DOI: 10.1478/AAPP.982A3

AAPP | Atti della Accademia Peloritana dei Pericolanti
Classe di Scienze Fisiche, Matematiche e Naturali
ISSN 1825-1242

Vol. 98, No. 2, A3 (2020)

ORACLE-SUPPORTED DRAWING OF THE GRÖBNER *ESCALIER*

MARIA EMILIA ALONSO [a], MARIA GRAZIA MARINARI [b], AND TEO MORA [b*]

(communicated by Paolo Valabrega)

ABSTRACT. The aim of this note is to discuss the following quite queer problem: to compute the reduced Gröbner basis of an ideal $\mathfrak{I}$ w.r.t. a term-ordering $\prec$ without knowing neither the ideal nor the term-ordering but only a degree bound of the required Gröbner basis, being allowed to pose a finite number of queries to an oracle which, given a term $\tau \in \mathscr{T}$, returns its *canonical form* $\mathrm{Can}(\tau, \mathfrak{I}, \prec)$ w.r.t. the unknown ideal $\mathfrak{I}$ and term-ordering $\prec$. This problem was suggested to us by the desire to definitely dispose of a very weak paper wrongly claiming a cryptographic application of (non commutative) Gröbner bases. The commutative reformulation is instead a non-obvious challenge and we consider it an helpful tool for understanding and visually describe the structure of the Gröbner escalier of an ideal; moreover it allows to describe (and compute) the corner set, an helpful tool for computing Macaulay decomposition of a (non-necessarily 0-dimensional) algebra.

Introduction

The aim of this note is to discuss the following quite queer

Problem 1. Given

- the free non-commutative polynomial ring, $\mathscr{P} := \mathbb{F}\langle X_1, \ldots, X_n \rangle$,
- the related word monoid $\mathscr{T} := \langle X_1, \ldots, X_n \rangle$, and
- a finite set $G := \{g_1, \ldots, g_l\} \subset \mathscr{P}$ of polynomials which are known to be members of an ideal $\mathfrak{I}$,

compute, w.r.t. a Noetherian semigroup ordering $\prec$ on $\mathscr{T}$,

> a finite subset $H \subset \Gamma(\mathfrak{I})$ of the reduced Gröbner basis $\Gamma(\mathfrak{I})$ of $\mathfrak{I}$ s.t., for each $g_i \in G$ its *normal form* $NF(g_i, H)$ w.r.t. H is zero,

without knowing neither the ideal $\mathfrak{I}$ nor the term-ordering $\prec$, but posing only a finite number of queries to an oracle, which

> given a term $\tau \in \mathscr{T}$ returns its *canonical form* $\mathrm{Can}(\tau, \mathfrak{I}, \prec)$ w.r.t. such ideal $\mathfrak{I}$ and term-ordering $\prec$. □

This queer problem has been suggested to us by Bulygin (2005), in a paper where a similar problem, but with stronger assumptions, is faced in order to set up a chosen-cyphertext attack against the cryptographic system proposed by Ackermann and Kreuzer (2006)[1].

The formulation of Problem 1 is partially due to the underlying application but is also due to the structure of the Gröbner bases in the non-commutative setting, which in general are infinite; however, even if we restrict to the Noetherian setting of the (commutative) polynomial ring $\mathscr{P} := \mathbb{F}[X_1, \ldots, X_n]$, we are unable (as we will show in Section **3.2** through easy counterexamples) to produce an algorithm which allows to return the (though finite) Gröbner basis of I, unless we have some further information allowing to bound such basis; the best we can do is to solve the following reformulation:

Problem 2. Within the commutative polynomial ring, $\mathscr{P} := \mathbb{F}[X_1, \ldots, X_n]$, and denoting by

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

the related monoid of terms, compute, w.r.t. a Noetherian semigroup ordering[2] $\prec$ on $\mathscr{T}$ and an ideal $\mathsf{I} \subset \mathscr{P}$, the reduced Gröbner basis $\Gamma(\mathsf{I})$ of I w.r.t. $\prec$, without knowing neither I nor $\prec$, but a degree bound of the elements of the reduced Gröbner basis $\Gamma(\mathsf{I})$ of I w.r.t. $\prec$, *i.e.* a value $D \in \mathbb{N}$ satisfying

$$D \geq d(\mathsf{I}) := \max\{\deg(\gamma_i) : \gamma_i \in \Gamma(\mathsf{I})\},$$

and posing a finite number of queries to an oracle, which

> given a term $\tau \in \mathscr{T}$ returns its *canonical form* $\mathrm{Can}(\tau, \mathsf{I}, \prec)$ w.r.t. the ideal I and the semigroup ordering $\prec$. □

Note that, except this requirement on the knowledge of a degree bound of the required reduced Gröbner bases, we set ourselves in the most general and classical setting: the ideal (notwithstanding our quotation of Macaulay) does not require to be homogeneous and the procedure works for each term-ordering. While originally inspired by the cryptographic challenge, we pursued this research because we consider that this query formulation can help to give a better grasp on the combinatorial structure of the *Gröbner sous-escalier* $\mathbf{N}(\mathsf{I}) := \mathscr{T} \setminus \mathbf{T}(\mathsf{I})$ (see the illuminating papers by Ceria (2019a,b)). Moreover, it provides an efficient algorithm to compute the *corner set* also for non-necessarily 0-dimensional ideals, which is a crucial tool for Macaulay's algorithm for computing primary decomposition (Macaulay 1913, 1916; Groebner 1970; Alonso *et al.* 2003; Ceria 2019a).

After recalling the basic notions and set up the notation (Section **1**) we solve first Problem 1 (Section **2**) and next Problem 2 (Section **3**) for which we propose a different, more combinatiorial, solution.

1. Notation and recalls on Gröbner Bases

We consider (Mora 2016, p. 5) a (non-necessarily commutative) monoid $\mathscr{T}$ generated by the set of variables $\{X_1, \ldots, X_n\}$, a field $\mathbb{F}$ and the monoid ring $\mathscr{P} := \mathrm{Span}_{\mathbb{F}}(\mathscr{T})$. For any set $F \subset \mathscr{P}$ we denote by $\mathsf{I} := \mathbb{I}(F) \subset \mathscr{P}$ the (bilateral) ideal generated by F.

[1]The interested reader is referred to the surveys by Levy-dit-Vehel *et al.* (2009) and Barkee *et al.* (2020).

[2]Since a semigroup in general has not necessarily a unity, with this formulation we want to be free of the irrelevant requirement that $\tau \mid \omega \implies \tau \prec \omega$.

Each $f \in \mathscr{P}$ can be uniquely (Mora 2016, p. 7) expressed as

$$f = \sum_{\tau \in \mathscr{T}} c(f,\tau)\tau \in \mathscr{P}.$$

We call *support* of f the set $\mathrm{supp}(f) := \{\tau \in \mathscr{T} : c(f,\tau) \neq 0\}$. Moreover, fixing a Noetherian semigroup ordering $\prec$ on $\mathscr{T}$, the *leading term*, *leading coefficient* and *leading monomial* of f are ordinately:

$$\mathbf{T}(f) := \max_{\prec}\{\tau \in \mathrm{supp}(f)\},\ \mathrm{lc}(f) := c(f,\mathbf{T}(f)) \text{ and } \mathbf{M}(f) := \mathrm{lc}(f)\mathbf{T}(f).$$

For each ideal $\mathsf{I} \subset \mathscr{P}$, we also consider

- the *semigroup ideal* (Mora 2016, Def. 46.1.4) $\mathbf{T}(\mathsf{I}) := \{\mathbf{T}(f) : f \in \mathsf{I}\}$,
- the *Gröbner sous-escalier* (Mora 2016, Def. 46.1.41) $\mathbf{N}(\mathsf{I}) := \mathscr{T} \setminus \mathbf{T}(\mathsf{I})$,
- the vector-space (Mora 2016, Lemma 46.1.42) $\mathbb{F}[\mathbf{N}(\mathsf{I})] := \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{I}))$,
- $\mathbf{G}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$ the unique minimal basis (Mora 2016, Cor. 46.1.44) of $\mathbf{T}(\mathsf{I})$.

We recall that for $f \in \mathscr{P}$ and $G \subset \mathscr{P}$,

- f has *Gröbner representation* (Mora 2016, Def. 50.4.3) in terms of G if
$$f = \sum_{i=1}^{\mu_f} c_i\lambda_i g_{j_i}\rho_i,\ c_i \in \mathbb{F}\setminus\{0\}, \lambda_i, \rho_i \in \mathscr{T}, g_{j_i} \in G, \mu_f \in \mathbb{N}$$
with $\mathbf{T}(f) = \lambda_1\mathbf{T}(g_{j_1})\rho_1 \succ \cdots \succ \lambda_i\mathbf{T}(g_{j_i})\rho_i \succ \cdots$;
- $h := NF(f,G,\prec) \in \mathscr{P}$ is a *normal form* of f w.r.t. G, if (Mora 2016, Def. 50.4.5)
  - $f - h \in \mathbb{I}(G)$ has a Gröbner representation in terms of G and
  - $h \neq 0 \implies \mathbf{T}(h) \notin \{\lambda\mathbf{T}(g)\rho : \lambda, \rho \in \mathscr{T}, g \in G\} =: \mathbf{T}(G)$.
- For each $f \in \mathscr{P}$, there is a unique *canonical form* (Mora 2016, Def. 46.1.43)
$$g := \mathrm{Can}(f,\mathsf{I},\prec) = \sum_{t \in \mathbf{N}(\mathsf{I})} \gamma(f,t)t \in \mathbb{F}[\mathbf{N}(\mathsf{I})]$$
s.t. $f - g \in \mathsf{I}$.
- A Gröbner basis of I (Mora 2016, Def. 46.1.17) is any set $\Gamma \subset \mathsf{I}$ s.t. $\{\mathbf{T}(\gamma) : \gamma \in \Gamma\}$ generates $\mathbf{T}(\mathsf{I})$.
- The *reduced Gröbner basis* (Mora 2016, Cor. 46.1.44) of I is the set
$$\Gamma(\mathsf{I}) := \{\tau - \mathrm{Can}(\tau,\mathsf{I},\prec) : \tau \in \mathbf{G}(\mathsf{I})\}.$$

Remark 3. Both notions of *normal* and *canonical* form are related with Buchberger Theory but their roles in it are slightly different.

- If we have an ideal $\mathsf{I} \subset \mathscr{P}$, a set $G \subset \mathsf{I}$ and an element $f \in \mathscr{P}$, Buchberger reduction (Mora 2016, Alg. 46.1.37) returns a normal form $h \in \mathscr{P}$; if $f \in \mathsf{I}$ and G is a Gröbner basis of I necessarily $h = 0$; if we know that $f \in \mathsf{I}$ and $h \neq 0$, then necessarily
  - $h = f - (f - h) \in \mathsf{I}$,
  - G is not a Gröbner basis of I, since $\mathbf{T}(h) \in \mathbf{T}(\mathsf{I}) \setminus \mathbf{T}(G)$,
  - $G \cup \{h\}$ is a better approximation of the Gröbner basis of I.

  Buchberger Algorithm for computing Gröbner bases (Mora 2016, Sect. 47.6.2) deduces from G a set $S \subset \mathsf{I}$ (Mora 2016, Not. 47.6.1), the so called S-polynomials, which tests whether G is a Gröbner basis of the ideal I it generates; either
  - all elements of S have 0 as normal form and G is Gröbner or

- G is not Gröbner while $G' := G \cup \{NF(f, G, \prec) : f \in S\} \setminus \{0\}$ is a better approximation of the Gröbner basis of I in the sense that

$$\mathbf{T}(G) \subsetneq \mathbf{T}(G') \subset \mathbf{T}(\mathsf{I}).$$

The subset $H \subset \Gamma(\mathsf{I})$ required by Problem 1 is in fact not Gröbner but is able to test $G \subset \mathsf{I}$.

- The canonical form is a particular normal form obtained by performing complete Buchberger reduction (Mora 2016, Fig. 46.2). The canonical form g of an element f is the only element $g \in \mathbb{F}[\mathbf{N}(\mathsf{I})]$ such that (Mora 2016, Lemma 46.1.42) $g \equiv f \mod \mathsf{I}$; in other words it is the "canonical" representation of the class $f + \mathsf{I}$ in the algebra $\mathscr{P}/\mathsf{I} \cong \mathbb{F}[\mathbf{N}(\mathsf{I})]$.

  As a consequence (Mora 2016, Cor. 46.1.44), once the minimal basis $\mathbf{G}(\mathsf{I})$ of $\mathbf{T}(\mathsf{I})$ is known,

$$\Gamma(\mathsf{I}) := \{\tau - \mathrm{Can}(\tau, \mathsf{I}, \prec) : \tau \in \mathbf{G}(\mathsf{I})\} \tag{1}$$

  is the required minimal reduced Gröbner basis of I.

Remark 4. Thus, the difficult (theoretically and algorithmically) part of the computation of the required minimal reduced Gröbner basis $\Gamma(\mathsf{I})$ has been reduced, through the swindler abuse of the "oracle", to the more elementary combinatorial problem of producing the minimal monomial basis $\mathbf{G}(\mathsf{I})$. This has no significant cryptographic aspects, since it simply takes advantage of a blatant weakness of the protocol. It is however very relevant for those 0-dimensional ideals which can be described through functionals (Alonso *et al.* 2003), a class which has recent applications in different fields as Error Correcting Codes (Ceria 2020; Ceria *et al.* 2020), Algebraic Statistics (Rapallo and Rogantin 2017) or reverse engineering (Laubenbacher and Stigler 2004). For such ideals, the recent mood (Rouillier 1999; Mourrain 2005; Lundqvist 2010; Mora 2018) (Mora 2015, Sect. 40.12, Sect. 41.15) of degrobnerizing effective ideal theory, provides several efficient combinatorial tools for producing the expected minimal basis $\mathbf{G}(\mathsf{I})$ and the required minimal reduced Gröbner basis $\Gamma(\mathsf{I})$ to I can be obtained using (1) thanks of Lundqvist's approach (Lundqvist 2010).

2. Oracle-supported Approximation of $\Gamma(\mathsf{I})$

Let us now specialize $\mathscr{T}$ to be the word monoid $\mathscr{T} := \langle X_1, \ldots, X_n \rangle$ so that in particular the following holds:

- for each term $\upsilon \in \mathscr{T}$ and variables X_l, X_r, since $\mathbf{G}(\mathsf{I})$ is the unique minimal basis (Mora 2016, Cor. 46.1.44) of $\mathbf{T}(\mathsf{I})$, we have by definition

$$X_l \upsilon X_r \in \mathbf{G}(\mathsf{I}) \iff X_l \upsilon \in \mathbf{N}(\mathsf{I}), \upsilon X_r \in \mathbf{N}(\mathsf{I}), X_l \upsilon X_r \in \mathbf{T}(\mathsf{I}); \tag{2}$$

- for each term $\upsilon \in \mathscr{T}$ and each variable X, since $\mathbf{N}(\mathsf{I}) := \mathscr{T} \setminus \mathbf{T}(\mathsf{I})$, we have

$$\omega = \upsilon X \in \mathbf{N}(\mathsf{I}) \implies \upsilon \in \mathbf{N}(\mathsf{I}),\ \omega = X\upsilon \in \mathbf{N}(\mathsf{I}) \implies \upsilon \in \mathbf{N}(\mathsf{I}). \tag{3}$$

If we ask our oracle the value of $\mathrm{Can}(\tau, \mathsf{I}, \prec)$ for any term $\tau \in \mathscr{T}$, we can deduce whether

(1) $\tau \in \mathbf{T}(\mathsf{I})$, in which case we obtain also $\mathrm{Can}(\tau, \mathsf{I}, \prec)$, or
(2) $\tau \in \mathbf{N}(\mathsf{I})$ *id est* $\tau = \mathrm{Can}(\tau, \mathsf{I}, \prec)$.

Procedure 5. By assumption, we are given the sets

$$\mathrm{supp}(g_j), g_j \in G,$$

so that, without needing to know the term-ordering $\prec$, we can deduce the sets

$$T_j := \{\tau \in \mathrm{supp}(g_j) : \tau \nmid \omega, \forall \omega \in \mathrm{supp}(g_j)\}.$$

Since for each j, there are $\tau \in T_j, \lambda, \rho \in \mathscr{T} : \tau = \lambda \mathbf{T}(f)\rho$ for some $f \in \Gamma(\mathsf{I})$ *e.g.* $\tau := \mathbf{T}(g_j) \in \mathbf{T}(\mathsf{I})$, we can produce a scheme, based on Equation (2), which in a finite number of steps produces an element of $\Gamma(\mathsf{I})$; we choose a set T_j and repeatedly we

- pick an element $\tau \in T_j$; if $\tau \notin \mathbf{T}(\mathsf{I})$, simply remove it, otherwise:
- for $\tau = X_l\omega \in \mathbf{T}(\mathsf{I})$ we test, querying the oracle, whether $\omega \in \mathbf{T}(\mathsf{I})$ in which case we set $\tau := \omega$ and repeat until we have an element $\tau = X_l\omega \in \mathbf{T}(\mathsf{I})$ for which $\omega \in \mathbf{N}(\mathsf{I})$;
- now, for $\omega = \upsilon X_r \in \mathbf{N}(\mathsf{I})$ we test whether $X_l\upsilon \in \mathbf{T}(\mathsf{I})$, in which case we set $\omega := \upsilon \in \mathbf{N}(\mathsf{I})$ and repeat until we have an element $\tau := X_l\upsilon X_r$ for which

$$X_l\upsilon \in \mathbf{N}(\mathsf{I}), \upsilon X_r \in \mathbf{N}(\mathsf{I}), X_l\upsilon X_r \in \mathbf{T}(\mathsf{I})$$

id est, thanks of (3), $X_l\upsilon X_r \in \mathbf{G}(\mathsf{I})$.

Remarking that we also have

$$\mathbf{G}(\mathsf{I}) \ni X_l\upsilon X_r \mid \tau \in \mathrm{supp}(g_j),$$

we can solve Problem 1 by a repeated application of the scheme above as follows: set $H := \emptyset$ and repeatedly

- apply the scheme above thus obtaining an element $\tau \in \mathbf{G}(\mathsf{I})$ and the polynomial $\mathrm{Can}(\tau, \mathsf{I}, \prec)$,
- set $H := H \cup \{\tau - \mathrm{Can}(\tau, \mathsf{I}, \prec)\}$, $G := \{NF(g, H) : g \in G\}$

until $G = \{0\}$.

At termination, which is granted by the finiteness of the set $\bigcup_j T_j$, the set H satisfies the conditions required in Problem 1. In fact,

- each element $g \in G$ has 0 as normal form w.r.t. H,
- for each h, $h = \tau - \mathrm{Can}(\tau, \mathsf{I}) \in \Gamma(\mathsf{I})$ and $\mathbf{T}(h) = \tau := X_l\upsilon X_r \in \mathbf{G}(\mathsf{I})$.

□

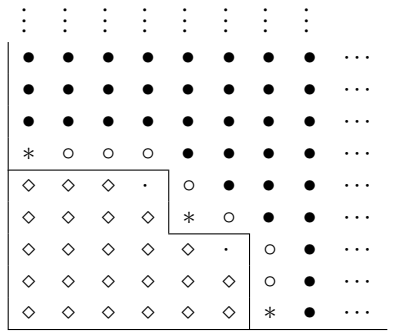
Clearly, in the non-commutative case, where in general Gröbner bases are infinite, we cannot hope to produce the whole basis of I.

3. Oracle-supported Deduction of $\Gamma(\mathsf{I})$ (commutative case)

3.1. Notation. We recall the following definitions and facts:

- For any $\tau \in \mathscr{T}, 1 \leq i \leq n$, the *$X_i$-th predecessor of τ* (Mora 2005, Def. 29.1.1) is $\frac{\tau}{X_i}$ if $X_i \mid \tau$, otherwise we say that τ does not have X_i-th predecessor.
- $\mathbf{B}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$, the *border of the ideal*, is defined (Marinari *et al.* 1993; Mora 2005, Def. 29.1.1) by
  $\mathbf{B}(\mathsf{I}) := \{\tau \in \mathbf{T}(\mathsf{I}) : \exists 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{N}(\mathsf{I})\}$,
- $\mathbf{J}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$ the *interior of the ideal*, is defined (Mora 2005, Lemma 29.3.2) by
  $\mathbf{J}(\mathsf{I}) := \{\tau \in \mathbf{T}(\mathsf{I}) : \forall 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{T}(\mathsf{I})\}$ and

FIGURE 1



- the unique minimal basis of $\mathbf{T}(\mathsf{I})$, $\mathbf{G}(\mathsf{I}) \subset \mathbf{B}(\mathsf{I})$, is characterized as (Mora 2005, Lemma 29.3.2)
  $\mathbf{G}(\mathsf{I}) := \{\tau \in \mathbf{B}(\mathsf{I}) : \forall\, 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{N}(\mathsf{I})\}$.
- $\mathbf{C}(\mathsf{I}) := \{\tau \in \mathbf{N}(\mathsf{I}) : \forall\, 1 \leq i \leq n, X_i\tau \in \mathbf{T}(\mathsf{I})\} \subset \mathbf{N}(\mathsf{I})$ is its *corner set* (Mora 2005, Def. 29.1.1). If I is 0-dimensional, $\mathbf{C}(\mathsf{I})$ "generates" $\mathbf{N}(\mathsf{I})$ in the sense that (Alonso *et al.* 2003)
$$\omega \in \mathbf{N}(\mathsf{I}) \iff \exists \tau \in \mathbf{C}(\mathsf{I}) : \omega \mid \tau.$$
- For each $f_1, f_2 \in \mathscr{P}$, the *S-polynomial of* f_1 *and* f_2 (Mora 2005, Def. 22.4.1) is
$$S(f_1,f_2) := \mathrm{lc}(f_2)^{-1}\frac{\delta(f_1,f_2)}{\mathbf{T}(f_2)}f_2 - \mathrm{lc}(f_1)^{-1}\frac{\delta(f_1,f_2)}{\mathbf{T}(f_1)}f_1,$$
where $\delta := \delta(f_1,f_2) := \mathrm{lcm}(\mathbf{T}(f_1),\mathbf{T}(f_2))$.
- A set $G = \{g_1,\ldots,g_s\}$ is a Gröbner basis of $\mathbb{I}(G)$ iff (Mora 2005, Th. 22.2.7, Th. 22.4.3) for each $i < j$ the S-polynomial $S(g_i,g_j)$ has a Gröbner representation in terms of G.
- (Buchberger's Second Criterion) (Mora 2005, Lemma 22.5.3)
  For each $f,g,h \in \mathscr{P} : \mathbf{T}(h) \mid \mathrm{lcm}(\mathbf{T}(f),\mathbf{T}(g))$, if both $S(f,h)$ and $S(g,h)$ have a Gröbner representation in terms of G, the same is true for $S(f,g)$.
- We also set $d(\mathsf{I}) := \max\{\deg(\zeta) : \zeta \in G(\mathsf{I})\}$.

Remark 6. To graphically visualize the situation we identify $\mathscr{T}$ with $\mathbb{N}^n$ in the following way:
$$X_1^{a_1}\cdots X_n^{a_n} \leftrightarrow \{(a_1,\ldots,a_n) \in \mathbb{R}^n : a_i \in \mathbb{N}, 1 \leq i \leq n\};$$
by 'line' (and one should better say 'half-line') of $\mathscr{T}$ we mean a set of aligned points of $\mathbb{N}^n \subset \mathbb{R}^n$ and similarly for 'plane', 'hyperplane', 'simplicial complex' etc..

In Fig. 1 we represent the monomial ideal $\mathsf{I} := \mathbb{I}(X_1^6, X_1^4X_2^3, X_2^5) \subset \mathscr{P}$ denoting

: $\diamond\ \mathbf{N}(\mathsf{I}) = \mathscr{T} \setminus \mathbf{T}_<(\mathsf{M})$ its *Gröbner escalier*;
: $\circ\ \mathbf{B}(\mathsf{I}) := \{X_h\tau : 1 \leq h \leq n, \tau \in \mathbf{N}(\mathsf{I}))\} \setminus \mathbf{N}(\mathsf{I})$, its *border set*;
: $\bullet\ \mathbf{J}(\mathsf{I}) := \mathbf{T}(\mathsf{I}) \setminus \mathbf{B}(\mathsf{I})$,
: $*\ \mathbf{G}(\mathsf{I}) \subset \mathbf{B}(\mathsf{I})$ the unique minimal basis of $\mathbf{T}(\mathsf{I})$,
: $\cdot\ \mathbf{C}(\mathsf{I}) := \{\tau \in \mathbf{N}(\mathsf{I}) : X_h\tau \in \mathbf{T}(\mathsf{I}), \forall h\}$ its *corner set*.

We point out that :

- for $n=2$, $\mathbf{B}(\mathsf{I})$ is a 'piecewise linear curve' $\mathscr{C}(\mathsf{I})$ consisting of contiguous horizontal and vertical 'segments' from which all the 'convex' vertices are removed and possibly the leftmost vertical segment and the bottom horizontal one are 'half-lines'[3];
- for $n \geq 3$, $\mathbf{B}(\mathsf{I})$ is a 'simplicial complex'[4], consisting of contiguous shares of 'hyperplanes' each of them parallel to a 'coordinate hyperplane' (the closest to a coordinate one possibly being infinite) from which all the 'protruding' i-th facets with $i \leq n-2$ are removed;
- $\mathbf{J}(\mathsf{I})$ is the set of points lying above the *escalier*;
- $\mathbf{G}(\mathsf{I})$ consists of the 'concave vertices' of the *escalier*;
- $\mathbf{N}(\mathsf{I})$ is the set of points below the *escalier* (for this named *sous-escalier*).

We will also call "0-*dimensional"*, ..., *"*$n-1$*-dimensional" point of the* escalier a point lying on a vertex ,..., on a $(n-1)$-facet (and not in a lower dimensional one) noticing that the elements of $\mathbf{G}(\mathsf{I})$ are particular "0-dimensional" points. □

Remark 7. For any ideal $\mathsf{I} \subset \mathscr{P}$, Noetherian semigroup ordering $\prec$, and degree value $\delta \in \mathbb{N}$ s.t. $\delta \leq d(\mathsf{I})-1$, setting $H := \{g \in \Gamma(\mathsf{I}), \deg(g) \leq \delta\}$ the two ideals I and $\mathsf{I}_\delta := \mathbb{I}(H)$ satisfy both:

$$\{f \in \mathsf{I} : \deg(f) \leq \delta\} = \{f \in \mathsf{I}_\delta : \deg(f) \leq \delta\} \text{ and } \mathsf{I}_\delta \subset \mathsf{I},$$

with

$$d(\mathsf{I}) \geq \delta + 1 > \delta \geq d(\mathsf{I}_\delta).$$

Thus, the algorithm we are going to sketch below, applied to the (unknown) ideal I, returns the correct answer I if the input data satisfy $D \geq \delta + 1$, but returns the wrong answer I_δ if $D \leq \delta < d(\mathsf{I})$. That is, we actually need to assume to know an upper bound D for $d(\mathsf{I})$ and only deal with terms belonging to the *box*

$$\mathscr{B}(D) := \{X_1^{a_1} \cdots X_n^{a_n} \in \mathscr{T} : 0 \leq a_i \leq D, \forall\, 1 \leq i \leq n\}.$$

□

Remark 8. In the non-0-dimensional case, the notion of *corner sets* can be generalized (Macaulay 1913, 1916) considering also elements $\tau = X_1^{a_1} \cdots X_n^{a_n}, a_i \in \mathbb{N} \cup \{\infty\}$ and setting

$$\omega \mid \tau \iff b_i \leq a_i, \text{ for each } \omega = X_1^{b_1} \cdots X_n^{b_n}.$$

It is then easy to see that there is a finite set

$$\mathbf{C}^\infty(\mathsf{I}) \subset \left\{X_1^{a_1} \cdots X_n^{a_n}, a_i \in \mathbb{N} \cup \{\infty\}\right\}$$

which satisfies

$$\omega \in \mathbf{N}(\mathsf{I}) \iff \text{ exists } \tau \in \mathbf{C}^\infty(\mathsf{I}) : \omega \mid \tau.$$

The algorithm we are proposing will return $\mathbf{G}(\mathsf{I}), \Gamma(\mathsf{I})$ and $\mathbf{C}^\infty(\mathsf{I})$. □

[3] As $\mathbf{B}(\mathsf{I}) \cup \{\text{all the convex vertices}\}$ looks like the profile of a stair A. Galligo introduced the term *escalier*.
[4] Still called *escalier*.

3.2. Cardinal-like counterexample. Before discussing Problem 2, we begin by observing that also in the commutative case $\mathscr{P} = \mathbb{F}[X_1, \ldots, X_n]$, with $\deg(X_i) = 1, \forall\, 1 \leq i \leq n$, a strong solution returning the complete basis of an ideal $\mathsf{I} \subset \mathscr{P}$ cannot be produced, unless further knowledge is assumed: in fact, given $\mathsf{I} \subset \mathbb{F}[X_1, \ldots, X_n]$ and a value $\delta \in \mathbb{N}, \delta < d(\mathsf{I})$, in general there are smaller ideals (see Remark 7) $\mathsf{I}_\delta \subsetneqq \mathsf{I}$ which satisfy

$$\{f \in \mathsf{I} : \deg(f) \leq \delta\} = \{f \in \mathsf{I}_\delta : \deg(f) \leq \delta\}. \tag{4}$$

Some concrete examples can be easily produced by taking[5] any ideal $\mathsf{J} \subset \mathscr{P}$, $d(\mathsf{J}) \leq \delta - 1$ and any element $h_0 \in \mathsf{J} \setminus X_2\mathsf{J}$; then, as we verify below, necessarily

$$X_2\mathsf{J} =: \mathsf{I}_\delta \subsetneqq \mathsf{I} := X_2\mathsf{J} + (h_0)$$

satisfy (4).

Let then $\mathsf{J} \subset \mathbb{F}[X_1, \ldots, X_n] := \mathscr{P}$ be an ideal, $\prec$ a Noetherian semigroup ordering, $\Gamma(\mathsf{J}) = \{\gamma_1, \ldots, \gamma_s\}$ the Gröbner basis of J w.r.t. $\prec$ and $\delta \in \mathbb{N}$ any degree value s.t. $\delta \geq d(\mathsf{J}) + 1$.

Enumerate the variables and the Gröbner basis elements in such a way that $X_1 \prec X_2 \prec \ldots \prec X_n$ and

$$i < j \iff \text{either } \begin{cases} \deg(\gamma_i) > \deg(\gamma_j) \text{ or} \\ \deg(\gamma_i) = \deg(\gamma_j) \text{ and } \mathbf{T}(\gamma_i) \succ \mathbf{T}(\gamma_j). \end{cases}$$

Denoting

$$\Omega := \min_{\prec}\{\tau \in \mathbf{T}(\mathsf{I}), \deg(\tau) = \delta + 1\}$$

and $d_i := \deg(\gamma_i) < \delta$, by definition we necessarily have

$$\Omega = X_1^{\delta+1-d_s}\mathbf{T}(\gamma_s).$$

We also let $h_0 := \Omega - \mathrm{Can}(\Omega, \mathsf{J}, \prec)$, so that $\mathrm{lc}(h_0) = 1, \mathbf{T}(h_0) = \Omega = X_1^{\delta+1-d_s}\mathbf{T}(\gamma_s)$, and $h_i := X_2\gamma_i, 1 \leq i \leq s$. We obtain:

Proposition 9. *With the above notation it holds $H := \{h_0, h_1, \ldots, h_s\}$ is a Gröbner basis w.r.t. $\prec$ of the ideal $\mathbb{I}(H) = X_2\mathsf{J} + (h_0)$.*

Proof Clearly if $S(\gamma_i, \gamma_j), 1 \leq i < j \leq s$, has the Gröbner representation in terms of $\Gamma(\mathsf{J})$, $S(\gamma_i, \gamma_j) = \sum_{\alpha=1}^{\mu_{ij}} c_\alpha \tau_\alpha \gamma_{\ell_\alpha}$, then $S(h_i, h_j) = X_2 \sum_{\alpha=1}^{\mu_{ij}} c_\alpha \tau_\alpha \gamma_{\ell_\alpha} = \sum_{\alpha=1}^{\mu_{ij}} c_\alpha \tau_\alpha h_{\ell_\alpha}$ is a Gröbner representation in terms of H.

Moreover, since $\Omega = \mathbf{T}(h_0) = X_1^{\delta+1-d_s}\mathbf{T}(\gamma_s)$ and

$$\mathbf{T}(h_s) = X_2\mathbf{T}(\gamma_s) \mid \mathrm{lcm}(\mathbf{T}(h_j), \Omega) = X_1^{\delta+1-d_s}X_2\,\mathrm{lcm}(\mathbf{T}(\gamma_j), \mathbf{T}(\gamma_s)), 1 \leq j < s,$$

as a direct consequence of Buchberger's Second Criterion, in order to prove the claim it is sufficient to show that the S-polynomial $S(h_s, h_0)$ between h_0 and h_s has a Gröbner representation in terms of H.

[5]Of course, our construction is indebted to the counterexample to Cardinal's Conjecture proposed by Mourrain (2005).

By assumption there $\exists \mu = \mu_{h_0}, \ell_\alpha \in \mathbb{N}, 1 \le \ell_\alpha \le s, c_\alpha \in \mathbb{F} \setminus \{0\}, \tau_\alpha \in \mathscr{T}$, s.t. we have a Gröbner representation

$$\mathsf{J} \ni h_0 = \Omega - \mathrm{Can}(\Omega, \mathsf{J}, \prec) = \mathrm{lc}(\gamma_s)^{-1} X_1^{\delta+1-d_s} \gamma_s + \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha \gamma_{\ell_\alpha}$$

where $\gamma_{\ell_\alpha} \in \Gamma(\mathsf{J})$ and

$$\Omega = X_1^{\delta+1-d_s} \mathbf{T}(\gamma_s) \succ \tau_1 \mathbf{T}(\gamma_{\ell_1}) \succ \tau_2 \mathbf{T}(\gamma_{\ell_2}) \succ \cdots;$$

thus we trivially obtain the required Gröbner representation

$$\begin{aligned} S(h_s, h_0) &= \mathrm{lc}(h_0)^{-1} \frac{\delta(h_s,h_0)}{\mathbf{T}(h_0)} h_0 - \mathrm{lc}(h_s)^{-1} \frac{\delta(h_s,h_0)}{\mathbf{T}(h_s)} h_s = \\ &= X_2 h_0 - \mathrm{lc}(\gamma_s)^{-1} X_1^{\delta+1-d_s} (X_2 \gamma_s) \\ &= X_2 \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha \gamma_{\ell_\alpha} = \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha h_{\ell_\alpha} \end{aligned}$$

where

$$\delta(h_s, h_0) = \mathrm{lcm}(\mathbf{T}(h_s), \mathbf{T}(h_0)) = \mathrm{lcm}(X_2 \mathbf{T}(\gamma_s), X_1^{\delta+1-d_s} \mathbf{T}(\gamma_s)) = X_1^{\delta+1-d_s} X_2 \mathbf{T}(\gamma_s).$$

□

3.3. Algorithm. We now give a combinatorial algorithm to solve Problem 2, using exactly the notation, the input and the requirements stated there. For each monomial ω we consider, the required information whether $\omega \in \mathbf{N}(\mathsf{I})$ or $\omega \in \mathbf{T}(\mathsf{I})$ is trivially deduced by the (ab)use of the oracle.

Let $\omega = X_1 \cdot \ldots \cdot X_n$, as $\omega^0 = 1 \in \mathbf{N}(\mathsf{I})$, we take iteratively $\omega^{i+1}, i \in \mathbb{N}$, until either $\omega^D \in \mathbf{N}(\mathsf{I})$ or we find $j \in \mathbb{N}, j \le D$, such that $\omega^{j-1} \in \mathbf{N}(\mathsf{I})$ and $\omega^j \in \mathbf{T}(\mathsf{I})$.

If $\omega^D \in \mathbf{N}(\mathsf{I})$ we can deduce that $\mathsf{I} = (0)$[6]. In the other case, for the found value $j \in \mathbb{N}$, by testing, for $1 \le i \le n$, whether $\frac{\omega^j}{X_i} \in \mathbf{T}(\mathsf{I})$, we can produce the set $\mathsf{P} := \{i : \frac{\omega^j}{X_i} \in \mathbf{T}(\mathsf{I})\}$ and the value $\#\mathsf{P}$ thus deducing which of the following cases arises:

(1) $\omega^j \in \mathbf{G}(\mathsf{I}) \iff \#\mathsf{P} = 0$ (i.e. all the predecessors of ω^j are in $\mathbf{N}(\mathsf{I})$),
(2) $\omega^j \in \mathbf{B}(\mathsf{I}) \setminus \mathbf{G}(\mathsf{I}) \iff 0 < \#\mathsf{P} < n$ (i.e. at most $n-1$ predecessors of ω^j are in $\mathbf{N}(\mathsf{I})$),
(3) $\omega^j \in \mathbf{J}(\mathsf{I}) \iff \#\mathsf{P} = n$ (i.e. all the predecessors of ω^j are in $\mathbf{T}(\mathsf{I})$).

3.3.1. *Two variables.*

Remark 10. Since $\mathsf{I} \neq (0)$, there are finitely many integers $a_1 > a_2 > \cdots > a_s, b_1 < b_2 < \cdots < b_s \in \mathbb{N}$ such that, denoting $\tau_i := X_1^{a_i} X_2^{b_i}$, it holds

$$\mathbf{G}(\mathsf{I}) = \{\tau_i, 1 \le i \le s\}.$$

As a consequnce we also have

$$\mathbf{C}(\mathsf{I}) = \{X_1^{a_1-1} X_2^{b_2-1}, X_1^{a_2-1} X_2^{b_3-1}, \ldots, X_1^{a_{s-1}-1} X_2^{b_s-1}\};$$

$\mathbf{C}^\infty(\mathsf{I})$ is then obtained adding $X_1^\infty X_2^{b_1-1}$ if $b_1 > 0$ and $X_1^{a_s-1} X_2^\infty$ if $a_s > 0$. □

[6]In fact each term τ with $\deg(\tau) \le D$ trivially satisfies $\tau \mid \omega^D$, i.e. $\omega^D \in \mathbf{N}(\mathsf{I})$ implies $\mathbf{G}(\mathsf{I}) = \emptyset$.

The correctness and completeness of the procedure is definitely trivial: assume to be on the top ω of the wall of a medieval castle and perform a patrol walk (in both directions) marking the coordinates of all the towers.

The procedure starts with a monomial $\omega = X_1^j X_2^j \in \mathbf{B}(\mathsf{I})$ and

(1) decides whether $\omega \in \mathbf{G}(\mathsf{I})$;
(2) lists all the terms $\tau = X_1^c X_2^d \in \mathbf{G}(\mathsf{I}) \cup \mathbf{C}^\infty(\mathsf{I})$ with $c \geq j$,
(3) lists all the terms $\tau = X_1^c X_2^d \in \mathbf{G}(\mathsf{I}) \cup \mathbf{C}^\infty(\mathsf{I})$ with $d \geq j$,

as follows

(1) $\omega \in \mathbf{G}(\mathsf{I}) \iff \#\mathsf{P} = 0 \iff \frac{\omega}{X_1} \in \mathbf{N}(\mathsf{I})$ and $\frac{\omega}{X_2} \in \mathbf{N}(\mathsf{I})$.

(2)
- if $\omega \in \mathbf{G}(\mathsf{I})$, iteratively testing whether
$$\frac{X_1^i}{X_2}\omega = X_1^{a+i} X_2^{b-1} \in \mathbf{T}(\mathsf{I}), 1 \leq i \leq D-a-b+2,$$
find the value i for which $\frac{X_1^i}{X_2}\omega \in \mathbf{N}(\mathsf{I})$ and either $i+a+b-1 = D$ or $\frac{X_1^{i+1}}{X_2}\omega \in \mathbf{T}(\mathsf{I})$:
  - if $i+a+b-1 = D$, since $\deg(\frac{X_1^i}{X_2}\omega) = D$ and $\frac{X_1^i}{X_2}\omega \in \mathbf{N}(\mathsf{I})$ we can deduce that $\frac{X_1^i}{X_2}\omega \in \mathbf{N}(\mathsf{I})$ for each $i \in \mathbb{N}$ and thus we enclose $X_1^\infty X_2^{b-1}$ in $\mathbf{C}^\infty(\mathsf{I})$ and the subprocedure 2. terminates;
  - if, instead, $\frac{X_1^{i+1}}{X_2}\omega \in \mathbf{T}(\mathsf{I})$, then $\frac{X_1^i}{X_2}\omega \in \mathbf{C}(\mathsf{I})$ and the subprocedure 2. restarts with $\omega := X_1^{a+i+1} X_2^{b-1}$.
- if $\frac{\omega}{X_1} \in \mathbf{T}(\mathsf{I})$ and $\frac{\omega}{X_2} \in \mathbf{N}(\mathsf{I})$ (and thus ω belongs to an horizontal segment of $\mathbf{B}(\mathsf{I})$), again we, iteratively testing whether
$$\frac{X_1^i}{X_2}\omega = X_1^{a+i} X_2^{b-1} \in \mathbf{T}(\mathsf{I}), 1 \leq i \leq D-a-b+2,$$
find the value i for which $\frac{X_1^i}{X_2}\omega \in \mathbf{N}(\mathsf{I})$ and either $i+a+b-1 = D$ or $\frac{X_1^{i+1}}{X_2}\omega \in \mathbf{T}(\mathsf{I})$:
  - if $i+a+b-1 = D$, we can deduce that $\frac{X_1^i}{X_2}\omega \in \mathbf{N}(\mathsf{I})$ for each $i \in \mathbb{N}$ and thus we enclose $X_1^\infty X_2^{b-1}$ in $\mathbf{C}^\infty(\mathsf{I})$ and the subprocedure 2. terminates;
  - if, instead, $\frac{X_1^{i+1}}{X_2}\omega \in \mathbf{T}(\mathsf{I})$, then we insert $\frac{X_1^i}{X_2}\omega$ in $\mathbf{C}^\infty(\mathsf{I})$ and the subprocedure 2. restarts with $\omega := X_1^{a+i+1} X_2^{b-1}$.
- if $\frac{\omega}{X_1} \in \mathbf{N}(\mathsf{I})$ and $\frac{\omega}{X_2} \in \mathbf{T}(\mathsf{I})$ (and thus ω belongs to a vertical segment of $\mathbf{B}(\mathsf{I})$), we, iteratively testing whether
$$\frac{\omega}{X_2^i} = X_1^a X_2^{b-i} \in \mathbf{T}(\mathsf{I}), i \leq b,$$
find the value i for which $\frac{\omega}{X_2^i} \in \mathbf{T}(\mathsf{I})$ and either $i = b$ or $\frac{\omega}{X_2^{i+1}} \in \mathbf{N}(\mathsf{I})$; in both cases we deduce that $\frac{\omega}{X_2^i} = X_1^a X_2^{b-i} \in \mathbf{G}(\mathsf{I})$ and we insert it there; moreover
  - if $i = b$, so that $\frac{\omega}{X_2^b} = X_1^a \in \mathbf{G}(\mathsf{I})$, the subprocedure 2. is completed;

- if, instead, $\frac{\omega}{X_2^i} \in \mathbf{N}(\mathfrak{l})$, the subprocedure 2. restarts with $\omega := X_1^a X_2^{b-i}$.

- $\frac{\omega}{X_1} \in \mathbf{N}(\mathfrak{l})$ and $\frac{\omega}{X_2} \in \mathbf{N}(\mathfrak{l})$ since $\omega \in \mathbf{T}(\mathfrak{l})$ we can deduce that $\frac{\omega}{X_1 X_2} \in \mathbf{C}(\mathfrak{l})$ and
  - we insert it there;
  - iteratively testing whether

$$\frac{\omega}{X_1^i} = X_1^{a-i} X_2^b \in \mathbf{T}(\mathfrak{l}), 2 \le a,$$

    we find the value i for which $\frac{\omega}{X_1^i} \in \mathbf{T}(\mathfrak{l})$ and either $i = a$ or $\frac{\omega}{X_1^{i+1}} \in \mathbf{N}(\mathfrak{l})$; in both cases we deduce that

$$\frac{\omega}{X_1^i} = X_1^{a-i} X_2^b \in \mathbf{G}(\mathfrak{l})$$

    and we insert it there; moreover
    - if $i = a$, so that $\frac{\omega}{X_1^i} = X_2^b \in \mathbf{G}(\mathfrak{l})$, the complete procedure terminates returning both $\mathbf{G}(\mathfrak{l})$ and $\mathbf{C}^\infty(\mathfrak{l})$
    - if, instead, $\frac{\omega}{X_1^{i+1}} \in \mathbf{N}(\mathfrak{l})$, the subprocedure 2. restarts with $\omega := X_1^{a-i} X_2^{b-1}$.

(3) - if $\omega \in \mathbf{G}(\mathfrak{l})$, iteratively testing whether

$$\frac{X_2^i}{X_1}\omega = X_1^{a-1} X_2^{b+i} \in \mathbf{T}(\mathfrak{l}), 1 \le i \le D - a - b + 2,$$

  find the value i for which $\frac{X_2^i}{X_1}\omega \in \mathbf{N}(\mathfrak{l})$ and either $i + a + b - 1 = D$ or $\frac{X_2^{i+1}}{X_1}\omega \in \mathbf{T}(\mathfrak{l})$:
  - if $i + a + b - 1 = D$, since $\deg(\frac{X_2^i}{X_1}\omega) = D$ and $\frac{X_2^i}{X_1}\omega \in \mathbf{N}(\mathfrak{l})$ we can deduce that $\frac{X_2^i}{X_1}\omega \in \mathbf{N}(\mathfrak{l})$ for each $i \in \mathbb{N}$ and thus we enclose $X_1^{a-1} X_2^\infty$ in $\mathbf{C}^\infty(\mathfrak{l})$ and the subprocedure 3. terminates;
  - if, instead, $\frac{X_2^{i+1}}{X_1}\omega \in \mathbf{T}(\mathfrak{l})$, then $\frac{X_2^i}{X_1}\omega \in \mathbf{C}^\infty(\mathfrak{l})$ and the subprocedure 2. restarts with $\omega := X_1^{a-1} X_2^{b+i+1}$.

- if $\frac{\omega}{X_2} \in \mathbf{T}(\mathfrak{l})$ and $\frac{\omega}{X_1} \in \mathbf{N}(\mathfrak{l})$, again we, iteratively testing whether

$$\frac{X_2^i}{X_1}\omega = X_1^{a-1} X_2^{b+i} \in \mathbf{T}(\mathfrak{l}), 1 \le i \le D - a - b + 2,$$

  find the value i for which $\frac{X_2^i}{X_1}\omega \in \mathbf{N}(\mathfrak{l})$ and either $i + a + b - 1 = D$ or $\frac{X_2^{i+1}}{X_1}\omega \in \mathbf{T}(\mathfrak{l})$:
  - if $i + a + b - 1 = D$, we can deduce that $\frac{X_2^i}{X_1} \in \mathbf{N}(\mathfrak{l})$ for each $i \in \mathbb{N}$ and thus we enclose in $X_2^\infty X_1^{b-1}$ in $\mathbf{C}^\infty(\mathfrak{l})$ and the subprocedure 3. terminates;
  - if, instead, $\frac{X_2^{i+1}}{X_1}\omega \in \mathbf{T}(\mathfrak{l})$, then we insert $\frac{X_2^i}{X_1}\omega$ in $\mathbf{C}^\infty(\mathfrak{l})$ and the subprocedure 2. restarts with $\omega := X_1^{a-1} X_2^{b+i+1}$.

- if $\frac{\omega}{X_2} \in \mathbf{N}(\mathfrak{l})$ and $\frac{\omega}{X_1} \in \mathbf{T}(\mathfrak{l})$, we, iteratively testing whether
$$\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbf{T}(\mathfrak{l}), i \leq a,$$
find the value i for which $\frac{\omega}{X_1^i} \in \mathbf{T}(\mathfrak{l})$ and either $i = a$ or $\frac{\omega}{X_1^{i+1}} \in \mathbf{N}(\mathfrak{l})$; in both cases we deduce that $\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbf{G}(\mathfrak{l})$ and we insert it there; moreover
  - if $i = a$, so that $\frac{\omega}{X_1^a} = X_2^b \in \mathbf{G}(\mathfrak{l})$, the subprocedure 2. is completed;
  - if, instead, $\frac{\omega}{X_1^i} \in \mathbf{N}(\mathfrak{l})$, the subprocedure 2. restarts with $\omega := X_1^{a-i}X_2^b$.
- $\frac{\omega}{X_1} \in \mathbf{N}(\mathfrak{l})$ and $\frac{\omega}{X_2} \in \mathbf{N}(\mathfrak{l})$ since $\omega \in \mathbf{T}(\mathfrak{l})$ we can deduce that $\frac{\omega}{X_1X_2} \in \mathbf{C}(\mathfrak{l})$ and
  - we insert it there;
  - iteratively testing whether
$$\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbf{T}(\mathfrak{l}), i \leq a,$$
we find the value i for which $\frac{\omega}{X_1^i} \in \mathbf{T}(\mathfrak{l})$ and either $i = a$ or $\frac{\omega}{X_1^{i+1}} \in \mathbf{N}(\mathfrak{l})$; in both cases we deduce that
$$\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbf{G}(\mathfrak{l})$$
and we insert it there; moreover
    - if $i = a$, so that $\frac{\omega}{X_1^i} = X_2^b \in \mathbf{G}(\mathfrak{l})$, the procedure terminates returning both $\mathbf{G}(\mathfrak{l})$ and $\mathbf{C}^\infty(\mathfrak{l})$
    - if, instead, $\frac{\omega}{X_1^{i+1}} \in \mathbf{N}(\mathfrak{l})$, the subprocedure 2. restarts with $\omega := X_1^{a-i}X_2^{b-1}$.

Example 11. Let $\mathscr{P} = \mathbb{F}[X,Y]$, $\omega = XY$.

(1) $\mathfrak{l} = (X^4Y, X^2Y^2, XY^3, Y^8), D = 8$ (see Fig. 2).
We have $\omega^1 \in \mathbf{N}(\mathfrak{l}), \omega^2 \in \mathbf{T}(\mathfrak{l})$ and $XY^2, X^2Y \in \mathbf{N}(\mathfrak{l})$, thus $\omega^2 \in \mathbf{G}(\mathfrak{l})$.
Considering $X^{2+i}Y, i \leq D-2$ we find, successively, $X^4Y \in \mathbf{G}(\mathfrak{l})$ and $X^3Y \in \mathbf{C}(\mathfrak{l})$; next evaluting X^5, X^6, X^7, X^8, since $X^8 \in \mathbf{N}(\mathfrak{l})$ we deduce $X^\infty \in \mathbf{C}^\infty(\mathfrak{l})$.
Next considering XY^{2+i}, we find, successively, $XY^3 \in \mathbf{G}(\mathfrak{l})$ and $XY^2 \in \mathbf{C}(\mathfrak{l})$; next evaluting Y^5, Y^6, Y^7, Y^8, we obtain $Y^8 \in \mathbf{G}(\mathfrak{l})$ and $Y^7 \in \mathbf{C}(\mathfrak{l})$.

(2) $\mathfrak{l} = (X^3Y^2), D = 5$ (see Fig. 3).
We have $\omega^1, \omega^2 \in \mathbf{N}(\mathfrak{l})$, $\omega^3 \in \mathbf{T}(\mathfrak{l})$ with $X^2Y^3 \in \mathbf{N}(\mathfrak{l})$ and $X^3Y^2 \in \mathbf{T}(\mathfrak{l})$.
Thus we have to consider $X^3Y^{3-i}, 0 < i \leq 3$, getting $X^3Y^2 \in \mathbf{G}(\mathfrak{l})$; next computing $X^2Y^3 \in \mathbf{N}(\mathfrak{l})$ we have $X^2Y^\infty \in \mathbf{C}^\infty(\mathfrak{l})$; finally computing $X^{2+i}Y, 0 < i \leq 2$ we find $X^4Y \in \mathbf{N}(\mathfrak{l})$ and $X^\infty Y \in \mathbf{C}^\infty(\mathfrak{l})$.

(3) $\mathfrak{l} = (X^4Y^3, X^2Y^4), D = 7$ (see Fig. 4). We have $\omega^1, \omega^2, \omega^3 \in \mathbf{N}(\mathfrak{l})$, $\omega^4 \in \mathbf{T}(\mathfrak{l})$ with $X^3Y^4, X^4Y^3 \in \mathbf{T}(\mathfrak{l})$. Since $X^4Y^2 \in \mathbf{N}(\mathfrak{l})$, we deduce $X^4Y^3 \in \mathbf{G}(\mathfrak{l})$; next considering $X^5Y^2 \in \mathbf{N}(\mathfrak{l})$ we obtain $X^\infty Y^2 \in \mathbf{C}^\infty(\mathfrak{l})$.
Next reconsidering $X^3Y^4 \in \mathbf{T}(\mathfrak{l})$ we first deduce that $X^3Y^3 \in \mathbf{C}(\mathfrak{l})$ and further the computation of $X^2Y^4 \in \mathbf{T}(\mathfrak{l})$ and $XY^4 \in \mathbf{N}(\mathfrak{l})$ imply $X^2Y^4 \in \mathbf{G}(\mathfrak{l})$. Finally since $XY^5, XY^6 \in \mathbf{N}(\mathfrak{l})$, we obtain $XY^\infty \in \mathbf{C}^\infty(\mathfrak{l})$.

FIGURE 2

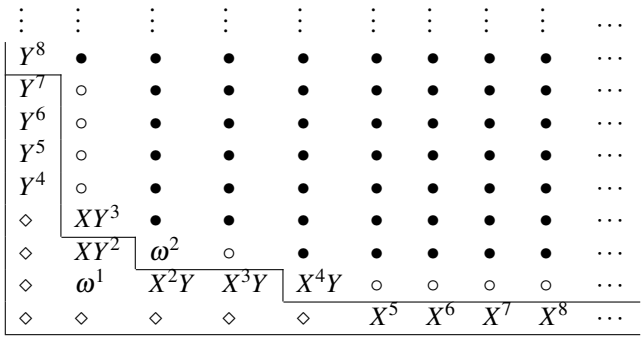


FIGURE 3

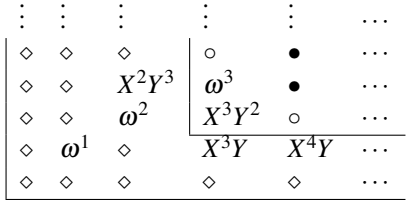
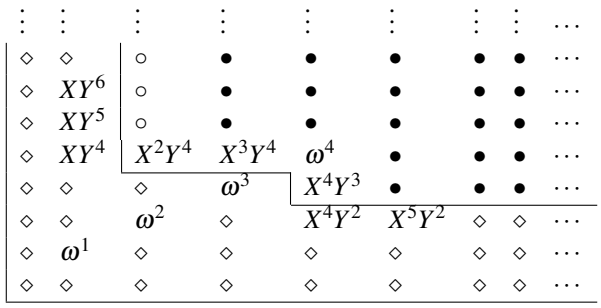


FIGURE 4



3.4. $n \geq 3$ **variables.** Unlike the case $n = 2$ where the algorithm consists literally into a walk along the border, the case $n \geq 3$ applies[7] the deeply studied (Janet 1920, 1927) relations among the slices $\mathbf{T}(\mathfrak{l})_j$, $j \in \mathbb{N}$, of $\mathbf{T}(\mathfrak{l}) \subset \mathscr{T}$:

$$\mathbf{T}(\mathfrak{l})_j := \{\tau = X_1^{a_1} X_2^{a_2} \dots X_{n-1}^{a_{n-1}} : \tau X_n^j \in \mathbf{T}(\mathfrak{l})\} \subset \mathscr{T}' := \mathscr{T} \cap \mathbb{K}[X_1, X_2, \dots X_{n-1}]$$

[7]More precisely, also the case $n = 2$ is just the specialization to the trivial case of the general approach; we considered didatically better to present it differently and with more details.

which satisfy $\mathbf{T}(\mathsf{I})_j \subseteq \mathbf{T}(\mathsf{I})_{j+1}$ so that, by Noetherianity there are finitely many positive integers $0 \leq b_1 < b_2 < \ldots < b_s \leq D$ for which

$$\emptyset \subsetneq \mathbf{T}(\mathsf{I})_{b_1} \subsetneq \mathbf{T}(\mathsf{I})_{b_2} \subsetneq \ldots \subsetneq \mathbf{T}(\mathsf{I})_{b_s} = \mathbf{T}(\mathsf{I})_{b_{s+1}} = \ldots = \mathbf{T}(\mathsf{I})_D = \ldots$$

Mainly, in order to deduce the generating set $\mathbf{G}(\mathsf{I})$ and the corner sets $\mathbf{C}(\mathsf{I})$ and $\mathbf{C}^\infty(\mathsf{I})$ of I, we will consider the relations among the corresponding sets of $\mathbf{T}(\mathsf{I})_j$ which we will denote $\mathbf{G}_j$, $\mathbf{C}_j$ and $\mathbf{C}_j^\infty$ and which trivially satisfy:

Lemma 12. *With the present notation and denoting*

$$\tau = X_1^{a_1} X_2^{a_2} \ldots X_{n-1}^{a_{n-1}}, a_i \in \mathbb{N} \cup \{\infty\},$$

we have

(1) $\mathbf{T}(\mathsf{I})_j = \mathbf{T}(\mathsf{I})_{j+1} \iff \mathbf{G}_j = \mathbf{G}_{j+1}, \mathbf{C}_j = \mathbf{C}_{j+1}, \mathbf{C}_j^\infty = \mathbf{C}_{j+1}^\infty$;
(2) $\tau X_n^j \in \mathbf{G}(\mathsf{I}) \iff \tau \in \mathbf{G}_j, \tau \notin \mathbf{G}_{j-1}$;
(3) $\tau X_n^{j-1} \in \mathbf{C}(\mathsf{I}) \iff \tau \in \mathbf{C}_{j-1}, \tau \notin \mathbf{C}_j$;
(4) $\tau X_n^{j-1} \in \mathbf{C}^\infty(\mathsf{I}) \iff \tau \in \mathbf{C}_{j-1}^\infty$ *and* $\tau \in \mathbf{T}(\mathsf{I})_j$. □

The procedure starts with a term $\omega = X_1^j X_2^j \ldots X_{n-1}^j X_n^j$ and:

(1) applies the same procedure on

$$\mathscr{T}' := \{\tau = X_1^{a_1} X_2^{a_2} \ldots X_{n-1}^{a_{n-1}}, (a_1, \ldots, a_{n-1}) \in \mathbb{N}^{n-1}\},$$

in order to describe $\mathbf{T}(\mathsf{I})_j$ and produce $\mathbf{G}_j$, $\mathbf{C}_j$ and $\mathbf{C}_j^\infty$;
(2) sets $u := d := j, \mathbf{G}_u := \mathbf{G}_d := \mathbf{G}_j, \mathbf{C}_u := \mathbf{C}_d := \mathbf{C}_j, \mathbf{C}_u^\infty := \mathbf{C}_d^\infty := \mathbf{C}_j^\infty$;
(3) list all terms $\tau X_n^d \in \mathbf{G}_d \cup \mathbf{C}_d^\infty, d \leq j$;
(4) list all terms $\tau X_n^u \in \mathbf{G}_u \cup \mathbf{C}_u^\infty, u \geq j$

as follows, where, for each $\upsilon := X_1^{a_1} X_2^{a_2} \ldots X_{n-1}^{a_{n-1}}, a_i \in \mathbb{N} \cup \{\infty\}$ we denote by $\bar{\upsilon} := X_1^{b_1} X_2^{b_2} \ldots X_{n-1}^{b_{n-1}} \in \mathscr{T}'$ the term with $b_i := \begin{cases} a_i & \text{if } a_i \in \mathbb{N} \\ D & \text{if } a_i = \infty. \end{cases}$

(1) Remark that the procedure after a sequence of calls to the same procedure with less variables will apply the procedure discussed in Section **3.3.1** for $\omega := X_1^j X_2^j$ in order to obtain the data for the ideal $\mathsf{J} := \{X_1^a X_2^b : X_1^a X_2^b X_3^j \ldots X_{n-1}^j X_n^j\}$ through a series of queries $\boxed{\upsilon \in \mathbf{T}(\mathsf{J})?}$; of course each such query should be formulated as $\boxed{\upsilon X_3^j \ldots X_{n-1}^j X_n^j \in \mathbf{T}(\mathsf{I})?}$.
(3) (a) while $\mathbf{T}(\mathsf{I})_d \neq \emptyset$ do
- if $\upsilon X_n^{d-1} \in \mathbf{T}(\mathsf{I})$ for all $\upsilon \in \mathbf{G}_d$, so that $\mathbf{T}(\mathsf{I})_{d-1} = \mathbf{T}(\mathsf{I})_d$ set $\mathbf{G}_{d-1} = \mathbf{G}_d, \mathbf{C}_{d-1} = \mathbf{C}_d, \mathbf{C}_{d-1}^\infty = \mathbf{C}_d^\infty, d := d-1$;
- otherwise
  - choose $\upsilon \in \mathbf{G}_d$ for which $\upsilon X_n^{d-1} \in \mathbf{N}(\mathsf{I})$, set

$$t := X_1 X_2 \ldots X_{n-1}$$

and compute the value ι s.t.

$$\upsilon t^\iota X_n^{d-1} \in \mathbf{T}(\mathsf{I}), \text{ while } \upsilon t^{\iota-1} X_n^{d-1} \in \mathbf{N}(\mathsf{I});$$

- apply the same procedure with input $\upsilon t^{\iota} X_n^{d-1} \in \mathbf{T}(\mathsf{I})$ in order to deduce $\mathbf{G}_{d-1}$, $\mathbf{C}_{d-1}$ and $\mathbf{C}^{\infty}_{d-1}$;
- comparing $\mathbf{T}(\mathsf{I})_{d-1}$ with $\mathbf{T}(\mathsf{I})_d$ deduce the elements $\tau X_n^d \in \mathbf{G}(\mathsf{I})$ and $\tau X_n^{d-1} \in \mathbf{C}^{\infty}(\mathsf{I})$;
- set $d := d-1$;

(b) having $\mathbf{T}(\mathsf{I})_d = \emptyset \neq \mathbf{T}(\mathsf{I})_{d+1}$ add $X_1^{\infty} \dots X_{n-1}^{\infty} X_n^d$ to $\mathbf{C}^{\infty}(\mathsf{I})$.

(4) (a) while $u < D$ do

- if $\bar{\upsilon} X_n^{u+1} \in \mathbf{T}(\mathsf{I})$ for all $\upsilon \in \mathbf{C}_u^{\infty}$ so that $\mathbf{T}(\mathsf{I})_u = \mathbf{T}(\mathsf{I})_{u+1}$ set $\mathbf{G}_{u+1} = \mathbf{G}_u, \mathbf{C}_{u+1} = \mathbf{C}_u, \mathbf{C}^{\infty}_{u+1} = \mathbf{C}^{\infty}_u$, $u := u+1$;
- otherwise
  - choose $\upsilon \in \mathbf{C}_u^{\infty}$ for which $\bar{\upsilon} X_n^{u+1} \in \mathbf{T}(\mathsf{I})$, set
    $$t := X_1 X_2 \dots X_{n-1}$$
    and compute the value ι s.t.
    $$\frac{\upsilon X_n^{d-1}}{t^{\iota}} \in \mathbf{T}(\mathsf{I}), \text{ while } \frac{\upsilon X_n^{d-1}}{t^{\iota+1}} \in \mathbf{N}(\mathsf{I});$$
  - apply the same procedure with input $\frac{\upsilon X_n^{d-1}}{t^{\iota}} \in \mathbf{T}(\mathsf{I})$ in order to deduce $\mathbf{G}_{u+1}$, $\mathbf{C}_{u+1}$ and $\mathbf{C}^{\infty}_{u+1}$;
  - comparing $\mathbf{T}(\mathsf{I})_u$ with $\mathbf{T}(\mathsf{I})_{u+1}$ deduce the elements $\tau X_n^{u+1} \in \mathbf{G}(\mathsf{I})$ and $\tau X_n^u \in \mathbf{C}^{\infty}(\mathsf{I})$;
  - set $u := u+1$;

(b) having $u = D$ and $\mathbf{T}(\mathsf{I})_j = \mathbf{T}(\mathsf{I})_D$ for all $j \geq D$ add τX_n^{∞} to $\mathbf{C}^{\infty}(\mathsf{I})$ for each $\tau \in \mathbf{C}_D^{\infty}$.

Example 13. Let $\mathscr{P} = \mathbb{F}[X,Y,Z]$, $\omega = XYZ$.
$\mathsf{I} = \mathbb{I}(XY^3Z^4, Y^5Z^2, X^3Y^2Z^2, X^4Z), D = 8$.

Of course $\mathbf{G}(\mathsf{I}) = \{XY^3Z^4, Y^5Z^2, X^3Y^2Z^2, X^4Z\}$ and

$$\mathbf{C}^{\infty}(\mathsf{I}) = \{X^{\infty}Y^{\infty}, X^3Y^{\infty}Z, X^2Y^4Z^3, X^2Y^2Z^{\infty}, X^3YZ^{\infty}, Y^4Z^{\infty}\}.$$

We have

$$\mathsf{I}_0 = \emptyset, \mathsf{I}_1 = \mathbb{I}(X^4), \mathsf{I}_3 = \mathsf{I}_2 = \mathbb{I}(Y^5, X^3Y^2, X^4),$$

and $\mathsf{I}_i = \mathbb{I}(Y^5, XY^3, X^3Y^2, X^4), i \geq 4$.

Since $\omega^2 \in \mathbf{N}(\mathsf{I}), \omega^3 \in \mathbf{T}(\mathsf{I})$ we draw I_3 (see Fig. 5) getting

$$\mathbf{G}_3 = \{Y^5, X^3Y^2, X^4\} \text{ and } \mathbf{C}_3^{\infty} = \{X^2Y^4, X^3Y\}.$$

Since, for $u = 4$, $X^2Y^4Z^4 \in \mathbf{T}(\mathsf{I})$ we draw I_4 (see Fig. 6) getting

$$\mathbf{G}_4 = \{Y^5, XY^3, X^3Y^2, X^4\} \text{ and } \mathbf{C}_4^{\infty} = \{Y^4, X^2Y^2, X^3Y\}$$

so that we enclose XY^3Z^4 in $\mathbf{G}(\mathsf{I})$ and $X^2Y^4Z^3$ in $\mathbf{C}^{\infty}(\mathsf{I})$.

Since $\mathsf{I}_D = \mathsf{I}_4$ we enlarge $\mathbf{C}^{\infty}(\mathsf{I})$ enclosing $Y^4Z^{\infty}, X^2Y^2Z^{\infty}, X^3YZ^{\infty}$.

For $d = 1$ we have $Y^5Z \in \mathbf{N}(\mathsf{I})$ (and also $X^3Y^2Z \in \mathbf{N}(\mathsf{I})$) so we draw I_1 (see Fig. 7) getting $\mathbf{G}_1 = \{X^4\}$ and $\mathbf{C}_1^{\infty} = \{X^3Y^{\infty}\}$.

We thus enclose Y^5Z^2 and $X^3Y^2Z^2$ in $\mathbf{G}(\mathsf{I})$. Since for $d = 0$, $X^4 \in \mathbf{N}(\mathsf{I})$ we obtain the final solution enclosing X^4Z to $\mathbf{G}(\mathsf{I})$ and both $X^3Y^{\infty}Z$ and $X^{\infty}Y^{\infty}$ in $\mathbf{C}^{\infty}(\mathsf{I})$. □

FIGURE 5

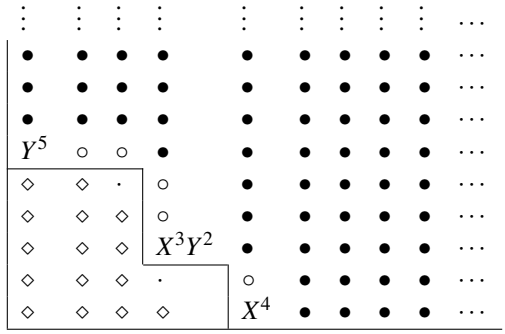


FIGURE 6

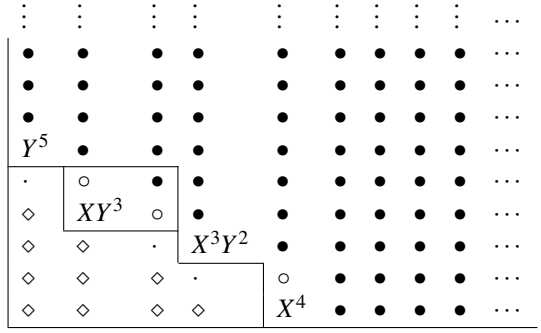
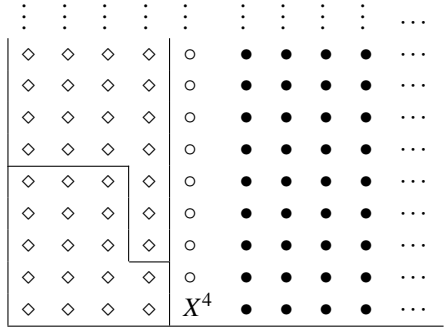


FIGURE 7



References

Ackermann, P. and Kreuzer, M. (2006). "Gröbner basis cryptosystems". *Applicable Algebra in Engineering, Communication and Computing* **17**(3-4), 173–194. DOI: 10.1007/s00200-006-0002-0.

Alonso, M. E., Marinari, M. G., and Mora, T. (2003). "The Big Mother of all Dualities: Möller Algorithm". *Communications in Algebra* **31**(2), 783–818. DOI: 10.1081/AGB-120017343.

Barkee, B., Ceria, M., Moriarty, T., and Visconti, A. (2020). "Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures". *Applicable Algebra in Engineering, Communications and Computing* **31**(3-4), 235–252. DOI: 10.1007/s00200-020-00428-w.

Bulygin, S. (2005). "Chosen-ciphertext attack on noncommutative Polly Cracker". arXiv: cs/0508015 [cs.IT].

Ceria, M. (2019a). "Bar Code and Janet-like division". arXiv: 1910.03572 [math.CO].

Ceria, M. (2019b). "Bar code for monomial ideals". *Journal of Symbolic Computation* **91**, 30–56. DOI: 10.1016/j.jsc.2018.06.012.

Ceria, M. (2020). *Half error locator polynomials for efficient decoding of binary cyclic codes*. (in preparation).

Ceria, M., Mora, T., and Sala, M. (2020). "HELP: a sparse error locator polynomial for BCH codes". *Applicable Algebra in Engineering, Communication and Computing* **31**, 215–233. DOI: 10.1007/s00200-020-00427-x.

Groebner, W. (1970). *Algebraische Geometrie*. Vol. 2. Bibliographisches Institut.

Janet, M. (1920). "Sur les systèmes d'équations aux dérivées partelles". *Journal de Mathématiques Pures et Appliquées* **3**, 65–151. URL: https://gallica.bnf.fr/ark:/12148/bpt6k1076122/f67n88.capture.

Janet, M. (1927). *Les systèmes d'équations aux dérivées partielles*. Mémorial des sciences mathématiques 21. Gauthier-Villars. URL: http://www.numdam.org/item/MSM_1927__21__1_0.

Laubenbacher, R. and Stigler, B. (2004). "A computational algebra approach to the reverse engineering of gene regulatory networks". *Journal of Theoretical Biology* **229**(4), 523–537. DOI: 10.1016/j.jtbi.2004.04.037.

Levy-dit-Vehel, F., Marinari, M. G., Perret, L., and Traverso, C. (2009). "A Survey on Polly Cracker Systems". In: *Gröbner Bases, Coding, and Cryptography*. Ed. by M. Sala, S. Sakata, T. Mora, C. Traverso, and L. Perret. Berlin, Heidelberg: Springer, pp. 285–305. DOI: 10.1007/978-3-540-93806-4_16.

Lundqvist, S. (2010). "Vector space bases associated to vanishing ideals of points". *Journal of Pure and Applied Algebra* **214**(4), 309–321. DOI: 10.1016/j.jpaa.2009.05.013.

Macaulay, F. S. (1913). "On the resolution of a given modular system into primary systems including some properties of Hilbert numbers". *Mathematische Annalen* **74**(1), 66–121. DOI: 10.1007/BF01455345.

Macaulay, F. S. (1916). *The Algebraic Theory of Modular Systems*. Cambridge Tracts in Mathematics and Mathematical Physics 19. Cambridge University Press. URL: https://archive.org/details/algebraictheoryo00macauoft.

Marinari, M. G., Möller, H. M., and Mora, T. (1993). "Gröbner bases of ideals defined by functionals with an application to ideals of projective points". *Applicable Algebra in Engineering, Communication and Computing* **4**(2), 103–145. DOI: 10.1007/BF01386834.

Mora, T. (2003). *Solving Polynomial Equation Systems I. The Kronecker-Duval Philosophy*. Vol. 1. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511542831.

Mora, T. (2005). *Solving Polynomial Equation Systems II. Macaulay's Paradigm and Gröbner Technology*. Vol. 2. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9781107340954.

Mora, T. (2015). *Solving Polynomial Equation Systems III. Algebraic Solving*. Vol. 3. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9781139015998.

Mora, T. (2016). *Solving Polynomial Equation Systems IV. Buchberger Theory and Beyond*. Vol. 4. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9781316271902.

Mora, T. (2018). "An FGLM-like algorithm for computing the radical of a zero-dimensional ideal". *Journal of Algebra and its Applications* **17**(1), 1850002. DOI: 10.1142/S0219498818500020.

Mourrain, B. (2005). "Bezoutian and quotient ring structure". *Journal of Symbolic Computation* **39**(3-4), 397–415. DOI: 10.1016/j.jsc.2004.11.010.

Rapallo, F. and Rogantin, M. P. (2017). "Algebraic characterization of regular fractions under level permutations". arXiv: 1705.01340v1 [stat.ME].

Rouillier, F. (1999). "Solving zero-dimensional systems through the rational univariate representation". *Applicable Algebra in Engineering, Communication and Computing* **9**(5), 433–461. DOI: 10.1007/s002000050114.

---

[a] Universidad Complutense de Madrid,
Departamento de Álgebra, Geometría y Topología,
Facultad de Ciencias Matemáticas,
Madrid, Spain

[b] Università degli Studi di Genova,
Dipartimento di Matematica,
Genova, Italy

* To whom correspondence should be addressed | email: theomora@disi.unige.it

Communicated 6 June 2019; manuscript received 19 August 2019; published online 28 October 2020