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 $I$ w.r.t. a term-ordering $≺$ 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 $τ \in T$, returns its canonical form $\text{Can}(τ, I, ≺)$ w.r.t. the unknown ideal $I$ and term-ordering $≺$. 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, $\mathcal{P} := \mathbb{F}(X_1, \ldots, X_n)$,
- the related word monoid $T := \langle X_1, \ldots, X_n \rangle$, and
- a finite set $G := \{g_1, \ldots, g_l\} \subset \mathcal{P}$ of polynomials which are known to be members of an ideal $I$,

compute, w.r.t. a Noetherian semigroup ordering $≺$ on $T$,

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

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

given a term $τ \in T$ returns its canonical form $\text{Can}(τ, I, ≺)$ w.r.t. such ideal $I$ and term-ordering $≺$.

□
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 \( \mathcal{P} := \mathbb{F}[X_1, \ldots, X_n] \), 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, \( \mathcal{P} := \mathbb{F}[X_1, \ldots, X_n] \), and denoting by

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

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

\[
D \geq d(I) := \max\{\deg(\gamma) : \gamma \in \Gamma(I)\},
\]

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

- given a term \( \tau \in \mathcal{T} \) returns its *canonical form* \( \text{Can}(\tau, I, \prec) \) w.r.t. the ideal \( I \) and the semigroup ordering \( \prec \). \( \square \)

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* \( \mathcal{N}(I) := \mathcal{T} \setminus T(I) \) (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 combinatorial, solution.

1. **Notation and recalls on Gröbner Bases**

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

---

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

2Since a semigroup in general has not necessarily a unity, with this formulation we want to be free of the irrelevant requirement that \( \tau | \omega \implies \tau \prec \omega \).
Each \( f \in \mathcal{P} \) can be uniquely (Mora 2016, p. 7) expressed as

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

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

\[
T(f) := \max\{ \tau \in \text{supp}(f) \}, \quad \text{l}c(f) := c(f, T(f)) \quad \text{and} \quad M(f) := \text{l}c(f)T(f).
\]

For each ideal \( I \subset \mathcal{P} \), we also consider:
- the semigroup ideal (Mora 2016, Def. 46.1.4) \( T(I) := \{ T(f) : f \in I \} \),
- the Gröbner sous-escalier (Mora 2016, Def. 46.1.41) \( N(I) := \mathcal{T} \setminus T(I) \),
- the vector-space (Mora 2016, Lemma 46.1.42) \( \mathbb{F}[N(I)] := \text{Span}_\mathbb{F}(N(I)) \),
- \( G(I) \subset T(I) \) the unique minimal basis (Mora 2016, Cor. 46.1.44) of \( T(I) \).

We recall that for \( f \in \mathcal{P} \) and \( G \subset \mathcal{P} \),
- \( f \) has Gröbner representation (Mora 2016, Def. 50.4.3) in terms of \( G \) if
  \[
f = \sum_{i=1}^{\mu_f} c_i \lambda_i g_{i,j} \rho_i, \quad c_i \in \mathbb{F} \setminus \{ 0 \}, \lambda_i, \rho_j \in \mathcal{T}, g_{i,j} \in G, \mu_f \in \mathbb{N}
\]
  with \( T(f) = \lambda_1 T(g_{i,j}) \rho_1 \succ \cdots \succ \lambda_{\mu_f} T(g_{i,j}) \rho_{\mu_f} \succ \cdots \);
- \( h := NF(f, G, \prec) \in \mathcal{P} \) 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 \( h \neq 0 \Rightarrow T(h) \notin \{ \lambda T(g) : \lambda, g \in G \} =: T(G) \).
- For each \( f \in \mathcal{P} \), there is a unique canonical form (Mora 2016, Def. 46.1.43) \( g := \text{Can}(f, I, \prec) = \sum_{\tau \in N(I)} \gamma(f, \tau) \tau \in \mathbb{F}[N(I)] \) s.t. \( f - g \in I \).
- A Gröbner basis of \( I \) (Mora 2016, Def. 46.1.17) is any set \( \Gamma \subset I \) s.t. \( \{ T(\gamma) : \gamma \in \Gamma \} \) generates \( T(I) \).
- The reduced Gröbner basis (Mora 2016, Cor. 46.1.44) of \( I \) is the set \( \Gamma(I) := \{ \tau - \text{Can}(\tau, I, \prec) : \tau \in G(I) \} \).

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 \( I \subset \mathcal{P} \), a set \( G \subset I \) and an element \( f \in \mathcal{P} \), Buchberger reduction (Mora 2016, Alg. 46.1.37) returns a normal form \( h \in \mathcal{P} \); if \( f \in I \) and \( G \) is a Gröbner basis of \( I \) necessarily \( h = 0 \); if we know that \( f \in I \) and \( h \neq 0 \), then necessarily
  \( h = f - (f-h) \in I \).
- \( G \) is not a Gröbner basis of \( I \), since \( T(h) \in T(I) \setminus T(G) \),
- \( G \cup \{ h \} \) 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 \( S \subset I \) (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
Remark 4. Thus, the difficult (theoretically and algorithmically) part of the computation of the required minimal reduced Gröbner basis $\Gamma(l)$ has been reduced, through the swindler abuse of the “oracle”, to the more elementary combinatorial problem of producing the minimal monomial basis $G(l)$. 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 et al. 2003), 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 degroebnerizing effective ideal theory, provides several efficient combinatorial tools for producing the expected minimal basis $G(l)$ and the required minimal reduced Gröbner basis $\Gamma(l)$ to $l$ can be obtained using (1) thanks of Lundqvist’s approach (Lundqvist 2010).

2. Oracle-supported Approximation of $\Gamma(l)$

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

- for each term $\nu \in \mathcal{T}$ and variables $X_l, X_r$, since $G(l)$ is the unique minimal basis (Mora 2016, Cor. 46.1.44) of $T(l)$, we have by definition
  \[ X_l \nu X_r \in G(l) \iff X_l \nu \in N(l), \nu X_r \in N(l), X_l \nu X_r \in T(l); \]  
  \[ \text{(2)} \]

- for each term $\nu \in \mathcal{T}$ and each variable $X$, since $N(l) := \mathcal{T} \setminus T(l)$, we have
  \[ \omega = \nu X \in N(l) \implies \nu \in N(l), \omega = X \nu \in N(l) \implies \nu \in N(l). \]  
  \[ \text{(3)} \]

If we ask our oracle the value of $\text{Can}(\tau, l, \prec)$ for any term $\tau \in \mathcal{T}$, we can deduce whether

1. $\tau \in T(l)$, in which case we obtain also $\text{Can}(\tau, l, \prec)$, or
2. $\tau \in N(l)$ "id est $\tau = \text{Can}(\tau, l, \prec)$.

Procedure 5. By assumption, we are given the sets
\[ \text{supp}(g_j), g_j \in G, \]
so that, without needing to know the term-ordering \( \prec \), we can deduce the sets
\[ T_j := \{ \tau \in \text{supp}(g_j) : \tau \upharpoonright \omega, \forall \omega \in \text{supp}(g_j) \}. \]
Since for each \( j \), there are \( \tau \in T_j, \lambda, \rho \in \mathcal{T} : \tau = \lambda T(f) \rho \) for some \( f \in \Gamma(1) \) e.g. \( \tau := T(g_j) \in T(1) \), we can produce a scheme, based on Equation (2), which in a finite number of steps produces an element of \( \Gamma(1) \); we choose a set \( T_j \) and repeatedly we

- pick an element \( \tau \in T_j \); if \( \tau \notin T(1) \), simply remove it, otherwise:
  - for \( \tau = X_i \omega \in T(1) \) we test, querying the oracle, whether \( \omega \in T(1) \) in which case we set \( \tau := \omega \) and repeat until we have an element \( \tau = X_i \omega \in T(1) \) for which \( \omega \in N(1) \);
  - now, for \( \omega = \upsilon X_r \in N(1) \) we test whether \( X_i \upsilon \in T(1) \), in which case we set \( \omega := \upsilon \in N(1) \) and repeat until we have an element \( \tau := X_i \upsilon X_r \) for which

\[ X_i \upsilon \in N(1), \upsilon X_r \in N(1), X_i \upsilon X_r \in T(1) \]

_id est_, thanks of (3), \( X_i \upsilon X_r \in G(1) \).

Remarking that we also have
\[ G(1) \ni X_i \upsilon X_r \mid \tau \in \text{supp}(g_j), \]
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 \( \tau \in G(1) \) and the polynomial \( \text{Can}(\tau, 1, \prec) \),
- set \( H := H \cup \{ \tau - \text{Can}(\tau, 1, \prec) \} \), \( G := \{ NF(g, H) : g \in G \} \)

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 \( h, h = \tau - \text{Can}(\tau, 1) \in \Gamma(1) \) and \( T(h) = \tau := X_i \upsilon X_r \in G(1) \).

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 \( \Gamma(1) \) (commutative case)

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

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

• the unique minimal basis of $T(l)$, $G(l) \subset B(l)$, is characterized as (Mora 2005, Lemma 29.3.2)

$$G(l) := \{ \tau \in B(l) : \forall 1 \leq i \leq n, \frac{T_i}{X_i} \in N(l) \}.$$  

• $C(l) := \{ \tau \in N(l) : \forall 1 \leq i \leq n, X_i \tau \in T(l) \} \subset N(l)$ is its corner set (Mora 2005, Def. 29.1.1). If $I$ is 0-dimensional, $C(l)$ "generates" $N(l)$ in the sense that (Alonso et al. 2003)

$$\omega \in N(l) \iff \exists \tau \in C(l) : \omega | \tau.$$  

• For each $f_1, f_2 \in \mathcal{P}$, the S-polynomial of $f_1$ and $f_2$ (Mora 2005, Def. 22.4.1) is

$$S(f_1, f_2) := \text{lcm}(f_2)^{-1} \delta(f_1, f_2) \frac{T(f_2)}{f_2} \text{lcm}(f_1)^{-1} \frac{T(f_1)}{f_1} f_1,$$

where $\delta := \delta(f_1, f_2) := \text{lcm}(T(f_1), T(f_2))$.

• 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 $f, g, h \in \mathcal{P}$: $T(h) | \text{lcm}(T(f), T(g))$, 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 $d(l) := \max \{ \deg(\zeta) : \zeta \in G(l) \}$.

**Remark 6.** To graphically visualize the situation we identify $\mathcal{I}$ with $\mathbb{N}^n$ in the following way:

$$X_{i1}^{a_1} \cdots X_{in}^{a_n} \leftrightarrow \{(a_1, \ldots, a_n) \in \mathbb{R}^n : a_i \in \mathbb{N}, 1 \leq i \leq n \};$$

by ‘line’ (and one should better say ‘half-line’) of $\mathcal{I}$ 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 $l := \mathbb{I}(X_1^0, X_1^1X_2^3, X_2^5) \subset \mathcal{P}$ denoting

• $\diamond N(l) := \mathcal{I} \setminus T_{<}(M)$ its Gröbner éscalier;

• $\diamond B(l) := \{ X_h \tau : 1 \leq h \leq n, \tau \in N(l) \} \setminus N(l)$, its border set;

• $\bullet J(l) := T(l) \setminus B(l)$;

• $\diamond G(l) \subset B(l)$ the unique minimal basis of $T(l)$;

• $\bullet C(l) := \{ \tau \in N(l) : X_h \tau \in T(l), \forall h \}$ its corner set.
We point out that:
- for $n = 2$, $B(l)$ is a ‘piecewise linear curve’ $\mathcal{C}(l)$ 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 $n \geq 3$, $B(l)$ 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;
- $J(l)$ is the set of points lying above the escalier;
- $G(l)$ consists of the ‘concave vertices’ of the escalier;
- $N(l)$ 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 $G(l)$ are particular “0-dimensional” points.

**Remark 7.** For any ideal $l \subset \mathcal{P}$, Noetherian semigroup ordering $<$, and degree value $\delta \in \mathbb{N}$ s.t. $\delta \leq d(l) - 1$, setting $H := \{ g \in \Gamma(l), \deg(g) \leq \delta \}$ the two ideals $l$ and $I_\delta := \{ (H) \}$ satisfy both:
\[ \{ f \in l : \deg(f) \leq \delta \} = \{ f \in I_\delta : \deg(f) \leq \delta \} \text{ and } I_\delta \subset l, \]
with
\[ d(l) \geq \delta + 1 > \delta \geq d(I_\delta). \]

Thus, the algorithm we are going to sketch below, applied to the (unknown) ideal $l$, returns the correct answer $l$ if the input data satisfy $D \geq \delta + 1$, but returns the wrong answer $I_\delta$ if $D \leq \delta < d(l)$. That is, we actually need to assume to know an upper bound $D$ for $d(l)$ and only deal with terms belonging to the box
\[ \mathcal{B}(D) := \{ X_1^{a_1} \cdots X_n^{a_n} \in \mathcal{T} : 0 \leq a_i \leq D, \forall 1 \leq i \leq n \}. \]

**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
\[ C^{\infty}(l) \subset \{ X_1^{a_1} \cdots X_n^{a_n}, a_i \in \mathbb{N} \cup \{ \infty \} \} \]
which satisfies
\[ \omega \in N(l) \iff \text{ exists } \tau \in C^{\infty}(l) : \omega \mid \tau. \]

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

---

\(^3\)As $B(l) \cup \{ \text{all the convex vertices} \}$ 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 \( \mathcal{P} = \mathbb{F}[X_1, \ldots, X_n] \), with \( \deg(X_i) = 1, \forall 1 \leq i \leq n \), a strong solution returning the complete basis of an ideal \( I \subset \mathcal{P} \) cannot be produced, unless further knowledge is assumed: in fact, given \( I \subset \mathbb{F}[X_1, \ldots, X_n] \) and a value \( \delta \in \mathbb{N}, \delta < d(I) \), in general there are smaller ideals (see Remark 7) \( I_\delta \subsetneq I \) which satisfy
\[
\{ f \in I : \deg(f) \leq \delta \} = \{ f \in I_\delta : \deg(f) \leq \delta \}.
\]
Some concrete examples can be easily produced by taking\(^5\) any ideal \( J \subset \mathcal{P}, d(J) \leq \delta - 1 \) and any element \( h_0 \in J \setminus X_2J \); then, as we verify below, necessarily
\[
X_2J =: I_\delta \subsetneq I := X_2J + (h_0)
\]
satisfy (4).

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

Enumerate the variables and the Gröbner basis elements in such a way that \( X_1 \prec X_2 \prec \ldots \prec X_n \) and
\[
i < j \iff \begin{cases} \deg(\gamma_i) > \deg(\gamma_j) \text{ or} \\ \deg(\gamma_i) = \deg(\gamma_j) \text{ and } T(\gamma_i) > T(\gamma_j). \end{cases}
\]
Denoting
\[
\Omega := \min_{\prec} \{ \tau \in T(I), \deg(\tau) = \delta + 1 \}
\]
and \( d_i := \deg(\gamma_i) < \delta \), by definition we necessarily have
\[
\Omega = X_i^{\delta+1-d_i} T(\gamma_i).
\]
We also let \( h_0 := \Omega - \text{Can}(\Omega, J, \prec) \), so that \( \text{lcm}(h_0) = 1, T(h_0) = \Omega = X_i^{\delta+1-d_i} T(\gamma_i) \), 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 \( \ideal I(H) = X_2J + (h_0) \).

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

Moreover, since \( \Omega = T(h_0) = X_i^{\delta+1-d_i} T(\gamma_i) \) and
\[
T(h_j) = X_2 T(\gamma_j) \mid \text{lcm}(T(h_j), \Omega) = X_i^{\delta+1-d_i} X_2 \text{lcm}(T(\gamma_j), T(\gamma_j)), 1 \leq j < s,
\]
as a direct consequence of Buchberger’s Second Criterion, in order to prove the claim it is sufficient to show that the S-polynomial \( S(h_j, h_0) \) 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 \( \exists \mu = \mu_{h_0}, \ell_\alpha \in \mathbb{N}, 1 \leq \ell_\alpha \leq s, c_\alpha \in \mathbb{F} \setminus \{0\}, \tau_\alpha \in \mathcal{F}, \) s.t. we have a Gröbner representation
\[
J \ni h_0 = \Omega - \text{Can}(\Omega, J, \prec) = \text{lc}(\gamma_s)^{-1}X_1^{\delta+1-d_s}\gamma_s + \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha \gamma_\alpha
\]
where \( \gamma_\alpha \in \Gamma(J) \) and
\[
\Omega = X_1^{\delta+1-d_s}T(\gamma_s) \succ \tau_1T(\gamma_{i_1}) \succ \tau_2T(\gamma_{i_2}) \succ \cdots;
\]
thus we trivially obtain the required Gröbner representation
\[
S(h_s, h_0) = \text{lc}(h_0)^{-1}\frac{\delta(h_s, h_0)}{T(h_0)} - h_0 = \frac{\delta(h_s, h_0)}{T(h_s)} h_s = X_2h_0 - \text{lc}(\gamma_s)^{-1}X_1^{\delta+1-d_s}(X_2\gamma_s) = X_2 \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha \gamma_\alpha = \sum_{\alpha=1}^{\mu} c_\alpha \tau_\alpha h_\alpha
\]
where
\[
\delta(h_s, h_0) = \text{lcm}(T(h_s), T(h_0)) = \text{lcm}(X_2T(\gamma_s), X_1^{\delta+1-d_s}T(\gamma_s)) = X_1^{\delta+1-d_s}X_2T(\gamma_s).
\]
\( \square \)

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 \( \omega \) we consider, the required information whether \( \omega \in \mathbb{N}(l) \) or \( \omega \in \mathbb{T}(l) \) is trivially deduced by the (ab)use of the oracle.

Let \( \omega = X_1 \cdots X_n \), as \( \omega^0 = 1 \in \mathbb{N}(l) \), we take iteratively \( \omega^{i+1}, i \in \mathbb{N} \), until either \( \omega^D \in \mathbb{N}(l) \) or we find \( j \in \mathbb{N}, j \leq D, \) such that \( \omega^{j-1} \in \mathbb{N}(l) \) and \( \omega^j \in \mathbb{T}(l) \).

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

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

3.3.1. Two variables.

Remark 10. Since \( \mathbf{l} \neq (0) \), 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
\[
\mathbb{G}(l) = \{\tau_i, 1 \leq i \leq s\}.
\]
As a consequence we also have
\[
\mathbb{C}(l) = \{X_1^{a_1-1}X_2^{b_2-1}, X_1^{a_2-1}X_2^{b_3-1}, \ldots, X_1^{a_s-1}X_2^{b_1-1}\};
\]
\( \mathbb{C}^\infty(l) \) is then obtained adding \( X_1^{a_1}X_2^{b_1-1} \) if \( b_1 > 0 \) and \( X_1^{a_1-1}X_2^\infty \) if \( a_s > 0. \) \( \square \)

\(^6\)In fact each term \( \tau \) with \( \deg(\tau) \leq D \) trivially satisfies \( \tau \mid \omega^D, \) i.e. \( \omega^D \in \mathbb{N}(l) \) implies \( \mathbb{G}(l) = \emptyset. \)
The correctness and completeness of the procedure is definitely trivial: assume to be on the top \( \omega \) 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 \( \omega = X_1^i X_2^j \in B(l) \) and

1. decides whether \( \omega \in G(l) \);
2. lists all the terms \( \tau = X_1^c X_2^d \in G(l) \cup C^\infty(l) \) with \( c \geq j \),
3. lists all the terms \( \tau = X_1^c X_2^d \in G(l) \cup C^\infty(l) \) with \( d \geq j \),

as follows

1. \( \omega \in G(l) \iff \#P = 0 \iff \frac{\omega}{X_1} \in N(l) \) and \( \frac{\omega}{X_2} \in N(l) \).
2. if \( \omega \in G(l) \), iteratively testing whether

\[
\frac{X_1^i}{X_2^j} \omega = X_1^{a+i} X_2^{b-1} \in T(l), 1 \leq i \leq D - a - b + 2,
\]

find the value \( i \) for which \( \frac{X_1^i}{X_2^j} \omega \in N(l) \) and either \( i + a + b - 1 = D \) or \( \frac{X_1^{i+1}}{X_2} \omega \in T(l) \):

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

- if \( \frac{\omega}{X_1} \in T(l) \) and \( \frac{\omega}{X_2} \in N(l) \) (and thus \( \omega \) belongs to an horizontal segment of \( B(l) \)), again we, iteratively testing whether

\[
\frac{X_1^i}{X_2^j} \omega = X_1^{a+i} X_2^{b-1} \in T(l), 1 \leq i \leq D - a - b + 2,
\]

find the value \( i \) for which \( \frac{X_1^i}{X_2^j} \omega \in N(l) \) and either \( i + a + b - 1 = D \) or \( \frac{X_1^{i+1}}{X_2^j} \omega \in T(l) \):

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

- if \( \frac{\omega}{X_1} \in N(l) \) and \( \frac{\omega}{X_2} \in T(l) \) (and thus \( \omega \) belongs to a vertical segment of \( B(l) \)), we, iteratively testing whether

\[
\frac{\omega}{X_1} = X_1^{a} X_2^{b-i} \in T(l), i \leq b,
\]

find the value \( i \) for which \( \frac{\omega}{X_1} \in T(l) \) and either \( i = b \) or \( \frac{\omega}{X_1^{i+1}} \in N(l) \); in both cases we deduce that \( \frac{\omega}{X_1} = X_1^{a} X_2^{b-i} \in G(l) \) and we insert it there; moreover

- if \( i = b \), so that \( \frac{\omega}{X_1} = X_1^{a} \in G(l) \), the subprocedure 2. is completed;
• if, instead, $\frac{\omega}{X_1^i} \in N(l)$, the subprocedure 2. restarts with $\omega := X_1^{a-i}X_2^{b-i}$.

• $\frac{\omega}{X_1^i} \in N(l)$ and $\frac{\omega}{X_2^i} \in N(l)$ since $\omega \in T(l)$ we can deduce that $\frac{\omega}{X_1^iX_2^j} \in C(l)$ and

○ we insert it there;

○ iteratively testing whether

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

we find the value $i$ for which $\frac{\omega}{X_1^i} \in T(l)$ and either $i = a$ or $\frac{\omega}{X_1^iX_2^j} \in N(l)$; in both cases we deduce that

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

and we insert it there; moreover

* if $i = a$, so that $\frac{\omega}{X_1^i} = X_2^b \in G(l)$, the complete procedure terminates

** returning both $G(l)$ and $C^{\infty}(l)$

* if, instead, $\frac{\omega}{X_1^iX_2^j} \in N(l)$, the subprocedure 2. restarts with $\omega := X_1^{a-i}X_2^{b-i}$.

(3) • if $\omega \in G(l)$, iteratively testing whether

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

find the value $i$ for which $\frac{X_1^i}{X_1^i} \omega \in N(l)$ and either $i + a + b - 1 = D$ or $\frac{X_1^{i+1}}{X_1^i} \omega \in T(l)$:

○ if $i + a + b - 1 = D$, since $\deg(\frac{X_1^i}{X_1^i} \omega) = D$ and $\frac{X_1^i}{X_1^i} \omega \in N(l)$ we can deduce

that $\frac{X_1^i}{X_1^i} \omega \in N(l)$ for each $i \in N$ and thus we enclose $X_1^{a-1}X_2^{\infty}$ in $C^{\infty}(l)$ and

the subprocedure 3. terminates;

○ if, instead, $\frac{X_1^{i+1}}{X_1^i} \omega \in T(l)$, then $\frac{X_1^i}{X_1^i} \omega \in C^{\infty}(l)$ and the subprocedure 2.

restarts with $\omega := X_1^{a-i}X_2^{b+i+1}$.

• if $\frac{\omega}{X_2^i} \in T(l)$ and $\frac{\omega}{X_1^i} \in N(l)$, again we, iteratively testing whether

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

find the value $i$ for which $\frac{X_1^i}{X_1^i} \omega \in N(l)$ and either $i + a + b - 1 = D$ or $\frac{X_1^{i+1}}{X_1^i} \omega \in T(l)$:

○ if $i + a + b - 1 = D$, we can deduce that $\frac{X_1^i}{X_1^i} \omega \in N(l)$ for each $i \in N$ and thus

we enclose in $X_2^{\infty}X_1^{b-1}$ in $C^{\infty}(l)$ and

the subprocedure 3. terminates;

○ if, instead, $\frac{X_1^{i+1}}{X_1^i} \omega \in T(l)$, then we insert $\frac{X_1^i}{X_1^i} \omega$ in $C^{\infty}(l)$ and the sub-

procedure 2. restarts with $\omega := X_1^{a-i}X_2^{b+i+1}$.
• if $\frac{\omega}{X_2^i} \in \mathbb{N}(l)$ and $\frac{\omega}{X_1^i} \in \mathbb{T}(l)$, we, iteratively testing whether

$$\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbb{T}(l), i \leq a,$$

find the value $i$ for which $\frac{\omega}{X_1^i} \in \mathbb{T}(l)$ and either $i = a$ or $\frac{\omega}{X_1^{a-i}} \in \mathbb{N}(l)$; in both cases we deduce that $\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbb{G}(l)$ and we insert it there; moreover

○ if $i = a$, so that $\frac{\omega}{X_1^i} = X_2^b \in \mathbb{G}(l)$, the subprocedure 2. is completed;

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

• $\frac{\omega}{X_1^i} \in \mathbb{N}(l)$ and $\frac{\omega}{X_2^i} \in \mathbb{N}(l)$ since $\omega \in \mathbb{T}(l)$ we can deduce that $\frac{\omega}{X_1^iX_2^i} \in \mathbb{C}(l)$ and

○ we insert it there;

○ iteratively testing whether

$$\frac{\omega}{X_1^i} = X_1^{a-i}X_2^b \in \mathbb{T}(l), i \leq a,$$

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

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

and we insert it there; moreover

* if $i = a$, so that $\frac{\omega}{X_1^i} = X_2^b \in \mathbb{G}(l)$, the procedure terminates returning both $\mathbb{G}(l)$ and $\mathbb{C}^\omega(l)$

* if, instead, $\frac{\omega}{X_1^i} \in \mathbb{N}(l)$, the subprocedure 2. restarts with $\omega := X_1^{a-i}X_2^{b-1}$.

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

(1) $l = (X^4Y, X^2Y^2, XY^3, Y^8), D = 8$ (see Fig. 2).

We have $\omega_1 \in \mathbb{N}(l)$, $\omega_2 \in \mathbb{T}(l)$ and $XY^2, X^2Y \in \mathbb{N}(l)$, thus $\omega^2 \in \mathbb{G}(l)$.

Considering $X^{2+i}Y, i \leq D - 2$ we find, successively, $X^4Y \in \mathbb{G}(l)$ and $X^3Y \in \mathbb{C}(l)$; next evaluating $X^5, X^6, X^7, X^8$, since $X^8 \in \mathbb{N}(l)$ we deduce $X^\omega \in \mathbb{C}^\omega(l)$.

Next considering $XY^{2+i}$, we find, successively, $XY^3 \in \mathbb{G}(l)$ and $XY^2 \in \mathbb{C}(l)$; next evaluating $Y^5, Y^6, Y^7, Y^8$, we obtain $Y^8 \in \mathbb{G}(l)$ and $Y^7 \in \mathbb{C}(l)$.

(2) $l = (X^3Y^2), D = 5$ (see Fig. 3).

We have $\omega_1, \omega_2 \in \mathbb{N}(l), \omega_3 \in \mathbb{T}(l)$ with $X^2Y^3 \in \mathbb{N}(l)$ and $X^3Y^2 \in \mathbb{T}(l)$.

Thus we have to consider $X^3Y^3-i, 0 < i \leq 3$, getting $X^3Y^2 \in \mathbb{G}(l)$; next computing $X^2Y^3 \in \mathbb{N}(l)$ we have $X^2Y^\omega \in \mathbb{C}^\omega(l)$; finally computing $X^{2+i}Y, 0 < i \leq 2$ we find $X^4Y \in \mathbb{N}(l)$ and $X^\omega Y \in \mathbb{C}^\omega(l)$.

(3) $l = (X^4Y^3, X^2Y^4), D = 7$ (see Fig. 4). We have $\omega_1, \omega_2, \omega_3 \in \mathbb{N}(l), \omega_4 \in \mathbb{T}(l)$ with $X^3Y^4, X^4Y^3 \in \mathbb{T}(l)$. Since $X^4Y^2 \in \mathbb{N}(l)$, we deduce $X^4Y^3 \in \mathbb{G}(l)$; next considering $X^5Y^2 \in \mathbb{N}(l)$ we obtain $X^\omega Y^2 \in \mathbb{C}^\omega(l)$.

Next reconsidering $X^3Y^4 \in \mathbb{T}(l)$ we first deduce that $X^3Y^3 \in \mathbb{C}(l)$ and further the computation of $X^{2+i}Y^4 \in \mathbb{T}(l)$ and $XY^4 \in \mathbb{N}(l)$ imply $X^2Y^4 \in \mathbb{G}(l)$. Finally since $XY^5, XY^6 \in \mathbb{N}(l)$, we obtain $XY^\omega \in \mathbb{C}^\omega(l)$. 

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 \( T(I)_j, j \in \mathbb{N}, \) of \( T(I) \subset \mathcal{T} : \)

\[
T(I)_j := \{ \tau = X_1^{a_1} X_2^{a_2} \cdots X_{n-1}^{a_{n-1}} : \tau X_j \in T(I) \} \subset \mathcal{T}' := \mathcal{T} \cap \mathbb{K}[X_1, X_2, \ldots X_{n-1}]
\]

\(^7\) More precisely, also the case \( n = 2 \) is just the specialization to the trivial case of the general approach; we considered didactically better to present it differently and with more details.
which satisfy $T(l)_j \subseteq T(l)_{j+1}$ so that, by Noetherianity there are finitely many positive integers $0 \leq b_1 < b_2 < \ldots < b_s \leq D$ for which

\[ \emptyset \subseteq T(l)_{b_1} \subseteq T(l)_{b_2} \subseteq \ldots \subseteq T(l)_{b_s} = T(l)_{b_s+1} = \ldots = T(l)_{D} = \ldots \]

Mainly, in order to deduce the generating set $G(l)$ and the corner sets $C(l)$ and $C^\infty(l)$ of $l$, we will consider the relations among the corresponding sets of $T(l)_j$ which we will denote $G_j$, $C_j$ and $C^\infty_j$ 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. $T(l)_j = T(l)_{j+1} \iff G_j = G_{j+1}, C_j = C_{j+1}, C^\infty_j = C^\infty_{j+1}$;
2. $\tau X^j_{d} \in G(l) \iff \tau \in C_j$;
3. $\tau X_{n-1}^{j-1} \in C(l) \iff \tau \in C_j$;
4. $\tau X_{n-1}^{j-1} \in C^\infty(l) \iff \tau \in C^\infty_j$ and $\tau \in T(l)_j$. \hfill $\Box$

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

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

in order to describe $T(l)_j$ and produce $G_j$, $C_j$ and $C^\infty_j$;
2. sets $u := d := j, G_u := G_d := G_j, C_u := C_d := C_j, C^\infty_u := C^\infty_d := C^\infty_j$;
3. list all terms $\tau X^d_{n-1} \in C_d$, $d \leq j$;
4. list all terms $\tau X^u_{u} \in C_u, u \geq j$.

as follows, where, for each $\nu := X_1^{a_1} X_2^{a_2} \ldots X_{n-1}^{a_{n-1}}, a_i \in \mathbb{N} \cup \{\infty\}$ we denote by $\bar{\nu} := X_1^{b_1} X_2^{b_2} \ldots X_{n-1}^{b_{n-1}} \in T(l)'$ 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 $J := \{X_1^a X_2^b : X_1^a X_2^b X_3^j \ldots X_{n-1}^j X_n^j\}$ through a series of queries $[\nu \in T(l) ?]$ of course each such query should be formulated as $[\nu X_3^j \ldots X_{n-1}^j X_n^j \in T(l) ?]$.

2. (a) while $T(l)_{d} \neq \emptyset$ do
   
   - if $\nu X_{n-1}^{d-1} \in T(l)$ for all $\nu \in G_d$, so that $T(l)_{d-1} = T(l)_d$ set $G_{d-1} = G_d, C_{d-1} = C_d, C^\infty_{d-1} = C^\infty_d, d' := d - 1$;
   
   - otherwise
     
     - choose $\nu \in G_d$ for which $\nu X_{n-1}^{d-1} \in N(l)$, set
       
       \[ \nu := X_1^1 X_2^1 \ldots X_{n-1}^1 \]

     and compute the value $t$ s.t.
  
  \[ \nu t X_{n-1}^{d-1} \in T(l), \nu t' X_{n-1}^{d-1} \in N(l); \]

Example 13. Let \( \mathcal{P} = \mathbb{F}[X, Y, Z] \), \( \omega = XYZ \).
\( l = \{XY^3Z^4, Y^5Z^2, X^3Y^2Z^2, X^4Z\} \)

Of course \( G(1) = \{XY^3Z^4, Y^5Z^2, X^3Y^2Z^2, X^4Z\} \) and
\[ C^\infty(1) = \{X^\infty Y^\infty, X^3 Y^\infty Z, X^2 Y^4 Z^3, X^2 Y^2 Z^\infty, X^3 YZ^\infty, Y^4 Z^\infty\}. \]

We have
\[ l_0 = \emptyset, l_1 = \{X^4\}, l_2 = l_3 = \{Y^5, X^3Y^2, X^4\}, \]
and \( l_i = \{Y^5, XY^3, X^3Y^2, X^4\}, i \geq 4 \).

Since \( \omega^2 \in N(1), \omega^3 \in T(1) \) we draw \( l_3 \) (see Fig. 5) getting
\[ G_3 = \{Y^5, X^3Y^2, X^4\} \text{ and } C^\infty_3 = \{X^2 Y^4, X^3 Y^3\}. \]

Since, for \( u = 4 \), \( X^2 Y^4 Z^4 \in T(1) \) we draw \( l_4 \) (see Fig. 6) getting
\[ G_4 = \{Y^5, XY^3, X^3Y^2, X^4\} \text{ and } C^\infty_4 = \{Y^4, X^2 Y^2, X^3 Y^3\} \]
so that we enclose \( XY^3 Z^4 \) in \( G(1) \) and \( X^2 Y^4 Z^4 \) in \( C^\infty(1) \).

Since \( l_D = l_4 \) we enlarge \( C^\infty(1) \) enclosing \( Y^4 Z^\infty, X^2 Y^2 Z^\infty, X^3 YZ^\infty \).

For \( d = 1 \) we have \( Y^5 Z^2 \in N(1) \) (and also \( X^3 Y^2 Z \in N(1) \)) so we draw \( l_1 \) (see Fig. 7) getting
\[ G_1 = \{X^4\} \text{ and } C^\infty_1 = \{X^3 Y^\infty\}. \]

We thus enclose \( Y^5 Z^2 \) and \( X^3 Y^2 Z^2 \) in \( G(1) \). Since for \( d = 0 \), \( X^4 \in N(1) \) we obtain the final solution enclosing \( X^3 Z \) to \( G(1) \) and both \( X^3 Y^\infty Z \) and \( X^\infty Y^\infty \) in \( C^\infty(1) \).
References


\(^a\) 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

© 2020 by the author(s); licensee Accademia Peloritana dei Pericolanti (Messina, Italy). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).