mathsf{I}_s = \mathsf{I},$$

then we have, for each σ

- $\lambda_\sigma = \ell_\sigma$,
- $\mathbf{N}(\mathsf{I}_\sigma) = \{t_1, \ldots, t_\sigma\}$ is an order ideal,
- $\mathsf{I}_\sigma \oplus \mathrm{Span}_k\{q_1, \ldots, q_\sigma\} = \mathcal{P}$,
- $\mathbf{T}(q_\sigma) = t_\sigma$.

In conclusion we have proved

Theorem 5 (Möller) *Let $\mathcal{P} := k[x_1, \ldots, x_n]$, and $<$ be any termordering. Let $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ be a set of k-linear functionals such that $\mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal.*

Then there are

- *an integer $r \in \mathbb{N}$,*
- *an order ideal $\mathbf{N} := \{t_1, \ldots, t_r\} \subset \mathcal{T}$,*
- *an ordered subset $\Lambda := \{\lambda_1, \ldots, \lambda_r\} \subset \mathbb{L}$,*
- *an ordered set $\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$,*

such that, denoting $L := \mathrm{Span}_k(\mathbb{L})$ and $\mathsf{I} := \mathfrak{P}(L)$, it holds:

1. $r = \deg(\mathsf{I}) = \dim_k(\mathbb{L})$,
2. $\mathbf{N}(\mathsf{I}) = \mathbf{N}$,
3. $\mathrm{Span}_k(\Lambda) = \mathrm{Span}_k(\mathbb{L})$,
4. $\mathrm{Span}_k\{t_1, \ldots, t_\sigma\} = \mathrm{Span}_k\{q_1, \ldots, q_\sigma\}, \forall \sigma \leq r$,
5. $\{q_1, \ldots, q_\sigma\}$, $\{\lambda_1, \ldots, \lambda_\sigma\}$ *are triangular*, $\forall \sigma \leq r$.

If, moreover, we have

- $\dim_k(L) = r = s$ *and*
- $L_\sigma := \mathrm{Span}_k(\{\ell_1, \dots, \ell_\sigma\})$ *is a* $\mathcal{P}$*-module,* $\forall\sigma$,

then it further holds

6. $\lambda_\sigma = \ell_\sigma$,
7. $\mathbf{N}(\mathsf{I}_\sigma) = \{t_1, \dots, t_\sigma\}$ *is an order ideal,*
8. $\mathsf{I}_\sigma \oplus \mathrm{Span}_k\{q_1, \dots, q_\sigma\} = \mathcal{P}$,
9. $\mathbf{T}(q_\sigma) = t_\sigma$

for each $\sigma \leq r$*, where* $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$. □

Corollary 6 (Lagrange Interpolation Formula) *Let* $\mathcal{P} := k[x_1, \dots, x_n]$, $<$ *be any termordering.* $\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ *be a set of* k*-linear functionals such that* $\mathsf{I} := \mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ *is a 0-dim. ideal.*

There exists a set $\mathbf{q} = \{q_1, \dots, q_s\} \subset \mathcal{P}$ *such that*

1. $q_i = \mathrm{Can}(q_i, \mathsf{I}) \in \mathrm{Span}_k(\mathbf{N}(\mathsf{I}))$;
2. $\mathbb{L}$ *and* $\mathbf{q}$ *are triangular;*
3. $\mathcal{P}/\mathsf{I} \cong \mathrm{Span}_k(\mathbf{q})$.

There exists a set $\mathbf{q}' = \{q'_1, \dots, q'_s\} \subset \mathcal{P}$ *such that*

1. $q'_i = \mathrm{Can}(q'_i, \mathsf{I}) \in \mathrm{Span}_k(\mathbf{N}(\mathsf{I}))$;
2. $\mathbb{L}$ *and* $\mathbf{q}'$ *are biorthogonal;*
3. $\mathcal{P}/\mathsf{I} \cong \mathrm{Span}_k(\mathbf{q}')$.

Let $c_1, \dots, c_s \in k$ *and let* $q := \sum_i c_i q'_i \in \mathcal{P}$*. Then, if* $\{g_1, \dots, g_t\}$ *denotes a Gröbner basis of* I*, one has*

1. q *is the unique polynomial in* $\mathrm{Span}_k(\mathbf{N}(\mathsf{I}))$ *such that* $\ell_i(q) = c_i$*, for each* i*;*
2. *for each* $p \in \mathcal{P}$ *it is equivalent*
   (a) $\ell_i(p) = c_i$*, for each* i*,*
   (b) $q = \mathrm{Can}(p, \mathsf{I})$,
   (c) *exist* $h_j \in \mathcal{P}$ *such that*
   $$p = q + \sum_{j=1}^{t} h_j g_j, \mathbf{T}(h_j)\mathbf{T}(g_j) \leq \mathbf{T}(p - q).$$

□

Möller's Algorithm [45, 22, 40, 2] is a procedure which, given a set of k-linear functionals $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ such that $\mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal, allows to compute the data whose existence is stated in Theorem 5. The stronger version of the algorithm (Figure 3) assumes that, for each $\sigma \leq s$ $L_\sigma := \mathrm{Span}_k(\{\ell_1, \ldots, \ell_\sigma\})$ is a $\mathcal{P}$-module, is performed by induction on σ and gives the complete structure of each ideal $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$.

Its correctness is based on the following

Lemma 7 *Let*

$\mathcal{P} := k[x_1, \ldots, x_n]$,

$<$ *be any termordering;*

$\mathbb{L} = \{\ell_1, \ldots, \ell_r\} \subset \mathcal{P}^*$ *be a set of linearly independent k-linear functionals such that* $\mathsf{I} := \mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ *is a zero-dimensional ideal*

and let

$\mathbf{N} := \{t_1, \ldots, t_r\} \subset \mathcal{T}$,

$\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$,

$G := \{g_1, \ldots, g_t\} \subset \mathcal{P}$,

be such that

- $\mathbf{N}$ *is an order ideal,*
- $\mathrm{Span}_k\{t_1, \ldots, t_r\} = \mathrm{Span}_k\{q_1, \ldots, q_r\}$,
- $\{q_1, \ldots, q_r\}$ *and* $\{\ell_1, \ldots, \ell_r\}$ *are triangular,*
- $\ell(g) = 0$ *for each* $g \in G$ *and each* $\ell \in \mathbb{L}$,
- $\mathbf{N} \sqcup \mathbf{T}_<(G) = \mathcal{T}$,
- *for each* $g \in G, g - \mathrm{lc}(g)\mathbf{T}_<(g) \in \mathrm{Span}_k(\mathbf{N})$,

then G is a reduced Gröbner basis of $\mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ *w.r.t.* $<$.

The assumption that for each $\sigma \leq s$, $L_\sigma := \mathrm{Span}_k(\{\ell_1, \ldots, \ell_\sigma\})$ can be satisfied if for instance the 0-dimensional ideal $\mathsf{I} = \mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ is described in terms of a *Macaulay representation* (cf. [3]), but often [4] is not satisfied, thus requiring an alternative version (Figure 4) performed by induction on the terms and not on the functionals and which returns also a basis of $\mathrm{Span}_k(\mathbb{L})$.

Remark 8 If, in the algorithm of Figure 3, we define p in instruction $\diamond$ as $p := x_h\mathsf{f}$ instead of $p := x_h t$, we have two counterbalancing effects:

[4] mainly in the solution of the FGLM-Problem, where in any case the functionals are properly reordered so they satisfy such property

Figure 3: Möller's Algorithm (1)

$(G_1, \dots, G_s, \mathbf{N}, \mathbf{q}) := \textbf{G-basis}(\mathbb{L}, <)$

where

$\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ is s.t.

$$L_\sigma := \mathrm{Span}_k(\{\ell_1, \dots, \ell_\sigma\})$$

is a $\mathcal{P}$-module, for each $\sigma \le s$,

$\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$, for each $\sigma \le s$,

$G_\sigma \subset \mathsf{I}_\sigma$ is the reduced Gröbner basis of $\mathsf{I}_\sigma, \forall \sigma \le s$,

$\mathbf{N} := \{t_1, \dots, t_s\}$ is an order ideal,

$\mathbf{q} := \{q_1, \dots, q_s\} \subset \mathcal{P}$ is a set triangular to $\mathbb{L}$,

$\mathbf{N}_\sigma := \{t_1, \dots, t_\sigma\} = \mathbf{N}(\mathsf{I}_\sigma)$, $\forall \sigma \le s$,

$q_\sigma \in \mathrm{Span}_k\{\mathbf{N}_\sigma\}$, and $\mathbf{T}(q_\sigma) = t_\sigma, \forall \sigma \le s$,

$\mathrm{Span}_k\{t_1, \dots, t_\sigma\} = \mathrm{Span}_k\{q_1, \dots, q_\sigma\}, \forall \sigma \le s$,

$\{q_1, \dots, q_\sigma\}$ and $\{\ell_1, \dots, \ell_\sigma\}$ are triangular $\forall \sigma$.

$\sigma := 1, t_1 := 1, \mathbf{N} := \{t_1\}$, $q_1 := \ell_1(1)^{-1} t_1$,

$\mathbf{q} := \{q_1\}, G_1 := \{x_h - \ell_1(x_h), 1 \le h \le n\}$,

%% $\mathbf{N}_\sigma \sqcup \mathbf{T}(G_\sigma) = \mathcal{T}$.

%% $\ell_j(f) = 0$ for all $f \in G_\sigma, 1 \le j \le \sigma$.

For $\sigma := 2..s$ **do**

- ◦ $t := \min\{\mathbf{T}(f) : f \in G_\sigma, \ell_\sigma(f) \ne 0\}$,
  Let $\mathsf{f} \in G_\sigma : \mathbf{T}(\mathsf{f}) = t$,
  $t_\sigma := t, q_\sigma := \ell_\sigma(\mathsf{f})^{-1}\mathsf{f}$, $\mathbf{N} := \mathbf{N} \cup \{t_\sigma\}$,
- • $\mathbf{q} := \mathbf{q} \cup \{q_\sigma\}$,
- ⋆ $G_\sigma := \{f - \ell_\sigma(f) q_\sigma : f \in G_{\sigma-1}\}$.
  For each $h = 1..n : x_h t \notin \mathbf{T}(G_\sigma)$ **do**
  - ⋄ $p := x_h t$,
  - ∗ **For** $i = 1..\sigma$ **do** $p := p - \ell_i(p) q_i$,
    $G_\sigma := G_\sigma \cup \{p\}$;

  %% $\mathbf{N}_\sigma \sqcup \mathbf{T}(G_\sigma) = \mathcal{T}$,

  %% $\ell_j(f) = 0$ for all $f \in G_\sigma, 1 \le j \le \sigma$.

- the final output, while still a Gröbner basis, is not, in principle, reduced;
- since $\mathsf{f} \in \mathsf{I}_\sigma$, we have $x_h\mathsf{f} \in \mathsf{I}_\sigma$ and $\ell_i(p) = 0$ for each $i \leq \sigma$ so that one can perform the instruction $*$ for the single value $i := \sigma$.

Equivalently, defining, in the algorithm of Figure 3, p in instruction $\diamond$ as

$$p := x_h\mathsf{f} - \ell_\sigma(x_h\mathsf{f})q_\sigma = \big(x_h - \ell_\sigma(x_h\mathsf{f})\ell_\sigma(\mathsf{f})^{-1}\big)\,\mathsf{f} \tag{1}$$

we can simply remove the instruction $*$.

Finally note that the algorithm discussed in [31] is the generalization to modules of the version of the algorithm of Figure 3 where, in instruction $\diamond$, p is defined as in (1) and the instructions $*$ and $\bullet$ are removed. $\square$

4 The FGLM Problem

For its elimination property, the *lex* ordering is a good tool for solving [Gianni–Kalkbrener Algorithm [28, 30, 51], Lazard's triangular sets[35, 34, 4, 5]] or for applications [see the CRHT-like algorithms in BCH codes[51]] but both practical experience and theoretical argument show that, in general, *lex* is a very bad choice for applying Buchberger Algorithm. On the other side the *degrevlex ordering* is the *optimal* choice for applying it. This suggests [22] the

Problem 9 (FGLM Problem) *Given*

- *a termordering $<$ on the polynomial ring $\mathcal{P} := k[x_1, \ldots, x_n]$,*
- *a zero-dimensional ideal $\mathsf{I} \subset \mathcal{P}$ and*
- *its reduced Gröbner basis $G_\prec$ w.r.t. the term-ordering $\prec$,*

to deduce the Gröbner basis $G_<$ of I w.r.t. $<$. $\square$

5 The FGLM Matrix

Let $\prec$ be a termordering and $\mathbf{N}_\prec(\mathsf{I}) = \{\tau_1, \ldots, \tau_s\}$; in order to apply Möller Algorithm to the FGLM Problem, we just need to choose as functionals $\mathbb{L} := \{\ell_1, \ldots, \ell_s\}$ the coefficients of the canonical forms $\ell_i(\cdot) := \gamma(\cdot, \tau_i, \mathbf{N}_\prec(\mathsf{I}))$ so that we need to compute

$$\mathbf{Rep}(f, \mathbf{N}_\prec(\mathsf{I})) := (\gamma(f, \tau_1, \mathbf{N}_\prec(\mathsf{I})), \ldots, \gamma(f, \tau_s, \mathbf{N}_\prec(\mathsf{I})))$$

for each $f \in \mathsf{B} := \{x_i\tau_j, 1 \leq i \leq n, 1 \leq j \leq s\}$.

The key idea of FGLM is to treat such elements by $\prec$-increasing ordering, so that, when the loop is treating a term $x_h\tau_l$, we have previously managed

Figure 4: Möller's Algorithm (2)

$(G, r, \mathbf{N}, \Lambda, \mathbf{q}) := \textbf{G-basis}(\mathbb{L}, <)$

where

$\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ is s.t. $\mathsf{I} := \mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal;

$G \subset \mathsf{I}$ is the reduced Gröbner basis of I w.r.t. $<$;

$r = \deg(\mathsf{I}) = \dim_k(\mathrm{Span}_k(\mathbb{L}))$;

$\mathbf{N} := \{t_1, \ldots, t_r\} = \mathbf{N}(\mathsf{I})$;

$1 = t_1 < t_2 < \ldots < t_i < t_{i+1} < \ldots < t_r$,

$\Lambda := \{\lambda_1, \ldots, \lambda_r\} \subset \mathbb{L}$, is a linearly independent basis of $\mathrm{Span}_k(\mathbb{L})$;

$\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$ is a set triangular to Λ;

$q_i \in \mathrm{Span}_k\{t_1, \ldots, t_i\}, \mathbf{T}(q_i) = t_i$, for each $i \leq r$;

$\mathrm{Span}_k\{t_1, \ldots, t_i\} = \mathrm{Span}_k\{q_1, \ldots, q_i\}$, for each $i \leq r$;

$\{q_1, \ldots, q_i\}$ and $\{\lambda_1, \ldots, \lambda_i\}$ are triangular, for each $i \leq r$.

$G := \emptyset, r := 1, t_1 := 1, \mathbf{N} := \{t_1\}$,

$v := (\ell_1(t_1), \ldots, \ell_s(t_1))$,

$\mu := \min\{j : \ell_j(1) \neq 0\}$,

$\lambda_1 := \ell_\mu$, $\Lambda := \{\lambda_1\}$,

$q_1 := \lambda_1(1)^{-1} t_1, \mathbf{q} := \{q_1\}$, $\mathrm{vect}(1) := \lambda_1(1)^{-1} v$,

%% $\mathrm{vect}(1) = (\ell_1(q_1), \ldots, \ell_s(q_1))$,

While $\mathbf{N} \sqcup \mathbf{T}(G) \neq \mathcal{T}$ **do**

$t := \min_<\{\tau \in \mathcal{T}, \tau \notin \mathbf{N} \sqcup \mathbf{T}(G)\}$,

$q := t, v := (\ell_1(q), \ldots, \ell_s(q))$

For $j = 1..r$ **do**

$v := v - \lambda_j(q)\,\mathrm{vect}(j), q := q - \lambda_j(q) q_j$,

%% $v = (\ell_1(q), \ldots, \ell_s(q))$.

If $v = 0$ **then**

$G := G \cup \{q\}$,

else

$r := r + 1$

$t_r := t, \mathbf{N} := \mathbf{N} \cup \{t_r\}$,

$\mu := \min\{j : \ell_j(q) \neq 0\}$,

$\lambda_r := \ell_\mu, \Lambda := \Lambda \cup \{\lambda_r\}$,

$q_r := \lambda_r(q)^{-1} q, \mathbf{q} := \mathbf{q} \cup \{q_r\}, \mathrm{vect}(r) := \lambda_r(q)^{-1} v$

%% $\mathrm{vect}(i) = (\ell_1(q_i), \ldots, \ell_s(q_i))$ for each $i, 1 \leq i \leq r$

$G, r, \mathbf{N}, \Lambda, \mathbf{q}$

the term τ_l and thus previously computed $\mathbf{Rep}(\tau_l, \mathbf{N}_\prec(\mathsf{I}))$ which satisfies the relation

$$\tau_l - \sum_{j=1}^{s} \gamma(\tau_l, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\tau_j = \tau_l - \mathrm{Can}(\tau_l, \mathsf{I}, \prec) \in \mathsf{I},$$

so that $x_h\tau_l - \sum_{j=1}^{s} \gamma(\tau_l, \tau_j, \mathbf{N}_\prec(\mathsf{I}))x_h\tau_j \in \mathsf{I}$, and

$$\begin{aligned}\mathrm{Can}(x_h\tau_l, \mathsf{I}, \prec) &= \sum_{j=1}^{s} \gamma(\tau_l, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\,\mathrm{Can}(x_h\tau_j, \mathsf{I}, \prec)\\ &= \sum_{i=1}^{s}\left(\sum_{j=1}^{s} \gamma(\tau_l, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\gamma(x_h\tau_j, \tau_i, \mathbf{N}_\prec(\mathsf{I}))\right)\tau_i.\end{aligned}$$

For the $\prec$-minimal $\omega := x_h\tau_l \in \mathsf{B}$ under consideration we have the following three cases:

- if $\omega \notin \mathbf{T}_\prec(\mathsf{I})$ then $\omega \in \mathbf{N}_\prec(\mathsf{I})$, so that we add ω to $\mathbf{N}$ and $\{\omega x_h : 1 \le h \le n\}$ to B;
- if there is $g \in G_\prec$ such that

  $$\mathbf{T}_\prec(g) = \omega \text{ and } g = \omega - \sum_{\tau \in \mathbf{N}_\prec(\mathsf{I})} \gamma(\omega, \tau, \mathbf{N}_\prec(\mathsf{I}))\tau,$$

  since the procedure iterates on $\prec$-increasing values of ω, we have

  $$\gamma(\omega, \tau, \mathbf{N}_\prec(\mathsf{I})) \neq 0 \implies \tau \prec \omega \implies \tau \in \mathbf{N};$$

- if there is $H, 1 \le H \le n, \tau \in \mathbf{T}_\prec(\mathsf{I})$ such that $\omega = x_H\tau$; thus $\tau \prec \omega$ has been already treated so that we have obtained a representation

  $$\mathrm{Can}(\tau, \mathsf{I}, \prec) = \sum_{j=1}^{s} \gamma(\tau, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\tau_j;$$

  since in such representation we have

  $$\gamma(\tau, \tau_j, \mathbf{N}_\prec(\mathsf{I})) \neq 0 \implies \tau_j \prec \tau \implies \tau_j \in \mathbf{N}, x_H\tau_j \prec x_H\tau = \omega = x_h\tau_l$$

  and $\tau = x_h\tau_\iota$ for $\tau_\iota := \frac{\tau_l}{x_H}$, we also have the representation

  $$\mathrm{Can}(x_H\tau, \mathsf{I}, \prec) = \sum_{j=1}^{s} \gamma(\tau, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\,\mathrm{Can}(x_H\tau_j, \mathsf{I}, \prec)$$

  and we can use the same formula as above to derive

  $$\begin{aligned}&\gamma(x_h\tau_l, \tau_i, \mathbf{N}_\prec(\mathsf{I})) = \gamma(x_H\tau, \tau_i, \mathbf{N}_\prec(\mathsf{I}))\\ =& \sum_{j=1}^{s} \gamma(\tau, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\gamma(x_H\tau_j, \tau_i, \mathbf{N}_\prec(\mathsf{I}))\\ =& \sum_{j=1}^{s} \gamma(x_h\tau_\iota, \tau_j, \mathbf{N}_\prec(\mathsf{I}))\gamma(x_H\tau_j, \tau_i, \mathbf{N}_\prec(\mathsf{I})).\end{aligned}$$

These remarks can be formalized in the algorithm descriped in Figure 5; Figure 6 proposes the instantiation of Möller's Algorithm (Figure 4) to the setting of the FGLM Problem.

6 Pointers

Remark (Compare [31]) that the Berlekamp-Massey Algorithm can be interpreted as a sort of FGLM Algorithm on modules with functionals depending on the state of the computation[5].

However, the earliest instance of the FGLM Algorithm goes back to 1936: in fact, Todd-Coxeter Algorithm [54] can be easily read [52] as a re-formulation of **FGLM-Matrix** (Figure 5) over groups view as quotients of a non-commutative polynomial rings modulo a bimonomial ideal.

The FGLM Problem was already solved essentially by means of the FGLM Algorithm in [14].

Möller's Algorithm was introduced for the first time in [45]: in that setting the considered functionals were point evaluation, the aim being multivariate interpolation; the same procedure was proposed in [27] as a tool to efficiently perform change of coordinate into a 0-dimensional ideal.

[22] introduced the FGLM Problem and solved it by means of Figure 6; the paper gives also a precise complexity analysis and introduced both the FGLM Matrix and the efficient algorithm (Figure 5) computing it.

[40] reconsidered Möller's and FGLM Algorithms, merging them and interpreting them in the setting of functionals; [2] is a survey which discusses also Macaulay's Algorithm to describe the structure of the canonical module $\mathfrak{L}(\mathsf{I})$.

The FGLM Algorithm *proper* solves the FGLM Problem only for a 0-dim. ideal; [37] explains how to extend it to a multi-dimensional ideal; the corresponding algorithm is however far from being fast. The same weakness is shared by the Gröbner Walk Algorithm [20].

The most efficient algorithm for the solution of the FGLM-Problem, at least in the multidimensional case, is the Hilbert Driven Algorithm [55]: assuming

[5]in fact, with Berlekamp's [9] notation we assume to have found the basis

$$\left\{(\sigma^{(k)}, \omega^{(k)}), (\tau^{(k)}, \gamma^{(k)})\right\}$$

of the module

$$M_k := \left\{(a(z), b(z)) \in \mathbb{Z}_2[z]^2 : (1+S)a(z) \equiv b(z) \bmod z^{k+1}\right\} \subset \mathbb{Z}_2[z]^2$$

and we consider the new functional $\lambda_{k+1} : \mathbb{Z}_2[z]^2 \to \mathbb{Z}_2$ defined by $\lambda_{k+1}(a(z), b(z)) := \Delta_1^{(k)}$ where $\Delta_1^{(k)} \in \mathbb{Z}_2$ is the value for which $(1+S)a(z) - b(z) \equiv \Delta_1^{(k)} z^{k+1} \bmod z^{k+2}$.

In other words we can consider the functionals $\lambda_k : \mathbb{Z}_2[z]^2 \to \mathbb{Z}_2, 0 \leq k \leq 2t$ defined by $\lambda_{k+1}(a(z), b(z)) := c_k$ where $\sum_k c_k z^k = (1+S)a(z) - b(z) \in \mathbb{Z}_2[[z]]$ and each module M_k satisfies

$$M_k := \left\{(a(z), b(z)) \in \mathbb{Z}_2[z]^2 : \lambda_i(a(z), b(z)) = 0, 0 \leq i \leq k\right\} \subset \mathbb{Z}_2[z]^2.$$

For this interpretation I am strongly indepted to [24, 29].

Figure 5: The FGLM Matrix

$(\mathbf{N}_\prec, \mathcal{M}) :=$ **FGLM-Matrix**$(G_\prec)$

where

$G_\prec \subset \mathsf{I}$ is the reduced Gröbner basis of I w.r.t. $\prec$;
$s = \deg(\mathsf{I})$,
$\mathbf{N}_\prec := \{\tau_1, \ldots, \tau_s\} = \mathbf{N}_\prec(\mathsf{I})$,
$1 = \tau_1 \prec \tau_2 \prec \ldots \prec \tau_j \prec \tau_{j+1} \prec \ldots \prec \tau_s$,
$\mathcal{M} = \mathcal{M}(\mathbf{N}_\prec) = \left\{ \left(a_{lj}^{(h)} \right) \in k^{s^2}, 1 \le h \le n \right\}$ is the set of the square matrices defined by the equalities $x_h \tau_l = \sum_j a_{lj}^{(h)} \tau_j$ in $\mathcal{P}/\mathsf{I} = \mathrm{Span}_k(\mathbf{N}_\prec)$;

$r := 1$, $\tau_1 := 1, \mathbf{N}_\prec := \{\tau_1\}$, $\mathsf{B} := \{x_h : 1 \le h \le n\}$,

While $\mathsf{B} \neq \emptyset$ **do**

$\omega := \min_\prec(\mathsf{B})$, $\mathsf{B} := \mathsf{B} \setminus \{\omega\}$,
$h, l : \omega := x_h \tau_l$
If $\omega \notin \mathbf{T}_\prec(\mathsf{I})$ **then**
$r := r + 1$
$\tau_r := \omega, \mathbf{N}_\prec := \mathbf{N}_\prec \cup \{\tau_r\}$, $\mathsf{B} := \mathsf{B} \cup \{x_h \tau_r : 1 \le h \le n\}$,
$a_{lr}^{(k)} := 1$;
else
if $\exists g := \mathbf{T}_\prec(g) - \sum_{j=1}^r \gamma(\omega, \tau_j, \mathbf{N}_\prec)\tau_j \in G_\prec : \mathbf{T}_\prec(g) = \omega = x_h \tau_l$ **then**
For $j = 1..r$ **do** $a_{lj}^{(h)} := \gamma(\omega, \tau_j, \mathbf{N}_\prec)$
else
Let $H, \iota : 1 \le H \le n, 1 \le \iota \le r : x_h \tau_\iota \in \mathbf{T}_\prec(G_\prec)$, $\tau_l = x_H \tau_\iota$;
For $i = 1..r$ **do** $a_{li}^{(h)} := \sum_{j=1}^r a_{\iota j}^{(h)} a_{ji}^{(H)}$
For each $H, i : x_H \tau_i = \omega$ **do**
For $j = 1..r$ **do** $a_{ij}^{(H)} := a_{lj}^{(h)}$;

$\mathbf{N}_\prec, \mathcal{M}$

Figure 6: The FGLM Algorithm

$(G, \mathbf{N}, \mathbf{q}) := \mathbf{FGLM}(G_{\prec}, <)$

where

$<$ and $\prec$ are termorderings on $\mathcal{P}$,

$\mathsf{I} \subset \mathcal{P}$ is a zero-dimensional ideal,

$G_{\prec} \subset \mathsf{I}$ is the reduced Gröbner basis of I w.r.t. $\prec$;

$s = \deg(\mathsf{I})$,

$\mathbf{N}_{\prec} := \{\tau_1, \ldots, \tau_s\} = \mathbf{N}_{\prec}(\mathsf{I})$,

$1 = \tau_1 \prec \tau_2 \prec \ldots \prec \tau_j \prec \tau_{j+1} \prec \ldots \prec \tau_s$,

$\mathcal{M} = \mathcal{M}(\mathbf{N}_{\prec}) = \left\{ \left(a_{lj}^{(h)} \right) \in k^{s^2}, 1 \leq h \leq n \right\}$ is the set of the square matrices defined by the equalities $x_h \tau_l = \sum_j a_{lj}^{(h)} \tau_j$ in $\mathcal{P}/\mathsf{I} = \mathrm{Span}_k(\mathbf{N}_{\prec})$;

$G \subset \mathsf{I}$ is the reduced Gröbner basis of I w.r.t. $<$,

$\mathbf{N} := \{t_1, \ldots, t_s\} = \mathbf{N}_{<}(\mathsf{I})$,

$1 = t_1 < t_2 < \ldots < t_j < t_{j+1} < \ldots < t_s$,

$\mu : \{1, \ldots, s\} \mapsto \{1, \ldots, s\}$ is a permutation,

$\mathbf{q} := \{q_1, \ldots, q_s\} \subset \mathcal{P}$ is a set triangular to $\left\{ \gamma(\cdot, \tau_{\mu(1)}, \mathbf{N}_{\prec}), \ldots, \gamma(\cdot, \tau_{\mu(s)}, \mathbf{N}_{\prec}) \right\}$

$q_i \in \mathrm{Span}_k\{t_1, \ldots, t_i\}, \mathbf{T}_{<}(q_i) = t_i$, for each $i \leq s$,

$\{q_1, \ldots, q_i\}$ and $\{\gamma(\cdot, \tau_{\mu(1)}, \mathbf{N}_{\prec}), \ldots, \gamma(\cdot, \tau_{\mu(i)}, \mathbf{N}_{\prec})\}$ are triangular for all $i \leq s$.

$(\mathbf{N}_{\prec}, \mathcal{M}) := \mathbf{FGLM\text{-}Matrix}(G_{\prec})$

$G := \emptyset, r := 1, t_1 := 1, \mathbf{N} := \{t_1\}, q_1 := 1, \mathbf{q} := \{q_1\}$,

$\mathsf{B} := \{x_h, 1 \leq h \leq n\}$

$\mathrm{vect}(1) := (1, 0, \ldots, 0), \mu(1) := 1$,

%% $\mathrm{vect}(1) = \mathbf{Rep}(q_1, \mathbf{N}_{\prec}), \mu(1) = \min\{j : \gamma(q_1, \tau_j, \mathbf{N}_{\prec}) \neq 0\}$

While $\mathsf{B} \neq \emptyset$ **do**

$t := \min_{<}(\mathsf{B}), \mathsf{B} := \mathsf{B} \setminus \{t\}$,
$l, h : t = x_h t_l = x_h \mathbf{T}_{<}(q_l)$
If $t \notin \mathbf{T}_{<}(G)$ **then**
  $q := x_h t_l$
  For $i = 1..s$ **do** $v_i := \sum_{j=1}^{s} \gamma(q_l, \tau_j, \mathbf{N}_{\prec}) a_{ji}^{(h)}$;
  $v := (v_1, \ldots, v_s)$
  %% $v = \mathbf{Rep}(q, \mathbf{N}_{\prec})$
  For $j = 1..r$ **do**
    $v := v - \gamma(q, \tau_{\mu(j)}, \mathbf{N}_{\prec})\,\mathrm{vect}(j), q := q - \gamma(q, \tau_{\mu(j)}, \mathbf{N}_{\prec}) q_j$,
    %% $v = \mathbf{Rep}(q, \mathbf{N}_{\prec})$
  If $v = 0$ **then**
    $G := G \cup \{q\}$,
  else
    $r := r + 1$
    $t_r := t, \mathbf{N} := \mathbf{N} \cup \{t_r\}$,
    $\mu(r) := \min\{j : \gamma(q, \tau_j, \mathbf{N}_{\prec}) \neq 0\}$,
    $q_r := \gamma(q, \tau_{\mu(r)}, \mathbf{N}_{\prec})^{-1} q, \mathrm{vect}(r) := \gamma(q, \tau_{\mu(r)}, \mathbf{N}_{\prec})^{-1} v$
    %%$\mathrm{vect}(i) = \mathbf{Rep}(q_i, \mathbf{N}_{\prec}), \forall i, 1 \leq i \leq r$
    $\mathbf{q} := \mathbf{q} \cup \{q_r\}$,
    $\mathsf{B} := \mathsf{B} \cup \{x_h t_r, 1 \leq h \leq n\}$,

$G, \mathbf{N}, \mathbf{q}$

wlog that I is homogeneous, the knowledge of the basis $G_{\prec}$ allows to compute the Hilbert function of I and thus, at each step, to predict how many new generators of a fixed degree are needed in the basis $G_{<}$; when such generators are produced, all other S-pairs of same degree are discarded and the Hilbert function of the monomial ideal $(\mathbf{T}_{<}(g) : g \in G_{<})$ is re-evaluated and the computation is performed in higher degree.

Recently new ideas have been proposed which, in my opinion, promise to be more efficient than the FGLM and the Hilbert Driven Algorithms [7, 53].

Möller's Algorithm has been generalized to projective spaces [1] and to non-commutative setting [10].

[11, 12, 13] use an improved version of the FGLM algorithm for binomial ideals in order to correct binary linear codes.

7 Duality (2)

Let us begin by remarking that a Gröbner representation of a 0-dimensional ideal $\mathsf{I} \subset \mathcal{P} := k[X_1, \ldots, X_n]$ allows to deduce easily the $\mathcal{P}$-module structure of its canonical module $\mathfrak{L}(\mathsf{I})$.

In fact

Lemma 10 *Let*

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

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

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

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

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

$\left(q_{ij}^{(h)}\right) \in k^{r^2}, 1 \leq k \leq r$ *be the matrices defined by* $X_h q_i = \sum_j q_{ij}^{(h)} q_j \bmod \mathsf{I}$,

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

Then

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

□

Denoting $\mathsf{m} := (X_1, \ldots, X_n)$ the maximal at the origin we recall that, given an ideal $\mathsf{I} \subset \mathcal{P}$, its m-*closuse* is the ideal $\bigcap_d \mathsf{I} + \mathsf{m}^d$, and I is called m-*closed* iff $\mathsf{I} = \bigcap_d \mathsf{I} + \mathsf{m}^d$.

We can produce a natural representation of $\mathcal{P}^*$, if we associate, to each term $\tau \in \mathcal{T}$, the functional $M(\tau) : \mathcal{P} \to k$ defined by

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

in fact, denoting $\mathbb{M} := \{M(\tau) : \tau \in \mathcal{T}\}$, we obtain $\mathcal{P}^* \cong k[[\mathbb{M}]]$.

Remark that, with this notation, 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 $\ell(f) = \sum_{t \in \mathcal{T}} a_t c_t$.

The $\mathcal{P}$-module structure of $\mathcal{P}^* \cong k[[\mathbb{M}]]$ is described by

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

We will say that a k-vector subspace $\Lambda \subset \mathrm{Span}_k(\mathbb{M})$ is *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[6] we must restrict ourselves to $\mathrm{Span}_k(\mathbb{M}) \cong k[\mathbb{M}]$.

Under this restriction, for each k-vector subspace $\Lambda \subset \mathrm{Span}_k(\mathbb{M})$ we denote

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

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

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

and we obtain

Lemma 11 *[38, 39, 32, 46, 40, 3] The mutually inverse maps $\mathfrak{I}(\cdot)$ and $\mathfrak{M}(\cdot)$ give a biunivocal, inclusion reversing, correspondence between the set of the m-closed ideals $\mathsf{I} \subset \mathcal{P}$ and the set of the stable k-vector subspaces $\Lambda \subset \mathrm{Span}_k(\mathbb{M})$.*

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

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

$$\deg(\mathsf{q}) = \dim_k(\mathfrak{M}(\mathsf{q}));$$

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

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

$\square$

[6] Recall that $\mathfrak{L}P(L) = L$ holds only if $\dim_k(L) < \infty$.

8 Macaulay Bases

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

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

so that

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

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

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

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

and remark that $\ell(\tau) \in \mathfrak{M}(\mathsf{I})$ requires $\ell(\tau) \in k[\mathbb{M}]$ which holds iff

$$\# \{t : \gamma(t, \tau, <) \neq 0\} < \infty$$

and is granted if $\{t : t > \tau\}$ is finite.

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

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

$$\tau_1 > \tau_2 > \cdots \tau_\nu > \cdots$$

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

In this setting the generalization of the notion of Gröbner basis is called Hironoka/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.

Thus let $<$ be a standard ordering on $\mathcal{T}$ and $\mathsf{I} \subset \mathcal{P}$ an m-closed ideal; denoting

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

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

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

we have

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

Definition 12 *[3]*
The set $\{\ell(\tau), \tau \in \mathbf{N}_<(\mathsf{I})\}$ *is called the* Macaulay basis *of* I*; each element* $\ell(\tau)$ *is called a* Noetherian equation. □

There is an algorithm [40, 3] which, given a finite basis (not necessarily Gröbner/standard) of an m-primary ideal I, computes its Macaulay basis. Such algorithm can be extended to an infinite procedure which, given a finite basis of an ideal $\mathsf{I} \subset \mathsf{m}$, returns the infinite Macaulay basis of its m-closure.

Definition 13 *[44] Let*

$\mathsf{I} \subset \mathcal{P}$ *be a 0-dimensional ideal;*

$\mathsf{Z} := \{\mathsf{a} \in k^n : f(\mathsf{a}) = 0, \forall f \in \mathsf{I}\}$*;*

for each $\mathsf{a} \in \mathsf{Z}$

- $\lambda_{\mathsf{a}} : \mathcal{P} \mapsto \mathcal{P}$ *the translation* $\lambda_{\mathsf{a}}(X_i) = X_i + a_i, \forall i$,
- $\mathfrak{m}_{\mathsf{a}} = (X_1 - a_1, \dots, X_n - a_n)$,
- $\mathfrak{q}_{\mathsf{a}}$ *the* $\mathfrak{m}_{\mathsf{a}}$*-primary component of* I,
- $\Lambda_{\mathsf{a}} := \mathfrak{M}(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}})) \subset \mathrm{Span}_k(\mathbb{M})$,
- $\ell_{\upsilon\mathsf{a}}$*, for each* $\upsilon \in \mathbf{N}_<(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}}))$*, the Noetherian equation* $\ell_{\upsilon\mathsf{a}} := \ell(\upsilon)$ *so that*
- $\{\ell_{\upsilon\mathsf{a}} : \upsilon \in \mathbf{N}_<(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}}))\}$ *is the Macaulay basis of* Λ_{a}.

A Macaualy representation *of* $\mathsf{I} = \bigcup_{\mathsf{a} \in \mathsf{Z}} \mathfrak{q}_{\mathsf{a}}$ *is the data*

- $\mathsf{Z} := \{\mathsf{a} \in k^n : f(\mathsf{a}) = 0, \forall f \in \mathsf{I}\}$,
- *for each* $\mathsf{a} \in \mathsf{Z}$ *the Macaulay basis* $\{\ell_{\upsilon\mathsf{a}} : \upsilon \in \mathbf{N}_<(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}}))\}$ *of* Λ_{a}

so that the lineraly independent set

$$\mathbb{L} := \{\ell_{\upsilon\mathsf{a}}\lambda_{\mathsf{a}} : \upsilon \in \mathbf{N}_<(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}})), \mathsf{a} \in \mathsf{Z}\} \subset \mathcal{P}^*$$

satisfies $\mathrm{Span}_k(\mathbb{L}) = \mathfrak{L}(\mathbb{L})$. □

9 Cerlienco–Mureddu Correspondence

Cerlienco and Mureddu [15, 16, 17] solve the following

Problem 14 *Given a finite set of points,*

$$\{\mathsf{a}_1, \dots, \mathsf{a}_s\} \subset k^n, \quad \mathsf{a}_i := (a_{i1}, \dots, a_{in}),$$

to compute $\mathbf{N}_<(\mathsf{I})$ *w.r.t. the lexicographical ordering* $<$ *induced by* $X_1 < \cdots < X_n$ *where* $\mathsf{I} := \{f \in \mathcal{P} : f(\mathsf{a}_i) = 0, 1 \le i \le s\}$. □

by means of an efficient combinatorial algorithm which to each *ordered* finite set of points

$$\mathsf{X} := \{\mathsf{a}_1, \dots, \mathsf{a}_s\} \subset k^n, \quad \mathsf{a}_i := (a_{i1}, \dots, a_{in}),$$

associates

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

satisfying

Theorem 15 *[15]* $\mathbf{N}(\mathsf{I}) = \mathbf{N}(\mathsf{X})$ *holds for each finite set of points* $\mathsf{X} \subset k^n$*.* $\square$

Since they do so by induction on $s = \#(\mathsf{X})$ let us consider the subset $\mathsf{X}' := \{\mathsf{a}_1, \dots, \mathsf{a}_{s-1}\}$, and the corresponding order ideal $\mathbf{N}' := \mathbf{N}(\mathsf{X}')$ and bijection $\Phi' := \Phi(\mathsf{X}')$.

If $s = 1$ the only possible solution is $\mathbf{N} = \{1\}, \Phi(\mathsf{a}_1) = 1$.

Denoting

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

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

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

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

Cerlinco–Mureddu Algorithm sets

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

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

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

$\mathsf{Z} := \pi_m(\mathsf{W});$

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

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

$\mathbf{N} := \mathbf{N}' \cup \{t_s\},$

$$\Phi(\mathsf{a}_i) := \begin{cases} \Phi'(\mathsf{a}_i) & i < s \\ t_s & i = s \end{cases}$$

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

Example 16 *For the following sequence of points we iteratively obtain*

$\mathsf{a}_1 := (0, 0, 1),$

$\Phi(\mathsf{a}_1) := t_1 := 1;$

$\mathsf{a}_2 := (0, 1, -2),$

$m = 1, d = 1, \mathsf{W} = \{(0, 1)\}, \tau = 1, \Phi(\mathsf{a}_2) := t_2 := X_2,$

$\mathsf{a}_3 := (2, 0, 2),$

$m = 0, d = 1, \mathsf{W} = \{(2, 0)\}, \tau = 1, \Phi(\mathsf{a}_3) := t_3 := X_1,$

$\mathsf{a}_4 := (0, 2, -2),$

$m = 1, d = 2, \mathsf{W} = \{(0, 2)\}, \tau = 1, \quad \Phi(\mathsf{a}_4) := t_4 := X_2^2,$

$\mathsf{a}_5 := (1, 0, 3),$

$m = 0, d = 2, \mathsf{W} = \{(1, 0)\}, \tau = 1, \Phi(\mathsf{a}_5) := t_5 := X_1^2,$

$\mathsf{a}_6 := (1, 1, 3),$

$m = 1, d = 1, \mathsf{W} = \{(0, 1), (1, 1)\}, \tau = X_1, \Phi(\mathsf{a}_6) := t_6 := X_1X_2.$

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

$\mathsf{a}_7 := (1, 1, 1),$

$m = 2, d = 1, \mathsf{W} = \{(1, 1, 1)\}, \tau = 1, \Phi(\mathsf{a}_7) := t_7 := X_3.$

$\mathsf{a}_8 := (2, 0, 1),$

$m = 2, d = 1, \mathsf{W} = \{(1, 1, 1), (2, 0, 1)\}, \tau = X_1, \Phi(\mathsf{a}_8) := t_8 := X_1X_3,$

$\mathsf{a}_9 := (2, 0, 0),$

$m = 2, d = 2, \mathsf{W} = \{(2, 0, 0))\}, \tau = 1, \Phi(\mathsf{a}_9) := t_9 := X_3^2,$

□

Remark 17 *[15]* Once, the set $\mathbf{N}(\mathsf{I}(\mathsf{X})) := \{t_1, \ldots, t_s\}$ is obtained via Cerlienco–Mureddu Algorithm and Theorem 15, one deduces

$$\mathbf{G}_<(\mathsf{I}(\mathsf{X})) := \{\tau_1, \ldots, \tau_r\}, \tau_1 < \tau_2 < \ldots < \tau_r, \tau_i := X_1^{d_1^{(i)}} \cdots X_n^{d_n^{(i)}}$$

and can obtain the lex Gröbner basis of $\mathsf{I}(\mathsf{X})$ by interpolation: for each $\tau_j \in \mathbf{G}(\mathsf{I}(\mathsf{X}))$ we have just to find the unknowns $a_{ij} \in \mathbb{F}$ which satisfy the linear equalities $v(\mathsf{X}, \tau_j) = \sum_{i=1}^{s} a_{ij} v(\mathsf{X}, t_i)$. □

[26] and [23] give a combinatorial reformulation of Cerlienco–Mureddu Algorithm which

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

– cominatorially recombines the tree,

– reeds on this tree the monomial structure.

Their formulation returns $\mathbf{N}$ but not Φ; more important,apparently it is *not* iterative.

A recent [36] Cerlienco—Mureddu-like proposal, very similar to those of [26] and [23], while still not iterative, suggests a clever interpolation formula which successfully makes effective the weak proposal of Remark 17.

[44] extends Cerlienco–Mureddu Algorithm to multiple points described via Macaulay representation.

10 Macaulay's Algorithm

Let

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

$\mathsf{I} \subset \mathcal{P}$ an m-closed ideal,

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

$\{\ell(\tau) : \tau \in \mathbf{N}_<(\mathsf{I})\}$, the (not-necessarily finite) Macaulay basis of I,

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

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

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

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

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

Let $J \subset \{1, \ldots, s\}$ 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 18 (Macaulay) *[38, 39] With the notation above, for each j, denoting*

$$\Lambda'_j := \mathrm{Span}_k\{\upsilon \cdot \ell(\omega_j) : \upsilon \in \mathcal{T} \cap \mathsf{m}\}$$

we have

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

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

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

Corollary 19 (Macaulay) *[38, 39] Let* I *be a zero-dimensional ideal,* $\deg(\mathsf{I}) = s$*. Then the Macaulay representation* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\}$ *of* I *can be properly ordered so that*

$L := \mathrm{Span}_k(\mathbb{L}) = \mathfrak{L}(\mathsf{I}),$

each subvectorspace $L_\sigma := \mathrm{Span}_k\{\ell_1, \ldots, \ell_\sigma\}$ *is a* $\mathcal{P}$*-module so that*

each $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$ *is a zero-dimensional ideal and*

there is a chain $\mathsf{I}_1 \supset \mathsf{I}_2 \supset \cdots \supset \mathsf{I}_s = \mathsf{I}.$ □

Macaulay's construction allowsw, as it was remarked by Gröbner[32, 50], to compute an irreducible decomposition of primaries ideals[7]:

Theorem 20 (Gröbner) *If* I *is* m*-primary, then:*

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

11 Reduced Irreducible Decomposition

It is well known [Lasker-Noether Decomposition Theorem] that

- each ideal $\mathsf{I} \subset \mathcal{P}$ is the finite intersection of irreducible ideals;
- irreducible ideals are primaries, but the converse, in general, is false;
- if, into such a representation, each primaries associated to a same prime are substituted by their intersection, then $\mathsf{I} \subset \mathcal{P}$ has a representation as intersection of finite primary[8] ideals;
- the primes associated to such primaries are unique as well as the isolated primaries.

It is instead less known that this formulation given by Noether [49] is an adapatation of a preliminary formulation with respect to which irreducibility and *reduceness* are sacrified in order to obtain uniqueness.

In fact Noether introduced the following

[7] For the definitions see the section below

[8] but not necessarily irreducible

Definition 21 (Noether) *[49]*

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

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* $\mathfrak{a} = \left(\bigcap_{\substack{i=1\\ j\neq i}}^{r} \mathfrak{q}_i\right) \cap {\mathfrak{q}_j}'$. □

and proved that

Theorem 22 (Noether) *[49] In a noetherian ring* R*, each ideal* $\mathfrak{a} \subset R$ *has a reduced representation* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$ *as intersection of finitely many irreducible ideals.*

In an irredundant primary decomposition of an ideal of a noetherian ring, each primary component can be chosen to be reduced. □

Example 23 *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. □

Example 24 *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 in this decomposition* $a = 0$*, we find again the previous decomposition* $(X^2, XY) = (X) \cap (X^2, Y)$*.* □

For an m-primary ideal, Theorem 20 give an algorithm to compute its reduced representation.

If I is not m-primary, its reduced representation can be obtained in the following way: let

$\nabla_\rho := \{M(\omega) : \omega \in \mathcal{T}, \deg(\omega) < \rho\}$,

$\mathbf{C}_<(\mathsf{I}) := \{\omega_1, \dots, \omega_t\}$,

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

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

$\Lambda \cap \nabla_\rho = \mathfrak{M}(\mathsf{q}')$;

$\mathsf{I} = \cap_{i=1}^r \mathsf{q}_i$ be an irredundant primary representation of I where $\sqrt{\mathsf{q}_1} = \mathsf{m}$,

$\mathsf{J} := \cap_{i=2}^r \mathsf{q}_i$,

$\mathsf{J} = \cap_{i=1}^u \mathfrak{i}_i$, a reduced representation of J;

$\mathbf{C}_<(\mathsf{q}') := \{\omega_1, \dots, \omega_t, \omega_{t+1}, \dots, \omega_s\} \supset \mathbf{C}_<(\mathsf{I})$,

for each $j, 1 \leq j \leq s$, $\Lambda_j := \mathrm{Span}_k\{\upsilon\ell(\omega_j) : \upsilon \in \mathcal{T}\}$ and

$\mathsf{q}_j := \mathfrak{I}(\Lambda_j)$;

$\mathsf{q} := \cap_{j=1}^t \mathsf{q}_j$.

Then

Corollary 25 *With the notation above, it holds:*

1. $\mathsf{J} := \mathsf{I} : \mathsf{m}^\infty = \cap_{i=2}^r \mathsf{q}_i$,
2. $\mathsf{q} \subset \mathsf{q}'$ *is a reduced* m*-primary component of* I*,*
3. $\mathsf{q}' := \cap_{j=1}^s \mathsf{q}_j$ *is a reduced representation of* q'*,*
4. $\mathsf{q} := \cap_{j=1}^t \mathsf{q}_j$ *is a reduced representation of* q*,*
5. $\mathsf{q}_i \supset \mathsf{J} \iff i > t$*,*
6. $\mathsf{I} = \cap_{i=1}^u \mathfrak{i}_i \bigcap \cap_{j=1}^t \mathsf{q}_j$ *is a reduced representation of* I*.* $\square$

Example 26 *For* $\mathsf{I} := (X^2, XY)$ *we have*

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

$\mathbf{C}_<(\mathsf{I}) = \{X\}$;

$\mathsf{I} : \mathsf{m}^\infty = (X)$

$\rho = 3$, $\mathsf{q}' = \mathsf{I} + \mathsf{m}^3 = (X^2, XY, Y^3)$, $\mathbf{C}_<(\mathsf{q}') = \{X, Y^2\}$;

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

$\omega_2 := Y^2, \Lambda_2 = \{M(1), M(Y), M(Y^2)\}, \mathfrak{q}_2 = (X, Y^3) \supset (X)$;

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

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 $a \in \mathbb{Q}, a \neq 0$,

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

we obtain

$\rho = 3,\ \Lambda \cap \nabla_\rho = \{M(1), M(X) - aM(Y), M(Y), M(Y^2)\}$,

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

$\omega_2 := Y^2, \Lambda_2 = \{M(1), M(Y), M(Y^2)\}, \mathfrak{q}_2 = (X, Y^3) \supset (X)$;

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

Example 27 *Let us now discuss deeply the same example by performing the generic change of coordinate*

$$\Phi : \mathbb{Q}[X, Y] \mapsto \mathbb{Q}[X, Y] : \Phi(X) = aX + bY, \Phi(Y) = cX + dY, ad - bc \neq 0 \neq a :$$

for $\mathsf{I} := (X^2, XY)$, *we obtain*

$\Phi(\mathsf{I}) = \big(aXY + bY^2, a^2X^2 - bY^2\big)$,

$\Lambda := \mathrm{Span}_k\{M(1), M(X), M(Y), a^2M(Y^2) - abM(XY) + b^2M(X^2), \cdots\}$

$\mathsf{J} = \mathsf{I} : \mathsf{m}^\infty = (aX + bY)$,

$\rho = 3,\ \mathbf{C}_<(\mathfrak{q}') = \{X, Y^2\}$;

$\Lambda \cap \nabla_\rho = \mathrm{Span}_k\{M(1), M(X), M(Y), a^2M(Y^2) - abM(XY) + b^2M(X^2)\}$;

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

$\omega_2 := Y^2, \Lambda_2 = \{M(1), aM(Y) - bM(X), a^2M(Y^2) - abM(XY) + b^2M(X^2)\}$,

$\quad \mathfrak{q}_2 = (aX + bY, Y^3) \supset (aX + bY)$;

whence $\Phi(\mathsf{I}) = (aX + bY) \cap (X^2, Y)$.

We have chosen $\{M(1), M(X), M(Y)\}$ *as basis of* ∇_2*; however, what we have to do is to extend the basis* $\{M(1), aM(Y) - bM(X)\}$ *of* $\mathfrak{M}(\mathsf{J}) \cap \nabla_2$*, in order to obtain a basis of* ∇_2*.*

Any choice $eM(Y) + fM(X), af + be \neq 0$ *is acceptable giving the reduced primary*

$$\mathfrak{I}(\{M(1), eM(Y) + fM(X)\}) = (X^2, eX - fY)$$

and the decomposition $\Phi(\mathsf{I}) = (aX + bY) \cap (X^2, eX - fY)$. □

12 Lazard Structural Theorem

Lazard Structural Theorem [33] is one of earlier important results within Gröbner Theory; it describes the structure of the lex Gröbner basis of a generic ideal in 2 variables; Gianni–Kalkbrenner's Theorem can be seen as its ultimate generalization.

Theorem 28 (Lazard) *Let $\mathcal{P} := k[X_1, X_2]$ and let $<$ be the lex. ordering induced by $X_1 < X_2$.*

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

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

Then

- $f_0 = PG_1 \cdots G_{k+1}$,
- $f_j = PH_jG_{j+1} \cdots G_{k+1}, 1 \leq j \leq k$,

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;

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

$H_{i+1} \in (G_1 \cdots G_i, \ldots, H_jG_{j+1} \cdots G_i, \ldots, H_{i-1}G_i, H_i), \forall i$. □

To remark that $k[X_1]$ is a principal ideal domain is all one needs in order to extend Lazard's proof of his Structural Theorem obtaining a description of strong Gröbner bases of ideals in $R[X]$, R a principal ideal domain:

Theorem 29 *Let R a principal ideal domain and $\mathcal{P} := R[X]$.*

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

$$\deg(f_0) \leq \deg(f_1) < \cdots \leq \deg(f_k).$$

Then

- $f_0 = PG_1 \cdots G_{k+1}$,
- $f_j = PH_jG_{j+1} \cdots G_{k+1}, 1 \leq j \leq k$,

where

P is the primitive part of $f_0 \in R[X]$;

$G_i \in R, 1 \leq i \leq k+1$;

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

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

$H_{i+1} \in (G_1 \cdots G_i, H_1 G_2 \cdots G_i, \ldots, H_j G_{j+1} \cdots G_i, \ldots, H_{i-1} G_i, H_i)$ for all i.

$\square$

More interesting is the generalization by Gianni–Kalkbrener which describes the structure of the lexicographical Gröbner basis of each 0-dimensional ideal

$$\mathsf{I} \subset \mathcal{P} = k[X_1, \ldots, X_n].$$

In order to describe the structure of the Gröbner basis of such an ideal, we needs to consider $\mathcal{P}$ also as a univariate polynomial in the variable X_n with coefficients in the polynomial ring $k[X_1, \ldots, X_{n-1}]$. In this way for each element $f \in \mathcal{P}$ we have:

$$f = \sum_{k=0}^{h} b_k(X_1, \ldots, X_{n-1}) X_n^k = Tp(f) + \cdots + Lp(f) X_n^h,$$

where we will denote by $Lp(f) = b_h(X_1, \ldots, X_{n-1})$ the *leading polynomial* and by $Tp(f) = b_0(X_1, \ldots, X_{n-1})$ the *trailing polynomial* of f.

Definition 30 *Let $\mathsf{I} \subset \mathcal{P}$ be an ideal and d an integer such that $d \leq n$. The d–th elimination ideal I_d is the ideal of $k[X_1, \ldots, X_d]$ defined by $\mathsf{I}_d = I \cap k[X_1, \ldots, X_d]$.*

We will consider a zero dimensional ideal $\mathsf{I} \subset \mathcal{P}$ and we name $\mathcal{Z}(\mathsf{I}_d) \subset \overline{k}^d$ the set of the roots of I_d.

Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $\mathsf{I} \subset \mathcal{P}$, w.r.t. the lexicographical ordering$<$ induced by $X_1 < \ldots, X - n$ and let us order it so that $T(g_1) < \cdots < T(g_s)$.

For each $\iota \leq n$, let G_ι be $G \cap k[X_1, \ldots, X_\iota]$, and

$$\forall \ell \in \mathbb{N},\ G_{\iota\ell} := \{g \in G_\iota \setminus G_{\iota-1} \mid \deg_{X_\iota}(g) = \ell\}$$

so that each G_ι can be decomposed into blocks of polynomials according to their degree with respect to the variable X_ι: $G_\iota = \sqcup_\ell G_{\iota\ell}$. In this way if $g \in G_{\iota\ell}$, we have

- $g \in k[X_1, \ldots, X_{\iota-1}][X_\iota] \setminus k[X_1, \ldots, X_{\iota-1}]$;
- $deg_{X_\iota}(g) = \ell$, i.e. $g = Lp(g) X_\iota^\ell + \ldots + Tp(g)$.

Theorem 31 ([28, 30]) *Let $\alpha := (a_1, \ldots, a_d) \in \mathcal{Z}(\mathsf{I}_d)$ and*

$$\Phi_\alpha : \mathcal{P} \to K[X_{d+1}, \ldots, X_n] \quad f(X) \to f(\alpha, X_{d+1}, \ldots, X_n).$$

Let σ be the minimal value such that $\Phi_\alpha(Lp(g_\sigma)) \neq 0$ and j, δ the values such that $g_\sigma \in G_{j\delta}$. Then

1. $j = d+1$;
2. for each $g \in G_{\iota\ell}$:
   - if $\iota \le d$ then $\Phi_\alpha(g) = 0$;
   - if $\iota = d+1 = j, \ell < \delta$ then $\Phi_\alpha(g) = 0$;
3. $\Phi_\alpha(g_\sigma) = \gcd\left(\Phi_\alpha(g) : g \in G_{d+1}\right) \in \overline{k}[X_{d+1}]$;
4. for each $a \in \overline{k}$;

$$(a_1, \dots, a_d, a) \in \mathcal{Z}(\mathsf{I}_{d+1}) \iff \Phi_\alpha(g_\sigma)(a) = 0.$$

13 Axis-of-Evil Theorem

The Axis-of-Evil Theorem [42, 43, 44] describes the combinatorial structure [Gröbner and border basis, linear and Gröbner representation] wrt the lex ordering of a 0-dimensional ideal $\mathsf{I} \subset \mathcal{P}$, in terms of its Macaulay representation.

Such description is "algorithmical" in terms of elementary combinatorial tools and linear interpolation and extends Cerlienco–Mureddu Correspondence and Lazard's Structural Theorem; the proof is essentially a direct application of Möller's Algorithm [45, 22].

It is summarized into 22[9] statements.

We report here one of its extreme statements:

Theorem 32 *Let*

$<$ *the lex ordering induced by* $X_1 < \cdots , X_n$,

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

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

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

$\mathbf{G}_<(\mathsf{I}) := \{\mathsf{t}_1, \dots, \mathsf{t}_r\}, \mathsf{t}_1 < \mathsf{t}_2 < \ldots < \mathsf{t}_r$, $\mathsf{t}_i := X_1^{d_1^{(i)}} \cdots X_n^{d_n^{(i)}}$ *the minimal basis of its associated monomial ideal* $\mathbf{T}_<(\mathsf{I})$;

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

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

$$\mathsf{Z}_{m\delta i} \subset k^m, \forall m, \delta, i : 1 \le i \le r, 1 \le m \le n, 1 \le \delta \le d_m^{(i)},$$

thus allowing to compute

[9] in honour of Trythemius, the founder of cryptography (*Steganographia* [1500], *Polygraphia* [1508]) which introdiced in german the 22^{th} letter **W** in order to perform german gematria.

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

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

- *and, by interpolation*[10] *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

ν *the maximal value such that* $d_\nu^{(i)} \neq 0, d_m^{(i)} = 0, m > \nu$ *so that*

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

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

Example 33 *For the nine points considered in Example 16 the corresponding Gröbner basis is* $G = \{g_1, g_2, g_3, g_4, f_1, f_2, f_3, f_4\}$ *where*

$$\begin{array}{lclcl} g_1 & := & X_1^3 - 3X_1^2 + 2X_1 & = & (X_1-2)(X_1-1)X_1 \\ g_2 & := & X_1^2X_2 - X_1X_2 & = & X_2(X_1-1)X_1, \\ g_3 & := & X_1X_2^2 - X_1X_2 & = & X_2(X_2-1)X_1, \\ g_4 & := & X_2^3 - 3X_2^2 + 2X_2 & = & X_2(X_2-1)(X_2-2), \end{array}$$

perfectly illustrating Lazard Structural Theorem, and

$$\begin{array}{lcl} f_1 & := & X_3X_1^2 - 3X_3X_1 + 2X_3 - 3X_2^2 - 6X_2X_1 + 9X_2 - X_1^2 + 3X_1 - 2, \\ f_2 & := & X_3X_2 + X_3X_1 - 2X_3 + 3X_2^2 + X_2X_1 - 7X_2 - 2X_1^2 + 3X_1 + 2, \\ f_3 & := & X_3^2X_1 - 2X_3^2 - 4X_3X_1 + 8X_3 - 15X_2^2 - 30X_2X_1 + 45X_2 + 3X_1 - 6, \\ f_4 & := & X_3^3 - 3X_3^2 + 3X_3X_1 - 4X_3 - 3X_2^2 - 6X_2X_1 + 9X_2 - 3X_1 + 6, \end{array}$$

satisfy $\pmod{(g_1, \ldots, g_4)}$

$$\begin{array}{lcl} f_1 & = & (X_1-2)(X_1-1)(X_3 - \frac{3}{2}X_2^2 + \frac{9}{2}X_2 - 1) \\ f_2 & = & (X_2 + X_1 - 2)(X_3 + 3X_2 - 2X_1 - 1) \\ f_3 & = & (X_1-2)(X_3-1)(X_3 - 5X_1 + 2) \\ f_4 & = & (X_3-1)X_3(X_3 + 3X_1^2 - 8X_1 + 2) \end{array}$$

where

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

- $(X_1^2 - 3X_1 + 2, X_2 + X_1 - 2, X_3 - 1)$ *is the Gröbner basis of the ideal whose roots are* $\{\pi_2(\mathsf{a}_7), \pi_2(\mathsf{a}_8)\}$,
- $\{\mathsf{a} \in \mathsf{X} : (X_1^2 - 3X_1 + 2)(\mathsf{a}) \neq 0\} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_4\}$ *to which Cerlienco–Mureddu Correspondence associates* $\{1, X_2, X_2^2\}$
- $\{\mathsf{a} \in \mathsf{X} : (X_2 + X_1 - 2)(\mathsf{a}) \neq 0\} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_5\}$ *to which Cerlienco–Mureddu Correspondence associates* $\{1, X_1, X_2\}$
- $\{\mathsf{a} \in \mathsf{X} : (X_1 - 2)(X_3 - 1)(\mathsf{a}) \neq 0\} = \{\mathsf{a}_2, \mathsf{a}_4, \mathsf{a}_5, \mathsf{a}_6\}$ *to which Cerlienco–Mureddu Correspondence associates* $\{1, X_1, X_2, X_1X_2\}$.
- $\{\mathsf{a} \in \mathsf{X} : (X_3^2 - X_3))(\mathsf{a}) \neq 0\} = \{\mathsf{a}_2, \mathsf{a}_3, \mathsf{a}_4, \mathsf{a}_5, \mathsf{a}_6\}$ *to which Cerlienco–Mureddu Correspondence associates* $\{1, X_1, X_1^2, X_2, X_1X_2\}$.

$\square$

References

[1] Abbott J., Bigatti A., Kreuzer M., Robbiano L., Computing Ideals of Points, *J. Symb.Comp.* **30** (2000), 341–356.

[2] Alonso M.E., Marinari M.G., The big Mother of all Dualities: Möller Algorithm, *Comm. Alg.* **31** (2003), 374–383.

[3] Alonso M.E., Marinari M.G., The big Mother of all Dualities 2: Macaulay's Duality, *J. AAECC* (2006).

[4] Aubry P., Lazard D., Moreno Maza M., On the theories of triangular sets, *J. Symb. Comp.* **28** (1999), 105–124.

[5] Aubry P., Moreno Maza M., Triangular Set for Solving Polynomial Systems: A Comparative Implementation of Four Methods, *J. Symb. Comp.* **28** (1999), 125–154.

[6] Auzinger W., Stetter H.J., An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Internat. Schriftenreihe Numer. Math.* **86** (1988), 11–30, Birkhäuser.

[7] Basiri A., Faugère J.-C., Changing the ordering of Gröbner Bases with LLL: Case of Two Variables, *Proc. ISSAC'03* (2003), 23-28, ACM.

[8] Bayer D., Stillman M., A Theorem on Refining Division Orders by the Reverse Lexicographic Order, *Duke J. Math.* **55** (1987), 321–328.

[9] Berlekamp, E.R. *Algebraic Coding Theory*, McGraw-Hill (1968).

[10] Borges-Trenard M.A., Borges-Quintana M., Computing Gröbner Bases by FGLM Techniques in a Noncommutative Settings, *J. Symb.Comp.* **30** (2000), 429–449.

[11] Borges-Quintana M., Borges-Trenard M. A., Martinez-Moro E., A general framework for applying FGLM techniques to linear codes. Accepted at *AAECC 16*.
http://arxiv.org/abs/math.AC/0509186

[12] Borges-Quintana M., Borges-Trenard M.A., Fitzpatrick P., Martinez-Moro E., Groebner bases and combinatorics for binary codes.
http://arxiv.org/abs/math.CO/0509164

[13] Borges-Quintana M., Borges-Trenard M.A., Martinez-Moro E., On a Gröbner bases structure associated to linear codes. Accepted at *Journal of Discrete Mathematical Sciences & Cryptography.*
http://arxiv.org/abs/math.AC/0506045

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

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

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

[17] Cerlienco L., Mureddu M., Multivariate Interpolation and Standard Bases for Macaulay Modules, *J. Algebra* **251** (2002), 686–726.

[18] Cioffi F., Minimally generating ideals of fat points in polynomial time using linear algebra, *Ricerche di Matematica* **XLVII**, (1999), 55–63.

[19] Cioffi F., Orecchia F., Computation of minimal generators of ideals of fat points, *Proc. ISSAC'01* (2001), 72–76, ACM.

[20] Collard S., Mall D., Kalkbrener M., The Gröbner Walk, *Preprint* (1993).

[21] Farr J., Gao S., Computing Gröbner bases for Vanishing Ideals of Finite Sets of Points, *Technical Report* (2005).

http://www.math.clemson.edu/faculty/Gao/papers/newgb.pdf

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

[23] Felszerghy B., Ráth B., Rónyai L., The lex game and some applications, *J. Symb. Comp.* **41** (2006), 663–681.

[24] Fitzpatrick P., Jennings S.M., Comparison of Two Algorithms for Decoding Alternant Codes, *J. AAECC* **9** (1998), 211-220.

[25] Galligo A., A propos du théorem de préparation de Weierstrass, *L. N. Math.* **409** (1974), 543–579, Springer.

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

http://www.math.clemson.edu/faculty/Gao/papers/GBstr.pdf

[27] Gianni P., Algebraic solution of systems of polynomial equations using Gröbner bases, *L. N. Comp. Sci.* **356** (1987), 247-257, Springer.

[28] Gianni P., Properties of Gröbner Bases under Specialization, *L. N. Comp. Sci.* **378** (1987), 293–297, Springer.

[29] Gianni P., Trager B., Incremental Decoding, *International Symposium in Honor of Bruno Buchberger's 60th Birthday. Logic, Mathematics and Computer Science: Interactions (LMCS 2002)* RISC - Linz (Austria), **02-60** (2002), 138-146.

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

[31] Guerrini E., O'Keefee H., Rimoldi A. Application of FGLM-like algorithms to coding theory. In *Gröbner Bases, Coding, and Cryptography*, RISC book series, Springer, Heidelberg, (to appear).

[32] Gröbner W., *Moderne Algebraische Geometrie*, Springer (1949).

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

[34] Lazard D., A new method for solving algebraic systems of positive dimension, *Disc. Appl. Math.* **33** (1991), 147–160.

[35] Lazard D., Solving zero-dimensional algebraic systems, *J. Symb. Comp.* **15** (1992), 117–132.

[36] Lederer D., The vanishing ideal of a finite set of closed points in affine space, *J. Pure and Applied Algebra* **212** (2008), 1116–1133.

[37] Licciardi S., Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion, *Proc. ISSAC'94* (1994) 191-196, ACM.

[38] 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.

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

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

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

[42] 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.

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

[44] Marinari M.G., Mora T.,Cerlienco–Mureddu Correpondence and Lazard Structural Theorem. *Investigaciones Mathematicas* **27** (2006), 155–178.

[45] Möller H.M., Buchberger B., The construction of multivariate polynomials with preassigned zeros, *L. N. Comp. Sci.* **144** (1982), 24–31, Springer.

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

[47] Möller H.M., Stetter, H.J., Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems, *Numer. Math.* **70** (1995), 311–329.

[48] Mourrain B., Bezoutian and quotient ring structure, *J. Symb. Comp.* **39** (2005), 397-415.

[49] Noether E., Idealtheorie in Ringbereichen, *Math. Annalen* **83** (1921), 25–66.

[50] Renschuch. B, *Elementare und praktische Idealtheorie*, Deutscher Verlag der Wissenschaften (1976).

[51] Orsini E., Decoding cyclic codes: the Cooper philosophy. In *Gröbner Bases, Coding, and Cryptography*, RISC book series, Springer, Heidelberg, (to appear).

[52] Reinhert B., Madlener K., A Note on Nielsen Reduction and Coset Enumeration, *Proc. ISSAC'98* , (1998), 171-178, ACM.

[53] Sala M., Personal communication (2005).

[54] Todd J., Coxeter H., A practical method for enumerating cosets of a finite abstract group, *Proc. Edinburgh Math. Soc.* **5** (1936), 26–34.

[55] Traverso C., Hilbert function and the Buchberger algorithm, *J. Symb. Comp.* **22** (1996), 355–376.