COMBINATORIAL-ALGEBRAIC TECHNIQUES IN GRÖBNER BASES THEORY

by

L. Cerlienco, M. Mureddu and F. Piras

Dipartimento di Matematica
Università di Cagliari
Via Ospedale 72 - 09124 Cagliari(Italy)

cerlienco@vaxca1.unica.it, mureddu@vaxca1.unica.it,
piras@vaxca1.unica.it

§ **0**. Preliminary notations and main definitions.

$\mathbb{K}[X]$	$K[x_1, \ldots, x_n] \simeq \mathbb{K}^{(\mathbb{N}^n)}$
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	natural, integral, rational, real, complex numbers
$\mathbf{i} := (i_1, \ldots, i_n)$	an arbitrary element of $\mathbb{N}^n$
$\mathbf{i}!$	$i_1! \cdots i_n!$
$\binom{\mathbf{h}}{\mathbf{i}}$	$\binom{h_1}{i_1} \cdots \binom{h_n}{i_n}$
$\mathbf{P}, \mathbf{Q}$	arbitrary elements of $\mathbb{R}^n$
$\leq$	the usual order on $\mathbb{N}$, as well as the product order it induces on $\mathbb{N}^n$
$\mathcal{F}$	an *n-dimensional Ferrers diagram*, i.e. any finite ideal of the poset $\mathbf{N}^n$: $\mathbf{j} < \mathbf{i} \in \mathcal{F} \Longrightarrow \mathbf{j} \in \mathcal{F}$
$\preceq$	a *term-ordering* on $\mathbb{N}^n$, i.e. a linear ordering which is compatible with the additive monoid structure on $\mathbb{N}^n$
$\preceq_{\mathbb{Z}}$, $\preceq_{\mathbb{Q}}$, $\preceq_{\mathbb{R}}$	extensions of the term-ordering $\preceq$ on $\mathbb{N}^n$ to $\mathbb{Z}^n$, $\mathbb{Q}^n$ and $\mathbb{R}^n$
$\preceq^{\mathbb{R}}$	a linear ordering on $\mathbb{R}^n$ which is compatible with the structure of $\mathbb{R}$-vector space

$\mathbb{K}$	an arbitrary field
$\mathbb{K}[x] \simeq \mathbb{K}^{(\mathbb{N})}$	the usual identification of the space $\mathbb{K}[x]$ of polynomials in the indeterminate x with the space $\mathbb{K}^{(\mathbb{N})}$ of the finite support sequences
$p(x) = \sum_{i=0}^{m} p_i x^i =$ $= (p_0, \dots, p_m, 0, \dots)_{-1}$	an element of $\mathbb{K}[x] \simeq \mathbb{K}^{(\mathbb{N})}$
$\mathbb{K}[x]^* \simeq \mathbb{K}[[x]] \simeq \mathbb{K}^{\mathbb{N}}$	the usual identification of the dual space $\mathbb{K}[x]^*$ of $\mathbb{K}[x]$ with both the space $\mathbb{K}[[x]]$ of the formal power series and the space $\mathbb{K}^{\mathbb{N}}$ of all sequences
$v = \sum_{i=0}^{\infty} v_i x^i = (v_i)_{i\in\mathbb{N}}$	an element of $\mathbb{K}[x]^* \simeq \mathbb{K}[[x]] \simeq \mathbb{K}^{\mathbb{N}}$
E	the *shift operator* $E\colon \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$, $(v_i)_{i\in\mathbb{N}} \mapsto (v_{i+1})_{i\in\mathbb{N}}$
$\mathbb{A} = (\mathbb{K}[x], m, u)$	the usual polynomial algebra; $m\colon \mathbb{K}[x] \otimes \mathbb{K}[x] \to \mathbb{K}[x]$, *multiplication*; $u\colon \mathbb{K} \to \mathbb{K}[x]$, *unity map*
$\mathcal{B} = (\mathbb{K}[x], m, u, \Delta, \varepsilon)$	the usual polynomial bialgebra; the maps Δ (*comultiplication* or *diagonalization*) and ε (*counity map* or *augmentation*) are defined as follows: $\begin{array}{lrcl} \Delta\colon & \mathbb{K}[x] & \longrightarrow & \mathbb{K}[x] \otimes \mathbb{K}[x] \simeq \mathbb{K}[x,y] \\ & p(x) & \mapsto & p(x+y), \\ \varepsilon\colon & \mathbb{K}[x] & \longrightarrow & \mathbb{K} \\ & p(x) & \mapsto & p(0). \end{array}$
$\mathbb{K}[X]$	$K[x_1, \dots, x_n] \simeq \mathbb{K}^{(\mathbb{N}^n)}$
$\mathbb{K}[x]^\circ \subset \mathbb{K}[x]^*$	the set of all the forms in $\mathbb{K}[x]^*$ whose kernel contains an ideal of $\mathbb{K}[x]$
$\mathcal{B}^\circ = (\mathbb{K}[x]^\circ, \Delta^\circ, \varepsilon^\circ, m^\circ, u^\circ)$	the dual bialgebra of the polynomial bialgebra $\mathcal{B}$; the maps Δ°, ε°, m° and u° are defined as follows:

$$\begin{array}{lccll}
\Delta^\circ\colon & \mathbb{K}[x]^\circ \otimes \mathbb{K}[x]^\circ & \longrightarrow & \mathbb{K}[x]^\circ & (\textit{multiplication}) \\
& ((v_i)_{i\in\mathbb{N}}), (w_j)_{j\in\mathbb{N}}) & \longmapsto & (\sum_{i+j=k} \binom{k}{i} v_i w_j)_{k\in\mathbb{N}} & \\[2ex]
\varepsilon^\circ\colon & \mathbb{K} & \longrightarrow & \mathbb{K}[x]^\circ & (\textit{unity map}) \\
& a & \mapsto & a(\delta_j^0)_{j\in\mathbb{N}} & \\[2ex]
m^\circ\colon & \mathbb{K}[x]^\circ & \longrightarrow & \mathbb{K}[x]^\circ \otimes \mathbb{K}[x]^\circ \subseteq \mathbb{K}^{\mathbb{N}\times\mathbb{N}} & (\textit{diagonalization}) \\
& (v_i)_{i\in\mathbb{N}} & \longmapsto & (w_{ij} := v_{i+j})_{(i,j)\in\mathbb{N}\times\mathbb{N}} & \\[2ex]
u^\circ\colon & \mathbb{K}[x]^\circ & \longrightarrow & \mathbb{K} & (\textit{augmentation}) \\
& (v_i)_{i\in\mathbb{N}} & \mapsto & v_0. &
\end{array}$$

$\mathbb{K}[X]$	$K[x_1, \dots, x_n] \simeq \mathbb{K}^{(\mathbb{N}^n)}$
$X := \{x_1, x_2, \dots, x_n\}$	a given set of indeterminates
$\mathbb{K}[X]$	$\mathbb{K}[x_1, \dots, x_n] \simeq \mathbb{K}^{(\mathbb{N}^n)}$ the usual identification of the space $\mathbb{K}[X]$ of polynomials in the indeterminates $x_1, \dots, x_n$ with the space $\mathbb{K}^{(\mathbb{N}^n)}$ of the finite support functions $\mathbb{N}^n \to \mathbb{K}$
I, J	ideals of $\mathbb{K}[x]$ or $\mathbb{K}[x_1, \dots, x_n]$
$M_X \subseteq K[X]$	the free abelian monoid on $X := \{x_1, x_2, \dots, x_n\}$
$\mathbf{x}^{\mathbf{i}}$	$\mathbf{x}^{\mathbf{i}} := x_1^{i_1} \cdots x_n^{i_n} \in M_X$, the *terms* of $K[X]$
$p(X) = \sum p_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$	an element of $\mathbb{K}[X] \simeq \mathbb{K}^{(\mathbb{N}^n)}$
$\mathbb{K}[X]^* \simeq \mathbb{K}[[X]] \simeq \mathbb{K}^{\mathbb{N}^n}$	the usual identification of the dual space $\mathbb{K}[X]^*$ of $\mathbb{K}[X]$ with both the space $\mathbb{K}[[X]]$ of formal power series and the space $\mathbb{K}^{\mathbb{N}^n}$ of all functions $\mathbb{N}^n \to \mathbb{K}$
$\mathbf{f} = \sum_{\mathbf{i} \in \mathbb{N}^n} f_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} = (f_{\mathbf{i}})_{\mathbf{i} \in \mathbb{N}^n}$	an element of $\mathbb{K}[X]^* \simeq \mathbb{K}[[X]] \simeq \mathbb{K}^{\mathbb{N}^n}$
$\mathbf{E}^{\mathbf{j}}$	the *shift operator* $\mathbf{E}^{\mathbf{j}} \colon \mathbb{K}^{\mathbb{N}^n} \to \mathbb{K}^{\mathbb{N}^n}$, $(f_{\mathbf{i}})_{\mathbf{i} \in \mathbb{N}^n} \mapsto (f_{\mathbf{i}+\mathbf{j}})_{\mathbf{i} \in \mathbb{N}^n}$
$p(\mathbf{E})$	for $p(X) = \sum p_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathbb{K}[X]$, the operator $p(\mathbf{E}) := \sum p_{\mathbf{i}} \mathbf{E}^{\mathbf{i}} \in \mathbb{K}[X]^*$
$\mathcal{B}_n = (\mathbb{K}[X], m_n, u_n, \Delta_n, \varepsilon_n)$	the multivariate polynomial bialgebra; the definition of the maps $m_n, u_n, \Delta_n, \varepsilon_n$ is analogous to that of $m, u, \Delta, \varepsilon$
$\mathbb{K}[X]^\circ \subset \mathbb{K}[X]^*$	the set of all the forms in $\mathbb{K}[X]^*$ whose kernel contains a cofinite ideal of $\mathbb{K}[X]$
$\mathcal{B}_n^\circ = (\mathbb{K}[X]^\circ, \Delta_n^\circ, \varepsilon_n^\circ, m_n^\circ, u_n^\circ)$	the dual bialgebra of the multivariate polynomial bialgebra $\mathcal{B}_n$
$v_{\mathbf{P}}$	$v_{\mathbf{P}} \colon \mathbb{K}[X] \to \mathbb{K}$, $p \mapsto p(\mathbf{P})$, the evaluation map at the point $\mathbf{P} \in \mathbb{K}^n$:
$\mathbf{D}_{\mathbf{i}}$	the linear map $\mathbf{D}_{\mathbf{i}} \colon \mathbb{K}[X] \to \mathbb{K}[X]$, $\mathbf{x}^{\mathbf{h}} \mapsto \binom{\mathbf{h}}{\mathbf{i}} \mathbf{x}^{\mathbf{h}-\mathbf{i}}$; we have the formula $\mathbf{D}_{\mathbf{i}}(fg) = \sum_{\mathbf{h}+\mathbf{k}=\mathbf{i}} \mathbf{D}_{\mathbf{h}}(f) \mathbf{D}_{\mathbf{k}}(g)$. Moreover, when the field $\mathbb{K}$ has characteristic zero, then $\mathbf{D}_{\mathbf{i}} = \dfrac{1}{\mathbf{i}!} \mathbf{D}^{\mathbf{i}} := \dfrac{1}{\mathbf{i}!} \dfrac{\partial^{i_1 + \cdots + i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$.
$v_{\mathbf{P}}^{\mathbf{i}}$	the composition $v_{\mathbf{P}} \circ \mathbf{D}_{\mathbf{i}}$, i.e. $v_{\mathbf{P}}^{\mathbf{i}} \colon \mathbb{K}[X] \to \mathbb{K}$, $p \mapsto (\mathbf{D}_{\mathbf{i}} p)(\mathbf{P})$

$\wp$ — $\{(\mathbf{P}_1, \mathcal{F}_1), \ldots, (\mathbf{P}_N, \mathcal{F}_N)\}$ each element $(\mathbf{P}_j, \mathcal{F}_j) \in \wp$ consists of a point $\mathbf{P}_j$ of $\mathbb{R}^n$ together with an n-dimensional Ferrers diagram $\mathcal{F}_j \subset \mathbb{N}^n$

$(\mathbf{P}, \mathbf{i}) \in \wp$ — this notation stands for $\mathbf{P} = \mathbf{P}_j$ and $\mathbf{i} \in \mathcal{F}_j$ for some $j \in \{1, \ldots, N\}$

$\Im(\wp)$ — the cofinite ideal $\Im(\wp) := \left\{p \in \mathbb{K}[X] \mid (\forall j)(\forall \mathbf{i} \in \mathcal{F}_j)\left(v^{\mathbf{i}}_{\mathbf{P}_j}(p) = 0\right)\right\}$ associated to $\wp = \{(\mathbf{P}_1, \mathcal{F}_1), \ldots, (\mathbf{P}_N, \mathcal{F}_N)\}$

§ 1. Introduction.

1.1 Since the generalization to the multivariate case of the notion of linearly recursive sequence (l.r.s.) plays a big part in what follows, it is convenient to assume this notion as a starting-point.

Let us recall that a sequence $v = (v_i)_{i \in \mathbb{N}}$, is said to be a I-l.r.s., I ideal of $\mathbb{K}[x]$, if, for every $p \in I$, we have $p(E)(v) = 0$ (E shift operator). Every element $p \in I$ is said to be a *characteristic polynomial* and the generator g of $I = (g)$ the *minimal polynomial* of the I-l.r.s. v.

An I-l.r.s. v is completely determined by its minimal polynomial g and by its initial values v_i, $0 \leq i < k = \deg(g)$, that is the values which the form v takes on the monomials $x^0, \ldots, x^{k-1}$ whose residue classes form a linear basis — in fact, the smallest one (among all monomial bases) with respect to the usual order on monomials — of the quotient algebra $\mathbb{K}[x]/I$. As a consequence, the set $\mathcal{S}(I)$ of all the I-l.r.s. is a k-dimensional $\mathbb{K}$-vector space ($k = \deg(g)$, $I = (g)$). Morover, $\mathcal{S}(I)$ is a cyclic $\mathbb{K}[x]$-submodule of the $\mathbb{K}[x]$-module $\mathbb{K}[x]^*$, where the scalar product is defined by $\mathbb{K}[x] \times \mathbb{K}[x]^* \longrightarrow \mathbb{K}[x]^*$, $(p, v) \longmapsto p(E)(v)$ (equivalently, $(p, v) \longmapsto [q \mapsto v(pq)]$). A generator of $\mathcal{S}(I)$ as $\mathbb{K}[x]$-module is any I-l.r.s. $v = (v_i)$ such that no proper divisor of the generator g of I is a characteristic polynomial for v; for instance, the I-l.r.s. v whose first k terms are $v_0 = v_1 = \cdots = v_{k-2} = 0$, $v_{k-1} = 1$.

1.2 Peterson and Taft [1] showed that the set $\mathbb{K}[x]^\circ = \bigcup \mathcal{S}(I)$ (I cofinite ideal) of all l.r.s. is the underlying set of the dual bialgebra $\mathcal{B}^\circ$ of the usual polynomial bialgebra $\mathcal{B}$.

In [2], the authors of the present note assumed the same bialgebraic point of view in order to generalize to the multivariate case the notion of I-l.r.s.. Let now $\mathcal{B}_n = (\mathbb{K}[X], m_n, u_n, \Delta_n, \varepsilon_n)$ be the multivariate polynomial bialgebra. The elements of the dual bialgebra $\mathcal{B}_n^\circ \subset \mathbb{K}[X]^*$ are precisely those linear forms $\mathbf{f} : \mathbb{K}[X] \to \mathbb{K}$ whose kernel contains a cofinite ideal $I \subseteq \mathbb{K}[X]$, that is an ideal I such that $\dim(\mathbb{K}[X]/I) < \infty$. Any such form $\mathbf{f}$ is called an *I-linearly recursive function.*

Contrary to the univariate case, in the present one a few calculation problems arise, due essentially to the simultaneous apparence of three new facts: (*i*) $\mathbb{K}[X]$ is not a principal domain, (*ii*) not every ideal of $\mathbb{K}[X]$ is cofinite and (*iii*) there are infinitely many different *term orderings* $\preceq$ on the monoid $M_X \subset \mathbb{K}[X]$.

1.3 The previous remarks require some more words. Let us consider the fact that in order to give in an effective way a linearly recursive function $\mathbf{f} = \sum_{\mathbf{i}\in\mathbb{N}^n} f_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} \in \mathcal{B}_n^\circ$ we need (*a*) a cofinite ideal $I = (g_1, \ldots, g_s) \subseteq \mathbb{K}[X]$ and (*b*) a monomial basis $(\mathbf{x}^{\mathbf{j}} + I)_{\mathbf{j}\in L}$, $L \subseteq \mathbb{N}^n$, for the quotient algebra $\mathbb{K}[X]/I$. In fact, the I-linearly recursive function $\mathbf{f}$ is completely determined by its "initial values" $f_{\mathbf{j}}$, $\mathbf{j} \in L$, all the other values $f_{\mathbf{i}}$, $\mathbf{i} \notin L$, being computed by means of the generators $g_1, \ldots, g_s$ of the ideal I. The idea is to use $g_1, \ldots, g_s$ as "scales of recurrence".

Nevertheless, in practice this is not yet enough. What we really need is (a') a reduced Gröbner basis $\mathrm{RGB}(I) = (h_1, \ldots, h_t)$ for the ideal I relative to the fixed term ordering $\preceq$ and (b') a monomial basis $(\mathbf{x}^{\mathbf{j}} + I)_{\mathbf{j}\in L}$ which is *minimal* with respect to $\preceq$, that is a basis $(\mathbf{x}^{\mathbf{j}}+I)_{\mathbf{j}\in L} = \{\mathbf{x}^{\mathbf{j}_1}+I, \ldots, \mathbf{x}^{\mathbf{j}_h}+I\}$, with $\mathbf{x}^{\mathbf{j}_1} \prec \mathbf{x}^{\mathbf{j}_2} \prec \ldots \prec \mathbf{x}^{\mathbf{j}_h}$, such that for every other monomial basis $(\mathbf{x}^{\mathbf{j}'}+I)_{\mathbf{j}'\in L'} = \{\mathbf{x}^{\mathbf{j}'_1}+I, \ldots, \mathbf{x}^{\mathbf{j}'_h}+I\}$, with $\mathbf{x}^{\mathbf{j}'_1} \prec \mathbf{x}^{\mathbf{j}'_2} \prec \ldots \prec \mathbf{x}^{\mathbf{j}'_h}$, we have $\mathbf{x}^{\mathbf{j}_r} \prec \mathbf{x}^{\mathbf{j}'_r}$ for every $r = 1, \ldots, h$. It is easy to check that a monomial basis $(\mathbf{x}^{\mathbf{j}} + I)_{\mathbf{j}\in L}$ is a *minimal* monomial basis only if $L \subseteq \mathbb{N}^n$ is an n-dimensional Ferrers diagram.

Notice that the minimal (with respect to $\preceq$) monomial basis $(\mathbf{x}^{\mathbf{j}}+I)_{\mathbf{j}\in L}$ is determined by $\mathrm{RGB}(I) = (h_1, \ldots, h_t)$ in the following way. Let $\mathbf{x}^{\mathbf{j}_r}$, $r = 1, \ldots, t$, be the leading term (with respect to $\preceq$) of the polynomial $h_r \in \mathrm{RGB}(I)$ and let $\overline{L} \subseteq \mathbb{N}^n$ be the poset filter of $\mathbb{N}^n$ (ordered by the usual product order $\leq$) generated by $\mathbf{j}_1, \ldots, \mathbf{j}_t$; then L is the complementary ideal $L = \mathbb{N}^n \setminus \overline{L}$.

1.4 The above remarks seemingly indicate that Gröbner bases theory be able to satisfy our computational needs. Unfortunatly, that theory provides no device to make sure *in advance* whether a given set of polynomials $(g_1, \ldots, g_s)$ generates a cofinite ideal. In [3] (see also [4]) a combinatorial algorithm producing cofinite ideals is described. More precisely, given a finite set $\wp := \{(\mathbf{P}_1, \mathcal{F}_1), \ldots, (\mathbf{P}_N, \mathcal{F}_N)\}$ ($\mathbf{P}_j \in \mathbb{K}^n$; $\mathcal{F}_j \subset \mathbb{N}^n$ is n-dimensional Ferrers diagram), it is not difficult to prove that the set

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

associated to $\{v^{\mathbf{i}}_{\mathbf{P}} \mid (\mathbf{P}, \mathbf{i}) \in \wp\} \subset \mathbb{K}^{\mathbb{N}^n}$ is a cofinite ideal. Notice that $\mathrm{codim}(\Im(\wp)) = \sum_{j=1}^N \#\mathcal{F}_j$ and that $\{P_1, \ldots, P_N\}$ is the affine variety of $\Im(\wp)$. The algorithms described in [3] produce first the monomial basis for $\mathbb{K}[x]/\Im(\wp)$ which is minimal with respect to the inverted lexicographical order $\preceq_{i.l.}$ and then a reduced Gröbner basis of $\Im(\wp)$.

1.5 Bearing in mind on the one hand that the forms $v_P^{\mathbf{i}}$, $P \in \mathbb{K}^n, \mathbf{i} \in \mathbb{N}^n$, are a linear basis of the dual bialgebra $\mathcal{B}_n^\circ$ (see [2], Prop. 6 and its Corollary) and on the other hand that not every cofinite ideal I is of the form $\Im(\wp)$, the following question naturally arises: under what general conditions a system of independent linear combinations of forms $v_P^{\mathbf{i}}$ may generate a subspace $H \subset \mathcal{B}_n^\circ$ which determines a cofinite ideal I as the maximal ideal contained in the kernel of all the forms in H (in other words, $H = \mathcal{S}(I)$ for some cofinite ideal $I \subset \mathbb{K}[X]$)? For instance, it is easy to prove that H must be both a finitely generated $\mathbb{K}[X]$-submodule of the $\mathbb{K}[X]$-module $\mathbb{K}[X]^*$ and a finite dimensional $\mathbb{K}$-subspace of $\mathbb{K}[X]^\circ$. The search for such necessary and sufficient conditions is a matter of a work-in-progress by Cerlienco and Mureddu.

1.6 From a more general point of view, analogous questions can be asked for general (i.e. not necessarily cofinite) ideals. This led Piras [5] to the notion of *Macaulay's inverse system*. This notion has been introduced by F. S. Macaulay [7] in the attempt to find linear conditions for solving the Ideal Membership Problem for a polymomial in $\mathbb{C}[x_1, \ldots, x_n]$.

According to Macaulay (yet he made use of a very cumbersome old-style language) the inverse system of an ideal I is the space of all the $\mathbb{C}$-linear forms $f\colon \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ whose kernel contains I. An immediate consequence of this definition is that the inverse system of an ideal I is isomorphic, as a $\mathbb{C}$-vector space, to the linear dual of $\mathbb{C}[x_1, \ldots, x_n]/I$. Therefore the dimension of the inverse system (in the original sense of Macaulay) of a non-cofinite ideal I is strictly greater than the dimension of $\mathbb{C}[x_1, \ldots, x_n]/I$, which is countable.

This trivial observation points to a contradiction in the theory of inverse systems as developed by Macaulay. In fact Macaulay has given an incorrect proof of two propositions (cfr. [7] p. 75 and p. 91) which imply that the dimension of an inverse system is at most countable. These two propositions played a central role in Macaulay's construction and their falsity would have devastating effects on the theory of inverse systems. However, the two properties seem to hold for proper subspaces of an inverse system. This fact has led Piras to modify Macaulay's definition in order to recover his main results. This modified definition of inverse system, as well as its main properties, are the subject of §**2**.

1.7 In the Gröbner bases computational framework, another question which has a combinatorial flavour naturally arises. When we are looking for a Gröbner basis for a given ideal, we have previously to fix a term ordering $\preceq$ on $\mathbb{N}^n$. Moreover, in the applications some particular term ordering is often needed. In the usual computer algebra systems which contain a Gröbner bases package (for instance, Maple, Mathematica, Reduce, Macaulay; see [12, Appendix C], [13]) only a few term orderings are allowed. This is, at the best of our knowledge, because a convenient representation of term orderings is not known. Even the interesting results of Robbiano [14] are not completely satisfactory from our point of view; in particular, Robbiano's representation does not permit an easy comparison between two such representations in order to decide whether they both represent the same term ordering (or not). In §3 a handy canonical representation of term orderings by which all these problems can be easily solved is given.

§ **2**. **Inverse systems.**

2.1 We will consider $\mathbb{K}[X]^*$ with its $\mathbb{K}[X]$-module structure defined by $\mathbb{K}[X] \times \mathbb{K}[X]^* \to \mathbb{K}[X]^*$, $(p, f) \mapsto p\cdot\mathbf{f}$, where $p\cdot\mathbf{f} = p(\mathbf{E})(\mathbf{f})$, equivalently, $(p\cdot\mathbf{f})(q) = \mathbf{f}(pq)$. If $Y \subseteq \mathbb{K}[X]^*$ we will put

$$\mathcal{P}(Y) = \{p \in \mathbb{K}[X] \mid p\cdot\mathbf{f} = 0 \text{ for all } \mathbf{f} \in Y\}.$$

Let I be an ideal of $\mathbb{K}[X]$. Any submodule H of $\mathbb{K}[X]^*$ such that $\mathcal{P}(H) = I$ will be said an *inverse system* of I. According to Macaulay (see [7], p. 68) <u>the</u> inverse system of the ideal I is the set

$$\mathcal{S}(I) = \left\{ \mathbf{f} \in \mathbb{K}[X]^* \;\middle|\; \big(p\cdot\mathbf{f}\big)(1) := \mathbf{f}(p) = 0 \text{ for every } p \in I \right\}.$$

$\mathcal{S}(I)$ is also an inverse system according to our definition.

Prop. 1 *$\mathcal{S}(I)$ is a $\mathbb{K}[X]$-submodule of $\mathbb{K}[X]^*$ which is an inverse system according to our definition as well, i. e. $\mathcal{P}(\mathcal{S}(I)) = I$. Moreover, $\mathcal{S}(I)$ is a $\mathbb{K}$-vectorspace isomorphic to the dual $\mathbb{K}$-vectorspace of $\mathbb{K}[X]/I$.* □

From **Prop. 1** we deduce:

- $\mathcal{S}(I)$ is a finite-dimensional vector space iff I is a cofinite ideal. When I is not cofinite, $\mathcal{S}(I)$ has non-countable dimension.
- With respect to a fixed term ordering on $\mathbb{K}[X]$, let us denote by $\mathrm{L{\small T}}(I)$ the ideal of $\mathbb{K}[X]$ generated by the leading terms of the elements of I; an element $\mathbf{f}$ of $\mathcal{S}(I)$ is fully determined by its values on the monomials $\mathbf{x}^{\mathbf{i}} \notin \mathrm{L{\small T}}(I)$, since the $(\mathbf{x}^{\mathbf{i}} + I)$'s are a basis for $\mathbb{K}[X]/I$.

The last remark allows us to describe some families of elements of $\mathcal{S}(I)$ that generate inverse systems with countable dimension as vectorspaces. For instance, consider the family of linear forms

$$\mathcal{R}_L = \left\{\mathbf{f}_{\mathbf{i}} \mid \mathbf{f}_{\mathbf{i}}(\mathbf{x}^{\mathbf{j}}) = \delta_{\mathbf{i}}^{\mathbf{j}} \text{ and } \mathbf{i}, \mathbf{j} \in L\right\} \subseteq \mathcal{S}(I)$$

(where $L = \{\mathbf{i} \in \mathbb{N}^n \mid \mathbf{x}^{\mathbf{i}} \notin \mathrm{L{\small T}}(I)\}$, and $\delta_{\mathbf{i}}^{\mathbf{j}} = \delta_{i_1}^{j_1} \cdots \delta_{i_n}^{j_n}$ is the multivariate Kronecker symbol).

Prop. 2 *For every polynomial $p \in \mathbb{K}[X]$ and every form $\mathbf{f}_{\mathbf{i}} \in \mathcal{R}_L$ we have:*

$$p \equiv \sum_{\mathbf{i} \in L} \mathbf{f}_{\mathbf{i}}(p)\mathbf{x}^{\mathbf{i}} \qquad (\mathrm{mod}\ I). \qquad \square$$

Note that using **Prop. 2** we can easily compute the values of the functionals $\mathbf{f_i}$. For every $\mathbf{j} \in \mathbb{N}^n$, $\mathbf{f_i}(\mathbf{x^j})$ is the coefficient of $\mathbf{x^i}$ in the remainder of $\mathbf{x^j}$ on division by the reduced Gröbner basis with respect to the fixed monomial ordering (i. e. $\mathbf{f_i}(\mathbf{x^j}) = a_\mathbf{i}$ where $\mathbf{x^j} \equiv \sum_{\mathbf{i}\in L} \mathbf{a_i x^i} \pmod{I}$).

Corollary 1. *The* $\mathbb{K}[X]$*-module* H_L*, generated by* $\mathcal{R}_L$*, is an inverse system of the ideal* I*.*

Corollary 2. $\mathbf{f} \in \mathcal{S}(I)$ *if and only if* $\mathbf{f} = \sum_{\mathbf{i}\in L} \mathbf{f}(\mathbf{x^i})\mathbf{f_i}$.

Corollary 3. *Let* I *be a cofinite ideal of* $\mathbb{K}[X]$*; then* $\mathcal{S}(I) = H_L$*.*

An equivalent statement of the following proposition has been first stated by Macaulay in [7], p. 91. Unfortunately, Macaulay's proof is not fully satisfactory. A correct proof is given in [6].

Prop. 3 *For every ideal* $I \subseteq \mathbb{K}[X]$*, there is an inverse system which is finitely generated as* $\mathbb{K}[X]$*-module.* □

In particular, it can be proved that every irreducible ideal has a cyclic inverse system.

2.2 In this section we generalize the results in **2.1** to the case of some power $\mathbb{K}[X]^l$. The $\mathbb{K}$-vectorspace $\mathbb{K}[X]^l$ and $(\mathbb{K}[X]^*)^l$ will be regarded also as $\mathbb{K}[X]$-modules. The scalar product is given by

$$\begin{aligned} \mathbb{K}[X] \times \mathbb{K}[X]^l &\longrightarrow \mathbb{K}[X]^l \\ \Big(p,\ (p_1,\dots,p_l)\Big) &\longmapsto (pp_1,\dots,pp_l) \end{aligned}$$

and, respectively, by

$$\begin{aligned} \mathbb{K}[X] \times (\mathbb{K}[X]^*)^l &\longrightarrow (\mathbb{K}[X]^*)^l \\ \Big(p,\ (\mathbf{f}_1,\dots,\mathbf{f}_l)\Big) &\longmapsto (p\cdot\mathbf{f}_1,\dots,p\cdot\mathbf{f}_l). \end{aligned}$$

For every $Y \subseteq (\mathbb{K}[X]^*)^l$, we put

$$\mathcal{P}(Y) = \Big\{ (p_1,\dots,p_l) \in \mathbb{K}[X]^l \ \Big|\ p_1\cdot\mathbf{f}_1 + \cdots + p_l\cdot\mathbf{f}_l = 0 \quad \text{for all } (\mathbf{f}_1,\dots,\mathbf{f}_l) \in Y \Big\}.$$

$\mathcal{P}(Y)$ is clearly a submodule of $\mathbb{K}[X]^l$; conversely, we want to show that for every submodule M of $\mathbb{K}[X]^l$ there is a subset Y of $(\mathbb{K}[X]^*)^l$ such that $\mathcal{P}(Y) = M$. Any such subset Y will be called an *inverse system* of the submodule M.

For the purposes of our discussion here, we first denote by $e_j(p)$ the element $(0,\dots,p,\dots,0)$ of $\mathbb{K}[X]^l$. Moreover, denote by $\mathcal{G}$ the reduced

Gröbner basis of M with respect to a fixed term ordering $\preceq$ on $\mathbb{K}[X]^l$ and by $\mathrm{Red}_{\preceq}(p_1, \ldots, p_l)$ the unique element obtained by reducing $(p_1, \ldots, p_l)$ modulo $\mathcal{G}$. (Concerning Gröbner bases theory relative to polynomial modules see [8].) The set

$$\left\{ e_j(\mathbf{x}^{\mathbf{p}}) + M \;\middle|\; e_j(\mathbf{x}^{\mathbf{p}}) \notin \mathrm{L{\scriptstyle T}}(M) \right\}$$

(where $\mathrm{L{\scriptstyle T}}(M)$ is the $\mathbb{K}[X]$-module generated by the leading terms of the elements of M) is a basis of the $\mathbb{K}$-vectorspace $\mathbb{K}[X]^l/M$. Let

$$L = \left\{ (\mathbf{p}, j) \in \mathbb{N}^n \times \{1, \ldots, l\} \;\middle|\; e_j(\mathbf{x}^{\mathbf{p}}) \notin \mathrm{L{\scriptstyle T}}(M) \right\}.$$

For every $(\mathbf{p}, j) \in L$ and every $1 \leq i \leq l$, let $\mathbf{f}^j_{\mathbf{p},i}$ be the $\mathbb{K}$-linear map from $\mathbb{K}[X]$ to $\mathbb{K}$ defined by

$$\text{(1)} \qquad \mathbf{f}^j_{\mathbf{p},i}(p) = \text{coeff. of } (e_j(\mathbf{x}^{\mathbf{p}}) + M) \text{ occurring in } (e_i(p) + M).$$

Prop. 4 *Let $\mathcal{R}_L(M)$ be the submodule of $(\mathbb{K}[X]^*)^l$ generated by the l-tuples $(\mathbf{f}^j_{\mathbf{p},1}, \ldots, \mathbf{f}^j_{\mathbf{p},l})$, $(\mathbf{p}, j) \in L$. Then $\mathcal{R}_L(M)$ is an inverse system of the submodule M, i. e. $\mathcal{P}(\mathcal{R}_L(M)) = M$.*

Proof: See [6]. □

Next we describe the maximal inverse system of the submodule $M \subseteq \mathbb{K}[X]^l$. Let $\langle (q_{1,1}, \ldots, q_{1,l}), \ldots, (q_{k,1}, \ldots, q_{k,l}) \rangle$ be a system of generators of M and let $\mathcal{S}(M)$ be the set of the l-tuples $(\mathbf{f}_1, \ldots, \mathbf{f}_l)$ of $(\mathbb{K}[X]^*)^l$ which are solutions of the linear system:

$$\text{(2)} \qquad \left\{ \begin{array}{lcccc} q_{1,1} \cdot w_1 + & \cdots & + q_{1,l} \cdot w_l & = & 0 \\ \multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ q_{k,1} \cdot w_1 + & \cdots & + q_{k,l} \cdot w_l & = & 0. \end{array} \right.$$

Prop. 5 *For every submodule M of $\mathbb{K}[X]^l$, we have*

$$(\mathbf{f}_1, \ldots, \mathbf{f}_l) \in \mathcal{S}(M) \iff (\forall i) \left(\mathbf{f}_i = \sum_{(\mathbf{p},j) \in L} \mathbf{f}_j(\mathbf{x}^{\mathbf{p}}) \mathbf{f}^j_{\mathbf{p},i} \right).$$

Thus, $\mathcal{P}(\mathcal{S}(M)) = M$.

Proof: See [6]. □

This proposition enables us to compute the general solution of the system (2). It is of the form

$$\Big(\sum_{(\mathbf{p},j) \in L} b_{\mathbf{p},j} \mathbf{f}^j_{\mathbf{p},1}, \ldots, \sum_{(\mathbf{p},j) \in L} b_{\mathbf{p},j} \mathbf{f}^j_{\mathbf{p},l} \Big).$$

where the linear forms $\mathbf{f}^j_{\mathbf{p},i}$ are defined as in (1) and $(b_{\mathbf{p},j})_{(\mathbf{p},j)\in L}$ is an arbitrary family of elements of $\mathbb{K}$.

When $\mathbb{K}$ is a field of characteristic zero, the same result can be also used for computing the solutions of a homogeneous system of linear partial differential equations with constant coefficients:

$$\left\{\begin{array}{l} q_{1,1}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\varphi_1+\cdots+q_{1,l}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\varphi_l=0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ q_{k,1}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\varphi_1+\cdots+q_{k,l}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\varphi_l=0. \end{array}\right. \tag{3}$$

In fact, making use of **Prop. 6** below, it is sufficient to observe that system (2) is mapped into (3) by the $\mathbb{K}$-linear isomorphism

$$\begin{aligned} \mathcal{E}:\mathbb{K}[X]^*&\longrightarrow\mathbb{K}[[\mathbf{u}]] \\ \mathbf{f}&\longmapsto\sum_{\mathbf{h}}\mathbf{f}(\mathbf{x}^{\mathbf{h}})\frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}. \end{aligned}$$

Prop. 6 *Let $\mathbb{K}$ be a field of characteristic zero. For every polynomial $p=\sum_{\mathbf{i}}a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\in\mathbb{K}[X]$ and every linear form $\mathbf{f}\in\mathbb{K}[X]^*$ we have:*

$$\mathcal{E}(p\cdot\mathbf{f})=\Big(\sum_{\mathbf{i}}a_{\mathbf{i}}\frac{\partial^{|\mathbf{i}|}}{\partial\mathbf{u}^{\mathbf{i}}}\Big)(\mathcal{E}(\mathbf{f})),\quad |\mathbf{i}|=i_1+\cdots+i_n.$$

Proof: See [6]. □

In explicit terms, if M is the $\mathbb{K}[X]$-module generated by the set

$$\{(q_{1,1},\dots,q_{1,l}),\dots,(q_{k,1},\dots,q_{k,l})\},$$

then we have

$$\begin{aligned} &q_{1,1}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\Big(\sum_{\mathbf{h}}\mathbf{f}_1(\mathbf{x}^{\mathbf{h}})\frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}\Big) \\ &\qquad+\cdots+q_{1,l}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\Big(\sum_{\mathbf{h}}\mathbf{f}_l(\mathbf{x}^{\mathbf{h}})\frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}\Big)=0 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &q_{k,1}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\Big(\sum_{\mathbf{h}}\mathbf{f}_1(\mathbf{x}^{\mathbf{h}})\frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}\Big) \\ &\qquad+\cdots+q_{k,l}(\frac{\partial}{\partial u_1},\dots,\frac{\partial}{\partial u_n})\Big(\sum_{\mathbf{h}}\mathbf{f}_l(\mathbf{x}^{\mathbf{h}})\frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}\Big)=0, \end{aligned}$$

if and only if $(\mathbf{f}_1, \dots, \mathbf{f}_l) \in \mathcal{S}(M)$. Thus, the general solution of (3) is

$$\left(\sum_{\mathbf{h}} \Big(\sum_{(\mathbf{p},j)\in B} b_{\mathbf{p},j} \mathbf{f}^j_{\mathbf{p},1}(\mathbf{x}^{\mathbf{h}}) \Big) \frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!}, \ \dots, \ \sum_{\mathbf{h}} \Big(\sum_{(\mathbf{p},j)\in B} b_{\mathbf{p},j} \mathbf{f}^j_{\mathbf{p},l}(\mathbf{x}^{\mathbf{h}}) \Big) \frac{\mathbf{u}^{\mathbf{h}}}{\mathbf{h}!} \right).$$

§ 3. Canonical matrix representation of term orderings.

3.1 Let $\preceq$ be a *term ordering* on $\mathbb{N}^n$, that is a linear order which is compatible with the monoid structure of $\mathbb{N}^n$: $0 \preceq \mathbf{i}$, $\quad \mathbf{i} \prec \mathbf{j} \Rightarrow \mathbf{i}+\mathbf{h} \prec \mathbf{j}+\mathbf{h}$. It is easily seen that $\preceq$ can be uniquely extended to a linear order on $\mathbb{Z}^n$ (resp.: $\mathbb{Q}^n$) compatible with the structure of $\mathbb{Z}$-module (resp.: $\mathbb{Q}$-vectorspace).

It can be also proved (see [11]) that any term ordering $\preceq$ is the restriction to $\mathbb{N}^n$ of at least one linear order $\preceq^{\mathbb{R}}$ on $\mathbb{R}^n$ which is compatible with the structure of $\mathbb{R}$-vectorspace. In the following, such an order will be simply referred as a *c.l.order*. As an example, consider the c.l.order $\preceq_{\overline{\mathbf{b}}}$ determined by a given basis $\overline{\mathbf{b}} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of $\mathbb{R}^n$ in the following way:

$$\mathbf{P} \prec_{\overline{\mathbf{b}}} \mathbf{Q} \quad \Longleftrightarrow \quad \begin{pmatrix} \alpha^1 \\ \vdots \\ \alpha^n \end{pmatrix} \prec_{lex} \begin{pmatrix} \beta^1 \\ \vdots \\ \beta^n \end{pmatrix}$$

where $\mathbf{P} = \sum_{i=1}^n \alpha^i \mathbf{b}_i$, $\mathbf{Q} = \sum_{i=1}^n \beta^i \mathbf{b}_i$ and $\preceq_{lex}$ is the usual lexicographic order.

Equivalently,

$$\mathbf{P} \prec_{\overline{\mathbf{b}}} \mathbf{Q} \quad \Longleftrightarrow \quad C\mathbf{P} \prec_{lex} C\mathbf{Q}$$

where $C^{-1} = B = (b^i_j)_{(i,j)\in\mathbf{n}^2}$ with $\mathbf{b}_j = (b^i_j)_{i\in\mathbf{n}}$ and $\mathbf{n} = \{1, \dots, n\}$. It is not difficult to check that two different bases $\overline{\mathbf{b}} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$, $\overline{\mathbf{b}}' = (\mathbf{b}'_1, \dots, \mathbf{b}'_n)$ determine the same c.l.order ($\preceq_{\overline{\mathbf{b}}} = \preceq_{\overline{\mathbf{b}}'}$) iff

$$B' = B \cdot \Lambda \qquad (\text{equivalently,} \quad C' = \Lambda^{-1} C)$$

where $\Lambda = (\lambda^i_j)$ is a lower triangular matrix with $\lambda^i_i > 0$.

The following fundamental result is due to Erdős [9] (see also [10], [11]).

Theorem (Erdős) *Let $\preceq^{\mathbb{R}}$ be a c.l.order on $\mathbb{R}^n$; then, there is a basis (in fact, infinitely many bases) $\overline{\mathbf{b}} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of $\mathbb{R}^n$ such that $\preceq^{\mathbb{R}} = \preceq_{\overline{\mathbf{b}}}$.*

In other words, (i) any c.l.order $\preceq^{\mathbb{R}}$ on $\mathbb{R}^n$ can be represented by a non-singular matrix C for which we have

$$\mathbf{P} \prec^{\mathbb{R}} \mathbf{Q} \quad \Longleftrightarrow \quad C\mathbf{P} \prec_{lex} C\mathbf{Q}, \tag{4}$$

and (ii) any two matrices C, C' which represent the same c.l.order $\preceq^{\mathbb{R}}$ satisfy the equivalence relation

$$C' = \Lambda^{-1}C. \tag{5}$$

We want to determine a *canonical matrix representation* of $\preceq^{\mathbb{R}}$. To this aim, let us define a *lexicographic matrix* to be an m by n matrix $A = (a^i_j)$ $(m \leq n)$ of the form

$$\begin{pmatrix} 0 & \dots & 0 & \pm 1 & * & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \pm 1 & \dots & * \\ 0 & \dots & \pm 1 & 0 & * & 0 & \dots & * \\ \cdot & \dots & \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ \pm 1 & \dots & 0 & 0 & * & 0 & \dots & * \\ 0 & \dots & 0 & 0 & \pm 1 & 0 & \dots & * \end{pmatrix},$$

that is a matrix satisfying the following conditions: (a) in each row of A there is at least one non-zero entry; (b) if we denote by $a^i_{j(i)}$ the first non-zero entry in the i-th row of A, then $a^i_{j(i)}$ is either 1 or -1; (c) for each $i = 1, \dots, n$ and for each $i' > i$ we have $a^{i'}_{j(i)} = 0$. Notice that the rank of a $m \times n$ lexicographic matrix A is m.

Prop. 7 *For every c.l.order $\preceq^{\mathbb{R}}$ on $\mathbb{R}^n$, there is one and only one $n \times n$ lexicographic matrix C for which (4) is true.*

Proof: The statement is a straightforward consequence of the Erdős Theorem and of (5). □

3.2 Consider now a term ordering $\preceq$ on $\mathbb{Q}^n$. Let $\preceq^{\mathbb{R}}$ be any c.l.order on $\mathbb{R}^n$ whose restriction is $\preceq$. Let $\overline{\mathbf{b}} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$, $B = (b^i_j)$, $C = (c^i_j) = B^{-1}$ and Λ have the same meaning as in **3.1**.

Let $T_{n-i} := (\mathbf{b}_{i+1}, \dots, \mathbf{b}_n) \subseteq \mathbb{R}^n =: T_n$, that is the $(n-i)$–dimensional subspace defined by the linear system

$$\begin{cases} c^1_1 x^1 + \cdots + c^1_n x^n = 0 \\ \dots\dots\dots\dots\dots\dots\dots \\ c^i_1 x^1 + \cdots + c^i_n x^n = 0 \end{cases}, \qquad \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix} \in \mathbb{R}^n.$$

Observe that the hyperplane $\pi_{i+1} := (\mathbf{b}_1, \dots \mathbf{b}_i, \mathbf{b}_{i+2}, \dots, \mathbf{b}_n) \subseteq \mathbb{R}^n$ (whose equation is $c^{i+1}_1 x^1 + \cdots + c^{i+1}_n x^n = 0$) divides T_{n-i} into three parts: the intersection $T_{n-i-1} = T_{n-i} \cap \pi_{i+1}$ and the two half-spaces T^+_{n-i}, T^-_{n-i} each of which contains only positive, resp. negative points.

When passing from $\preceq^{\mathbb{R}}$ to $\preceq$, it may happen that all rational points of T_{n-i} belong to π_{i+1} as well, so that

$$\sum c^1_j x^j = \dots = \sum c^i_j x^j = 0 \quad \Rightarrow \quad \sum c^{i+1}_j x^j = 0$$

for every rational point $(x^1, \dots, x^n)_{-1} \in \mathbb{Q}^n$ or, which is the same, the two n-tuples of vectors

$$\begin{pmatrix} c_1^1 \\ \vdots \\ c_1^i \end{pmatrix}, \dots, \begin{pmatrix} c_n^1 \\ \vdots \\ c_n^i \end{pmatrix}$$

and

$$\begin{pmatrix} c_1^1 \\ \vdots \\ c_1^i \\ c_1^{i+1} \end{pmatrix}, \dots, \begin{pmatrix} c_n^1 \\ \vdots \\ c_n^i \\ c_n^{i+1} \end{pmatrix}$$

have the same rational dimension. In this case, when you are interested to rational points alone, the information contained in the $(i+1)$-th row of the matrix C is useless, so that we can harmlessly cut that row off. From this and from **Prop. 7** we deduce the following results.

Prop. 8 *Let $C = (c_j^i)$ be an $m \times n$ matrix $(m \leq n)$ and let $\preceq$ be the order on $\mathbb{N}^n$ defined by*

$$\text{(6)} \qquad \mathbf{i} \prec \mathbf{j} \iff C\mathbf{i} \prec_{lex} C\mathbf{j} \qquad \forall \mathbf{i}, \mathbf{j} \in \mathbb{N}^n.$$

Then, $\preceq$ is a term ordering iff the columns of C are rationally independent.□

Prop. 9 *For every term ordering $\preceq$ on $\mathbb{N}^n$, there is one and only one $m \times n$ lexicographic matrix $C = (c_j^i)$ satisfying (6) such that for every $i = 1, \dots, m-1$ the rational dimension of the vectors*

$$\begin{pmatrix} c_1^1 \\ \vdots \\ c_1^i \end{pmatrix}, \dots, \begin{pmatrix} c_n^1 \\ \vdots \\ c_n^i \end{pmatrix}$$

is strictly less than the rational dimension of the vectors

$$\begin{pmatrix} c_1^1 \\ \vdots \\ c_1^i \\ c_1^{i+1} \end{pmatrix}, \dots, \begin{pmatrix} c_n^1 \\ \vdots \\ c_n^i \\ c_n^{i+1} \end{pmatrix}.$$

□

3.3 Let $\preceq$ be the term ordering on $\mathbb{N}^n$ represented by the $m \times n$ matrix

$$\hat{C} = \begin{pmatrix} c_1^{\iota_1} & \dots & c_n^{\iota_1} \\ \cdot & \dots & \cdot \\ c_1^{\iota_m} & \dots & c_n^{\iota_m} \end{pmatrix} \qquad (m \leq n).$$

For $h = 1, \ldots, m$, let us denote by d_h the rational dimension of the n vectors

$$\begin{pmatrix} c_1^{\iota_1} \\ \vdots \\ c_1^{\iota_h} \end{pmatrix} \cdots \begin{pmatrix} c_n^{\iota_1} \\ \vdots \\ c_n^{\iota_h} \end{pmatrix}. \tag{7}$$

We shall say that the matrix $\hat{C}$ is *rationally reduced* if $d_1 < d_2 < \ldots < d_m = n$. It is clear that any matrix can be rationally reduced by cutting a few suitable rows off from it.

We give now an algorithm which associates a rationally reduced lexicographic matrix $\tilde{C}$ to any matrix $\hat{C}$. This matrix $\tilde{C}$ is said to be the *canonical lexicographic representation* of the term ordering $\preceq$. Indeed, it can be proved (see [11]) that two different matrices $\hat{C}$ and $\hat{D}$ represent the same term ordering on $\mathbb{N}^n$ iff $\tilde{C} = \tilde{D}$.

It is convenient to divide our algorithm into two parts. The first part is aimed to "capture" a c.l.order $\preceq^{\mathbb{R}}$ (in fact, the most suitable one for our purposes) whose restriction to $\mathbb{N}^n$ is $\preceq$; it consists in constructing an $n \times n$ matrix $C = (c_j^i)$ by putting $n - m$ new rows inside those of $\hat{C}$, as described below. The second part of the algorithm consists in (i) reducing C in its lexicographic form C' and then (ii) cutting the rows whose indices are different from $1, d_1 + 1, \ldots, d_{m-1} + 1$ off from C'.

Without loss of generality we may assume that the given matrix $\hat{C}$ is rationally reduced and also that, for each $h = 1, \ldots, m$, the first d_h vectors in (7) are rationally independent.

The first part of the algorithm is described by recursion on $h \in \{1, \ldots, m\}$. For $h = 1$, simply put $c_j^1 = c_j^{\iota_1}$, $j = 1, \ldots, n$. For $h > 1$, let

$$\begin{pmatrix} c_1^1 & \ldots & c_n^1 \\ \cdot & \ldots & \cdot \\ c_1^{i_{h-1}} & \ldots & c_n^{i_{h-1}} \end{pmatrix} \tag{8}$$

be the rows of C already determined. At this stage we have: (a) $i_{h-1} = d_{h-2} + 1$ (here we are conventionally assuming $d_0 := 0$); (b) the columns in (8) whose indices are greater than d_{h-1} rationally depend on the first d_{h-1} columns (which are rationally independent). We add to the matrix (8) the $d_{h-1} - d_{h-2}$ new rows $(c_j^{i_{h-1}+1}), \ldots, (c_j^{i_h})$ chosen as follows. The first $k := d_{h-1} - d_{h-2} - 1$ of these rows form the lexicographic matrix Γ for which: (a) the entries of the first $d_{h-2} + 1$ columns of Γ are zero; (b) the subsequent $k = d_{h-1} - d_{h-2} - 1$ columns form the $k \times k$ matrix $(a_s^r := \delta_{k-s+1}^r)$ (δ_t^r Kronecker symbol); (c) the columns whose indices are greater than d_{h-1} must satisfy the same rational relations which hold for the columns of (8). Finally, we put $c_j^{i_h} := c_j^{\iota_h}$ $\quad (j = 1, \ldots, n;\ i_h = d_{h-1} + 1)$.

References

[1] B. Peterson, E.J. Taft, *The Hopf algebra of linearly recursive sequences*, Aeq. Math. 20 (1980), 1-17

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

[3] L. Cerlienco, M. Mureddu, *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. 139 (1995) (also in the "Actes du 4^e Colloque *Séries formelles et combinatoire algébrique*, Montréal, 1992)

[4] L. Cerlienco, M. Mureddu, *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* ≥ 2, Publ. I.R.M.A. Strasbourg, 1993, 461/S-24 Actes 24^e Séminaire Lotharingien, p.39-76

[5] F. Piras, *Some remarks on Macaulay's inverse systems*, Abstracts of the Talks of the "3rd International Symposium on effective methods in algebraic geometry", Santander (Spain), April 5–9,1994

[6] F. Piras, *Duals of polynomial modules and derivations in the formal power series algebras*, Rapporto interno n. 13, Dipartimento di Matematica, Cagliari (1994)

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

[8] H. M. Möller, F. Mora. *New Constructive Methods in Classical Ideal Theory*, J. of Alg. **100** (1986), 138-178.

[9] J. Erdős, *On the structure of ordered real vector spaces*, Publ. Math. Debrecen, 4 (1956), 334-343

[10] L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon Press, 1994

[11] L. Cerlienco, M. Mureddu, *Rappresentazione matriciale degli ordini l.c. su* $\mathbb{R}^n$ *e su* $\mathbb{N}^n$, Rapporto interno n. 16, Dipartimento di Matematica, Cagliari (1994)

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

[13] M.Stillman, M.Stillman, D.Bayer *Macaulay User Manual*, 1994

[14] L.Robbiano, *Term Orderings on the Polynomial Ring*, Proceedings of EUROCAL 85. Springer Lec. Notes Comp. Sci. 204, 513–517

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