Rend. Sem. Mat. Univ. Politec. Torino
Vol. 72, 3–4 (2014), 213 – 233

M. Ceria

A PROOF OF THE “AXIS OF EVIL THEOREM” FOR DISTINCT POINTS

Abstract. In this work we provide a complete and constructive proof of Marinari-Mora's “Axis of Evil Theorem”. Given a finite set $\mathbf{X} \subseteq \mathbb{A}^n(\mathbf{k})$ of distinct points and fixed on $\mathcal{P} := \mathbf{k}[x_1,...,x_n]$ the lexicographical order, the theorem states that one can produce a “linear” factorization for a minimal Groebner basis of the ideal $I(\mathbf{X}) \triangleleft \mathcal{P}$, via interpolation and a combinatorial algorithm. We display here the related algorithm showing its termination and correctness.

1. Introduction.

In this paper we face the problem of constructing a linear factorization of a suitable lexicographical Groebner basis for every zerodimensional radical ideal $I \triangleleft \mathcal{P}$.
In the literature we can find many papers studying the zerodimensional ideals of $\mathcal{P}$.
This work, in particular, is inspired by [1] and [13, 14, 15], by M.G. Marinari and T. Mora, in which they study zerodimensional ideals, not necessarily radical, describing them via their Macaulay bases.
One of the most significant results, named “Axis of Evil theorem” by T. Mora in some lecture notes written soon after, presents a precise description for the structure of these ideals in the most interesting cases.
In what follows, we will call the Axis of Evil Theorem AoE for short.

The AoE theorem (see for example [1]) represents, to all intents and purposes, an enhancement for the description of a Groebner basis of an ideal in $\mathbf{k}[x_1,x_2]$ given by Lazard in [9], in the case of radical ideals of $\mathcal{P}$ and also for some of the non radical ones, namely Cerlienco-Mureddu ideals [18].
Roughly speaking, it states that I admits a minimal Groebner basis w.r.t. the lexicographical order (we assume $x_1 < x_2 < ... < x_n$) constituted by polynomials f_τ which have a “linear factorization" i.e. a decomposition in factors of the following shape. If $\tau := x_1^{d_1} \cdots x_n^{d_n}$ then f_τ is the product of factors $x_m - g_{m\delta}(x_1,\dots,x_{m-1})$, one for each choice of integers (m,δ), $1 \leq m \leq n$ and $1 \leq \delta \leq d_m$.
In order to get such a basis, in [1, 13, 14, 15], the authors use Cerlienco-Mureddu algorithm and an interpolation over suitable sets of functionals. These sets represent a partition of the set characterizing I.
The book [18] states the result, but with no proof, giving meaningful examples showing the existence of a minimal Groebner basis of the form stated above.
Aim of this work is to provide a complete, totally algorithmic proof of the AoE in the case of radical ideals, namely when $I = I(\mathbf{X})$ is the ideal of a finite set of distinct points $\mathbf{X}$.
The resulting algorithm will be called *Axis of Evil algorithm* (see section 4).

The starting point of our procedure is the identification of the lexicographical Groebner escalier $\mathsf{N} = \mathsf{N}(I)$, which can be constructed directly from $\mathbf{X}$, using one of the well known combinatorial algorithms as Cerlienco-Mureddu Correspondence [2, 3, 4], Lex Game [7, 11], Gao-Rodrigues-Stroomer algorithm [8] or Lederer's algorithm [10].
Then we exploit an algorithm due to Lazard [6] in order to get the basis of the initial ideal of I efficiently.
Finally, we use interpolation over suitable subsets of the set of points $\mathbf{X}$, in order to get the "linear factorization" we are looking for.
After defining the notation (section 2) and briefly recalling both Cerlienco-Mureddu Correspondence and Lazard algorithm (section 3), we explain the Axis of Evil algorithm, outlining its main properties (section 4).

Finally, in section 5 we give a detailed example of execution of the algorithm.

2. Notation.

Throughout this paper we follow the notation of [18].
We denote by $\mathcal{P} := \mathbf{k}[x_1,...,x_n]$ the ring of polynomials in n variables and coefficients in the base field $\mathbf{k}$. The *semigroup of terms* in the variables $x_1,...,x_m$ is:

$$\mathcal{T}[m] := \{x_1^{\alpha_1}\cdots x_m^{\alpha_m}, (\alpha_1,...,\alpha_m) \in \mathbb{N}^m\}.$$

We simply write $\mathcal{T}$ if $m = n$.
For each *semigroup ordering* $<$ on $\mathcal{T}$ (i.e. a total ordering on $\mathcal{T}$, such that $\tau_1 < \tau_2 \Rightarrow \sigma\tau_1 < \sigma\tau_2, \forall \sigma, \tau_1, \tau_2 \in \mathcal{T}$), we can represent a polynomial $f \in \mathcal{P}$ as a linear combination of terms arranged w.r.t. $<$:

$$f = \sum_{i=1}^{r} c(f,\tau_i)\tau_i : c(f,\tau_i) \in \mathbf{k}^*, \tau_i \in \mathcal{T}, \tau_1 > ... > \tau_r;$$

we denote by $\mathsf{T}(f) := \tau_1$ the *leading term* of f and call *tail* of f the polynomial $tail(f) := f - c(f,\tau_1)\tau_1$.
We always consider the *lexicographical order* on $\mathcal{P}$ induced by $x_1 < ... < x_n$, i.e: $x_1^{\alpha_1}\cdots x_n^{\alpha_n} < x_1^{\beta_1}\cdots x_n^{\beta_n} \Leftrightarrow \exists j \,|\, \alpha_j < \beta_j, \alpha_i = \beta_i, \forall i > j$. This is a *term order*, that is a semigroup ordering such that $1 < x_i, \forall x_i \in \{x_1,...,x_n\}$ or, equivalently, it is a *well ordering*.
For each term $\tau \in \mathcal{T}$, if $x_j | \tau$, we call j-th *predecessor* of τ the term $\frac{\tau}{x_j}$.
A subset $\mathsf{N} \subseteq \mathcal{T}$ is an *order ideal* if $\tau \in \mathsf{N} \Rightarrow \sigma \in \mathsf{N}, \forall \sigma | \tau$. Observe that the subset of $\mathbb{N}^n$ of the exponents of terms in an order ideal is called *Ferrers diagram* (see, for example, [18]). A subset $\mathsf{N} \subseteq \mathcal{T}$ is an order ideal if and only if $\mathcal{T} \setminus \mathsf{N} = J$ is a *semigroup ideal* (i.e. $\tau \in J \Rightarrow \sigma\tau \in J, \forall \sigma \in \mathcal{T}$). For all subsets $A \subset \mathcal{P}$, $\mathsf{T}\{A\} := \{\mathsf{T}(g), g \in A\}$. We denote by $\mathsf{T}(A)$ the semigroup ideal of leading terms w.r.t. a fixed semigroup ordering $\{\tau\mathsf{T}(g), \tau \in \mathcal{T}, g \in A\}$. Notice that for each ideal $I \triangleleft \mathcal{P}$, $\mathsf{T}(I) = \mathsf{T}\{I\}$.
For each semigroup ideal $J \subset \mathcal{T}$, we have $\mathsf{N}(J) := \mathcal{T} \setminus \mathsf{T}(J)$ and the monomial basis

$\mathsf{G}(J)$ of the semigroup ideal J satisfies the conditions below

$$\mathsf{G}(J) = \{\tau \in J \,|\, \text{each predecessor of } \tau \text{ is in } \mathsf{N}(J)\} = \\ = \{\tau \in \mathcal{T} \,|\, \mathsf{N}(J) \cup \{\tau\} \text{ order ideal}, \tau \notin \mathsf{N}(J)\}.$$

For any ideal $I \triangleleft \mathcal{P}$ the basis of the semigroup ideal $\mathsf{T}(I) = \mathsf{T}\{I\}$ is called *monomial basis* of I and denoted again by $\mathsf{G}(I)$.

LEMMA 1. *Fix a term order $<$ on $\mathcal{P}$ and consider an ideal $I \triangleleft \mathcal{P}$; we denote by abuse of notation $\mathsf{N}(I) := \mathsf{N}(\mathsf{T}(I))$ w.r.t. $<$. The following statements hold:*
1) $\mathcal{P} = I \oplus Span_k(\mathsf{N}(I))$;
2) $\mathcal{P}/I \cong Span_k(\mathsf{N}(I))$;
3) $\forall f \in \mathcal{P}$, $\exists! g \in Span_k(\mathsf{N}(I))$, such that $f - g \in I$.

The polynomial g of lemma 1 is called *canonical form* of f w.r.t. I and usually denoted by $Can(f, I)$.

DEFINITION 1. *For each term order $<$ on $\mathcal{T}$:*

- *a* Groebner basis *of I is a set $\mathcal{G} \subset I$ s.t. $\mathsf{T}(\mathcal{G}) = \mathsf{T}\{I\}$;*
- *a* minimal Groebner basis *is a Groebner basis $\mathcal{H}$ s.t. $\mathsf{T}\{\mathcal{H}\} = \mathsf{G}(I)$. Then, divisibility relations among the leading terms of its members do not exist;*
- *the unique* reduced Groebner basis *of I is the set $\mathcal{G}'(I) := \{\tau - Can(\tau, I) : \tau \in \mathsf{G}(I)\}$. Each member of the reduced Groebner basis has a monic leading term which does not divide any term of another member.*

Let $\mathbf{X} = \{P_1, ..., P_S\} \subset \mathbf{k}^n$ be a finite set of distinct points, $P_i := (a_{i1}, ..., a_{in})$; we denote by $I(\mathbf{X}) := \{f \in \mathcal{P} : f(P_i) = 0, \forall i\}$ the *ideal of points* of $\mathbf{X}$.
Finally, we define the projection maps:

$$\pi_m : \mathbf{k}^n \to \mathbf{k}^m \qquad\qquad \pi^m : \mathbf{k}^n \to \mathbf{k}^{n-m+1}$$

$$(\alpha_1, .., \alpha_n) \mapsto (\alpha_1, ..., \alpha_m), \qquad\qquad (\alpha_1, .., \alpha_n) \mapsto (\alpha_m, ..., \alpha_n)$$

With the same notation π_m we denote also

$$\begin{aligned} \pi_m : \mathcal{T} &\longrightarrow \mathcal{T}[m] \\ x_1^{\alpha_1} \cdots x_n^{\alpha_n} &\mapsto x_1^{\alpha_1} \cdots x_m^{\alpha_m}. \end{aligned} \tag{1}$$

3. Cerlienco-Mureddu Correspondence and Lazard algorithm.

Consider a finite ordered set of distinct points $\underline{\mathbf{X}} := (P_1, ..., P_S) \subset \mathbf{k}^n$ and let $\mathbf{X} = \{P_1, ..., P_S\}$ the associated non-ordered set.

L. Cerlienco and M. Mureddu [2, 3, 4] provided a purely combinatorial algorithm computing a monomial basis $\mathcal{B} = \{[\tau_1],...,[\tau_S]\}$ for the quotient algebra $\mathcal{P}/I(\mathbf{X})$ with $\tau_1 < ... < \tau_S$ w.r.t. lex, namely $\mathsf{N}(I(\mathbf{X})) = \mathcal{T} \setminus \mathsf{T}(I(\mathbf{X}))$.
The basis $\mathcal{B}$ obtained by their algorithm is *minimal* w.r.t. $<$, i.e. for each monomial basis $\mathcal{B}' = \{[\tau'_1],...,[\tau'_S]\}$, with $\tau'_1 < ... < \tau'_S$ it holds $\tau_i \leq \tau'_i$, $\forall i = 1,...,S$.
In the aforesaid papers, they define an operator Φ, associating to each $\underline{\mathbf{X}}$ an ordered Ferrers diagram $\Phi(\underline{\mathbf{X}}) := (\delta_1,...,\delta_S) \subset \mathbb{N}^n$, $\delta_i \neq \delta_j$ for $i \neq j$ such that

- $|\Phi(\underline{\mathbf{X}})| = |\underline{\mathbf{X}}| = S$;
- $\forall m < S$ $(\delta_1,..\delta_m) = \Phi((P_1,...,P_m))$.

This way, they determine a biunivocal correspondence between $\underline{\mathbf{X}}$ and $\Phi(\underline{\mathbf{X}})$, associating δ_i to each P_i, $i = 1,...,S$.
From now on, we denote by $\Phi(\mathbf{X}) := \{\delta_1,...,\delta_S\}$ the non-ordered set associated to $\Phi(\underline{\mathbf{X}})$. Clearly, a biunivocal correspondence between $\mathbf{X}$ and $\Phi(\mathbf{X})$ is naturally established from the one described above.
The set $\Phi(\mathbf{X})$ contains the exponents lists of the terms in $\mathsf{N}(I(\mathbf{X}))$, the lexicographical Groebner escalier associated to $I(\mathbf{X})$. Identifying each $\delta_i \in \mathbb{N}^n$ with $x^{\delta_i} \in \mathcal{T}$, we can say that Cerlienco and Mureddu state a biunivocal correspondence between $\mathbf{X}$ and $\mathsf{N}(I(\mathbf{X}))$. We call it *Cerlienco-Mureddu correspondence* and we denote it by Φ by abuse of notation. We write then indifferently $\Phi(P_i) = \delta_i$ and $\Phi(P_i) = x^{\delta_i}$, depending on the context.
The input of Cerlienco-Mureddu algorithm is the ordered set $\underline{\mathbf{X}}$; the output is the set $\Phi(\underline{\mathbf{X}})$.
In order to describe the algorithm, for $P \in \mathbf{k}^n$, we let

$$\Pi_s(P,\underline{\mathbf{X}}) := \{P_i \in \underline{\mathbf{X}} \,|\, \pi_s(P_i) = \pi_s(P)\},$$

$$\Pi^s(P,\underline{\mathbf{X}}) := \{P_i \in \underline{\mathbf{X}} \,|\, \pi^s(P_i) = \pi^s(P)\},$$

extending in the obvious way the meaning of $\pi_s(\mathbf{d}), \pi^s(\mathbf{d}), \Pi_s(\mathbf{d},D), \Pi^s(\mathbf{d},D)$ to $\mathbf{d} \in \mathbb{N}^n \subset \mathbf{k}^n$ and $D \subset \mathbb{N}^n$.

We sketch below the main steps of Cerlienco-Mureddu algorithm.

- $S = |\underline{\mathbf{X}}| = 1$ then $\Phi(\underline{\mathbf{X}}) = \{(0,...,0)\}$. By definition, the only order ideal with cardinality one is the singleton $\{1\}$.
- If $S > 1$, suppose to know by induction hypothesis the ordered set $\Phi(\mathbf{X}') = (\delta_1,...,\delta_{\mathbf{S-1}})$ with $\mathbf{X}' = (P_1,...,P_{S-1})$ and look for $\delta_S = \Phi(P_S) = (\delta_{S,1},...,\delta_{S,n})$, performing the following steps.
    1. Compute the σ-*value* of P_S w.r.t. $\underline{\mathbf{X}'}$ (denoted by $\sigma(P_S,\underline{\mathbf{X}'})$ or by σ for short) namely the maximal integer number σ s.t. $\Pi_{\sigma-1}(P_S,\underline{\mathbf{X}'}) \neq \emptyset$. Notice that $1 \leq \sigma \leq n$. Indeed, for each $j \geq n+1$, $\Pi_{j-1}(P_S,\underline{\mathbf{X}'}) = \emptyset$ and we assume by convention that $\Pi_0(P,\underline{\mathbf{Y}}) \neq \emptyset$, for each point P and for each set $\mathbf{Y}$.

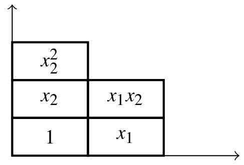
The numbers $\delta_{S,i}$, $i = 1,\dots,n$ are computed iteratively as follows.

2. If $i > \sigma$, $\delta_{S,i} = 0$, so that, at the present state, $\delta_{\mathbf{S}} = (\underbrace{?,\dots,?}_{\sigma-1},\underbrace{0,\dots,0}_{n-\sigma+1})$.
3. If $i = \sigma$, compute the maximal integer m s.t
$$\pi_{\sigma-1}(P_m) = \pi_{\sigma-1}(P_S),$$
$$\pi^{\sigma+1}(\delta_m) = (0,\dots,0) = \pi^{\sigma+1}(\delta_S),$$
called σ-*antecedent* of P_S w.r.t. $\mathbf{X}'$ and $\Phi(\mathbf{X}')$ and set $\delta_{S,\sigma} = \delta_{m,\sigma} + 1$.
4. If $i < \sigma$ compute the set
$$\mathcal{W}(P_S,\underline{\mathbf{X}}) := \{P \in \underline{\mathbf{X}} |\text{ denoted } \Phi(P) := \delta, \pi^{\sigma}(\delta) = (\delta_{S,\sigma},0,\dots,0)\} =$$
$$= \{P_{j_1},\dots,P_{j_r}\}.$$
It holds $P_{j_r} = P_S$. Set $Q := \pi_{\sigma-1}(\mathcal{W}(P_S,\underline{\mathbf{X}})) \subset \mathbf{k}^{\sigma-1}$.
Notice that if $h < r$, $\pi_{\sigma-1}(P_{j_h}) \neq \pi_{\sigma-1}(P_S)$ and, more generally, if $h < k \leq r$, then $\pi_{\sigma-1}(P_{j_h}) \neq \pi_{\sigma-1}(P_{j_k})$, so also $|Q| = r$. Being $r < S$, by induction hypothesis $\Phi(Q) = \{\widetilde{\delta_1},\dots,\widetilde{\delta_r}\}$ and it holds $\widetilde{\delta_i} = \pi_{\sigma-1}(\delta_{\mathbf{j_i}})$, for $i = 1,\dots,$ $r-1$. We set then $\pi_{s-1}(\delta_{\mathbf{S}}) = \widetilde{\delta_r}$.

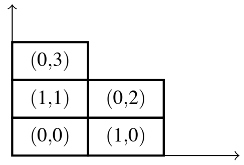
Cerlienco and Mureddu proved the following

PROPOSITION 1. *([2]) With the above notation* $\{[x^{\delta}] | \delta \in \Phi(\mathbf{X})\}$ *is a minimal monomial basis for* $\mathcal{P}/I(\mathbf{X})$ *with respect to lex.*

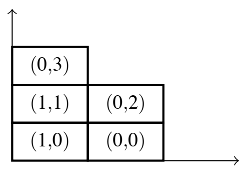
EXAMPLE 1. Take the set $\mathbf{X} = \{(0,0),(1,0),(1,1),(0,2),(0,3)\} \subset \mathbf{k}^2$. Applying Cerlienco-Mureddu algorithm on $\mathbf{X}$, we get $\mathsf{N}(I(\mathbf{X})) = \{1, x_1, x_2, x_1x_2, x_2^2\}$. Since $\mathcal{T} \cong \mathbb{N}^2$, we identify each $x_1^{\alpha_1}x_2^{\alpha_2} \in \mathsf{N}(I(\mathbf{X}))$ with $(\alpha_1,\alpha_2) \in \mathbb{N}^2$ and we represent the terms of the Groebner escalier in a bidimensional picture:



Finally, we can represent the elements in $\mathbf{X}$ in an analogous picture, substituting each term $\tau \in \mathsf{N}(I(\mathbf{X}))$ with the point $\Phi^{-1}(\tau)$:



REMARK 1. We point out that the output $\Phi(\underline{\mathbf{X}})$ of Cerlienco-Mureddu algorithm is different if we modify the order of the input points contained in $\mathbf{X}$.
For example if we take the set $\mathbf{X}' = \{(1,0),(0,0),(1,1),(0,2),(0,3)\} \subset \mathbf{k}^2$, instead of example 1's $\mathbf{X} = \{(0,0),(1,0),(1,1),(0,2),(0,3)\}$, we get $\Phi(\underline{\mathbf{X}'}) = \{1, x_1, x_2, x_1x_2, x_2^2\}$ and we can represent the biunivocal correspondence via the picture below



which is different from the one displayed in example 1.
Clearly the support is the same, being actually the lexicographical Groebner escalier of $I(\mathbf{X}) = I(\mathbf{X}')$.

We call the picture above (2-dimensional) *tower picture* of $\mathbf{X}$, because of its shape.
The above argument can be generalized to $n > 2$ variables, obtaining n-dimensional tower pictures.

Lazard algorithm is a very simple but powerful tool in order to study zerodimensional ideals.
It has been developed in [6], actually being a part of FGLM algorithm. For more details, see [6], [12], Lemma 13 pg. 117, [18], Alg.29.2.3 pg. 424.
Given $\mathsf{N}(I(\mathbf{X})) = \{\tau_1, ..., \tau_S\}$, Lazard algorithm computes the monomial basis $\mathsf{G}(I(\mathbf{X}))$ of the zerodimensional radical ideal $I(\mathbf{X}) \triangleleft \mathcal{P}$, iteratively on the terms in $\mathsf{N}(I(\mathbf{X}))$.
If $|\mathsf{N}(I(\mathbf{X}))| = 1$, namely $\mathsf{N}(I(\mathbf{X})) = \{1\}$, then the monomial basis is $\mathsf{G}_1 := \mathsf{G}(I(\mathbf{X})) = \{x_1, ..., x_n\}$[‡]. Set $L = [x_1, ..., x_n]$ i.e. store a list containing the products $1 \cdot x_j$, for $j = 1, ..., n$.
The above steps constitute the basis for the procedure.
Let now $|\mathsf{N}(I(\mathbf{X}))| > 1$, $\mathsf{G}_{i-1} := \{\tau'_1, ..., \tau'_h\}$ be the monomial basis associated to the order ideal $\mathsf{N}_{i-1} := \{\tau_1 = 1, \tau_2, ..., \tau_{i-1}\}$, $i \le S$ and L be the list (ordered w.r.t. lex) containing products of the form $\tau_k x_j$, for $k = 1, ..., i-1$, $j = 1, ..., n$, with $\tau_k x_j \notin \mathsf{N}_{i-1}$.
We do not allow repetitions in L, so if $\sigma = x_{j_0}\tau_{j_0} = x_{j_1}\tau_{j_1}$, σ is reported only once in L, but it is marked with a number, i.e. the number of times it has been computed.
Consider then $\tau_i \in \mathsf{N}(I(\mathbf{X}))$; in order to compute the monomial basis G_i associated to $\mathsf{N}_i = \{\tau_1, ..., \tau_i\}$, Lazard algorithm performs the steps displayed below on τ_i.

- removes τ_i from L;
- Computes all the products $\sigma_{j,i} = x_j \tau_i$, for each $j = 1, ..., n$.
- Inserts each $\sigma_{j,i}$ in L. For each $\sigma_{\bar{j},i}$ already appearing in L, the algorithm upgrades the number of times it has been computed and selected for insertion.

[‡]For each $j \in \underline{\mathbf{n}}$, the only existing predecessor of x_j is $1 \in \mathsf{N}(I(\mathbf{X}))$. No other term σ can belong to $\mathsf{G}(I(\mathbf{X}))$, being multiple of at least one variable.

- All the terms appearing in L, marked exactly with the number of the variables dividing them, are the elements of G_i, the monomial basis associated to N_i.

For more details on both Cerlienco-Mureddu correspondence and Lazard algorithm, see also [18].

4. The Axis of Evil algorithm.

The Axis of Evil Theorem by Marinari and Mora [1, 13, 14, 15, 18] remarkably improves Lazard structural theorem [9], extending it to the case of n variables, $n > 2$, provided that the given ideal $I \triangleleft \mathcal{P}$ is zerodimensional and radical.
In this work, we give a constructive proof for

THEOREM 1 (Marinari-Mora). *Consider a zerodimensional radical ideal $I \triangleleft \mathcal{P}$, fixing on $\mathcal{P}$ the lexicographical order "$<$", induced by $x_1 < ... < x_n$. Denote by $\mathsf{N}(I)$ the associated (lexicographical) Groebner escalier and by*

$$\mathsf{G}(I) = \{\tau_1, ..., \tau_r\} \subset \mathcal{T}, \quad \tau_i := x_1^{d_{i,1}} \cdots x_n^{d_{i,n}}$$

the monomial basis for the (lexicographical) semigroup ideal $\mathsf{T}(I)$.
Then, there exist polynomials

$$\gamma_{m\delta i} = x_m - g_{m\delta i}(x_1, ..., x_{m-1}),$$

for each $i \in \{1, ..., r\}$, $m \in \{1, ..., n\}$ and $\delta \in \{1, ..., d_{i,m}\}$ such that the products

$$f_i = \prod_m \prod_\delta \gamma_{m\delta i}, \; i = 1, ..., r$$

form a minimal Groebner basis of I, with respect to $<$.

Clearly, for the polynomials f_i of theorem 1, we have $\mathsf{T}(f_i) = \tau_i$ for $i = 1, ..., r$. Hence, taken a finite set of distinct points $\mathbf{X} = \{P_1, ..., P_S\}$ and denoted by $I := I(\mathbf{X})$ the ideal of $\mathbf{X}$, in order to find the factorized minimal Groebner basis $\mathcal{G} := \mathcal{G}(I(\mathbf{X}))$ of I we need to get the monomial basis $\mathsf{G}(I)$.
As explained in section 3, we can obtain $\mathsf{G}(I)$ directly from $\mathsf{N}(I)$ via Lazard algorithm, whereas $\mathsf{N}(I)$ can be computed via Cerlienco-Mureddu correspondence. Actually, there are some alternative algorithms to Cerlienco-Mureddu correspondence, namely Felszeghy-B. Ráth-Rónyai Lex Game [7], Gao-Rodrigues-Stroomer method [8] or Lederer's algorithm [10]. Following [18] we only use Cerlienco-Mureddu correspondence, but we can indifferently employ any of the other methods in order to get $\mathsf{N}(I)$.
We point out that the polynomials $\gamma_{m\delta i}$ of theorem 1 are only *linear in the leading terms*. From now on, we will call such a factorization (linear) *Axis of Evil factorization*.
The pseudocode of the algorithm is displayed in 1 below.
For an implementation, see [19].

Algorithm 1 The Axis of Evil algorithm.

procedure AoE$(\mathbf{X}, \mathsf{N}(I(\mathbf{X})), \mathsf{G}(I(\mathbf{X})) := \{\tau_1,...,\tau_r\}) \to R$ ▷ R contains a factorized minimal Groebner basis of I.
Require: Denote $\tau_j = x_1^{d_{j,1}} \cdots x_n^{d_{j,n}}$ for $j = 1,...,r$.
    $R = \emptyset$
    for $j = 1$ to r **do**
        $N_1(\tau_j) := \{x_1^i \mid i < d_{j,1}\}$
        $A_1(\tau_j) := \{\Phi^{-1}(x_1^i x_2^{d_{j,2}} \cdots x_n^{d_{j,n}}) \mid i < d_{j,1}\} \subset \mathbf{X}$.
        $B_1(\tau_j) := \pi_1(A_1(\tau_j)) \subset k$.
        $\gamma_{1\tau_j} := \prod_{a \in B_1(\tau_j)}(x_1 - a)$.
        for $m = 2$ to n **do**
            $\zeta_{m\tau_j} := \prod_{\nu=1}^{m-1} \gamma_{\nu\tau_j}$.
            $D_{m0} := \{P_i \in \mathbf{X} / \zeta_{m\tau_j}(P_i) \neq 0\}$.
            if $|D_{m0}| = 0$ **then**
                $R = [R, \zeta_{m\tau_j}]$.
                break
            end if
            $N_m(\tau_j) := \{\omega \in \mathcal{T}[m], \tau_j > \omega x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}} \in \mathsf{N}\}$.
            for $\delta = 1$ to $d_{j,m}$ **do**
                $A_{m\delta}(\tau_j) := \{\Phi^{-1}(v x_m^{d_{j,m}-\delta} x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}}) \mid v \in \mathcal{T}[m-1], v x_m^{d_{j,m}-\delta} \in N_m(\tau_j)\} \cap D_{m(\delta-1)}(\tau_j)$.
                $E_{m\delta}(\tau_j) := \Phi(\pi_m(A_{m\delta}(\tau_j)))$.

$$\gamma_{m\delta\tau_j} := x_m + \sum_{\omega \in E_{m\delta}(\tau_j)} c(\gamma_{m\tau_j}, \omega)\omega,$$

such that $\gamma_{m\delta\tau_j}(P) = 0, \forall P \in A_{m\delta}(\tau_j)$.
                $\xi_{m\delta} := \prod_{\nu=1}^{m-1} \gamma_{\nu\tau_j} \prod_{d=1}^{\delta} \gamma_{md\tau}$.
                $D_{m\delta}(\tau_j) := \{P_i \in \mathbf{X} / \xi_{m\delta}(P_i) \neq 0\} \subseteq \mathbf{X}$
                if $|D_{m\delta}(\tau_j)| = 0$ **then**
                    $R = [R, \xi_{m\delta}]$.
                    break
                end if
            end for
            $\gamma_{m\tau_j} := \prod_\delta \gamma_{m\delta\tau_j}$.
        end for
    end for
return R.
end procedure

Since $I \triangleleft \mathcal{P}$ is a zerodimensional ideal, then $\mathsf{G}(I)$ contains a pure power of each variable so, in particular, $\tau_1 := x_1^{d_{1,1}} \in \mathsf{G}(I)$ and it is the smallest term w.r.t. lex in the monomial basis. Computing the Axis of Evil factorization of $f_1 \in \mathcal{G}$, such that $\mathsf{T}(f_1) = \tau_1$, is particularly simple. Indeed, all the terms $1, x_1, ..., x_1^{d_{1,1}-1} \in \mathsf{N}(I)$. As a consequence of Cerlienco-Mureddu Correspondence (or Moeller algorithm [16]), $1, x_1, \ldots, x_1^{d_{1,1}-1} \in \mathsf{N}(I)$ means that the points in $\mathbf{X}$ have exactly $d_{1,1}$ different first coordinates. If we compute the set

$$N_1(\tau_1) := \{x_1^i / \, i < d_{1,1}\},$$

we get exactly $N_1(\tau_1) = \{1, x_1, \ldots, x_1^{d_{1,1}-1}\}$.
These terms correspond, by Cerlienco-Mureddu correspondence, to the first $d_{1,1}$ points with different first coordinates, say $A_1(\tau_1) = \{P_{\alpha_1}, \ldots, P_{\alpha_{d_{1,1}}}\}$.
For each $1 \le j \le d_{1,1}$, let a_j be the first coordinate of P_{α_j}.
We let $B_1(\tau_1) = \{a_1, \ldots, a_{d_{1,1}}\}$ and we compute the polynomial

$$\gamma_{1\tau_1} := \prod_{j=1}^{d_{1,1}} (x_1 - a_j).$$

Since $\mathsf{T}(\gamma_{1\tau_1}) = \tau_1$ and $\gamma_{1\tau_1}$ vanishes over all $\mathbf{X}$, $f_1 = \gamma_{1\tau_1}$, we have found an element of the minimal Groebner basis $\mathcal{G}$. Moreover, besides the factors composing f_1 being reduced, f_1 is also reduced itself, since

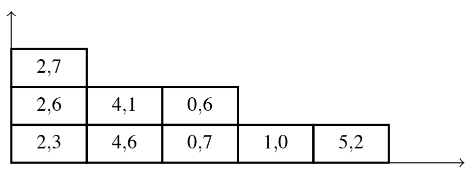
$$Supp(f_1) \setminus \{\tau_1\} \subseteq \{1, x_1, \ldots, x_1^{d_{1,1}-1}\} \subseteq \mathsf{N}(I).$$

We point out that f_1 has been determined as the product of exactly $d_{1,1}$ factors.

EXAMPLE 2. Let us consider the set

$$\mathbf{X} = \{(2,3),(4,6),(0,7),(1,0),(5,2),(2,6),(4,1),(0,6),(2,7)\} \subset \mathbb{R}^2.$$

The corresponding Groebner escalier is
$\mathsf{N}(I(\mathbf{X})) = \{1, x_1, x_1^2, x_1^3, x_1^4, x_2, x_1x_2, x_1^2x_2, x_2^2\}$.
The associated tower picture is



The monomial basis is $\mathsf{G}(I(\mathbf{X})) = \{x_1^5, x_1^3x_2, x_1x_2^2, x_2^3\}$ and we consider $x_1^5 = \min_<(\mathsf{G}(I(\mathbf{X})))$.
We examine the execution of Algorithm 1 on $\mathbf{X}$, for the part related to x_1^5. For this term we get $N_1(\tau_1) := \{1, x_1, x_1^2, x_1^3, x_1^4\}$, corresponding via Cerlienco-Mureddu correspondence to the points $A_1(\tau_1) = \{(2,3),(4,6),(0,7),\ (1,0),(5,2)\}$. The projection $\pi_1(A_1(\tau_1))$ is the set containing the first coordinates, so it turns out to be $B_1(\tau_1) = \{2,4,0,1,5\}$. Then, through the steps displayed in lines from 4 to 7 of Algorithm 1, we obtain the polynomial

$$f_1 = \gamma_{1\tau_1} = x_1(x_1-2)(x_1-4)(x_1-1)(x_1-5) = x_1^5 - 12x_1^4 + 49x_1^3 - 78x_1^2 + 40x_1,$$

clearly vanishing at all $\mathbf{X}$.
We know that f_1 belongs to the minimal Groebner basis of theorem 1, but it also belongs to the reduced Groebner basis, since $x_1, x_1^2, x_1^3, x_1^4 \in \mathsf{N}(I(\mathbf{X}))$. Actually, if we compute using Singular [5] the reduced Groebner basis of $I(\mathbf{X})$ we get

- $x_1^5 - 12x_1^4 + 49x_1^3 - 78x_1^2 + 40x_1$, that is exactly our f_1;
- $2x_1^3x_2 - 12x_1^2x_2 + 16x_1x_2 - x_1^4 + 7x_1^3 - 14x_1^2 + 8x_1$;
- $4x_1x_2^2 - 8x_2^2 + 6x_1^2x_2 - 64x_1x_2 + 104x_2 - 9x_1^4 + 107x_1^3 - 426x_1^2 + 664x_1 - 336$;
- $12x_2^3 - 192x_2^2 - 18x_1^2x_2 + 36x_1x_2 + 972x_2 - 149x_1^4 + 1583x_1^3 - 5218x_1^2 + 5296x_1 - 1512$.

Now, we show the execution of Algorithm 1 on a generic term $\tau_j = x_1^{d_{j,1}} \cdots x_n^{d_{j,n}}$, $j \leq r = |\mathsf{G}(I(\mathbf{X}))|$, in order to produce the polynomial $f_j \in \mathcal{G}$ with $\mathsf{T}(f_j) = \tau_j$ of theorem 1.
Similarly to what done for τ_1, we first study the first coordinates, namely we compute the set

$$N_1(\tau_j) := \{x_1^i / \, i < d_{j,1}\}.$$

Notice that, even if in line 4 of algorithm 1 we define the set $N_1(\tau_j)$ by characterizing explicitly its elements, we have that

$$N_1(\tau_j) = \{\omega \in \mathcal{T}[1], \tau_j > \omega x_2^{d_{1,2}} \cdots x_n^{d_{1,n}} \in \mathsf{N}(I)\},$$

so this set is constructed exactly in the same way as the $N_m(\tau_j)$'s, with $2 \leq m \leq n$. Moreover, notice that for $N_1(\tau_j)$ we have $d_{1,2} = ... = d_{1,n} = 0$.
By Cerlienco-Mureddu correspondence, each term in $\mathsf{N}(I)$ is associated to a point of $\mathbf{X}$, so we can define $A_1(\tau_j) := \{\Phi^{-1}(x_1^i x_2^{d_{j,2}} \cdots x_n^{d_{j,n}}) / \, i < d_{j,1}\} \subset \mathbf{X}$ and we get $B_1(\tau_j) := \pi_1(A_1(\tau_j)) \subset \mathbf{k}$. The factors in x_1 are of the form $(x_1 - a)$ for $a \in B_1(\tau_j)$, so the partial factor in $x_1^{d_{j,1}}$ is

$$\gamma_{1\tau_j} := \prod_{a \in B_1(\tau_j)} (x_1 - a).$$

At this point, we have executed the steps displayed in lines from 4 to 7 of Algorithm 1.
We construct now the set $D_{20} := \{P_i \in \mathbf{X} / \gamma_{1\tau_j}(P_i) \neq 0\}$, containing all the points in the given $\mathbf{X}$ such that $\gamma_{1\tau_j}$ does not vanish in them. If D_{20} is empty, then $f_j = \gamma_{1\tau_j}$. In this case, we stop the execution on τ_j (we have executed what prescribed in lines 9-14).
We notice that such an eventuality happens only for the term τ_1 since, by the minimality of $\mathsf{G}(I)$, only one pure power of x_1 can occur in $\mathsf{G}(I)$.
Otherwise, we construct the set

$$N_2(\tau_j) := \{\omega \in \mathcal{T}[2], \tau_j > \omega x_3^{d_{j,3}} \cdots x_n^{d_{j,n}} \in \mathsf{N}(I)\},$$

containing the terms ω in the two variables x_1, x_2 such that $\tau_j > \omega x_3^{d_{j,3}} \cdots x_n^{d_{j,n}}$ in the Groebner escalier (line 15) and, for each δ from 1 to $d_{j,2}$ we compute the set of points in which to interpolate, namely

$$A_{2\delta}(\tau_j) := \{\Phi^{-1}(v x_2^{d_{j,2}-\delta} x_3^{d_{j,3}} \cdots x_n^{d_{j,n}}) | v \in \mathcal{T}[1], v x_2^{d_{j,2}-\delta} \in N_2(\tau_j)\} \cap D_{2(\delta-1)}(\tau_j)$$

and the set of terms appearing in the current factor, i.e. $E_{2\delta}(\tau_j) := \Phi(\pi_2(A_{2\delta}(\tau_j)))$.
With the above data, we perform the interpolation step and we finally get the factor

$$\gamma_{2,\delta\tau_j} := x_2 + \sum_{\omega \in E_{2\delta}(\tau_j)} c(\gamma_{2\tau_j}, \omega)\omega,$$

such that $\gamma_{2,\delta\tau_j}(P) = 0, \forall P \in A_{2\delta}(\tau_j)$.
We compute then $D_{2\delta}(\tau_j) := \{P_i \in \mathbf{X} / \xi_{2\delta}(P_i) \neq 0\} \subseteq \mathbf{X}$, where $\xi_{2\delta}$ is the product of all the factors we have already computed for τ_j. We stop if $D_{2\delta}(\tau_j)$ is empty.
Repeating for each δ, we get all the factors with leading term x_2.
At this point, we check whether the product of the current factors vanishes over all $\mathbf{X}$. If so, such a product is f_j, otherwise, we repeat for $x_3, \ldots, x_n$, stopping the procedure on τ_j and storing f_j when we reach the last coordinate or when the product of the current factors vanishes over all $\mathbf{X}$ (see line 8-14).

Once f_j has been stored, we proceed in the same way with all the other elements of $\mathsf{G}(I(\mathbf{X}))$ (line 3).

REMARK 2.

(i) Since each polynomial has the shape $x_m - f$, $f \in \mathbf{k}[x_1, \ldots, x_{m-1}]$ it obviously holds that $\mathsf{T}(\gamma_{m\delta\tau_j}) = x_m$.

(ii) Even if Algorithm 1 leans on Cerlienco-Mureddu correspondence, whose most important feature is iterativity on the points, it is *not iterative* on the elements of $\mathbf{X}$.
Indeed all the Cerlienco-Mureddu biunivocal correspondence and the monomial basis have to be known in order to proceed in the execution of the algorithm.

(iii) Let $\tau_j := x_1^{d_{j,1}} \cdots x_n^{d_{j,n}} \in \mathsf{G}(I(\mathbf{X}))$.
The output polynomial $f_j = \tau_j + tail(f_j) \in \mathcal{G}(I(\mathbf{X}))$ has exactly, as required, $d_j = \sum_{i=1}^n d_{j,i}$ factors: $d_{j,1}$ with leading term x_1, $d_{j,2}$ with leading term x_2 and so on. Each variable x_i, $i = 1, \ldots, n$, appears only $d_{j,i}$ times in the execution of the algorithm, $j = 1, \ldots, n$, as one can see by lines 4, 7 and 16 of Algorithm 1.

REMARK 3. The sets

$$N_m(\tau_j) := \{\omega \in \mathcal{T}[m], \tau_j > \omega x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}} \in \mathsf{N}(I)\}$$

are constructed in order to find the points where to interpolate.
We point out that $N_m(\tau_j) \subseteq N_h(\tau_j)$ for $m \leq h$.

If $\omega \in N_m(\tau_j)$, $\omega \in \mathcal{T}[m]$ and $\tau_j > \omega x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}} \in \mathsf{N}(I)$. Since $m \leq h$, $\omega \in \mathcal{T}[h]$; as $\omega x_{h+1}^{d_{j,h+1}} \cdots x_n^{d_{j,n}} \mid \omega x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}}$ we have $\omega x_{h+1}^{d_{j,h+1}} \cdots x_n^{d_{j,n}} \in \mathsf{N}(I)$ and

$$\omega x_{h+1}^{d_{j,h+1}} \cdots x_n^{d_{j,n}} \leq \omega x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}} < \tau_j$$

.

Since for each term $\mu \in \mathsf{N}(I)$ such that $\mu > \tau_j$, Cerlienco-Mureddu provides a point $P_{\mu'}$ such that $\mu' < \mu$ and $\exists k \in \{1,...,n\} : \pi_k(P_\mu) = \pi_k(P_{\mu'})$, in order to obtain polynomials vanishing at all the points of $\mathbf{X}$ it is not necessary to interpolate in the whole $\Phi^{-1}(\mathsf{N})$ as it suffices to consider only those corresponding to $\mu \in \mathsf{N}(I)$ with $\mu < \tau_j$.

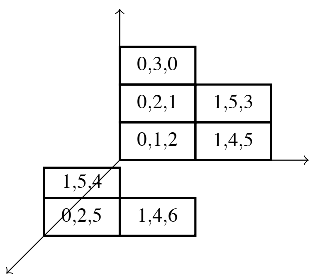
The example 3 below concretely illustrates what explained in remark 3.

EXAMPLE 3. Consider the set

$$\mathbf{X} = \{(0,1,2),(1,4,5),(0,2,1),(1,5,3),(0,3,0),(0,2,5),(1,4,6),(1,5,4)\} \subseteq \mathbf{k}^3.$$

The lexicographical Groebner escalier of the ideal of points $I := I(\mathbf{X})$ is

$$\mathsf{N}(I) = \{1, x_1, x_2, x_1x_2, x_2^2, x_3, x_1x_3, x_2x_3\}:$$



The monomial basis is then $\mathsf{G}(I) = \{x_1^2, x_1x_2^2, x_2^3, x_1x_2x_3, x_2^2x_3, x_3^2\}$.
We focus on $\tau_2 = x_1x_2^2$ and we observe that $x_2x_3 \in \mathsf{N}(I)$ is greater than τ_2 w.r.t. the lexicographical order induced by $x_1 < x_2 < x_3$.
With the notation due to Cerlienco-Mureddu, we can say that $\Phi^{-1}(x_2x_3) = (1,5,4)$, and we can notice that:

- the factor $x_2 - 5$ produced in order to make f_2 vanish on the point $(1,5,3)$ also makes f_2 vanish on the point $(1,5,4)$, since $\pi_2(1,5,3) = (1,5) = \pi_2(1,5,4)$;
- we have $(1,5,3) = \Phi^{-1}(x_1x_2)$ and $x_1x_2 < \tau_2$.

For the sake of completeness, we report here the whole Axis of Evil factorization of I, computed using Singular:

x_1^2: $f_1 = x_1(x_1 - 1)$;

$$x_1x_2^2\colon\; f_2 = x_1(x_2-5)(x_2-4);$$
$$x_2^3\colon\; f_3 = (x_2-3)(x_2-3x_1-2)(x_2-3x_1-1);$$
$$x_1x_2x_3\colon\; f_4 = (x_1-1)(x_2-2)(x_3+x_2-3);$$
$$x_2^2x_3\colon\; f_5 = (x_2-5)(x_2-2x_1-2)(x_3+x_2-3)$$
$$x_3^2\colon\; f_6 = (x_3+2x_2-5x_1-9)(x_3+x_1x_2+x_2-10x_1-3).$$

REMARK 4. For each $\delta \in \{0,...,d_{j,m}\}$ and for each $\tau_j \in \mathsf{G}(I(\mathbf{X})), \tau_j \neq \tau_1$, define the sets

$$S_{m\delta}(\tau_j) := \{vx_m^{d_{j,m}-\delta} \in N_m(\tau_j),\, v \in \mathcal{T}[m-1]\} \subset N_m(\tau_j).$$

Notice that, for $\delta_1, \delta_2 \in \{0,...,d_{j,m}\}$, $\delta_1 \neq \delta_2$, we get $S_{m\delta_1}(\tau_j) \cap S_{m\delta_2}(\tau_j) = \emptyset$ and that $N_m(\tau_j) = \bigcup_{\delta=0}^{d_{j,m}} S_{m\delta}(\tau_j)$: the subsets $S_{m\delta}(\tau_j)$ which are nonempty form a partition of $N_m(\tau_j)$.
Even if in Algorithm 1 there is no need to define explicitly the subsets $S_{m\delta}(\tau_j)$, those for $\delta \in \{1,...,d_{j,m}\}$ are essentially used in the construction of the sets $A_{m\delta}(\tau_j)$, $\delta \in \{1,...,d_{j,m}\}$ (see line 17). This means that the subsets $S_{m\delta}(\tau_j)$ come into play in the choice of the points where to interpolate while constructing the current factor.
Notice that

$$S_{m0}(\tau_j) = \{vx_m^{d_{j,m}} \in N_m(\tau_j),\, v \in \mathcal{T}[m-1]\} \subset N_m(\tau_j).$$

is not used in the construction (in line 16 we consider $\delta = 1,...,d_{j,m}$), even if by any chance $S_{m0}(\tau_j) \neq \emptyset$. Actually, it holds $S_{m0}(\tau_j) \subseteq N_{m-1}(\tau_j)$, so each $\sigma \in S_{m0}(\tau_j)$ has already been considered: the current factorized polynomial already vanishes in $\Phi^{-1}(\sigma x_{m+1}^{d_{j,m+1}} \cdots x_n^{d_{j,n}})$.

REMARK 5.

(1) The steps described in lines 18 and 19 of Algorithm 1, namely the contruction of $E_{m\delta}(\tau_j)$ and of the associated interpolating polynomial $\gamma_{m\delta\tau_j}$ can be performed in different ways. For example $E_{m\delta}(\tau_j)$ can be computed via Cerlienco-Mureddu correspondence on the points of $\pi_m(A_{m\delta}(\tau_j))$ [2, 3, 4], or via the alternative methods described in [7, 8, 10]. Moreover, there are many interpolation methods in order to compute $\gamma_{m\delta\tau_j}$.
We point out that a possible way to compute both $E_{m\delta}(\tau_j)$ and $\gamma_{m\delta\tau_j}$ is to apply Moeller algorithm [16] to $\pi_m(A_{m\delta}(\tau_j))$.

(2) Fix a term $\tau_j \in \mathsf{G}(I)$. If some $P = (a_1,...,a_n) \in \mathbf{X}$ belongs to $A_{m\delta}(\tau_j)$, $2 \leq m \leq n$, $1 \leq \delta \leq d_{j,m}$, then the linear factor vanishing in P, namely $\gamma_{m\delta\tau_j}$, is constructed involving only the first m coordinates of P, i.e. $a_1,...,a_m$.

(3) Although the minimal Groebner basis $f_1,...,f_r$ got from the Axis of Evil algorithm is not the reduced one, we can point out that the single linear factors $\gamma_{m\delta\tau_j}$ we get, are reduced in the sense that

$$Supp(\gamma_{m\delta\tau_j}) \setminus \{x_m\} \subseteq \{\tau \in \mathsf{N}(I) \,|\, \tau < x_m\},$$

by the construction of $E_{m\delta}(\tau_j)$.

EXAMPLE 4. If we consider the set $\mathbf{X} = \{(0,0),(1,2),(0,2),(3,4),(0,6)\}$, the minimal Groebner basis produced by the Axis of Evil algorithm is

$$\mathcal{G} = \{x^3 - 4x^2 + 3x, xy - x^2 - x, y^3 - \frac{4}{3}xy^2 - 8y^2 + \frac{32}{3}xy + 12y - 16x\},$$

and the linear factors identifying $\mathcal{G}$ are $a = x$, $b = x-1$, $c = x-3$, $d = y-x-1$, $e = y-6$, $f = y-2$ and $g = y - \frac{4}{3}x$. Factors a, b, c, e, f are of the form $x-l, y-h$, with l,h constants, so their support is formed by the leading terms x or y and by $1 \in \mathsf{N}$. Factors d and g satisfy again the property of remark 5 (3), since

- $Supp(y-x-1) \setminus \{y\} = \{1,x\} \subset \mathsf{N}(I)$ and $1 < x < y$;
- $Supp(y - \frac{4}{3}x) \setminus \{y\} = \{x\} \subset \mathsf{N}(I)$ and $x < y$.

REMARK 6. Developing an algorithm one has to face the problems of *termination* and *correctness*.
Termination of our algorithm is guaranteed since it is made up for the following three nested loops:

– a loop on the elements of $\mathsf{G}(I)$ (line 3);

– a loop on the variables of the polynomial ring (line 8);

– for each variable appearing in a term $\tau_j \in \mathsf{G}(I)$, a loop on its exponent (line 16).

The first loop is clearly finite by Dickson's Lemma (c.f. [18]), whereas the second is finite since the polynomial ring has a finite number of variables. Concerning the third one, it is trivially finite since the exponents are natural numbers. Moreover, the steps inside each loop can be performed in a finite time. Indeed, the algorithm could go to infinity if it were $|\mathsf{N}(I)| = \infty$, but this is not the case for our zerodimensional radical ideal I. Moreover, the Axis of Evil Algorithm relies on Cerlienco-Mureddu algorithm and Moeller algorithm so also the computation of the set $A_{m\delta}(\tau_j)$ and the interpolation step terminate.

Let us study the correctness of the algorithm.

PROPOSITION 2. *The factorized polynomials we get from Algorithm 1 vanish on each point of* $\mathbf{X}$.

Proof. Consider the polynomial associated to $\tau = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathsf{G}(I)$ and name it f_τ. We prove that it vanishes on $P_\mu \in \mathbf{X}$, corresponding, via Cerlienco-Mureddu , to the term $\mu = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathsf{N}(I)$.
Since $\tau \in \mathsf{G}(I)$ and $\mu \in \mathsf{N}(I)$, $\tau \neq \mu$. Therefore, there are only two possibilities:

1. $\mu <_{Lex} \tau$. By definition of Lex, $\exists i$, $1 \le i \le n$ with $\alpha_i > \beta_i$, say $\beta_i = \alpha_i - \delta, \delta > 0$ and $\alpha_j = \beta_j$ for each $i+1 \le j \le n$. We set $\omega := x_1^{\beta_1} \cdots x_i^{\beta_i}$. By hypothesis, $\mu = \omega x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n} < \tau$ and $\mu \in \mathsf{N}(I)$, so $\omega \in N_i(\tau)$.

   Moreover $P_\mu = \Phi^{-1}(\mu) = \Phi^{-1}(x_1^{\beta_1} \cdots x_{i-1}^{\beta_{i-1}} x_i^{\alpha_i - \delta} x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n})$ so, either

   $P_\mu \notin D_{i(\delta-1)}(\tau)$ (thus f_τ vanishes in P_μ), or $P_\mu \in A_{i\delta}(\tau)$ but, in this case, by the interpolation step (lines 18-19), f_τ vanishes in P_μ.

2. $\mu >_{Lex} \tau$. Now $\exists i$, $1 \le i \le n$ with $\beta_i > \alpha_i$, $\beta_j = \alpha_j$ for $j \in \{i+1, ..., n\}$.

   By Cerlienco-Mureddu correspondence, $\exists \mu' := x_1^{\beta'_1} \cdots x_n^{\beta'_n} \in \mathsf{N}(I)$ such that:

   a. $\Phi^{-1}(\mu') = P_{\mu'}$ with $\pi_{i-1}(P_\mu) = \pi_{i-1}(P_{\mu'})$;
   b. $\beta'_h = \alpha_h, \forall h \in \{i, i+1, ..., n\}$.

   If $\mu' < \tau$, then $\mu' \in N_{i-1}(\tau)$ so, as in 1., f_τ vanishes in $P_{\mu'}$ and the linear factor making f_τ vanish in $P_{\mu'}$ is computed involving at most the first $i-1$ coordinates of P_μ (c.f. remark 5(2)), so f_τ turns out to vanish also in P_μ. If $\mu' > \tau$, we can repeat with μ' instead of μ and conclude by induction.

□

COROLLARY 1. *The ideal generated by the output polynomials is exactly* $I(\mathbf{X})$.

Proof. The polynomials $f_1, ..., f_r$ of theorem 1 form a minimal Groebner basis because they vanish on all the points of $\mathbf{X}$ (lemma 2) and because their heads $\mathsf{T}(f_1) = \tau_1, ...,$ $\mathsf{T}(f_r) = \tau_r$ form exactly $\mathsf{G}(I(\mathbf{X}))$.

If $\tau_j = x_1^{d_{j,1}} \cdots x_n^{d_{j,n}} \in \mathsf{G}(I(\mathbf{X}))$, the output polynomials contain *exactly* $\sum_{i=1}^n d_i$ factors. It is impossible for a "partial product" (less than $\sum_{i=1}^n d_i$ factors) to vanish on the whole $\mathbf{X}$. Indeed, if so, there would be a polynomial $f \in I(I(\mathbf{X}))$ such that $\mathsf{T}(f) \notin (\mathsf{G}(I(I(\mathbf{X}))))$, being $\mathsf{T}(f) \mid \tau_j \in \mathsf{G}(I(I(\mathbf{X})))$.

□

Algorithm 1 and corollary 1 constitute a constructive proof of the Axis of Evil Theorem 1.
Moreover, corollary 1 implies also that the termination criteria for Algorithm 1 are correct.

REMARK 7. As mentioned above, Cerlienco-Mureddu correspondence works on an ordered set of points. We point out that, for each ordering given to $\mathbf{X}$, Algorithm 1 allows to produce an Axis of Evil factorization for a minimal Groebner basis of $I(\mathbf{X})$.

It is well known that Cerlienco-Mureddu correspondence allows to compute the Groebner escalier of zerodimensional ideals, *even if they are not radical*. Unfortunately, in general, it is *not possibile* to produce an Axis of Evil factorization in case of

multiplicity.
We display here a meaningful example of this fact, due to M.G. Marinari and T. Mora.

EXAMPLE 5 ([14, 18]). Consider the following ideal, given with its primary decomposition:
$J := (x_1^2, x_2+x_1, x_3) \cap (x_1^2, x_2-x_1, x_3-1) =$
$= (x_1^2, x_1x_2, x_2^2, x_1x_3 - \frac{1}{2}x_1 - \frac{1}{2}x_2, x_2x_3 - \frac{1}{2}x_1 - \frac{1}{2}x_2, x_3^2 - x_3) \triangleleft \mathbb{C}[x_1,x_2,x_3]$.
Denote by $f_1,...,f_6$ the generators. J is 0-dimensional being $x_1^2, x_2^2, x_3^2 \in \mathsf{T}(J)$ (see [18]), but it is not radical as $\sqrt{J} = (x_2, x_3^2 - x_3, x_1)$. For such an ideal the Axis of Evil does not hold. Consider the polynomial $f_4 = x_1x_3 - \frac{1}{2}x_1 - \frac{1}{2}x_2$.
According to theorem 1, its factorization should be of the form:

$$(x_1+l)(x_3+f(x_1,x_2)),\ l \in \mathbf{k},\ f(x_1,x_2) \in \mathbf{k}[x_1,x_2]$$

and we should have

$$(x_1+l)(x_3+f(x_1,x_2)) \equiv f_4 \bmod (f_1,f_2,f_3).$$

Since f_1, f_2, f_3 are *terms*, the degree one terms in f_4 have to come from the product, not being possible for them to come from the reduction.
We show that it is impossible for $-\frac{1}{2}x_2$. We would like to have a product of the form

$$k * hx_2,$$

with h,k constants such that $hk = -\frac{1}{2}$, in particular both different from 0.
A priori, there are two possibilities:
- $(x_1+k)(x_3+hx_2+...)$;
- $(x_1+hx_2+...)(x_3+k+...)$.

The second one is impossible: the polynomial having x_1 as head can not contain variables greater than x_1, so we consider only:

$$(x_1+k+...)(x_3+hx_2+...) \text{ obtaining } x_1x_3+hx_1x_2+kx_3-\frac{1}{2}x_2+...$$

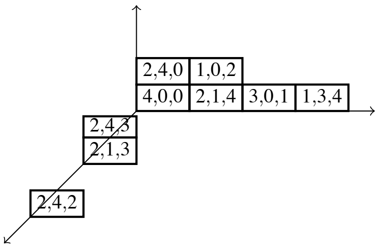
We can delete the term x_1x_2 but kx_3 can not be reduced.

The Axis of Evil Theorem can be generalized in case of Cerlienco-Mureddu ideals (see [18] for more details).

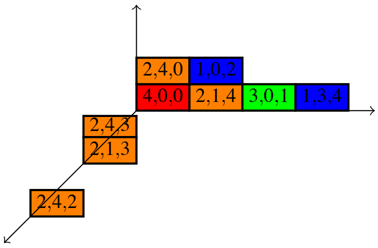
5. The Axis of Evil in pratice: a detailed example.

In this paragraph, we simulate in detail the Axis of Evil algorithm, giving a precise example of its main features. We will examine the tower picture associated to the given set, in order to mark the points making the current factorized polynomial vanish at each step.
Consider the set
$\mathbf{X} = \{(4,0,0),(2,1,4),(2,4,0),(3,0,1),(2,1,3),(1,3,4),(2,4,3),(2,4,2),(1,0,2)\}$.

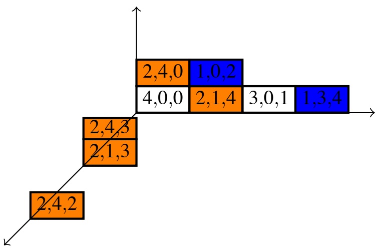
First of all we get $\mathsf{N} = \{1, x_1, x_2, x_1^2, x_3, x_1^3, x_2x_3, x_3^2, x_1x_2\}$, applying Cerlienco- Mureddu algorithm on $\mathbf{X}$; then we obtain $\mathsf{G} = \{x_1^4, x_1^2x_2, x_2^2, x_1x_3, x_2x_3^2, x_3^3\}$ via Lazard algorithm.



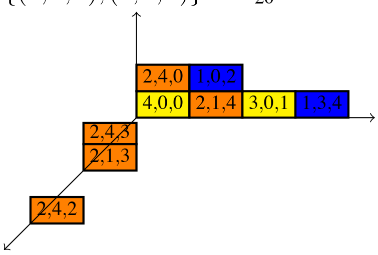
The sets $\mathbf{X}$, N and $\mathsf{G} = \{\tau_1, \ldots, \tau_6\}$ are exactly the input for the Axis of Evil algorithm. We denote them by τ_i for $i = 1, \ldots, 6$.
Starting with $\boldsymbol{\tau_1} = \mathbf{x_1^4}$, we get $N_1(\tau_1) = \{1, x_1, x_1^2, x_1^3\}$ and $A_1(\tau_1) = \{(4,0,0), (2,1,4), (3,0,1), (1,3,4)\}$, containing the corresponding points via Cerlienco-Mureddu, whose first coordinates belong to $B_1(\tau_1) = \{4,2,3,1\}$.



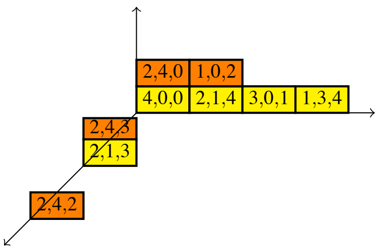
We get $\gamma_{1\tau_1} = (x_1 - 4)(x_1 - 2)(x_1 - 3)(x_1 - 1)$: all the linear factors depend only on x_1 and they have been computed at the same time. We highlight in the picture the points making $\gamma_{1\tau_1}$ vanish and we distinguish them, using colours, w.r.t. the linear factor vanishing on them (i.e. w.r.t. their first coordinates).
Set $m = 2$: $\zeta_{2\tau_1} = \gamma_{1\tau_1}$. Since, as we can also see in the picture above, $D_{20}(\tau) = \emptyset$, we stop here obtaining, as first result, a polynomial $f_1 := \zeta_{2\tau_1} = \gamma_{1\tau}$, whose leading term is $\tau_1 \in \mathsf{G}$, whereas the lower terms belong to N. By construction, $f_1 \in I(\mathbf{X})$, since it vanishes in every point of $\mathbf{X}$: it belongs to our minimal Groebner basis.



For $\boldsymbol{\tau_2} = \mathbf{x_1^2x_2}$ we get $N_1(\tau_2) = \{1, x_1\}$, $A_1(\tau_2) = \{(2,4,0), (1,0,2)\}$ and the corresponding first coordinates are $B_1(\tau_2) = \{2,1\}$, so $\gamma_{1\tau_2} = (x_1 - 2)(x_1 - 1)$.
Passing to $m = 2$ we have $\zeta_{m\tau_2} = \gamma_{1\tau_2}$ and $D_{20}(\tau_2) = \{(4,0,0), (3,0,1)\}$ (the two non-colored points in the picture). We cannot stop here, since we got a polynomial *not vanishing at all the points*.
Moreover, we point out that $\mathsf{T}(\zeta_{m\tau_2}) \neq \tau_2 \in \mathsf{G}$.
We compute $N_2(\tau_2) = \{1, x_1, x_1^2, x_1^3, x_2, x_1x_2\}$; doing so, we find all the terms of the previous step and some new ones. We start the loop on δ: for $\delta = 1$, $A_{21}(\tau_2) = \{(4,0,0), (3,0,1)\} = D_{20}$.

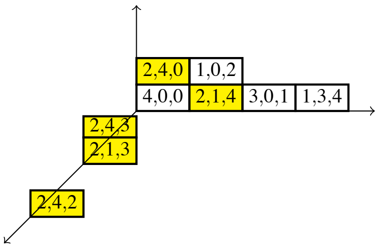


The terms $vx_m^{d_m - \delta}$ of line 17 of Algorithm 1 are $1, x_1, x_1^2, x_1^3$, corresponding to the points P_1, P_2, P_4, P_6. Since the polynomial already vanishes on P_2, P_6, we consider only P_1, P_4. We get $E_{21}(\tau_2) = \{1, x_1\}$, $\gamma_{21\tau_2} = x_2$; $\xi_{21} = \gamma_{1\tau_2}\gamma_{21\tau_2} = (x_1 - 2)(x_1 - 1)x_2$; $D_{21}(\tau_2) = \emptyset$.
Remark that $\gamma_{2\tau_2}$ is actually $\gamma_{21\tau_2}$.
Continue with $\boldsymbol{\tau_3} = \mathbf{x_2^2}$: $N_1(\tau_3) = \emptyset$; $A_1(\tau_3) = \emptyset$; $B_1(\tau_3) = \emptyset$. For $m = 2$, $D_{20}(\tau_3) = \mathbf{X}$; $N_2(\tau_3) = \{1, x_1, x_1^2, x_1^3, x_2, x_1x_2\}$. We set $\delta = 1$, getting $A_{21}(\tau_3) = \{(2,4,0), (1,0,2)\}$; $E_{21}(\tau_3) = \{1, x_1\}$; $\gamma_{21\tau_3} = x_2 - 4x_1 + 4$; $\xi_{21} = \gamma_{1\tau_3}\gamma_{21\tau_3} = x_2 - 4x_1 + 4$.

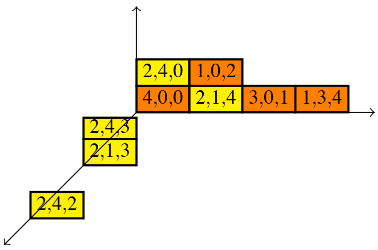


We have $D_{21}(\tau_3) = \{(4,0,0),(2,1,4),(3,0,1),(2,1,3),(1,3,4)\}$. Setting $\delta = 2$, we get $A_{22}(\tau_3) = \{(4,0,0),(2,1,4),(3,0,1),(1,3,4)\}$. The terms $vx_m^{d_m-\delta}$ are $1, x_1, x_1^2, x_1^3$ corresponding exactly to P_1, P_2, P_4, P_6. $E_{22}(\tau_3) = \{1, x_1, x_1^2, x_1^3\}$; $\gamma_{22\tau_3} = 2x_2 - x_1^2 + 7x_1 - 12$; $\xi_{22} = (x_2 - 4x_1 + 4)(2x_2 - x_1^2 + 7x_1 - 12)$; $D_{22}(\tau_3) = \emptyset$;

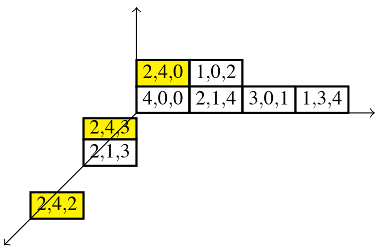
Consider $\tau_4 = \mathbf{x_1 x_3}$:



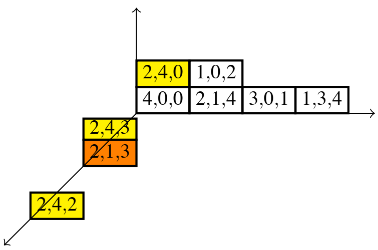
$N_1(\tau_4) = \{1\}$; $A_1(\tau_4) = \{(2,1,3)\}$; $B_1(\tau_4) = \{2\}$ $\gamma_{1\tau_4} = (x_1 - 2)$. Set $m = 2$: $N_2(\tau_4) = \{1\}$, $D_{20}(\tau_4) = \{(4,0,0),(3,0,1),(1,3,4),(1,0,2)\}$. For $\delta = 1$; $D_{21}(\tau) = D_{20}(\tau)$; Set $m = 3$: $N_3(\tau_4) = \{1, x_1, x_2, x_1^2, x_3, x_1^3, x_1x_2\}$; $\zeta_{3\tau_4} = (x_1 - 2)$; $D_{30}(\tau_4) = \{(4,0,0),(3,0,1),(1,3,4),(1,0,2)\}$.



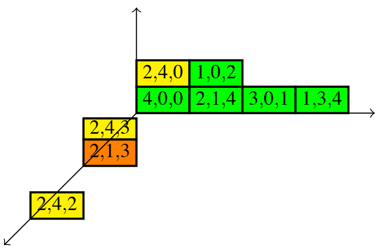
For $\delta = 1$, $A_{31}(\tau_4) = \{(4,0,0),(3,0,1),(1,3,4),(1,0,2)\}$. The terms are $1, x_1, x_1^2, x_1^3, x_2, x_1x_2$, corresponding to $P_1, P_2, P_3, P_4, P_6, P_9$, and P_2, P_3 can be neglected. We have $E_{31}(\tau_4) = \{1, x_1, x_1^2, x_2\}$; $\gamma_{31}(\tau_4) = 6x_3 - 4x_2 + x_1^2 - x_1 - 12$; $\xi_{31} = (x_1 - 2)(6x_3 - 4x_2 + x_1^2 - x_1 - 12)$; $D_{31}(\tau_4) = \emptyset$ and $\gamma_{3\tau_4} = \gamma_{31}(\tau_4)$.



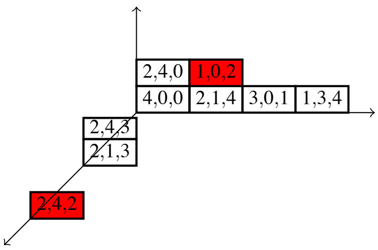
Set $\tau_5 = \mathbf{x_2 x_3^2}$: we get $N_1(\tau_5) = \emptyset$; $A_1(\tau_5) = \emptyset$; $B_1(\tau_5) = \emptyset$. For $m = 2$ we have $N_2(\tau_5) = \{1\}$; $D_{20}(\tau_5) = \mathbf{X}$; $\delta = 1$: $A_{21}(\tau_5) = \{(2,4,2)\}$; $E_{21}(\tau_5) = \{1\}$; $\gamma_{21\tau_5} = x_2 - 4$ $\xi_{21} = x_2 - 4$; $D_{21}(\tau_5) = \{(4,0,0),(2,1,4),(3,0,1),(2,1,3),(1,3,4),(1,0,2)\}$;



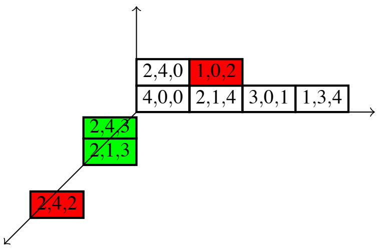
For $m = 3$ we get $\zeta_{3\tau_5} = x_2 - 4$; $D_{30}(\tau_5) = D_{21}(\tau_5)$; $N_3(\tau) = \mathsf{N}(\mathbf{X})$. We set $\delta = 1$ and we obtain $A_{31}(\tau) = \{(2,1,3)\}$; $E_{31}(\tau) = \{1\}$; $\gamma_{21\tau} = x_3 - 3$; $\xi_{31} = (x_2 - 4)(x_3 - 3)$; $D_{31}(\tau) = \{(4,0,0),(2,1,4),(3,0,1),(1,3,4),(1,0,2)\}$;



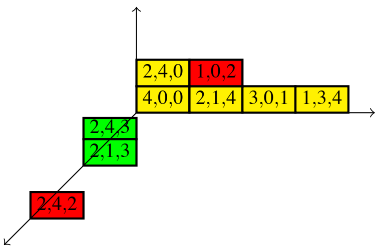
For $\delta = 2$ $A_{32}(\tau) = D_{31}(\tau)$; $E_{32}(\tau) = \{1, x_1, x_1^2, x_1^3, x_2\}$;
$\gamma_{32\tau} = x_3 - 4x_2 - 5x_1^3 + 41x_1^2 - 96x_1 + 48$;
$\xi_{32} = (x_2 - 4)(x_3 - 3)(x_3 - 4x_2 - 5x_1^3 + 41x_1^2 - 96x_1 + 48)$; $D_{32}(\tau) = \emptyset$;
$\gamma_{3\tau} = (x_3 - 3)(x_3 - 4x_2 - 5x_1^3 + 41x_1^2 - 96x_1 + 48)$;



For $\tau_6 = \mathbf{x_3^3}$, $N_1(\tau_6) = \emptyset$; $A_1(\tau_6) = \emptyset$ and $B_1(\tau_6) = \emptyset$. Set then $m = 2 : D_{20}(\tau_6) = \mathbf{X}$; $N_2(\tau_6) = \emptyset$. For $\delta = 1$, we obtain $A_{21}(\tau_6) = \emptyset$ and $D_{21}(\tau_6) = \mathbf{X}$. Setting $m = 3$ we get $D_{30} = \mathbf{X}$; $N_3(\tau_6) = \mathsf{N}(\mathbf{X})$. For $\delta = 1$, $A_{31}(\tau_6) = \{(2,4,2)\}$; $E_{31}(\tau_6) = \{1\}$; $\gamma_{31\tau_6} = x_3 - 2$; $\xi_{31} = x_3 - 2$; $D_{31}(\tau_6) = \{(4,0,0), (2,1,4), (2,4,0), (3,0,1), (2,1,3), (1,3,4), (2,4,3)\}$.



Now we consider $\delta = 2$.
For this value, we have $A_{32}(\tau_6) = \{(2,1,3), (2,4,3)\}$, $E_{32}(\tau_6) = \{1, x_2\}$ and the polynomial $\gamma_{32\tau_6} = x_3 - 3$.
Then $\xi_{32} = (x_3 - 2)(x_3 - 3)$ and, finally, the set $D_{32} = \{(4,0,0), (2,1,4), (2,4,0), (3,0,1), (1,3,4)\}$;



For $\delta = 3$, $A_{33}(\tau_6) = D_{32}$; $E_{33}(\tau_6) = \{1, x_1, x_1^2, x_1^3, x_2\}$; $\gamma_{33\tau_6} = 6x_3 + 8x_2 - 5x_1^3 + 35x_1^2 - 54x_1 + 24$.
Then $\xi_{33} = (x_3 - 2)(x_3 - 3)(6x_3 + 8x_2 - 5x_1^3 + 35x_1^2 - 54x_1 + 24)$; $D_{33}(\tau_6) = \emptyset$.
$\gamma_{3\tau_6} = (x_3 - 2)(x_3 - 3)(6x_3 + 8x_2 - 5x_1^3 + 35x_1^2 - 54x_1 + 24)$.

The factorized minimal Groebner basis for $I(\mathbf{X})$ w.r.t. lex is:

$$\mathcal{G}(I(\mathbf{X})) = \Big\{(x_1 - 4)(x_1 - 2)(x_1 - 3)(x_1 - 1), (x_1 - 2)(x_1 - 1)x_2,$$
$$(x_2 - 4x_1 + 4)(2x_2 - x_1^2 + 7x_1 - 12), (x_1 - 2)(6x_3 - 4x_2 + x_1^2 - x_1 - 12),$$
$$(x_2 - 4)(x_3 - 3)(6x_3 - 4x_2 - 5x_1^3 + 41x_1^2 - 96x_1 + 48),$$
$$(x_3 - 2)(x_3 - 3)(6x_3 + 8x_2 - 5x_1^3 + 35x_1^2 - 54x_1 - 24)\Big\},$$

whereas the reduced Groebner basis of $I(\mathbf{X})$ w.r.t. lex is:

$$\begin{gathered}\mathcal{G}'(I(\mathbf{X})) = \Big\{x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2x_1^2 - 3x_2x_1 + 2x_2, \\ x_2^2 - 2x_2x_1 - x_2 + 2x_1^3 - 16x_1^2 + 38x_1 - 24, x_3x_1 - 2x_3 - \tfrac{2}{3}x_2x_1 + \tfrac{4}{3}x_2 + \\ + \tfrac{1}{6}x^3 - \tfrac{1}{2}x_1^2 - \tfrac{5}{3}x_1 + 4, x_3^2x_2 - 4x_3^2 - 7x_3x_2 + 28x_3 + \tfrac{8}{3}x_2x_1 + \\ + \tfrac{20}{3}x_2 - \tfrac{16}{3}x^3 + 48x^2 - \tfrac{344}{3}x_1 + 32, x_3^3 - 5x_3^2 + \tfrac{8}{3}x_3x_2 - \tfrac{14}{3}x_3 - \tfrac{16}{9}x_2x_1 \\ - \tfrac{40}{9}x_2 + \tfrac{73}{9}x_1^3 - \tfrac{197}{3}x_1^2 + \tfrac{1358}{9}x_1 - 72\Big\},\end{gathered}$$

Since we have considered the elements of $\mathsf{G}(I(\mathbf{X}))$ in lexicographical order ($x_1 < ... < x_n$), the reduced Groebner basis is obtained by reducing the polynomials in $\mathcal{G}(I(\mathbf{X}))$, each one w.r.t. the previous ones.

Acknowledgments

I would like to offer my special thanks to Professor Maria Grazia Marinari, for her help and suggestions, which helped me to develop this work.
Advice given by Professor Margherita Roggero has been a great help in the drawing up of this paper.

References

[1] M.E. Alonso, M.G. Marinari, T. Mora, *The big Mother of all Dualities 2: Macaulay Bases*, Applicable Algebra in Engineering, Communication and Computing archive Vol. 17 Issue 6, November 2006, 409 – 451.

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

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

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

[5] W. Decker, G.M. Greuel, G. Pfister, H. Schönemann, Singular 3-1-4 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2012).

[6] J.C. Faugere, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering,* J. Symb. Comp., 16 (1993) 329-344.

[7] B. Felszeghy, B. Ráth, L. Rónyai *The lex game and some applications*, J. Symbolic Computation 41 (2006), 663 – 681.

[8] S. Gao, V.M. Rodrigues, J. Stroomer, *Groebner basis structure of finite sets of points*, (2003),preprint.

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

[10] M. LEDERER, *The vanishing ideal of a finite set of closed points in affine space*, Journal of Pure and Appliead Algebra 212, (2008), pagg. 1116 – 1133.

[11] S. LUNDQVIST, *Vector space bases associated to vanishing ideals of points*, Journal of Pure and Applied Algebra, 214, Issue 4, (2010), pagg 309 – 321.

[12] S. LUNDQVIST, *Complexity of Comparing Monomials and Two Improvements of the Buchberger-Moeller Algorithm*, Mathematical Methods in Computer Science, 2008, Springer.

[13] M.G. MARINARI AND TEO MORA, *Cerlienco-Mureddu Correspondence and Lazard Structural Theorem.*, Revista Investicación Operacional, Vol.27, No.2, 155-178, 2006.

[14] M.G. MARINARI AND TEO MORA, *A remark on a remark by Macaulay or Enhancing Lazard Structural Theorem.*, Bulletin of the Iranian Mathematical Society Vol. 29 No. 1 (2003), pagg. 1 – 45.

[15] M.G. MARINARI AND TEO MORA, *Some Comments on Cerlienco-Mureddu Algorithm and Enhanced Lazard Structural Theorem*, Rejected by ISSAC-2004 (2004).

[16] M.G. MARINARI, H.M MOELLER, T. MORA, *Groebner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points*, Applicable Algebra in Engineering, Communication and Computing, vol. 4, 1993, Springer.

[17] M.G . MARINARI AND L. RAMELLA, *Borel Ideals in three variables*, Beiträge zur Algebra und Geometrie. Contributions to Algebra and Geometry, Vol 47 (2006), N. 1, 195 – 209.

[18] T. MORA, *Solving polynomial equation systems: Macaulay's paradigm and Groebner technology*, Cambridge University Press, 2005.

[19] S. STEIDEL, `pointid.lib`. Procedures for computing a factorized lex GB of the vanishing ideal of a set of points via the Axis-of-Evil Theorem (M.G. Marinari, T. Mora) (2011).

AMS Subject Classification: 13P10.

Michela CERIA
Dipartimento di Matematica
Università di Trento
Via Sommarive 14
38123 Povo, Trento, ITALY
e-mail: `michela.ceria@unitn.it`

Lavoro pervenuto in redazione il 15.10.2014, e, in forma definitiva, il 15.12.2014