From algebraic sets to monomial linear bases by means of combinatorial algorithms.

L. Cerlienco and M. Mureddu

Summary. Let K be a field; let $\mathcal{P} \subset K^n$ be a finite set and let $\Im(\mathcal{P}) \subset K[x_1, \ldots, x_n]$ be the ideal of $\mathcal{P}$. A purely combinatorial algorithm to obtain a linear basis of the quotient algebra $K[x_1, \ldots, x_n]/\Im(\mathcal{P})$ is given. Such a basis is represented by an n-dimensional Ferrers diagram of monomials which is minimal with respect to the inverse lexicographical order $\preceq_{i.l.}$. It is also shown how this algorithm can be extended to the case in which $\mathcal{P}$ is an *algebraic multiset*. A few applications are stated (among them, how to determine a reduced Gröbner basis of $\Im(\mathcal{P})$ with respect to $\preceq_{i.l.}$ without using Buchberger's algorithm).

1 Introduction

1.1 Let $\mathbf{N}$ be the monoid of non-negative integers. Denote by $\mathbf{i} := (i_1, \ldots, i_n)$ an arbitrary element in the power $\mathbf{N}^n$. The usual order on $\mathbf{N}$, as well as the partial order it induces on $\mathbf{N}^n$, will be denoted by $\leq$.

Define an *n-dimensional Ferrers diagram* to be any finite ideal of the poset $\mathbf{N}^n$, i.e. any non-empty finite subset $\mathcal{F} \subseteq \mathbf{N}^n$ such that $\mathbf{j} < \mathbf{i} \in \mathcal{F} \Longrightarrow \mathbf{j} \in \mathcal{F}$. An element $\mathbf{i} = (i_1, \ldots, i_n) \notin \mathcal{F}$ is said to be a *co-minimal element* for the Ferrers diagram $\mathcal{F}$ if it is a minimal element of the complementary filter $\mathbf{N}^n \setminus \mathcal{F}$, i.e. if $(i_1, \ldots, i_{r-1}, i_r - 1, i_{r+1}, \ldots, i_n) \in \mathcal{F}$ for each r such that $i_r \geq 1$. Of course, $\mathbf{i} \notin \mathcal{F}$ is a co-minimal element iff $\mathcal{F}' := \{\mathbf{i}\} \cup \mathcal{F}$ is a Ferrers diagram.

We will write $\preceq$ for any *term-ordering* on $\mathbf{N}^n$, i.e. a linear ordering which is compatible with the monoid structure on $\mathbf{N}^n$:

$$\mathbf{0} \prec \mathbf{i} \qquad \text{for every } \mathbf{i} \neq \mathbf{0} \text{ in } \mathbf{N}^n,$$

$$\mathbf{i} \preceq \mathbf{j} \Longrightarrow \mathbf{i}+\mathbf{r} \preceq \mathbf{j}+\mathbf{r} \qquad \text{for every } \mathbf{i},\mathbf{j},\mathbf{r} \in \mathbf{N}^n.$$

It is well known that every term-ordering on $\mathbf{N}^n$ is also a well-ordering.

1.2 Let K be a field and let $X := \{x_1, x_2, \ldots, x_n\}$ be a given set of indeterminates. Let us consider the usual polynomial algebra $K[X] := K[x_1, \ldots, x_n]$. Denote by $M_X \subseteq K[X]$ the free abelian monoid on X. The elements of M_X (i.e. the monic monomials) will be called *terms* of $K[X]$ and denoted by $\mathbf{x}^{\mathbf{i}} := x_1^{i_1} \cdots x_n^{i_n}$ with $\mathbf{i} := (i_1, \ldots, i_n) \in \mathbf{N}^n$. The orders $\leq$ and $\preceq$ on $\mathbf{N}^n$, as well as the notion of Ferrers diagram, extend to M_X in an obvious way.

An ideal J of the algebra $K[X]$ is said to be *cofinite* if

$$\operatorname{codim}(J) := \dim (K[X]/J) < \infty.$$

Given a finite set $\mathcal{P} := \{P_1, \ldots, P_N\} \subseteq K^n$, the ideal

$$\Im(\mathcal{P}) := \{p \in K[X] \mid (\forall P \in \mathcal{P})(p(P) = 0)\}$$

of the algebraic set $\mathcal{P}$ is cofinite. More generally, when K is algebraically closed, from the *Nullstellensatz* it follows that an ideal $J \subseteq K[X]$ is a cofinite ideal iff the algebraic set of J, i.e.

$$\mathcal{V}(J) := \{P \in K^n \mid (\forall p \in J)(p(P) = 0)\},$$

is finite. In this case we have $\#\mathcal{V}(J) = \operatorname{codim}(\sqrt{J}) \leq \operatorname{codim}(J)$ (cfr. [5] p.23).

For a given ideal J, any linear basis $\mathcal{L}_J$ of the quotient algebra $K[X]/J$ whose elements are of the form $[\mathbf{x}^{\mathbf{i}}]_J := \mathbf{x}^{\mathbf{i}} + J$ will be called a *monomial basis*. If $\mathcal{L}_J = \{\mathbf{x}^{\mathbf{i}} + J \mid \mathbf{i} \in L \subseteq \mathbf{N}^n\}$ is a monomial basis, we shall say that $\{\mathbf{x}^{\mathbf{i}} \mid \mathbf{i} \in L\}$ is a *system of representatives* for the monomial basis $\mathcal{L}_J$. Obviously, if $\mathcal{L}_J = \{\mathbf{x}^{\mathbf{i}} + J \mid \mathbf{i} \in L\}$ is a monomial basis of $K[X]/J$, then any polynomial $p \in K[X]$ is congruent modulo J to exactly one polynomial of the form $\sum_{\mathbf{i} \in L} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$, $a_{\mathbf{i}} \in K$. Given an arbitrary term-ordering $\preceq$ on M_X, a monomial basis $\mathcal{L}_J = \{\mathbf{x}^{\mathbf{i}_1} + J, \ldots, \mathbf{x}^{\mathbf{i}_N} + J\}$ with $\mathbf{x}^{\mathbf{i}_1} \prec \ldots \prec \mathbf{x}^{\mathbf{i}_N}$ is said to be *minimal* with respect to $\preceq$ if for any other monomial basis $\mathcal{L}'_J = \{\mathbf{x}^{\mathbf{i}'_1} + J, \ldots, \mathbf{x}^{\mathbf{i}'_N} + J\}$ with $\mathbf{x}^{\mathbf{i}'_1} \prec \ldots \prec \mathbf{x}^{\mathbf{i}'_N}$ we have $\mathbf{x}^{\mathbf{i}_j} \preceq \mathbf{x}^{\mathbf{i}'_j}$ for $j = 1, \ldots, N$. Equivalently, $\mathcal{L}_J = \{\mathbf{x}^{\mathbf{i}_1} + J, \ldots, \mathbf{x}^{\mathbf{i}_N} + J\}$, $\mathbf{x}^{\mathbf{i}_1} \prec \ldots \prec \mathbf{x}^{\mathbf{i}_N}$, is *minimal* with respect to $\preceq$ if every term $\mathbf{x}^{\mathbf{i}}$, such that $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{i}_j}$, is linearly dependent (modulo J) on $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_{j-1}}$. Of course, both $\mathcal{L}_J$ and $\mathcal{L}'_J$, $\mathcal{L}_J \neq \mathcal{L}'_J$, could be minimal with respect to different term-orderings. It is not hard to prove that if $\mathcal{L}_J = \{\mathbf{x}^{\mathbf{i}_j} + J \mid j = 1, \ldots, N\}$ is a minimal monomial basis then $L = \{\mathbf{i}_1, \ldots, \mathbf{i}_N\} \subseteq \mathbf{N}^n$ is an n-dimensional Ferrers diagram. In fact, if $\mathbf{x}^{\mathbf{i}} \notin \mathcal{L}_J$, then

$$\mathbf{x}^{\mathbf{i}} = \sum_{\mathbf{x}^{\mathbf{i}_j} \prec \mathbf{x}^{\mathbf{i}}} \lambda_j \mathbf{x}^{\mathbf{i}_j} \qquad \text{modulo } J.$$

Thus,

$$\mathbf{x}^{\mathbf{i}+\mathbf{r}} = \sum_{\mathbf{x}^{\mathbf{i}_j} \prec \mathbf{x}^{\mathbf{i}}} \lambda_j \mathbf{x}^{\mathbf{i}_j+\mathbf{r}} \qquad \text{modulo } J$$

where $\mathbf{r} \in \mathbf{N}^n$ and $\mathbf{x}^{\mathbf{i}_j} \prec \mathbf{x}^{\mathbf{i}_j+\mathbf{r}} \prec \mathbf{x}^{\mathbf{i}+\mathbf{r}}$ as $\preceq$ is a term-ordering. Since either $\mathbf{x}^{\mathbf{i}_j+\mathbf{r}} + J$ belongs to $\mathcal{L}_J$ or $\mathbf{x}^{\mathbf{i}_j+\mathbf{r}} + J$ is a linear combination of smaller elements in $\mathcal{L}_J$, from the above congruence we deduce that the same is true for $\mathbf{x}^{\mathbf{i}+\mathbf{r}} + J$:

$$\mathbf{x}^{\mathbf{i}+\mathbf{r}} = \sum_{\mathbf{x}^{\mathbf{i}_j} \prec \mathbf{x}^{\mathbf{i}+\mathbf{r}}} \mu_j \mathbf{x}^{\mathbf{i}_j} \qquad \text{modulo}\, J.$$

Hence, $\mathbf{i} \notin L \Rightarrow \mathbf{i}+\mathbf{r} \notin L$, i.e. $\mathbf{i}+\mathbf{r} \in L \Rightarrow \mathbf{i} \in L$; thus, L is a Ferrers diagram.

1.3 In the search for a minimal monomial basis $\mathcal{L}_{\mathcal{P}}$, in the following section we present a purely combinatorial algorithm to get it from $\mathcal{P}$. In fact, making use of the **Algorithm MB** below, we associate a Ferrers diagram $\mathcal{MB}(\mathcal{P}) = \{\mathbf{d}_1, \ldots, \mathbf{d}_N\} \subseteq \mathbf{N}^n$ to any finite set $\mathcal{P} := \{P_1, \ldots, P_N\} \subseteq K^n$. The Ferrers diagram $\mathcal{MB}(\mathcal{P})$ gives the monomial basis $\mathcal{L}_{\mathcal{P}} = \{\mathbf{x}^{\mathbf{d}} + \Im(\mathcal{P}) \mid \mathbf{d} \in \mathcal{MB}(\mathcal{P})\}$ which is minimal with respect to the inverse lexicographical ordering $\preceq_{i.l.}$ with $x_1 \prec_{i.l.} x_2 \prec_{i.l.} \ldots \prec_{i.l.} x_n$.

The implementation of **Algorithm MB**, as well as that of its applications described in section **4**, presents no serious difficulties.

2 The Algorithm MB

2.1 Let $\mathcal{P} := \{P_1, \ldots, P_N\} \subseteq K^n$. For $1 \leq j \leq N$ and for $0 \leq s \leq n$, put
$\underline{\mathcal{P}} := (P_1, \ldots, P_N)$;
$\mathbf{d}_j = (d_{j,1}, \ldots, d_{j,n}) \in \mathbf{N}^n$;
$\pi_s \colon K^n \longrightarrow K^s, \quad (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_s)$ ($\pi_0(P)$ is assumed to be the empty sequence);
$\pi^s \colon K^n \longrightarrow K^{n-s+1}, \quad (x_1, \ldots, x_n) \mapsto (x_s, \ldots, x_n)$.

Given a list $\underline{\mathcal{P}} := (P_1, \ldots, P_N)$ of points, we determine an ordered set $\underline{\mathcal{F}} := (\mathbf{d}_1, \ldots, \mathbf{d}_N)$.

MB1. [Initialize.]
Set $\mathbf{d}_1 \leftarrow \mathbf{d}_2 \leftarrow \ldots \mathbf{d}_N \leftarrow (0, \ldots, 0)$; $i \leftarrow 1$.
(*In the beginning the coordinates of all the elements of* $\underline{\mathcal{F}}$ *are zero.*)

MB2. [Put the first i points of the list $\underline{\mathcal{P}}$ in $\mathcal{Q}$.]
Set $\mathcal{Q} \leftarrow \{P_j \mid 1 \leq j \leq i\}$.

MB3. [Find which coordinate of $\mathbf{d}_{i+1}$ has to be changed, say $d_{i+1,s}$.]
Set $s \leftarrow \max\{k \geq 1 \mid \pi_{k-1}(P_j) = \pi_{k-1}(P_{i+1})$, for some $P_j \in \mathcal{Q}\}$.
($s-1$ *is the length of the longest initial segment shared by* P_{i+1} *and some point* $P_j \in \mathcal{Q}$. *If* $s > 1$, *then in successive steps this value decreases.*)

MB4. [Find the points that determine the s-th coordinate of $\mathbf{d}_{i+1}$.]
Set $\mathcal{E} \leftarrow \{j \mid P_j \in \mathcal{Q},\ \ \pi_{s-1}(P_j) = \pi_{s-1}(P_{i+1}),\ \ \pi^{s+1}(\mathbf{d}_j) = \pi^{s+1}(\mathbf{d}_{i+1})\}$.
($\mathcal{E}$ contains the indices of the points of $\mathcal{Q}$ which have the first $s-1$ coordinates equal to those of P_{i+1} and whose corresponding elements in $\underline{\mathcal{F}}$ have the $n-s$ rightmost coordinates equal to those of $\mathbf{d}_{i+1}$. $\mathcal{E}$ is always non-empty.)

MB5. [Assign the value to the s-th coordinate of $\mathbf{d}_{i+1}$.]
Set $d_{i+1,s} \leftarrow (1 + \max\{d_{j,s} \mid j \in \mathcal{E}\})$.

MB6. [Did you determine the first coordinate of $\mathbf{d}_{i+1}$?]
If $s > 1$

MB6.1. [Find the points that determine another coordinate of $\mathbf{d}_{i+1}$.]
Set $\mathcal{Q} \leftarrow \{P_j \mid 1 \leq j \leq i,\ \pi^s(\mathbf{d}_j) = \pi^s(\mathbf{d}_{i+1}) = (d_{i+1,s}, \ldots, d_{i+1,n})\}$.
($\mathcal{Q}$ contains the points of $\underline{\mathcal{P}}$ different from P_{i+1} whose corresponding elements in $\underline{\mathcal{F}}$ have the $n-s+1$ rightmost coordinates equal to those of $\mathbf{d}_{i+1}$.)

MB6.2. [Is $\mathcal{Q}$ empty?]
If $\mathcal{Q} \neq \emptyset$, return to step **MB3.**

MB7. [Increase i.]
Set $i \leftarrow i + 1$. If $i < N$, return to step **MB2.**

MB8. [Done.] Terminate the algorithm.

2.2 Let $\underline{\mathcal{P}} := (P_1, \ldots, P_N)$ and $\underline{\mathcal{F}} := (\mathbf{d}_1, \ldots, \mathbf{d}_N)$ as in **2.1**. We put: $\mathcal{MB}(\mathcal{P}) := \{\mathbf{d}_1, \ldots, \mathbf{d}_N\}$; $\delta_{\underline{\mathcal{P}}}: \mathcal{P} \to \mathcal{MB}(\mathcal{P})$, $P_i \mapsto \mathbf{d}_i$. Notice that now and in the following notations such as $\underline{\mathcal{P}}$ and $\underline{\mathcal{F}}$ always denote *ordered sets* whose underlying sets are $\mathcal{P}$ and $\mathcal{F}$, respectively; moreover, the order on $\underline{\mathcal{F}}$, as well as the map $\delta_{\underline{\mathcal{P}}}$, depends on both the ordered set $\underline{\mathcal{P}}$ and the **Algorithm MB**. One could think that $\mathcal{MB}(\mathcal{P})$ is ill-defined, namely that it depends on the order which has been used for arranging the points $P_1, \ldots, P_N$ when starting **Algorithm MB** (i.e. on the list $\underline{\mathcal{P}}$) rather than on the set $\mathcal{P} = \{P_1, \ldots, P_N\}$ itself. Well, this is not true. In fact, the following properties hold.

Lemma 1 *Let $\underline{\mathcal{P}} := (P_1, \ldots, P_i, P_{i+1}, \ldots, P_N)$, $\underline{\mathcal{P}'} := (P_1, \ldots, P_{i+1}, P_i, \ldots, P_N)$. Let $\underline{\mathcal{F}} := (\mathbf{d}_1, \ldots, \mathbf{d}_i, \mathbf{d}_{i+1}, \ldots, \mathbf{d}_N)$ and $\underline{\mathcal{F}'} := (\mathbf{d}'_1, \ldots, \mathbf{d}'_i, \mathbf{d}'_{i+1}, \ldots, \mathbf{d}'_N)$ be the lists associated by* **Algorithm MB** *with $\underline{\mathcal{P}}$ and $\underline{\mathcal{P}'}$ respectively. Then, $\{\mathbf{d}_1, \ldots, \mathbf{d}_N\} = \{\mathbf{d}'_1, \ldots, \mathbf{d}'_N\}$.*

Proof. Consider

$$P_i = (a_{i,1}, \ldots, a_{i,r-1}, a_{i,r}, \ldots, a_{i,n}),$$

$$P_{i+1} = (a_{i+1,1}, \ldots, a_{i+1,r-1}, a_{i+1,r}, \ldots, a_{i+1,n}),$$

$$\mathbf{d}_i = (d_{i,1}, \ldots, d_{i,r-1}, d_{i,r}, \ldots, d_{i,n}),$$

$$\mathbf{d}_{i+1} = (d_{i+1,1}, \ldots, d_{i+1,r-1}, d_{i+1,r}, \ldots, d_{i+1,n})$$

where r is such that $d_{i,r} \neq d_{i+1,r}, d_{i,r+1} = d_{i+1,r+1}, \ldots, d_{i,n} = d_{i+1,n}$. It may happen that either i) $(a_{i,1}, \ldots, a_{i,r-1}) \neq (a_{i+1,1}, \ldots, a_{i+1,r-1})$ (in which case $\mathbf{d'}_i = \mathbf{d}_{i+1}$ and $\mathbf{d'}_{i+1} = \mathbf{d}_i$), or ii) $(a_{i,1}, \ldots, a_{i,r-1}) = (a_{i+1,1}, \ldots, a_{i+1,r-1})$ (in which case we have $a_{i,r} \neq a_{i+1,r}$, since otherwise $d_{i,r+q} \neq d_{i+1,r+q}$ for some $q \geq 1$. From this we deduce $\mathbf{d'}_i = \mathbf{d}_i$ and $\mathbf{d'}_{i+1} = \mathbf{d}_{i+1}$).
First notice that obviously $\mathbf{d}_1 = \mathbf{d'}_1, \ldots, \mathbf{d}_{i-1} = \mathbf{d'}_{i-1}$. We prove that we also have $\mathbf{d}_{i+2} = \mathbf{d'}_{i+2}, \ldots, \mathbf{d}_N = \mathbf{d'}_N$ by distinguishing the case i) from the case ii). In the first case the proof is easy. In fact, when calculating $\mathbf{d}_{i+t}$ and/or $\mathbf{d'}_{i+t}$, the set $\mathcal{E}$ defined in **MB4** cannot contain both i and $i+1$ since $\pi^{s+1}(\mathbf{d}_i) \neq \pi^{s+1}(\mathbf{d}_{i+1})$ for every $s \leq r$ and $\pi_{s-1}(P_i) \neq \pi_{s-1}(P_{i+1})$ for every $s > r$.
In case ii), suppose that $\mathbf{d}_{i+2} = \mathbf{d'}_{i+2}, \ldots, \mathbf{d}_{N-1} = \mathbf{d'}_{N-1}$; consider $\mathbf{d}_N = (d_{N,1}, \ldots, d_{N,t-1}, d_{N,t} \neq 0, d_{N,t+1} = 0, \ldots, d_{N,n} = 0)$, so that $(a_{N,1}, \ldots, a_{N,t-1})$ is the longest initial segment of the coordinates that P_N shares with some P_j, $j < N$. By arguing separately in the three cases $t = r$, $t < r$ and $t > r$, it is not difficult to prove that $\mathbf{d'}_N = \mathbf{d}_N$. $\square$

As a straightforward consequence of **Lemma 1** we obtain the following proposition.

Prop. 1 *Let $\underline{\mathcal{P}}$ and $\underline{\mathcal{F}}$ be as in* **Lemma 1**. *Let $\underline{\mathcal{F}'} := (\mathbf{d'}_1, \ldots, \mathbf{d'}_N)$ be the list associated by* **Algorithm MB** *with the list of points $\underline{\mathcal{P}'} = (P_{\sigma(1)}, \ldots, P_{\sigma(N)})$, where $\sigma \in S_N$. (S_N is the symmetric group.) Then, for some $\tau \in S_N$ we have $(\mathbf{d'}_1, \ldots, \mathbf{d'}_N) = (\mathbf{d}_{\tau(1)}, \ldots, \mathbf{d}_{\tau(N)})$.* $\square$

Corollary 1 *If $\mathcal{P} \subseteq \mathcal{Q}$, then $\mathcal{MB}(\mathcal{P}) \subseteq \mathcal{MB}(\mathcal{Q})$.* $\square$

Prop. 2 *Let $\underline{\mathcal{P}}$ and $\underline{\mathcal{F}}$ be as in* **Lemma 1**. *It is possible to rearrange the points $P_1, \ldots, P_N$ in a suitable list $\underline{\mathcal{P}'} = (P_{\sigma(1)}, \ldots, P_{\sigma(N)})$ such that the elements in the corresponding list $\underline{\mathcal{F}'} = (\mathbf{d}_{\tau(1)}, \ldots \ldots, \mathbf{d}_{\tau(N)})$ are in inverse lexicographical order $\preceq_{i.l.}$: $s < t \Rightarrow \mathbf{d}_{\tau(s)} \prec_{i.l.} \mathbf{d}_{\tau(t)}$.*

Proof. Let $P_j = (a_{j,1}, \ldots, a_{j,r-1}, a_{j,r}, \ldots, a_{j,n})$, $\mathbf{d}_j = (d_{j,1}, \ldots, d_{j,r-1}, d_{j,r}, \ldots, d_{j,n})$, $j = 1, \ldots, N$. It suffices to observe that if, for some i, $\mathbf{d}_{i+1} := \delta_{\underline{\mathcal{P}}}(P_{i+1}) \prec_{i.l.} \mathbf{d}_i := \delta_{\underline{\mathcal{P}}}(P_i)$ (i.e. $d_{i,r} > d_{i+1,r}, d_{i,r+1} = d_{i+1,r+1}, \ldots, d_{i,n} = d_{i+1,n}$ for some $r \leq n$), then we have necessarily the case i) considered in the proof of **Lemma 1**. $\square$

Lemma 2 *Let $\underline{\mathcal{P}}$ and $\underline{\mathcal{F}}$ be as in* **Lemma 1**. *Let $\mathbf{d}_N = (d_{N,1}, \ldots, d_{N,n})$. If $d_{N,i} \neq 0$, then there is some $k < N$ such that $\mathbf{d}_k = (d_{N,1}, \ldots, d_{N,i-1}, d_{N,i} - 1, d_{N,i+1}, \ldots, d_{N,n})$.*

Proof. When calculating the first $i-1$ coordinates $d_{N,1},\ldots,d_{N,i-1}$ of $\mathbf{d}_N = \delta_{\underline{\mathcal{P}}}(P_N)$, we have to consider the set $\{P_{j_1},\ldots,P_{j_s},P_{j_{s+1}} = P_N\} \subseteq \mathcal{P}$, $j_1 < \ldots < j_s < N$, of all points $P_{j_r} \in \mathcal{P}$ such that $\pi^i(\delta_{\underline{\mathcal{P}}}(P_{j_r})) = (d_{N,i},\ldots,d_{N,n})$. Putting $\underline{\tilde{\mathcal{P}}} := (\pi_{i-1}(P_{j_1}),\ldots,\pi_{i-1}(P_{j_s}),\pi_{i-1}(P_N))$, we have $\pi_{i-1}(\delta_{\underline{\mathcal{P}}}(P_N)) = \delta_{\underline{\tilde{\mathcal{P}}}}(\pi_{i-1}(P_N)) = (d_{N,1},\ldots,d_{N,i-1})$. For every $r \in \{1,\ldots,s+1\}$, there is a point $P_{j'_r} \in \mathcal{P}$, $j'_r < j_r$, such that $d_{j'_r,i} = d_{j_r,i} - 1 = d_{N,i} - 1, d_{j'_r,i+1} = d_{j_r,i+1} = d_{N,i+1},\ldots,d_{j'_r,n} = d_{j_r,n} = d_{N,n}$ and $\pi_{i-1}(P_{j'_r}) = \pi_{i-1}(P_{j_r})$. Up to a suitable rearrangement of the points in $\underline{\mathcal{P}}$, we may assume that $j'_1 < \ldots < j'_{s+1}$. In order to calculate $\pi_{i-1}(\delta_{\underline{\mathcal{P}}}(P_{j'_{s+1}}))$ we have to consider the set $\mathcal{Q} := \{P_l \in \mathcal{P} \mid l \le j'_{s+1}, \pi^i(\mathbf{d}_l) = (d_{j'_{s+1},i},\ldots,d_{j'_{s+1},n}) = (d_{N,i}-1, d_{N,i+1}\ldots,d_{N,n})\}$. Of course $P_{j'_r} \in \mathcal{Q}$. Let $\tilde{\mathcal{Q}} := \{\pi_{i-1}(P) \mid P \in \mathcal{Q}\} \subseteq K^{i-1}$; we have $\tilde{\mathcal{P}} \subseteq \tilde{\mathcal{Q}}$. Hence $\mathcal{MB}(\tilde{\mathcal{P}}) \subseteq \mathcal{MB}(\tilde{\mathcal{Q}}) \subseteq \mathbf{N}^{i-1}$; in particular $(d_{N,1},\ldots,d_{N,i-1}) \in \mathcal{MB}(\tilde{\mathcal{Q}})$. It follows that there exists a point $P_k \in \mathcal{Q}$ such that $\delta_{\underline{\mathcal{P}}}(P_k) = (d_{N,1},\ldots,d_{N,i-1},d_{N,i}-1,d_{N,i+1}\ldots,d_{N,n})$. $\square$

As a straightforward consequence of **Lemma 2** we get:

Prop. 3 *The set $\mathcal{MB}(\mathcal{P})$ is an n-dimensional Ferrers diagram.* $\square$

Prop. 4 *The set $\mathcal{L}_{\mathcal{P}} = \{\mathbf{x}^{\mathbf{d}} + \Im(\mathcal{P}) \mid \mathbf{d} \in \mathcal{MB}(\mathcal{P})\}$ is a monomial linear basis for $K[X]/\Im(\mathcal{P})$.*

Proof. By induction on the dimension n of K^n.

For $n = 1$, we have $\mathcal{P} = \{\rho_1,\ldots,\rho_N\}$, $\rho_i \in K$, and $\Im(\mathcal{P}) = (g)$, with $g = \Pi_{i=1}^N(x-\rho_i)$. **Algorithm MB** gives $\mathcal{MB}(\mathcal{P}) = \{0,1,\ldots,N-1\}$; hence $\mathcal{L}_{\mathcal{P}} = \{\mathbf{x}^{\mathbf{d}} + \Im(\mathcal{P}) \mid \mathbf{d} \in \mathcal{MB}(\mathcal{P})\} = \{1+(g), x+(g),\ldots,x^{N-1}+(g)\}$, which is a monomial basis for $K[X]/(g)$.

Suppose now that the statement is true for every finite subset of $K^{n'}$, $n' < n$, and prove it for $\mathcal{P} = \{P_1,\ldots,P_N\} \subset K^n$. As $\dim K[X]/\Im(\mathcal{P}) = N = \#\mathcal{MB}(\mathcal{P})$, it remains to prove that the residue classes modulo $\Im(\mathcal{P})$ of the monomials $\mathbf{x}^{\mathbf{d}}$, $\mathbf{d} \in \mathcal{MB}(\mathcal{P})$, are linearly independent over $K[X]/\Im(\mathcal{P})$; in other words, we have to prove that any polynomial

$$p(x_1,\ldots,x_n) = \sum_{\mathbf{d}\in\mathcal{MB}(\mathcal{P})} \alpha_{\mathbf{d}} x^{\mathbf{d}}, \qquad \alpha_{\mathbf{d}} \in K \tag{1}$$

belonging to $\Im(\mathcal{P})$ is the zero polynomial.

Putting $\mathcal{F} := \mathcal{MB}(\mathcal{P})$, $\mathcal{F}_r := \{\mathbf{d} = (d_1,\ldots,d_n) \in \mathcal{F} \mid d_n = r\}$ and $\mathcal{P}_r := \{P \in \mathcal{P} \mid \delta_{\underline{\mathcal{P}}}(P) \in \mathcal{F}_r\}$, it is easy to check that

$$\mathcal{MB}(\pi_{n-1}(\mathcal{P}_r)) = \pi_{n-1}(\mathcal{F}_r). \tag{2}$$

Let us write polynomial (1) in the form

$$p(x_1,\ldots,x_n) = \sum_{r=0}^{h} p_r(x_1,\ldots,x_{n-1})x_n^r \tag{3}$$

where $h = \max\{d_n \mid \mathbf{d} = (d_1, \dots, d_n) \in \mathcal{F}\}$ and

$$(4) \qquad p_r(x_1, \dots, x_{n-1}) = \sum_{(d_1,\dots,d_{n-1}) \in \pi_{n-1}(\mathcal{F}_r)} \alpha_{(d_1,\dots,d_{n-1},r)} x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}.$$

The polynomial $p(x_1, \dots, x_n) \in \Im(\mathcal{P})$ has to vanish at every point in $\mathcal{P}$. Consider a point $P = (a_1, \dots, a_n) \in \mathcal{P}_h \subseteq \mathcal{P}$; because of **MB5**, there exists in $\mathcal{P}$ exactly $h+1$ points that have the same first $n-1$ coordinates as $P = (a_1, \dots, a_n)$. It follows that the polynomial

$$p(a_1, \dots, a_{n-1}, x_n) = \sum_{r=0}^{h} p_r(a_1, \dots, a_{n-1}) x_n^r$$

vanishes identically. In particular $p_h(a_1, \dots, a_{n-1}) = 0$ for every $(a_1, \dots, a_{n-1}) \in$ $\in \mathcal{Q}_h := \pi_{n-1}(\mathcal{P}_h)$. Hence

$$(5) \qquad p_h(x_1, \dots, x_{n-1}) \in \Im(\mathcal{Q}_h) \subseteq K[x_1, \dots, x_{n-1}].$$

By (2) and (4) we have

$$(6) \qquad p_h(x_1, \dots, x_{n-1}) = \sum_{(d_1,\dots,d_{n-1}) \in \mathcal{MB}(\mathcal{Q}_h)} \alpha_{(d_1,\dots,d_{n-1},h)} x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}.$$

Because of the inductive hypothesis, the set $\{x_1^{d_1} \cdots x_{n-1}^{d_{n-1}} + \Im(\mathcal{Q}_h) \mid (d_1, \dots$ $\dots, d_{n-1}) \in \mathcal{MB}(\mathcal{Q}_h)\}$ is a monomial basis for $K[x_1, \dots, x_{n-1}]/\Im(\mathcal{Q}_h)$. ¿From this and from (5) we deduce that polynomial (6) vanishes identically. Hence

$$(7) \qquad p(x_1, \dots, x_n) = \sum_{r=0}^{h-1} p_r(x_1, \dots, x_{n-1}) x_n^r.$$

Arguing for $r = h-1, h-2, \dots, 1, 0$ as for $r = h$, we conclude that $p_r(x_1, \dots, x_{n-1})$ is the zero polynomial for every $r \in \{0, \dots, h\}$. □

Prop. 5 *The monomial linear basis $\mathcal{L}_{\mathcal{P}} = \{\mathbf{x}^{\mathbf{d}} + \Im(\mathcal{P}) \mid \mathbf{d} \in \mathcal{MB}(\mathcal{P})\}$ for $K[X]/\Im(\mathcal{P})$ is minimal with respect to inverse lexicographical order $\preceq_{i.l.}$ on M_X.*

Proof. Let $\underline{\mathcal{P}} = (P_1, \dots, P_N)$, $\underline{\mathcal{F}} := \underline{\mathcal{MB}(\mathcal{P})} = (\mathbf{d}_1, \dots, \mathbf{d}_N)$; $\mathbf{d}_i = (d_{i,1}, \dots,$ $d_{i,n})$, $P_i = (a_{i,1}, \dots, a_{i,n})$ for $i = 1, \dots, N$. Assume that $\mathbf{d}_1 \prec_{i.l.} \dots \prec_{i.l.} \mathbf{d}_N$. Let $N' \leq N$ and let $\mathbf{d} = (d_1, \dots, d_n) \prec_{i.l.} \mathbf{d}_{N'}$. We have to prove that $\mathbf{x}^{\mathbf{d}}$ is linearly dependent (modulo $\Im(\mathcal{P})$) on $\mathbf{x}^{\mathbf{d}_1}, \dots, \mathbf{x}^{\mathbf{d}_{N'-1}}$, i.e. there exists in $\Im(\mathcal{P})$ a non-zero polynomial $p(x_1, \dots, x_n)$ of the form

$$(8) \qquad p(x_1, \dots, x_n) = \sum_{i=1}^{N'-1} \alpha_i \mathbf{x}^{\mathbf{d}_i} + \alpha \mathbf{x}^{\mathbf{d}}.$$

Obviously, we may assume that $\mathbf{d}_{N'-1} \prec_{i.l.} \mathbf{d}$. Because of **MB6.1** of **Algorithm MB**, without loss of generality we may also assume that $d_n < d_{N',n}$. Thus, $h := d_{N',n} > 0$ and $d_{j,n} < h$ for every $j \in \{1, \ldots, N'-1\}$.

Let us first prove that there is a polynomial of the form (8) which belongs to $\Im(\mathcal{P}') \supseteq \Im(\mathcal{P})$, where $\mathcal{P}' = \{P_1, \ldots, P_{N'}\}$. Equivalently, let us show that the linear homogeneous system

$$(9) \qquad \sum_{i=1}^{N'-1} \alpha_i a_{s,1}^{d_{i,1}} \cdots a_{s,n}^{d_{i,n}} + \alpha a_{s,1}^{d_1} \cdots a_{s,n}^{d_n} = 0, \qquad (s = 1, \ldots, N')$$

admits a non-zero solution $(\alpha_1, \ldots, \alpha_{N'-1}, \alpha)$. In fact the N' by N' matrix A whose $s-th$ row is

$$a_{s,1}^{d_{1,1}} \cdots a_{s,n}^{d_{1,n}} \qquad \ldots \qquad a_{s,1}^{d_{N'-1,1}} \cdots a_{s,n}^{d_{N'-1,n}} \qquad a_{s,1}^{d_1} \cdots a_{s,n}^{d_n}$$

(that is, the evaluation at P_s of the list of monomials $\mathbf{x}^{\mathbf{d}_1}, \ldots, \mathbf{x}^{\mathbf{d}_{N'-1}}, \mathbf{x}^{\mathbf{d}}$) is a singular matrix. In order to prove this, consider the $h+1$ points $P_{t_1}, \ldots, P_{t_h}$ and $P_{t_{h+1}} = P_{N'}$ $(1 \leq t_j \leq N')$ which have the same $n-1$ first coordinates as $P_{N'}$ (**MB5** ensures that $\mathcal{P}$ contains $h+1$ such points). Let A' be the $h+1$ by N' submatrix of A whose rows correspond to these points. It is enough to show that A' has rank less than $h+1$. In fact, any $h+1$ by $h+1$ minor C of A' has columns which correspond to monomials $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n}$, $\mathbf{i} \in \{\mathbf{d}_1, \ldots, \mathbf{d}_{N'-1}, \mathbf{d}\}$, so that i_n may assume only the h values $0, 1, \ldots, h-1$; since the $(n-1)$-tuples $(a_{j,1}, \ldots, a_{j,n-1})$ are always the same for $j \in \{t_1, \ldots, t_{h+1}\}$, we conclude that $C = 0$. This completes the proof that there is a polynomial $p(x_1, \ldots, x_n)$ of the form (8) which belongs to $\Im(\mathcal{P}')$.

Let us now prove that we have $p(P_l) = 0$ for every $P_l \in \mathcal{P} \setminus \mathcal{P}'$. Let $P_l = (a_{l,1}, \ldots, a_{l,n-1}, a_{l,n})$ be such a point; consider the polynomial

$$q_l(x_n) := p(a_{l,1}, \ldots, a_{l,n-1}, x_n) = \sum_{s=0}^{h-1} q_{l,s} x_n^s.$$

Since $\mathbf{d}_{N'} \prec_{i.l.} \mathbf{d}_l$, i.e. $h = d_{N',n} \leq d_{l,n}$, there are in $\mathcal{P}'$ at least h points which have the same $n-1$ first coordinates as P_l; it follows that the polynomial $q_l(x_n)$ vanishes identically. Thus, $p(P_l) = 0$. $\square$

2.3 In the case where $n = 2$ **Algorithm MB** can be given the following simplified form.

Assume that

$$\mathcal{P} = \{(a_1, b_{1,1}), \ldots, (a_1, b_{1,h_1}), \ldots, (a_m, b_{m,1}), \ldots, (a_m, b_{m,h_m})\}$$

with $h_1 + \ldots + h_m = N$, $h_1 \geq \ldots \geq h_m$ and $i \neq j \Rightarrow a_i \neq a_j$. Then,

$$\mathcal{MB}(\mathcal{P}) = \{(p, q) \mid 0 \leq p < m,\ 0 \leq q < h_p\}.$$

3 Generalization to the algebraic multisets

3.1 All that we have stated up to now can be generalized to what we might call *algebraic multisets* in the following sense.

Consider the linear map

$$\begin{array}{rcl} \mathbf{D_i}\colon K[X] & \longrightarrow & K[X] \\ \mathbf{x^h} & \longmapsto & \binom{\mathbf{h}}{\mathbf{i}}\mathbf{x^{h-i}} \end{array}$$

where $\mathbf{h} = (h_1, \ldots, h_n)$, $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbf{N}$ and $\binom{\mathbf{h}}{\mathbf{i}} := \binom{h_1}{i_1} \cdot \ldots \cdot \binom{h_n}{i_n}$. We have the formula

(10) $$\mathbf{D_i}(fg) = \sum_{\mathbf{h+k=i}} \mathbf{D_h}(f)\mathbf{D_k}(g).$$

Observe that when the field K has characteristic zero, then

$$\mathbf{D_i} = \frac{1}{\mathbf{i}!}\mathbf{D^i} := \frac{1}{\mathbf{i}!}\frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1}\cdots\partial x_n^{i_n}}$$

where $\mathbf{i}! := i_1! \cdots i_n!$.
Let v_P be the evaluation map at the point P:

$$\begin{array}{rcl} v_P\colon K[X] & \longrightarrow & K \\ q & \longmapsto & q(P). \end{array}$$

Define the linear map $v_P^{\mathbf{i}}$ as the composition $v_P \circ \mathbf{D_i}$, i.e.

$$\begin{array}{rcl} v_P^{\mathbf{i}}\colon K[X] & \longrightarrow & K \\ q & \longmapsto & (\mathbf{D_i}q)(P). \end{array}$$

For every ideal J of $K[X]$ and every $P \in \mathcal{V}(J)$, put

$$\mathcal{F}_J(P) := \left\{\mathbf{i} \in \mathbf{N}^n \,\middle|\, (\forall p \in J)\left(v_P^{\mathbf{i}}(p) = 0\right)\right\}.$$

Prop. 6 *i) $\mathcal{F}_J(P)$ is an n-dimensional Ferrers diagram; ii) if $(g_1, \ldots, g_s)$ is a system of generators of J, then $\mathcal{F}_J(P)$ is the largest n-dimensional Ferrers diagram contained in the set*

$$\left\{\mathbf{i} \in \mathbf{N}^n \,\middle|\, v_P^{\mathbf{i}}(g_j) = 0 \textit{ for every } 1 \le j \le s\right\}.$$

Proof. Let $P = (a_1, \ldots, a_n)$. Let $\mathbf{i} \in \mathcal{F}_J(P)$ and let $\mathbf{j} < \mathbf{i}$. Let us prove that $\mathbf{j} \in \mathcal{F}_J(P)$. Let $f := (\mathbf{x} - P)^{\mathbf{i-j}} = (x_1 - a_1)^{i_1-j_1} \cdots (x_n - a_n)^{i_n-j_n}$. We have $v_P^{\mathbf{h}}(f) = (\mathbf{D_h}f)(P) = \delta_{\mathbf{h}}^{\mathbf{i-j}}$. ¿From (10) we deduce that for every $g \in J$ we have

$$0 = v_P^{\mathbf{i}}(fg) = \sum_{\mathbf{h+k=i}} v_P^{\mathbf{h}}(f) \cdot v_P^{\mathbf{k}}(g) = v_P^{\mathbf{j}}(g).$$

Hence $\mathbf{j} \in \mathcal{F}_J(P)$. The second part of the statement is a straightforward consequence of i) and of (10). $\square$

We define a *finite n-dimensional algebraic multiset*, or simply an *algebraic multiset*, to be a set $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$; each element $(P_j, \mathcal{F}_j) \in \wp$ consists of a point P_j of K^n together with an n-dimensional Ferrers diagram $\mathcal{F}_j \subset \mathbf{N}^n$, which will be called the *algebraic diagram* of the point P_j. We shall freely make use of the notation $(P, \mathbf{i}) \in \wp$, or also $P \in \wp$, to mean that $P = P_j$ and $\mathbf{i} \in \mathcal{F}_j$ for some $j \in \{1, \ldots, N\}$. To every algebraic multiset $\wp = \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$ we associate the set

$$\Im(\wp) := \left\{ p \in K[X] \mid (\forall j)(\forall \mathbf{i} \in \mathcal{F}_j) \left(v^{\mathbf{i}}_{P_j}(p) = 0 \right) \right\}.$$

It is not difficult to prove that $\Im(\wp)$ is a cofinite ideal of $K[X]$ and that $\mathcal{F}_{\Im(\wp)}(P_j) = \mathcal{F}_j$ for every $j \in \{1, \ldots, N\}$. Moreover, one can prove that

$$\operatorname{codim} \Im(\wp) = \#\wp := \sum_{j=1}^{N} \#\mathcal{F}_j.$$

The question now is: how do we get a monomial linear basis for $K[X]/\Im(\wp)$? Once more the problem can be solved by applying a slightly modified version of **Algorithm MB** (in fact **Algorithm MB** itself with a few obvious changes) to a suitable set $\mathcal{R}(\wp) \subset (K \times \mathbf{N})^n$ associated with the algebraic multiset $\wp$. The set $\mathcal{R}(\wp)$ will be called the *canonical representation* of the algebraic multiset $\wp$. To be precise, consider the bijection

$$\begin{array}{rcl} u\colon K^n \times \mathbf{N}^n & \longrightarrow & (K \times \mathbf{N})^n \\ ((a_1, \ldots, a_n), (i_1, \ldots, i_n)) & \longmapsto & ((a_1, i_1), \ldots, (a_n, i_n)). \end{array}$$

Put

$$\mathcal{R} = \mathcal{R}(\wp) := \{u(P, \mathbf{i}) \mid (P, \mathbf{i}) \in \wp\}.$$

and

$$\mathcal{MB}(\wp) := \mathcal{MB}(\mathcal{R}).$$

It is possible (though by no means trivial) to prove that $\mathcal{MB}(\wp)$ satisfies properties analogous to those of $\mathcal{MB}(\mathcal{P})$; in particular, i) $\mathcal{MB}(\wp)$ is an n-dimensional Ferrers diagram and ii) the set $\mathcal{L}_\wp := \{\mathbf{x}^{\mathbf{i}} + \Im(\wp) \mid \mathbf{i} \in \mathcal{MB}(\wp)\}$ is a monomial linear basis of $K[X]/\Im(\wp)$ which is minimal with respect to the inverse lexicographical order.

4 Applications

Both **Algorithm MB** and its generalization may come in handy for solving various problems. Let us examine a few of them.

4.1 First of all, let us see how to determine a system of generators $(\gamma_1, \ldots, \gamma_r)$ for the ideal $\Im(\wp)$ of a finite algebraic multiset $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$. In fact, the set $\{\gamma_1, \ldots, \gamma_r\}$ we shall obtain is also a *reduced Gröbner basis* of $\Im(\wp)$ with respect to $\preceq_{i.l.}$. (The notion of reduced Gröbner basis as well as related topics can be found in [1], [3], [8].) It goes without saying that the same procedure works also when $\wp$ is a finite algebraic set.

Let $\mathcal{L}_\wp := \{\mathbf{x}^\mathbf{d} + \Im(\wp) \mid \mathbf{d} \in \mathcal{MB}(\wp)\} = \{\mathbf{x}^{\mathbf{d}_1}, \ldots, \mathbf{x}^{\mathbf{d}_m}\}$, where $m = \#\wp = \mathrm{codim}(\Im(\wp))$, be the monomial linear basis obtained in **3.1** and let $\{\mathbf{r}_1, \ldots, \mathbf{r}_r\}$ be the set of the co-minimal elements of the Ferrers diagram $\mathcal{MB}(\wp)$. For each $\mathbf{r}_i$, $i = 1, \ldots, s$, define the polynomial $\gamma_i \in K[X]$ to be the following determinant. The first row of γ_i is the list $(\mathbf{x}^{\mathbf{d}_1}, \ldots, \mathbf{x}^{\mathbf{d}_m}, \mathbf{x}^{\mathbf{r}_i})$, while the successive rows are lists of the form $(v^\mathbf{i}_{P_j}(\mathbf{x}^{\mathbf{d}_1}), \ldots, v^\mathbf{i}_{P_j}(\mathbf{x}^{\mathbf{d}_m}), v^\mathbf{i}_{P_j}(\mathbf{x}^{\mathbf{r}_i}))$, one for each $(P_j, \mathbf{i}) \in \wp$. It can easily be proved that the list $(\gamma_1, \ldots, \gamma_r)$ is a reduced Gröbner basis of $\Im(\wp)$ with respect to the inverse lexicographical order. Once the basis $(\gamma_1, \ldots, \gamma_r)$ has been found, a Gröbner basis with respect to a different term-ordering may be computed by making use of the methods given in [4].

4.2 Consider a linear form $f \in K[X]^* \cong K[[X]]$. If $\mathrm{Ker}(f)$ contains a cofinite ideal J of $K[X]$, then f is said to be an *n-linearly recursive function* and J is called a *characteristic ideal* of f. This notion has been introduced in [2] as a generalization of that of *linearly recursive sequence*, to which it reduces when $n = 1$. An n-linearly recursive function f is uniquely determined by its *characteristic ideal* J and by its *initial values*, which are the values assumed by f on a system of representatives of a linear basis of $K[X]/J$. The set of n-linearly recursive functions may also be regarded as the dual bialgebra of the usual polynomial bialgebra on $K[X]$. When working on these subjects, it may happen that examples (perhaps, *suitable* examples) of n-linearly recursive functions are needed. How to construct them? It is convenient to divide the answer to this question into two parts.

(A) Let us first suppose that we know a system of generators $(g_1, \ldots, g_s)$ of the characteristic ideal J of the n-linearly recursive functions we are considering. In this case we may calculate a reduced Gröbner basis $G_\preceq := RGB(g_1, \ldots, g_s)$ of $(g_1, \ldots, g_s)$ with respect to some term-ordering $\preceq$ on M_X. Let $G_\preceq = (\gamma_1, \ldots, \gamma_r)$, $\gamma_j \in K[X]$, and let $\mathbf{y}_j \in M_X$ be the leading term (with respect to $\preceq$) of the polynomial γ_j. Then the set $\{\mathbf{x}^\mathbf{d} + J \mid \mathbf{x}^\mathbf{d} \in B\}$, where $B = M_X \setminus \cup_{j=1}^r \mathbf{y}_j \cdot M_X$, is a monomial linear basis for $K[X]/J$, which is minimal with respect to $\preceq$. It follows that any n-linearly recursive function whose characteristic ideal is J is uniquely determined by the set of its *initial values* $\{f(\mathbf{x}^\mathbf{d}) \mid \mathbf{x}^\mathbf{d} \in B\}$, all the other values $f(\mathbf{x}^\mathbf{i})$, $\mathbf{x}^\mathbf{i} \notin B$, being calculated by making use of the polynomials $\gamma_j \in G_\preceq$ as *scales of recurrence.*

(B) If instead the characteristic ideal is not given, we are quite unlikely to obtain one of them (remember it must be cofinite!) just choosing at random a set of generators: most of the time we would get a non-cofinite ideal or, when cofinite, a trivial one. The correct way to do this consists instead in choosing a finite algebraic multiset (possibly, a finite algebraic set) $\wp$ and then determining both the monomial linear basis $\mathcal{L}_\wp$ of $K[X]/\Im(\wp)$ and a set of generators for $\Im(\wp)$ by means of the machinery described above.

4.3 Lastly, consider the following interpolation problem. Given a finite n-dimensional algebraic multiset $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$ and a set of values $\{\alpha_{j,\mathbf{i}} \mid j = 1, \ldots, N \text{ and } \mathbf{i} \in \mathcal{F}_j\} \subset K$ determine the *unique* polynomial p of the form $\sum_{\mathbf{x^i} \in B} a_\mathbf{i} \mathbf{x}^\mathbf{i}$ ($a_\mathbf{i} \in K$ and B is a system of representatives of a monomial linear basis of $K[X]/\Im(\wp)$) such that $v^\mathbf{i}_{P_j}(p) = \alpha_{j,\mathbf{i}}$.

This problem appears to be an n-dimensional natural generalization of the unidimensional one which is solved by means of the Lagrange-Hermite interpolation formula. Once more, the key point for solving this problem is to determine the monomial basis $\mathcal{L}_\wp$. Let $\mathcal{L}_\wp = \{\mathbf{x}^{\mathbf{d}_1} + \Im(\wp), \ldots, \mathbf{x}^{\mathbf{d}_m} + \Im(\wp)\}$ and let $\mathcal{A}$ be the $m \times m$ matrix whose rows are of the form $(v^\mathbf{i}_{P_j}(\mathbf{x}^{\mathbf{d}_1}), \ldots, (v^\mathbf{i}_{P_j}(\mathbf{x}^{\mathbf{d}_m}))$, one for each $(P_j, \mathbf{i}) \in \wp$. Since $\mathcal{L}_\wp$ is a linear basis of $K[X]/\Im(\wp)$, the matrix $\mathcal{A}$ is non-singular. Consider the vector $\overline{\alpha}$ whose components are the values $\alpha_{j,\mathbf{i}} = v^\mathbf{i}_{P_j}(p)$ (arranged according to the order that has been used for the rows of $\mathcal{A}$). The components of the vector $\overline{\beta} := \mathcal{A}^{-1} \cdot \overline{\alpha}$ are the coefficients of the desired polynomial.

Appendix.

1) Example of **Algorithm MB** for a 4-dimensional set.

$$
\begin{array}{rcl}
\mathcal{P} & \longleftrightarrow & \mathcal{F} = \mathcal{MB}(\mathcal{P}) \\
 & & \\
P_1 = (2,3,9,4) & \longleftrightarrow & \mathbf{d}_1 = (0,0,0,0) \\
P_2 = (2,5,7,3) & \longleftrightarrow & \mathbf{d}_2 = (0,1,0,0) \\
P_3 = (2,3,3,2) & \longleftrightarrow & \mathbf{d}_3 = (0,0,1,0) \\
P_4 = (2,5,5,1) & \longleftrightarrow & \mathbf{d}_4 = (0,1,1,0) \\
P_5 = (6,1,1,3) & \longleftrightarrow & \mathbf{d}_5 = (1,0,0,0) \\
P_6 = (2,3,3,6) & \longleftrightarrow & \mathbf{d}_6 = (0,0,0,1) \\
P_7 = (8,3,4,0) & \longleftrightarrow & \mathbf{d}_7 = (2,0,0,0) \\
P_8 = (6,5,6,3) & \longleftrightarrow & \mathbf{d}_8 = (1,1,0,0) \\
P_9 = (4,7,6,6) & \longleftrightarrow & \mathbf{d}_9 = (3,0,0,0) \\
P_{10} = (4,1,7,7) & \longleftrightarrow & \mathbf{d}_{10} = (2,1,0,0) \\
P_{11} = (2,5,7,8) & \longleftrightarrow & \mathbf{d}_{11} = (0,1,0,1) \\
P_{12} = (4,3,0,3) & \longleftrightarrow & \mathbf{d}_{12} = (0,2,0,0) \\
P_{13} = (1,1,2,5) & \longleftrightarrow & \mathbf{d}_{13} = (4,0,0,0) \\
P_{14} = (2,1,9,0) & \longleftrightarrow & \mathbf{d}_{14} = (1,2,0,0) \\
P_{15} = (4,1,7,6) & \longleftrightarrow & \mathbf{d}_{15} = (1,0,0,1) \\
P_{16} = (8,1,8,0) & \longleftrightarrow & \mathbf{d}_{16} = (3,1,0,0) \\
P_{17} = (2,1,7,6) & \longleftrightarrow & \mathbf{d}_{17} = (0,2,1,0) \\
P_{18} = (4,3,3,3) & \longleftrightarrow & \mathbf{d}_{18} = (1,0,1,0) \\
P_{19} = (4,1,1,0) & \longleftrightarrow & \mathbf{d}_{19} = (1,1,1,0) \\
P_{20} = (8,1,2,4) & \longleftrightarrow & \mathbf{d}_{20} = (2,0,1,0) \\
P_{21} = (6,3,4,8) & \longleftrightarrow & \mathbf{d}_{21} = (2,2,0,0) \\
P_{22} = (2,9,6,7) & \longleftrightarrow & \mathbf{d}_{22} = (0,3,0,0) \\
P_{23} = (2,3,7,1) & \longleftrightarrow & \mathbf{d}_{23} = (0,0,2,0) \\
P_{24} = (2,1,7,5) & \longleftrightarrow & \mathbf{d}_{24} = (0,2,0,1) \\
P_{25} = (4,1,1,2) & \longleftrightarrow & \mathbf{d}_{25} = (0,0,1,1) \\
P_{26} = (2,7,6,5) & \longleftrightarrow & \mathbf{d}_{26} = (0,4,0,0) \\
P_{27} = (2,5,5,4) & \longleftrightarrow & \mathbf{d}_{27} = (1,0,1,1) \\
P_{28} = (2,3,7,7) & \longleftrightarrow & \mathbf{d}_{28} = (0,1,1,1) \\
P_{29} = (2,3,0,2) & \longleftrightarrow & \mathbf{d}_{29} = (0,0,3,0) \\
P_{30} = (2,1,1,1) & \longleftrightarrow & \mathbf{d}_{30} = (0,1,2,0) \\
P_{31} = (4,3,3,7) & \longleftrightarrow & \mathbf{d}_{31} = (1,1,0,1) \\
P_{32} = (8,5,6,4) & \longleftrightarrow & \mathbf{d}_{32} = (3,2,0,0) \\
P_{33} = (4,5,5,2) & \longleftrightarrow & \mathbf{d}_{33} = (1,3,0,0) \\
P_{34} = (2,1,1,8) & \longleftrightarrow & \mathbf{d}_{34} = (0,2,1,1) \\
P_{35} = (8,1,1,1) & \longleftrightarrow & \mathbf{d}_{35} = (1,0,2,0) \\
P_{36} = (4,5,5,5) & \longleftrightarrow & \mathbf{d}_{36} = (1,2,0,1) \\
P_{37} = (6,1,8,8) & \longleftrightarrow & \mathbf{d}_{37} = (3,0,1,0) \\
P_{38} = (2,7,8,4) & \longleftrightarrow & \mathbf{d}_{38} = (0,3,1,0)
\end{array}
$$

The system of representatives for the corresponding monomial basis is given in the following table.

1	x_1	x_1^2	x_1^3	x_1^4
x_2	x_1x_2	$x_1^2x_2$	$x_1^3x_2$	
x_2^2	$x_1x_2^2$	$x_1^2x_2^2$	$x_1^3x_2^2$	
x_2^3	$x_1x_2^3$			
x_2^4				

x_3	x_1x_3	$x_1^2x_3$	$x_1^3x_3$
x_2x_3	$x_1x_2x_3$		
$x_2^2x_3$			
$x_2^3x_3$			

x_3^2	$x_1x_3^2$
$x_2x_3^2$	

x_3^3

x_4	x_1x_4
x_2x_4	$x_1x_2x_4$
$x_2^2x_4$	$x_1x_2^2x_4$

x_3x_4	$x_1x_3x_4$
$x_2x_3x_4$	
$x_2^2x_3x_4$	

2) Example of **Algorithm MB** for a 3-dimensional algebraic multiset.

Consider the algebraic multiset $\wp$ given by

$$P_1 = (0,0,0) \quad \mathcal{F}_1 = \begin{bmatrix} (0,0,0) & (1,0,0) & & (0,0,1) \\ (0,1,0) & & & \end{bmatrix}$$

$$P_2 = (0,0,1) \quad \mathcal{F}_2 = \begin{bmatrix} (0,0,0) & (1,0,0) & (2,0,0) & (0,0,1) & (1,0,1) \end{bmatrix}$$

$$P_3 = (1,1,0) \quad \mathcal{F}_3 = \begin{bmatrix} (0,0,0) & (1,0,0) & (0,0,1) & (1,0,1) & (0,0,2) \\ (0,1,0) & (1,1,0) & (0,1,1) & & (0,1,2) \end{bmatrix}$$

$$P_4 = (1,1,1) \quad \mathcal{F}_4 = \begin{bmatrix} (0,0,0) \\ (0,1,0) \end{bmatrix}$$

The canonical representation $\mathcal{R} = \mathcal{R}(\wp)$ of $\wp$ (whose elements are intentionally arranged at random) as well as the corresponding 3-dimensional Ferrers diagram $\mathcal{MB}(\mathcal{R})$ are as follows.

$\wp$	$\longleftrightarrow$	$\mathcal{R}$	$\longleftrightarrow$	$\mathcal{F} = \mathcal{MB}(\mathcal{R})$
$(1,1,0),(0,0,2)$	$\longleftrightarrow$	$R_1 = (10,\ 10,\ 02)$	$\longleftrightarrow$	$\mathbf{d}_1 = (0,\ 0,\ 0)$
$(1,1,0),(0,1,2)$	$\longleftrightarrow$	$R_2 = (10,\ 11,\ 02)$	$\longleftrightarrow$	$\mathbf{d}_2 = (0,\ 1,\ 0)$
$(0,0,1),(1,0,1)$	$\longleftrightarrow$	$R_3 = (01,\ 00,\ 11)$	$\longleftrightarrow$	$\mathbf{d}_3 = (1,\ 0,\ 0)$
$(1,1,0),(1,0,1)$	$\longleftrightarrow$	$R_4 = (11,\ 10,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_4 = (2,\ 0,\ 0)$
$(0,0,1),(0,0,1)$	$\longleftrightarrow$	$R_5 = (00,\ 00,\ 11)$	$\longleftrightarrow$	$\mathbf{d}_5 = (3,\ 0,\ 0)$
$(1,1,0),(0,0,1)$	$\longleftrightarrow$	$R_6 = (10,\ 10,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_6 = (0,\ 0,\ 1)$
$(0,0,1),(2,0,0)$	$\longleftrightarrow$	$R_7 = (02,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_7 = (4,\ 0,\ 0)$
$(0,0,0),(1,0,0)$	$\longleftrightarrow$	$R_8 = (01,\ 00,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_8 = (1,\ 0,\ 1)$
$(1,1,0),(0,0,0)$	$\longleftrightarrow$	$R_9 = (10,\ 10,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_9 = (0,\ 0,\ 2)$
$(0,0,0),(0,1,0)$	$\longleftrightarrow$	$R_{10} = (00,\ 01,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{10} = (1,\ 1,\ 0)$
$(0,0,0),(0,0,0)$	$\longleftrightarrow$	$R_{11} = (00,\ 00,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{11} = (2,\ 0,\ 1)$
$(0,0,0),(0,0,1)$	$\longleftrightarrow$	$R_{12} = (00,\ 00,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_{12} = (1,\ 0,\ 2)$
$(1,1,0),(0,1,0)$	$\longleftrightarrow$	$R_{13} = (10,\ 11,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{13} = (0,\ 1,\ 1)$
$(1,1,0),(1,0,0)$	$\longleftrightarrow$	$R_{14} = (11,\ 10,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{14} = (3,\ 0,\ 1)$
$(0,0,1),(0,0,0)$	$\longleftrightarrow$	$R_{15} = (00,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{15} = (0,\ 0,\ 3)$
$(1,1,0),(0,1,1)$	$\longleftrightarrow$	$R_{16} = (10,\ 11,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_{16} = (0,\ 1,\ 2)$
$(1,1,0),(1,1,0)$	$\longleftrightarrow$	$R_{17} = (11,\ 11,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{17} = (2,\ 1,\ 0)$
$(0,0,1),(1,0,0)$	$\longleftrightarrow$	$R_{18} = (01,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{18} = (2,\ 0,\ 2)$
$(1,1,1),(0,1,0)$	$\longleftrightarrow$	$R_{19} = (10,\ 11,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{19} = (1,\ 0,\ 3)$
$(1,1,1),(0,0,0)$	$\longleftrightarrow$	$R_{20} = (10,\ 10,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{20} = (0,\ 1,\ 3)$

Therefore, a monomial linear basis of $K[X]/\Im(\wp)$ consists of the equivalence classes (modulo $\Im(\wp)$) of the following monomials

$$\begin{array}{|ccccc}
\hline
1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\
x_2 & x_1x_2 & x_1^2x_2 & &
\end{array}
\qquad
\begin{array}{|cccc}
\hline
x_3 & x_1x_3 & x_1^2x_3 & x_1^3x_3 \\
x_2x_3 & & &
\end{array}$$

$$\begin{array}{|ccc}
\hline
x_3^2 & x_1x_3^2 & x_1^2x_3^2 \\
x_2x_3^2 & &
\end{array}
\qquad
\begin{array}{|cc}
\hline
x_3^3 & x_1x_3^3 \\
x_2x_3^3 &
\end{array}$$

The reduced Gröbner basis of $\Im(\wp)$ with respect to $\preceq_{i.l}$ consists of the following polynomials:

$g_1 = x^5 - 2x^4 + x^3;$
$g_2 = x^3y - 2x^2y + xy;$
$g_3 = y^2 + 2x^2y - 4xy - 3x^4 + 4x^3;$
$g_4 = x^4z - 2x^3z + x^2z - x^4 + 2x^3 - x^2;$
$g_5 = xyz - yz - x^3z + x^2z - x^4 + 2x^3 - x^2;$
$g_6 = x^3z^2 - x^2z^2 + x^4 - 2x^3 + x^2;$
$g_7 = x^2z^3 - xz^3 - 2x^2z^2 + 2xz^2 - x^3z + 2x^2z - xz - x^4 + 2x^3 - x^2;$
$g_8 = z^4 + xz^3 - 2z^3 + x^2z^2 - 2xz^2 + z^2 + x^3z - 2x^2z + xz + x^4 - 2x^3 + x^2.$

Acknowledgements

The authors thank T.Mora, O.Murru, F.Piras and R.Pirastu for their advice during several discussions. We are also indebted to the referees of the "Acts the 4th Conference *Formal Power Series and Algebraic Combinatorics*, Montreal, 1992" for a few useful suggestions.

References

[1] B. Buchberger, *An Algorithmic Method in Polynomial Ideal Theory*, in "N. K. Bose (ed): Recent Trends in Multidimensional System Theory", D. Reidel Publishing Co. , Dordrecht-Boston, 1985, pp. 184-232

[2] L. Cerlienco, F. Piras, *On the Continuous Dual of a Polynomial Bialgebra*, Communications in Algebra, 19(10), 2707–2727 (1991)

[3] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Springer-Verlag, New York, 1992

[4] J.C. Faugère, P. Gianni, D. Lazar, T. Mora, *Efficient computation of zero-dimensional-Gröbner bases by change of ordering*, Submitted to J. Symb. Comp. Technical Report LITP 89-52 (1989)

[5] W. Fulton, *Algebraic curves*, The Benjamin/Cummings, Reading, Mass., 1981

[6] M.G. Marinari, H.M. Möller, T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, J. Appl. Alg. 4 (1993), 1-43

[7] H.M. Möller, B. Buchberger, *The construction of multivariate polynomials with preassigned zeros*, in "Computer Algebra (Marseille, 1982)", Lecture Notes in Comp. Sci., 144, Springer, Berlin-New York, 1982, pp.24-31

[8] L. Robbiano, *Introduzione all'algebra computazionale.* Appunti per il corso INDAM. (Roma 1986/87)

Authors address:
Luigi Cerlienco, Marina Mureddu
Dipartimento di Matematica.
Via Ospedale 72 — I-09124 Cagliari (Italy)
Tel. 0039-070-6758529/36 — Fax 0039-070-6758511
e-mail:
CERLIENCO@VAXCA1.UNICA.IT
MUREDDU@VAXCA1.UNICA.IT