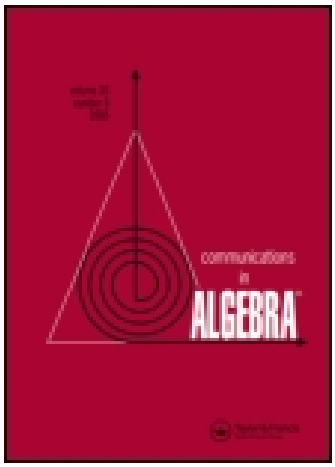

Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/lagb20

The Big Mother of all Dualities: Möller Algorithm

Maria Emilia Alonso [a d], Maria Grazia Marinari [b] & Teo Mora [b c]

[a] Departamento Algebra, Fac.CC. Matemáticas, Universidad Complutense de Madrid, Madrid, Spain

[b] DIMA, Università di Genova, Genova, Italy

[c] DISI, Università di Genova, Genova, Italy

[d] Departamento Algebra, Fac.CC. Matemáticas, Universidad Complutense de Madrid, Madrid, 28040, Spain

Published online: 31 Aug 2006.

To cite this article: Maria Emilia Alonso, Maria Grazia Marinari & Teo Mora (2003) The Big Mother of all Dualities: Möller Algorithm, Communications in Algebra, 31:2, 783-818, DOI: 10.1081/AGB-120017343

To link to this article: http://dx.doi.org/10.1081/AGB-120017343

COMMUNICATIONS IN ALGEBRA®
Vol. 31, No. 2, pp. 783–818, 2003

The Big Mother of all Dualities: Möller Algorithm

Maria Emilia Alonso,[1,*] Maria Grazia Marinari,[2] and Teo Mora[2,3]

[1]Departamento Algebra, Fac.CC. Matemáticas, Universidad Complutense de Madrid, Madrid, Spain
[2]DIMA and [3]DISI, Università di Genova, Genova, Italy

ABSTRACT

Duality was introduced in Computer Algebra in 1982 by Möller and since that has been widely used. We give a survey of Möller algorithm and its applications, presenting a new one to the computation of canonical modules. "Its dual application" allow us to give answer to a question posed to us by Stetter.

Key Words: Groebner bases; Polynomial systems; Artinian rings.

AMS Classificaton: (Primary) 13P10; 13E10; 13M10.

*Correspondence: Maria Emilia Alonso, Departamento Algebra, Fac.CC. Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, Spain; E-mail: m_alonso@mat.ucm.es.

DOI: 10.1081/AGB-120017343 0092-7872 (Print); 1532-4125 (Online)

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

INTRODUCTION

Duality was introduced in Computer Algebra in 1982 by the seminal paper (Buchberger and Möller, 1982) but the relevance of this result became clear after

- The same duality exposed in Buchberger and Möller (1982) was indipendently applied in Auzinger, Stetter (1988) to produce an algorithm for solving any squarefree 0-dimensional ideal $\mathfrak{I} \subset K[X_1, \ldots, X_n]$ and
- The algorithm developed in Buchberger and Möller (1982) was applied in Faugère et al. (1993) in order to solve the FGLM-problem.
- The ideas of Buchberger and Möller (1982), and Faugère et al. (1993) were merged in Marinari (1993) (see also Lakshmann, 1991) proposing an algorithm which produces the Gröbner basis of an (affine/projective) ideal $\mathfrak{I} = \bigcap_{i=1}^{r} \mathfrak{q}_i \subset K[X_1, \ldots, X_n]$, where each $\mathfrak{q}_i$ is a primary ideal at an algebraic point, equivalently given by its inverse system, or Gröbner basis, or even any basis (see Marinari, 1996).

Already in an informal talk at MEGA-92 (Traverso, 1992) it was proposed to use the structure of a 0-dimensional ideal $\mathfrak{I} \subset K[X_1, \ldots, X_n]$, which is produced by Möller Algorithm, in order to reduce its algebraic operations to linear algebra operations; this led to the notion of *Gröbner representation* which we weak here to the one of *relaxed Gröbner representation* (Sec. 4.4).

A preliminary draft of this survey – which included also the computation of the canonical module of a 0-dimensional ideal (Sec. 5.4) – was already presented in a Tutorial Lecture in ISSAC'96 (Mora, 1996).

When we found out that

- The non-commutative generalization of Möller Algorithm allowed an elementary interpretation of Todd-Coxeter Algorithm (Reinhert, 1998);
- Möller Algorithm produced a very efficient proof of a structure theorem of 0-dimensional ideals in 2 variables merging the theorems by Lazard (1985) and Cerlienco–Mureddu (1990) (cf. Mora, 1999);
- Our application of Möller Algorithm to the computation of the canonical modules Alonso et al. (2000) can be directly applied *mutatis mutandis* in order to solve a problem posed to us by H. Stetter (Sec. 6.2),

we were strongly convinced that Möller Algorithm is indeed a crucial tool within Computer Algebra and we thought worthwhile to polish our old notes in order to provide a survey of the Algorithm and its applications, in the most general setting which seemed significant to us (left-modules of non-commutative polynomial rings).

1. THE STAGE

Let K be an effective field and let V be a K-vector space; if $dim_K(V) < \aleph_0$ and $V^{\#} := \mathrm{Hom}_K(V, K)$, one has $dim_K(V) = dim_K(V^{\#})$ and there are bases $\{v_1, \ldots, v_r\}$, $\{\ell_1, \ldots, \ell_r\}$ resp. of V and $V^{\#}$ so that $\ell_i(v_j) = \delta_{ij}$. To mimic this situation in the infinite dimensional case, we fix any basis $\{v_i : i \in I\}$ of V and we consider the non degenerate symmetric bilinear form

$$\nabla : V \times V \mapsto K : \nabla(v_i, v_j) := \delta_{ij}, \forall i, j \in I.$$

Moreover, $\forall \ell \in V$, we let $\lambda_\ell : V \mapsto K$ denote the functional defined by

$$\lambda_\ell(v) := \nabla(\ell, v).$$

We then set

$$V^* := \{\lambda_\ell : \ell \in V\} \subset V^{\#}.$$

Through the paper $\mathscr{P} := K\langle X_1, \ldots, X_n\rangle$ is the non-commutative ring of polynomials and the commutative cases will be explicitly pointed out.

Moreover, $\mathbb{T} := \langle X_1, \ldots, X_n\rangle$ is the multiplicative semigroup of *words* over the symbols $\{X_1, \ldots, X_n\}$, which can be thought as natural K-basis of $\mathscr{P}$.

Remark 1.1. Each K-linear functional $\mathscr{P}^{\#} \ni \ell : \mathscr{P} \to K$ is characterized by its values on any basis B of $\mathscr{P}$; in fact, each $f \in \mathscr{P}$ can be uniquely expressed as $f = \sum_{\beta \in \mathbf{B}} c(f, \beta)\beta$, with $c(f, \beta) \in K$, and, by K-linearity, we have

$$\ell(f) = \sum_{\beta \in \mathbf{B}} c(f, \beta)\ell(\beta). \qquad \square$$

Remark 1.2. Using as basis of $\mathscr{P}$ the canonical basis $\mathbb{T}$ each $\ell \in \mathscr{P}^{\#}$ can be encoded by means of a series

$$\sum_{t \in \mathbb{T}} \ell(t)t \in K\langle\langle X_1, \ldots, X_n\rangle\rangle$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

in such a way that to each series $\sum_{t\in\mathbb{T}}\gamma(t)t\in K\langle\langle X_1,\ldots,X_n\rangle\rangle$ is associated the K-linear functional $\ell\in\mathscr{P}^{\#}$ defined by

$$\ell(f):=\sum_{t\in\mathbb{T}}c(f,t)\gamma(t),\quad \forall f\in\mathscr{P},\ f=\sum_{t\in\mathbb{T}}c(f,t)t.$$

Clearly functionals in $\mathscr{P}^*$ are exactly those which are actually encoded by polynomials. □

Remark 1.3. $\mathscr{P}^{\#}$ (resp. $\mathscr{P}^*$) has a natural structure of left-$\mathscr{P}$-module, which is obtained defining, for each $\ell\in\mathscr{P}^{\#}$ and $f\in\mathscr{P}$, $(\ell\cdot f)\in\mathscr{P}^{\#}$ as

$$(\ell\cdot f)(g):=\ell(fg),\quad \forall g\in\mathscr{P}.$$ □

Remark 1.4. The following are equivalent:

1. There exist n linear operators $\mathfrak{X}_1,\ldots,\mathfrak{X}_n\in\mathrm{Hom}_K(V,V)$.
2. V is a left $\mathscr{P}$-module.
3. V^* is a right $\mathscr{P}$-module.

The relation is the obvious one: denoting

$$X_iv:=\mathfrak{X}_i(v)\in V,\quad \forall v\in V,$$

and

$$wX_i:=w\circ\mathfrak{X}_i\in V^*,\quad \forall w\in V^*,$$

we have

$$(wX_i)(v)=w(X_iv),\quad \forall v\in V,\ w\in V^*.$$

Of course, also the following are equivalent:

- $\mathfrak{X}_i(\mathfrak{X}_j(v))=\mathfrak{X}_j(\mathfrak{X}_i(v))$, $\forall v\in V$, $\forall i,j$.
- V is a $K[X_1,\ldots,X_n]$-module.
- V^* is a $K[X_1,\ldots,X_n]$-module. □

From now on we will always assume that V is given as a finite left $\mathscr{P}$-module (so that V^* is finite too), by assigning linear operators $\mathfrak{X}_i\in\mathrm{Hom}_K(V,V)$ and a finite set $\mathbf{1}:=\{e_1,\ldots,e_\nu\}\subset V$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

This induces the canonical $\mathscr{P}$-homomorphism

$$\Phi : \mathscr{P}^\nu \mapsto V, \quad \Phi(f_1, \ldots, f_\nu) = \sum_i f_i e_i$$

(and, by abuse of notation, we will also denote by **1** the basis of $\mathscr{P}^\nu$ over $\mathscr{P}$) which allows to apply the Gröbner technology to V.

Let us set $\mathbb{T}^\nu := \{\tau e_i : \tau \in \mathbb{T}, e_i \in \mathbf{1}\}$, which is a K-basis of $\mathscr{P}^\nu$, and let us impose on it a well-ordering $<$ s.t.

$$\forall \tau_1,\ \tau_2 \in \mathbb{T}^\nu,\ \forall i,\ 1 \le i \le n,\ \tau_1 < \tau_2 \Longrightarrow X_i\tau_1 < X_i\tau_2;$$

then each element $f \in \mathscr{P}^\nu$ can be uniquely expressed as

$$f = \sum c_i\tau_i, c_i \in K\backslash\{0\}, \tau_i \in \mathbb{T}^\nu, \tau_1 > \tau_2 > \cdots$$

and we can define its {*maximal term*$T(f) := \tau_1$; in the same way for each set $F \subseteq \mathscr{P}^\nu$, we will denote $T(F) := \{\tau T(f) : \tau \in \mathbb{T}, f \in F, f \neq 0\}$.

Setting $\mathscr{U} := \ker(\Phi)$ and $N(\mathscr{U}) := \mathbb{T}^\nu \backslash T(\mathscr{U})$ we have

$$\mathscr{P}^\nu \cong \mathscr{U} \oplus V, V \cong \mathscr{P}^\nu/\mathscr{U} \cong \mathrm{Span}_K(N(\mathscr{U})).$$

Thanks to these isomorphisms, we can consider $\mathscr{T} := N(\mathscr{U})$ as a K-basis of V so that the (linear algebra) Gröbner technology discussed in Marinari (1993) and Mora (1994) can be projected from $\mathscr{P}^\nu$ to V.

In particular, $\mathscr{T}$ can be ordered (only as a set!) by $<$ and each element $f \in V$ can be uniquely expressed as

$$f = \sum c_i\tau_i, \quad c_i \in K\backslash\{0\}, \tau_i \in \mathscr{T}, \tau_1 > \tau_2 > \cdots$$

and we can denote $T(f) := \tau_1$ its maximal term.

Lemma 1.5. $\forall f \in V,\ \forall j,\ X_jT(f) \in \mathscr{T} \Longrightarrow T(\mathfrak{X}_j(f)) = X_jT(f)$.

Proof. Let $f := \sum_{i=1}^r c_i\tau_i, c_i \in K\backslash\{0\}, \tau_i \in \mathscr{T}$ with $T(f) = \tau_1$. Let us partition $\{1, \ldots, r\} = I_N \sqcup I_T$ where

$$I_N := \{i : X_j\tau_i \in N(\mathscr{U})\} \quad \text{and} \quad I_T := \{i : X_j\tau_i \in T(\mathscr{U})\}.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Then

$$\mathfrak{X}_j(f) = \sum_{i=1}^{r} c_i \mathfrak{X}_j(\tau_i) = \sum_{i\in I_N} c_i \mathfrak{X}_j(\tau_i) + \sum_{i\in I_T} c_i \mathfrak{X}_j(\tau_i)$$
$$= \sum_{i\in I_N} c_i X_j\tau_i + \sum_{i\in I_T} c_i \Phi(X_j\tau_i) = \sum_{i\in I_N} c_i X_j\tau_i + \sum_{i\in I_T}\sum_{\tau\in N(\mathscr{U})} c_i c_{i\tau}\tau,$$

where $\Phi(X_j\tau_i) = \sum_{\tau\in N(\mathscr{U})} c_{i\tau}\tau$ and $X_j\tau - \sum_{\tau\in N(\mathscr{U})} c_{i\tau}\tau \in \mathscr{U}$; the result holds since

- $X_j\tau_1 = X_j T(f) \in N(\mathscr{U})$ by assumption.
- $X_j\tau_1 > X_j\tau_i$, $\forall i \in I_N$.
- $X_j\tau_1 > X_j\tau_i > \tau$, $\forall i \in I_T$, $\forall \tau : c_{i\tau} \neq 0$. □

For each K-vector subspace $W \subset V$, let us denote:

- $\mathbf{T}(W) := \{T(f) : f \in W\}$.
- $\mathbf{N}(W) := \mathscr{T} \setminus \mathbf{T}(W)$.
- $\mathbf{B}(W) := \mathbf{T}(W) \cap (\mathbf{1} \cup \{X_j\tau : 1 \leq j \leq n,\ \tau \in \mathbf{N}(W)\})$.

Lemma 1.6. *For each K-vector subspace $W \subset V$, it holds:*

1. $V = W \oplus \mathrm{Span}_K(\boldsymbol{N}(W))$.
2. *There is a K-vector space isomorphism between V/W and* $\mathrm{Span}_K(\boldsymbol{N}(W))$.
3. *For each $f \in V$ there is a unique $g := Can(f, W) \in \mathrm{Span}_K(\boldsymbol{N}(W))$ s.t. $f - g \in W$.* □

Definition 1.7. *If $W \subset V$ is a K-vector subspace, the* border-basis (*shortly: the* B-basis) *of W w.r.t. $<$, is the subset*

$$\mathscr{B}(W) := \{\tau - Can(\tau, W) : \tau \in \mathbf{B}(W)\}.$$ □

Lemma 1.8. *Let $W \subset V$ be a left $\mathscr{P}$-submodule. For each $\tau \in \mathscr{T}$ it holds*

$$\tau \in \mathbf{T}(W) \Longleftrightarrow \exists \tau_l \in \mathbb{T}, \quad \tau_r \in \mathbf{B}(W) : \tau = \tau_l\tau_r.$$

Proof. Let $\tau := Y_m Y_{m-1} \cdots Y_1 e_j$, with $Y_i \in \{X_1, \ldots, X_n\}$, $e_j \in \mathbf{1}$, and let us denote $\tau_0 := e_j, \tau_i := Y_i\tau_{i-1}$, $\forall i > 0$. Either $\tau \in \mathbf{N}(W)$ or there is a least i s.t. $\tau_i \in \mathbf{T}(W)$. If $i = 0$ the result holds with

$$\tau_l := Y_m Y_{m-1} \cdots Y_1, \quad \tau_r := \tau_0 \in \mathbf{T}(W) \cap \mathbf{1} \subset \mathbf{B}(W).$$

Otherwise $\tau_{i-1} \in \mathbf{N}(W)$ and the result holds with

$$\tau_l := Y_m \cdots Y_{i+1}, \quad \tau_r := \tau_i = Y_i \tau_{i-1} \in \mathbf{B}(W).$$

Conversely, if $\tau = \tau_l \tau_r$ with $\tau_l \in \mathbb{T}, \tau_r \in \mathbf{B}(W)$, let $f := \tau_l(\tau_r - Can(\tau_r, W)) \in W$. Then $\tau_l \tau_r = T(f) \in \mathbf{T}(W)$. □

2. THE MOTHER OF DUALITY

For each K-vector subspace $W \subset V$, let

$$\mathfrak{L}(W) := \{\ell \in V^* : \ell(g) = 0, \forall g \in W\};$$

for each K-vector subspace $M \subset V^*$, let

$$\mathfrak{Q}(M) := \{g \in V : \ell(g) = 0, \forall \ell \in M\}.$$

Lemma 2.1 (Marinari et al., 1993)**.** *Let $W \subset V$ be a K-vector subspace and $g \in V$; then*

$$\ell(g) = 0, \forall \ell \in \mathfrak{L}(W) \Longrightarrow g \in W.$$

Let $M \subset V^*$ be a K-vector subspace and $\ell \in V^*$; then

$$\ell(g) = 0, \forall g \in \mathfrak{Q}(M) \Longrightarrow \ell \in M.$$

Proof. Let B be a K-basis of W; assume $g \notin W$ and complete $B \cup \{g\}$ to a K-basis B' of V. Clearly, any $\ell \in V^*$ is uniquely characterized by giving $\ell(f)$, $\forall f \in B'$.

So let ℓ be s.t. $\ell(g) \neq 0$, $\ell(f) = 0$, $\forall f \in B' - \{g\}$. Then $\ell \in \mathfrak{L}(W)$ and $\ell(g) \neq 0$.

The second statement comes by dualizing the proof of the first statement: we consider a K-basis B of M and an element $\ell \notin M$ and we complete $B \cup \{\ell\}$ to a K-basis B' of V^*. Clearly, any $f \in V$ is uniquely characterized by giving $\ell(f)$, $\forall \ell \in B'$.

So let g be s.t. $\ell(g) \neq 0$, $\lambda(g) = 0$, $\forall \lambda \in B' - \{\ell\}$. Then $g \in \mathfrak{Q}(M)$ and $\ell(g) \neq 0$. □

Remark 2.2. The result of Lemma 2.1 does not hold if we consider the whole $V^{\#}$ (instead of restricting ourselves to V^*), as the following example shows. □

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Example 2.3. In general, for a K-vector subspace $L \subset \mathscr{P}^{\#}$ it doesn't necessarily hold $L = \mathfrak{L}\mathfrak{Q}(L)$.

Let us set in the commutative case $\mathscr{P} = K[X]$ and let us denote, $\forall i \in \mathbb{N}$, $\lambda_i \in \mathscr{P}^{\#}$ the linear functional s.t.

$$\lambda_i(X^j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Then for $L := \{\lambda_i, i \in \mathbb{N}\} \subset \mathscr{P}^{\#}$, we have

$$\mathfrak{Q}(L) = \{0\} \quad \text{and} \quad \mathfrak{L}\mathfrak{Q}(L) \cong \mathscr{P}^{\#} \neq L \cong \mathscr{P}^{*}$$

since L consists only of the functionals encoded by polynomials in $K[[X]] \simeq \mathscr{P}^{\#}$ while functionals encoded as series, like the linear functional λ defined as $\lambda(X^j) := 1$, $\forall j \in \mathbb{N}$, do not belong to L. □

Definition 2.4. *Let* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$ *and* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$.
$\mathbb{L}$ *and* $\mathbf{q}$ *are said to be*

- Triangular *if* $\ell_i(q_j) = 0$ *if* $i < j$.
- Biorthogonal *if* $\ell_i(q_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$ □

Lemma 2.5 (Marinari et al., 1993)**.**

1. *Given* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$, *the following are equivalent:*
   (a) *There exists* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$ *biorthogonal to* $\mathbb{L}$.
   (b) *There exists* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$ *triangular to* $\mathbb{L}$.
   (c) $\mathbb{L}$ *is linearly independent.*
2. *Given* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$, *the following are equivalent:*
   (a) *There exists* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$ *biorthogonal to* $\mathbf{q}$.
   (b) *There exists* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$ *triangular to* $\mathbf{q}$.
   (c) $\mathbf{q}$ *is linearly independent.*

Proof. Assume $\mathbb{L}$ is not linearly independent, so that there are $c_1, \ldots, c_s \in K$ not all zero, say $c_s \neq 0$, s.t. $\sum c_i \ell_i = 0$ and assume that $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$ is biorthogonal to $\mathbb{L}$. Then $0 = \sum c_i \ell_i(q_s) = c_s \ell_s(q_s) = c_s \neq 0$, gives a contradiction.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Assume now $\mathbb{L}$ linearly independent, and let us prove the existence of $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$ biorthogonal to $\mathbb{L}$, arguing by induction on s.

If $s = 1$, the linear independence of $\{\ell_1\}$ means $\ell_1 \neq 0$ and so the existence of $g \in V$ s.t. $\ell_1(g) \neq 0$.

So let us assume the existence of $\{q_1, \ldots, q_{s-1}\} \subset V$ which is biorthogonal to $\{\ell_1, \ldots, \ell_{s-1}\}$. Since $\ell_s \notin \mathrm{Span}_K(\{\ell_1, \ldots, \ell_{s-1}\})$ then

$$\ell := \ell_s - \ell_s(q_1)\ell_1 - \cdots - \ell_s(q_{s-1})\ell_{s-1} \neq 0$$

and there is $g \in V : \ell(g) \neq 0$. Setting

$$g' := g - \ell_1(g)q_1 - \cdots - \ell_{s-1}(g)q_{s-1}$$

it holds

$$\ell_s(g') = \ell_s(g) - \ell_1(g)\ell_s(q_1) - \cdots - \ell_{s-1}(g)\ell_s(q_{s-1}) = \ell(g) \neq 0,$$

while for $i < s$

$$\begin{aligned}\ell_i(g') &= \ell_i(g) - \ell_1(g)\ell_i(q_1) - \cdots - \ell_{s-1}(g)\ell_i(q_{s-1}) \\ &= \ell_i(g) - \ell_i(g)\ell_i(q_i) = 0,\end{aligned}$$

so that $\mathbf{q} := \{q_1, \ldots, q_{s-1}, g'\} \subset V$ is triangular to $\mathbb{L}$.

From it we obtain a biorthogonal set

$$\mathbf{q}' := \{q'_1, \ldots, q'_s\} \subset V$$

setting

$$\begin{aligned}q'_s &:= \ell_s(g')^{-1}g' \qquad \text{and} \\ q'_j &:= q_j - \ell_s(q_j)\ell_s(g')^{-1}g' \quad \forall j < s.\end{aligned}$$

This ends the proof since for $n = 1$ the statement is obvious.

The second statement is proved dually. □

Let $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$ and $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$, we denote

$$L := \mathrm{Span}_K(\mathbf{L}), \quad Q := \mathrm{Span}_K(\mathbf{q}).$$

Lemma 2.6. *If* $\mathbb{L}$ *and* $\mathbf{q}$ *are biorthogonal, then:*

1. $V \cong Q \oplus \mathfrak{Q}(L)$, $V/\mathfrak{Q}(L) \cong Q$.
2. $V^* \cong L \oplus \mathfrak{L}(Q)$, $V/\mathfrak{L}(Q) \cong L$.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Proof. Let $q \in V$ and let $q^{(1)} := \sum_i \ell_i(q) q_i$, $q^{(2)} := q - q^{(1)}$ so that $q^{(1)} \in Q$, $\ell_j(q^{(2)}) = 0 \, \forall j$, $q^{(2)} \in \mathfrak{Q}(L)$ and $V = Q \oplus \mathfrak{Q}(L)$.

If $q \in Q \cap \mathfrak{Q}(L)$ then $q \in Q \Longrightarrow q = \sum_i c_i q_i$ and

$$q \in \mathfrak{Q}(L) \Longrightarrow \forall j, c_j = \sum_i c_i \ell_j(q_i) = \ell_j(q) = 0$$

so that $Q \cap \mathfrak{Q}(L) = \{0\}$. □

Theorem 2.7 (Lagrange Interpolation Formula)**.** *Keeping the above notation, let* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathscr{P}^*$ *be a linearly indipendent set, let* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset \mathscr{P}$ *be biorthogonal to* $\mathbb{L}$.

Then, for each $(c_1, \ldots, c_s) \in K^s$ *and each* $g \in \mathscr{P}$ *it holds*

$$\ell_j(g) = c_j, \forall j \Longleftrightarrow \exists h \in \mathfrak{Q}(L) : g = h + \sum_i c_i q_i.$$

Proof. For $g = h + \sum_i c_i q_i$, $h \in \mathfrak{Q}(L)$, we have

$$\ell_j(g) = \ell_j(h) + \sum_j c_i \ell_j(q_i) = c_j, \quad \forall j.$$

If $\ell_j(g) = c_j$, $\forall j$, then for $h := g - \sum_i c_i q_i$ we have

$$\ell_j(h) = \ell_j(g) - \sum_j c_i \ell_j(q_i) = c_j - c_j = 0, \quad \forall j,$$

so that $h \in \mathfrak{Q}(L)$. □

Remark 2.8. Keeping the above notation and assumptions, and $\forall f \in V$ denoting

- $\rho(f, \mathbf{q}) := (c_1, \ldots, c_s) : f = \sum_i c_i q_i \, mod \, \mathfrak{Q}(L)$.
- $v(f, \mathbb{L}) := (\ell_1(f), \ldots, \ell_s(f))$.

it holds:

$$\forall f \in Q, \, \rho(f, \mathbf{q}) = v(f, \mathbf{L}).$$ □

Theorem 2.9. *$\mathfrak{L}$ and $\mathfrak{Q}$ define a duality between the K-vector subspaces of V and those of V^*. Under this duality, to a vector subspace $M \subset V^*$,*

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

with $dim_K(M) < \aleph_0$*, corresponds a vector subspace* $W \subset V$*, with* $dim_K(V/W) < \aleph_0$.

Proof. Let $W \subset V$ and let $M = \mathfrak{L}(W) \subset V^*$; the equalities $\mathfrak{Q}(\mathfrak{L}(W)) = W$ and $\mathfrak{L}(\mathfrak{Q}(M)) = M$ follow by Lemma 2.1 and the dimensionality statement arises from 2.6. □

Remark 2.10. Let Q, $W \subset V$ be s.t. $V = Q \oplus W$. For each $\ell \in V^*$ let $\bar{\ell}$ denote its restriction to W. Then $W^* = \{\bar{\ell} : \ell \in \mathfrak{L}(Q)\}$. In fact, each $L \in W^*$ can be extended to a linear functional $\ell \in V^*$ s.t. $L = \bar{\ell}$ by simply defining $\ell(q + w) = L(w)$, $\forall q \in Q$, $\forall w \in W$. □

Lemma 2.11.

1. *$W \subset V$ is a left $\mathscr{P}$-submodule if and only if $\mathfrak{L}(W)$ is a right $\mathscr{P}$-submodule.*
2. *$M \subset V^*$ is a right $\mathscr{P}$-submodule if and only if $\mathfrak{Q}(M)$ is a left $\mathscr{P}$-submodule.*

Proof.

$$\begin{aligned} W \text{ is a left } \mathscr{P}\text{-submodule} &\iff \forall g \in W, \forall j, X_j g \in W \\ &\iff \forall g \in W, \forall j, \forall \ell \in \mathfrak{L}(W), \\ &\qquad (\ell X_j)(g) = \ell(X_j g) = 0 \\ &\iff \forall \ell \in \mathfrak{L}(W), \forall j, \ell X_j \in \mathfrak{L}(W) \\ &\iff \mathfrak{L}(W) \text{ is a right } \mathscr{P}\text{-submodule.} \end{aligned}$$ □

Corollary 2.12. *$\mathfrak{L}$ and $\mathfrak{Q}$ define a duality between left $\mathscr{P}$-submodules of V and right $\mathscr{P}$-submodules of V^*.* □

3. THE SIRE OF ALGORITHMS

Möller Algorithm, that we are presenting now, solves the following

Problem 3.1. Given a finite sequence $\mathbb{L} = \{\ell_1, \ldots, \ell_r\} \subset V^*$ generating (as a K-vector space) a right $\mathscr{P}$-submodule $L \subset V^*$, compute:

- An integer s.
- An order set $\mathbf{N} := \{t_1, \ldots, t_s\}\mathbb{T}$ (i.e., such that $t | t_i$ for some i, implies $t \in N$).
- $\forall \tau \in \mathbf{1} \cup \{X_k t_i,\ 1 \le k \le n,\ 1 \le i \le s\}$, an element $g_\tau \in V$.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

- $\forall k,\ 1 \le k \le n$, an s-square matrix $M(k) := (a_{ij}^k)$.
- An ordered set $\mathbb{L}' := \{\ell'_1, \ldots, \ell'_s\} \subset \mathbb{L}$.

which, denoting

- $W \subset V$ the $\mathscr{P}$-submodule $W := \mathfrak{Q}(L)$.
- $\forall i,\ 1 \le i \le s,\ q_i := g_{t_i}$.
- $\mathbf{q} := \{q_1, \ldots, q_s\}$.
- $\mathbf{B} := (\mathbf{1} \cup \{X_k t_i,\ 1 \le k \le n,\ 1 \le i \le s\}) \setminus \mathbf{N}$.

satisfy the following properties:

- $\dim_K(W) = s \le r$.
- $\mathbf{N} = \mathbf{N}(W)$.
- $e_1 = t_1 < t_2 < \cdots < t_i < \cdots < t_s$.
- $\mathbf{B} = \mathbf{B}(W)$.
- $\mathscr{B}(W) = \{g_\tau : \tau \in \mathbf{B}\}$.
- $\mathrm{Span}_K(\mathbf{q}) = \mathrm{Span}_K(\mathbf{N}) \cong V/W$.
- $\forall k,\ 1 \le k \le n,\ \forall i,\ 1 \le i \le s,\ \mathrm{Can}(X_k q_i,\ W) = \sum_j a_{ij}^k q_j$.
- $\mathrm{Span}_K(\mathbb{L}') = \mathrm{Span}_K(\mathbb{L})$.
- $\forall i,\ T(q_i) = t_i$.
- $\forall i \le j,\ \ell'_i(q_j) = \delta_{ij}$.

We point out here that (after Faugére et al., 1993) the set of matrices $M(k) := (a_{ij}^k) \in M_s(K),\ \forall k,\ 1 \le k \le n$, is called the *set of the Matphi matrices of W*

Möller Algorithm was originally introduced in 1982 in Buchberger and Möller (1982) for the (commutative) case $V = \mathscr{P}$, the linear functionals being point evaluations.

It was reproposed in Faugére et al. (1993) (cf. also Gianni and Mora, 1989), with important improvements and a complexity analysis, as a tool to solve the FGLM-problem: here again $V = \mathscr{P}$ (commutative) and functionals were the coefficients in a canonical form of a polynomial by a Gröbner basis; Marinari et al. (1993) presents the complete theory for $\mathscr{P}$ in the commutative case, efficiently implemented in Abbott et al. (2000) and exploited in Cioffi (1999).

Somehow different representations and algorithms are discussed in Mourrain (1997, 1999) (based on Faugére's methods (Faugére, 1999) and in Cioffi and Orecchia (2001) (all in the commutative case).

Möller Algorithm has been recently generalized in the non-commutative polynomial ring setting (Reinhert et al., 1998) as a tool to interpret Todd-Coxeter Algorithm via Gröbner technology, and to the

two-sided ideal case (Borges-Trenard et al., 2000). However, hints to Möller Algorithm in non-commutative polynomial rings are already present in Labonté (1999) which is even older than Gianni and Mora (1989).

Möller Algorithm can be informally described as follows: three lists N, H and $List$ are considered. The first one contains terms in $\mathbf{N}(W)$, the second one contains elements in the border basis of W with respect to $<$. The third one is an auxiliary tool. Every step treats the minimal term $t := T(f) \in \mathscr{T}$ which is neither in N nor in $T(H)$. The three lists are updated until $List = \emptyset$, which implies that every term in $\mathscr{T}$ is either in N or in $T(H)$.

Algorithm 3.2 (Möller)**.**

$N := \emptyset$; $H := \emptyset$; $s := 0$;

$List := \{(1, e_i) : e_i \in \mathbf{1}\}$;

$\mathbb{L}' := \emptyset$; $\mathbf{B} := \emptyset$; $\mathbf{q} := \emptyset$;

While $List \neq \emptyset$ **do**

Choose $(X, q) \in List \mid T(Xq) = min_{<}\{T(Yp) : (Y, p) \in List\}$

$f := Xq$

$List := List \backslash \{(X, q)\}$

$t := T(f)$

$(p, (c_1, \ldots, c_s), v(p, \mathbb{L})) :=$ **Gauss-reduce**$(f; q_1, \ldots, q_s)$

%% $\ell'_i(p) = 0$, $\forall i \leq s$

If $t \notin N \cup T(H)$ **then**

If $v(p, \mathbb{L}) = 0$ **then**

$H := H \cup \{p\}$

$\mathbf{B} := \mathbf{B} \cup \{t\}$, $g_t := p$

else

$s := s + 1$

$\pi(s) := min\{i : \ell_i(p) \neq 0\}$

$\ell'_s := \ell_{\pi(s)}$

$\mathbb{L}' := \mathbb{L}' \cup \{\ell'_s\}$

$q_s := \ell'_s(p)^{-1} \cdot p$

$c_s := c_s + \ell'_s(p)e_s$

$t_s := t$

$N := N \cup \{t_s\}$

$List := List \cup \{(X_j, q_s) : j = 1..n\}$

If $(X, q) = (X_k, q_i)$ **then**

For $j = 1..s$ **do** $a_{ij}^k := c_j$

Where,

$(p,(c_1, \ldots, c_s), v(p, \mathbb{L})) :=$ **Gauss-reduce**$(f;q_1, \ldots, q_s)$

$p := f,\ c_i := 0,\ v := v(f, \mathbb{L})$

For $i = 1..s$ **do**

$p := p - \ell'_i(p)q_i$

$c_i := c_i - \ell'_i(p)$

$v := v - \ell'_i(p)v(q_i, \mathbb{L})$

$v(p, \mathbb{L}) := v$ □

In other words, $(p, (c_1, \ldots, c_s), v(p, \mathbb{L})) :=$ **Gauss-reduce**$(f; q_1, \ldots, q_s)$ performs Gaussian reduction on $v(f, \mathbb{L})$ with respect to the linearly independent set $\{v(q_i, \mathbb{L}), i = 1 \ \ldots \ s\}$ and performs the same linear operation on f using $q_1, \ldots, q_s$.

In order to prove the correctness of the algorithm, we need just to remark that the terms $T(Xq)$ corresponding to the pairs (X, q) which are inserted in *List* are exactly the terms in the set

$$\mathbf{1} \cup \{X_j t \mid t \in \mathbf{N}(W), j \in \{1, \ldots, n\}\} = \mathbf{N}(W) \sqcup \mathbf{B}(W).$$

Each term t is inserted in

- $T(H) \subseteq \mathbf{B}(W)$, if it is linearly dependent modulo W with the elements of N.
- N, otherwise (so that constantly $N \subseteq \mathbf{N}(W)$).

Therefore

$$\mathbf{N}(W) \sqcup \mathbf{B}(W) = N \sqcup T(H), N \subseteq \mathbf{N}(W), T(H) \subseteq \mathbf{B}(W),$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

which implies $N = \mathbf{N}(W)$, $T(H) = \mathbf{B}(W)$ and the correctness of the algorithm.

Example 3.3. Along all this note we will present the following elementary example:

$V := K[X, Y]$, $\mathbb{L} = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5\}$ where $\forall f \in V$,

$$\ell_1(f) = f(0,0), \quad \ell_2(f) = f(1,0), \quad \ell_3(f) = f(0,1),$$
$$\ell_4(f) = f(1,-1), \quad \ell_5(f) = f(0,-1).$$

Denoting f_i the polynomial treated in the ith **While**-loop, $\rho_i := \rho(f_i, \mathbf{q})$, $v_i := v(f_i, \mathbb{L})$, $V_i := v(q_i, \mathbb{L})$, and using the deg-lex ordering

$$1 < X < Y < X^2 < XY < Y^2 < X^3 < \cdots$$

the computation is:

	$H = \emptyset$
$N = \emptyset$	$List = \{1\}$
	$i = 1$
$f_1 = 1$	$= 1$
$v_1 = (1,1,1,1,1)$	$V_1 = (1,1,1,1,1)$
$\rho_1 = (1,0,0,0,0)$	$q_1 = 1$
$N = \{1\}$	$List = \{X_{q_1}, Y_{q_1}\}$
	$i = 2$
$f_2 = X_{q_1}$	$= X$
$v_2 = (0,1,0,1,0)$	$V_2 = (0,1,0,1,0)$
$\rho_2 = (0,1,0,0,0)$	$q_2 = X$
$N = \{1, X\}$	$List = \{Y_{q_1}, X_{q_2}, Y_{q_2}\}$
	$i = 3$
$f_3 = Y_{q_1}$	$= Y$
$v_3 = (0,0,1,-1,-1)$	$V_3 = (0,0,1,-1,-1)$
$\rho_3 = (0,0,1,0,0)$	$q_3 = Y$
$N = \{1, X, Y\}$	$List = \{X_{q_2}, Y_{q_2}, X_{q_3}, Y_{q_3}\}$
	$i = 4$
$f_4 = X_{q_2}$	$= X^2$
$v_4 = (0,1,0,1,0)$	
$\rho_4 = (0,1,0,0,0)$	$H = H \cup \{X^2 - X\}$
	$i = 5$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$f_5 = Y_{q_2}$ $= XY$
$v_5 = (0,0,0,-1,0)$ $V_4 = (0,0,0,1,0)$
$\rho_5 = (0,0,0,-1,0)$ $q_4 = -XY$
$N = \{1, X, Y, XY\}$ $List = \{X_{q_3}, Y_{q_3}, X_{q_4}, Y_{q_4}\}$
$i = 6$
$f_6 = X_{q_3}$ $= XY$
$v_6 = (0,0,0,-1,0)$
$\rho_6 = (0,0,0,-1,0)$
$i = 7$
$f_7 = Y_{q_3}$ $= Y^2$
$v_7 = (0,0,1,1,1)$ $V_5 = (0,0,0,0,1)$
$\rho_7 = (0,0,1,2,2)$ $q_5 = \frac{1}{2}Y^2 + XY + \frac{1}{2}Y$
$N = \{1, X, Y, XY, Y^2\}$ $List = \{X_{q_4}, Y_{q_4}, X_{q_5}, Y_{q_5}\}$
$i = 8$
$f_8 = X_{q_4}$ $= -X^2Y$
$v_8 = (0,0,0,1,0)$
$\rho_8 = (0,0,0,1,0)$ $H = H \cup \{-X^2Y + XY\}$
$i = 9$
$f_9 = Y_{q_4}$ $= -XY^2$
$v_9 = (0,0,0,-1,0)$
$\rho_9 = (0,0,0,-1,0)$ $H = H \cup \{-XY^2 - XY\}$
$i = 10$
$f_{10} = X_{q_5}$ $= \frac{1}{2}XY^2 + X^2Y - \frac{1}{2}XY$
$v_{10} = (0,0,0,0,0)$
$\rho_{10} = (0,0,0,0,0)$
$i = 11$
$f_{11} = Y_{q_5}$ $= \frac{1}{2}Y^3 + XY^2 - \frac{1}{2}Y^2$
$v_{11} = (0,0,0,0,-1)$
$\rho_{11} = (0,0,0,0,-1)$ $H = H \cup \{\frac{1}{2}Y^3 - \frac{1}{2}Y\}$ □

4. THE SCION OF THE ALGORITHMS

4.1. Left Multiplication by X_i

Deducing from the computations done by Möller Algorithm the "*Matphi*" matrices $\mathrm{M}(k) := (a_{ij}^k)_{ij}$ s.t. $\forall i,\ 1 \le i \le s,\ \mathfrak{X}_k(q_i) = \sum_j a_{ij}^k q_j$, it is just a question of bookkeeping.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Example 4.1. Continuing the computation started in Example 3.3, we easily get:

$$\mathrm{M}(1) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \mathrm{M}(2) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \qquad \square$$

4.2. Border Basis

Obviously, knowing the matrices M(k) allows us to apply Möller Algorithm to the finite sequence $\{\gamma_1, \ldots, \gamma_s\}$ of functionals defined by $Can(f, W) = \sum_{j=1}^{s} \gamma_i(f) q_i$, in order to solve the FGLM-problem (as it was originally proposed in Faugére et al. (1993)):

Problem 4.2 (Faugére et al., 1993)**.** Given a Gröbner basis of W w.r.t. a term-ordering $<_1$, compute its Gröbner basis w.r.t. another term-ordering $<_2$. $\square$

4.3. The Structure of *Matphi*

Keeping the notation of *Problem* 3.1., we state the following

Lemma 4.3. *$\forall k, 1 \le k \le n$, $\forall j, \mu$ such that $1 \le \mu < j \le s$, if $t_j = X_k t_\mu$ then*

1. $a_{ij}^k = 0$, $\forall i < \mu$.
2. $a_{\mu j}^k \neq 0$.
3. $a_{\mu l}^k = 0$, $\forall l > j$.

Proof. For each i, since $g := \mathrm{Can}(X_k q_i, W) = \sum_{l=1}^{s} a_{il}^k q_l$, if $a_{ij}^k \neq 0$, then

$$X_k t_i \ge t_j = X_k t_\mu,$$

i.e. $i \ge \mu$.

Moreover, in the representation

$$g := \mathrm{Can}(X_k q_\mu, W) = \sum_{l=1}^{s} a_{\mu l}^k q_l,$$

it holds $T(g) = X_k t_\mu = t_j < t_l$, $\forall l > j$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Therefore $a^k_{\mu l} = 0, \forall l > j$; if $a^k_{\mu j} = 0$ too, then $g = \sum_{l=1}^{j-1} a^k_{\mu l} q_l$, giving the contradiction $X_k t_\mu = T(g) < t_j = X_k t_\mu$. □

We point out that the converse of the Lemma does not hold. Namely, conditions i), ii) and iii) for k, j, μ with $\mu < j$ do not imply $X_k t_\mu = t_j$. In order to estimate the "lack of reciprocity" of the Lemma we introduce the following definitions. These definitions will be given in a general setting, since later in the paper we will deal with the problem of realizing a set of commuting matrices as *Matphi* matrices in an Artinian $\mathscr{P}$-module.

Definition 4.4. *Let $\mathfrak{M} := \{N(k) : 1 \le k \le n\}$ be a set of s-square matrices, $N(k) := (a^k_{ij})$. Define, $\forall k$, $j : 1 \le k \le n$, $1 \le j \le s$*

$$\mathsf{c}(k,j) := \begin{cases} \min\{i : i < j, a^k_{ij} \neq 0\} & \text{if } \exists i < j : a^k_{ij} \neq 0 \\ 0 & \text{if } \forall i < j : a^k_{ij} = 0 \end{cases}.$$ □

Definition 4.5. *Let $\mathfrak{M} := \{N(k) : 1 \le k \le n\}$ be a set of s-square matrices, $N(k) := (a^k_{ij})$. Define, $\forall k$, $\mu : 1 \le k \le n$, $1 \le \mu \le s$*

$$\mathsf{r}(k,\mu) := \begin{cases} \max\{i : i > \mu, a^k_{\mu i} \neq 0\} & \text{if } \exists i > \mu : a^k_{\mu i} \neq 0 \\ 0 & \text{if } \forall i > \mu : a^k_{\mu i} = 0 \end{cases}.$$ □

Remark 4.6. From the definitions it is straightforward that, for all $1 \le k \le n$, $1 \le \mu < j \le s$, if $\mathsf{c}(k, j) = \mu$, then $\mathsf{r}(k, \mu) \ge j$. Also $\mathsf{r}(k, \mu) = j$ implies $\mathsf{c}(k, j) \le \mu$.

In the case of *Matphi* matrices, we have the following properties:

- For every $j > 1$ there exist k, μ, $t_j = X_k t_\mu$, so that $\mathsf{r}(k, \mu) = j$.
- From the μth row of $M(k)$, setting $j := \mathsf{r}(k, \mu)$ we read

$$(a^k_{\mu j})^{-1} X_k q_\mu = q_j + \sum_{l<j} (a^k_{\mu j})^{-1} a^k_{\mu l} q_l.$$

- In the same way, from the jth column of M(k), setting $\mu := \mathsf{c}(k, j)$ we read

$$(a^k_{\mu j})^{-1} \lambda_j X_k = \lambda_\mu + \sum_{i>\mu} (a^k_{\mu j})^{-1} a^k_{ij} \lambda_i.$$

- If $\mathsf{r}(k, \mu) = j$ (resp. $\mathsf{c}(k, j) = \mu$) then, $X_k t_\mu \ge t_j$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

In fact $\mathrm{Can}(X_k q_\mu, W) = a^k_{\mu j} + \sum_{l<j}^{s} a^k_{\mu l} q_l$. Since $a^k_{\mu j} \neq 0$, it must be $X_k t_\mu \geq t_j$. On the other hand $\mathsf{c}(k, j) = \mu$ implies $j' := \mathsf{r}(k, \mu) \geq j$, and so $X_k t_\mu \geq t_{j'} \geq t_j$.

Example 4.7. Let W be $K[X, Y]/\mathsf{I}$, where $\mathsf{I} := (Y^3 - X^3 - X^2 Y, XY^2, X^3 Y, X^4) \subset K[X, Y]$. Then, the given generators of I are a G-basis with respect to the deglex term ordering with $X < Y$; so that $\mathscr{P}/\mathsf{I}$ can be represented by $\mathbf{N} := \{1, X, Y, X^2, XY, Y^2, X^3, X^2 Y\}$. The multiplication matrix by Y in $\mathscr{P}/\mathsf{I}$ is $M(2) = (a_{ij})$, where $a_{13} = a_{25} = a_{36} = a_{48} = a_{67} = a_{68} = 1$, and $a_{ij} = 0$ otherwise. This example shows that $\mathsf{c}(k, j) = \mu$ does not imply $\mathsf{r}(k, \mu) = j$ and viceversa. In fact, $\mathsf{r}(2, 6) = 8$ and $\mathsf{c}(2, 8) = 4$. Also $\mathsf{c}(2, 7) = 6$ but $\mathsf{r}(2, 6) = 8$.

An slight modification of this example shows that $\mathsf{c}(k, j) = \mu$ and $\mathsf{r}(k, \mu) = j$, do not imply $X_k t_\mu = t_j$. Namely, let $\mathsf{I} := (Y^3 - X^3, XY^2, X^3 Y, X^4)$. Then, again the given generators are a G-basis with respect to the deglex term ordering, so that $\mathscr{P}/\mathsf{I}$ can be represented by the same $\mathbf{N}$. The new multiplication by Y matrix is $M(2) = (b_{ij})$. Where $b_{ij} = a_{ij}$ for all $(i, j) \neq (6, 8)$, and $b_{68} = 0$. Hence $\mathsf{c}(2, 7) = 6$ and $\mathsf{r}(2, 6) = 7$, but $Y.Y^2 \neq X^3$.

4.4. Gröbner Representation

In an informal talk at MEGA-92 (Traverso, 1992) (a preliminary discussion is in Alonso et al., 1992, Marinari et al., 1996) it was proposed to use the data produced by Möller Algorithm – in particular, $\mathbf{q}$, $\mathscr{B}$ and $M(k)$ – as an arithmetical tool for 0-dimensional ideals $I \subset \mathscr{P}$ (commutative), reducing "advanced" arithmetical operations like Duval division to elementary linear algebra; in particular it was explicitly suggested to reduce Gröbner basis computation of an ideal $J \supset I$ to elementary linear algebra.

This led to the following

Definition 4.8. *Let $W \subset \mathscr{P}^\nu$ be a left $\mathscr{P}$-module such that $s := \dim_K(\mathscr{P}^\nu / W)$ is finite.*

We call a Gröbner representation *of W the datum $(\mathbf{q}, \mathfrak{M})$ consisting of*

- $\mathbf{q} = \{q_1, \ldots, q_s\} \subset \mathscr{P}^\nu$ *s.t.* $\mathscr{P}^\nu / W = \mathrm{Span}_K(\mathbf{q})$, *and*
- $\mathfrak{M} := \{M(k) : 1 \leq k \leq n\}$, *where $M(k)$ are the matrices $M(k) := (a^k_{ij})_{ij}$ s.t.* $\forall i, 1 \leq i \leq r$, $\mathfrak{X}_k(q_i) = \sum_j a^k_{ij} q_j$. □

In this setting we let $\mathscr{B}(W) := \{X_i q_j - \mathrm{Can}(X_i q_j, W)\} \setminus 0$ and call it *relaxed border basis of W*. From now on, whenever we will speak of

border basis of a given submodule $W \subset \mathscr{P}^\nu$ we will have in mind this generalized meaning.

A stimulating question posed to us by Stetter, allowed us to find out that all one needs (cf. Sec. 6) is just the *Matphi* matrices. For this we introduce

Definition 4.9. *Let $W \subset \mathscr{P}^\nu$ be a left $\mathscr{P}$-module such that $s := \dim_K(\mathscr{P}^\nu / W)$ is finite.*

We call a relaxed Gröbner representation of W the assignment of the set $\mathfrak{M} := \{M(k) : 1 \le k \le n\}$, where $M(k)$ represents the effect of $\mathfrak{X}_k$ w.r.t. a (non necessarily known) K-basis $\mathbf{q} = \{q_1, \ldots, q_s\}$ of $\mathscr{P}^\nu / W$. □

In the setting of Gröbner representation, Traverso proposed to use linear algebra in order to solve the following

Problem 4.10. Given

- A zero-dimensional ideal $\mathsf{I} \subset \mathscr{P}$ (commutative case) by means of a Gröbner representation

$$\mathbf{q} = \{1 = q_1, \ldots, q_s\}, \quad \mathbf{M} = \left(a_{ij}^{(k)}\right),$$

- Any finite set of elements $F := \{g_1, \ldots, g_h\} \in \mathscr{P}$, via their *Gröbner descriptions,* i.e.,

$$\mathbf{c}^j := (c_1^j, \ldots, c_s^j) := \rho(g_j, \mathbf{q})$$

so that

$$Can(g_j, \mathsf{I}) = \sum_i c_i^j q_i \quad \text{and} \quad g_j - \sum_i c_i^j q_i \in \mathsf{I}.$$ □

The algorithm proposed by Traverso allows us to compute with good complexity the Gröbner representation of the ideal $\mathsf{J} := \mathsf{I} + (F)$. □

Actually Traverso proposed an algorithm solving the problem with good complexity.

The basic idea is the following: if we consider an element $g \in F$, having Gröbner description $g - \sum_{i=1}^{l} c_i q_i \in \mathsf{I}$, $c_l \neq 0$, and we enlarge I by

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

adding g to it, then we obtain the relation $q_l \cong -\sum_{i=1}^{l-1} c_l^{-1} c_i q_i \bmod(\mathsf{I}+(g))$; from the K-vector space decomposition

$$\mathscr{P} = \mathsf{I} \oplus \mathrm{Span}_K(\mathbf{q})$$

we therefore obtain

$$\mathscr{P} = (\mathsf{I}+(g)) \oplus \mathrm{Span}_K(\mathbf{q} \setminus \{q_l\});$$

we must here keep track of relation, by substituting, in each Gröbner description $\sum_i d_i q_i$ of the poynomials g_j and $X_k q_i$ (respectively encoded in the vectors $\mathbf{c}^j$ and in the rows of the matrices of M) the instances of q_l with $-\sum_{i=1}^{l-1} c_l^{-1} c_i q_i$, thus getting $\sum_i (d_i - c_l^{-1} c_i d_l) q_i$.

Since J is an ideal, $g \in \mathsf{J} \Longrightarrow X_h g \in \mathsf{J}$ (each $X_h g$ must be inserted in the list F in order to be treated in the same way).

At termination, if $I \subset \{1, \ldots, n\}$ denotes the set of indices of the elements q_i which have not been removed from $\mathbf{q}$ in this procedure, then J is decribed by the Gröbner representation

$$\mathbf{q}' = \{q_i, i \in I\}, M' = \left(a_{ij}^{(k)}\right)_{i,j \in I}.$$

The above situation has the obvious generalization: □

Problem 4.11. Given

- A submodule $W \subset V$ by means of a relaxed Gröbner representation.
- A finite set $\{g_1, \ldots, g_h\} \subset V$ which generates a module W' such that $W \subset W' \subset V$, each g_i being given via a *Gröbner description*

  $$\mathbf{c}^j := (c_1^j, \ldots, c_s^j)$$

  so that $Can(g_j, W) = \sum_i c_i^j q_i$,

compute the relaxed Gröbner representation of W'. □

Definition 4.12. *Let $\mathfrak{M} := \{N(k) : 1 \le k \le n\}$ be a set of s-square matrices, $N(k) := (a_{ij}^k)$.*

1. *For each pair A, B of s-square matrices, we will denote*

   $$A\mathfrak{M}B := \{A\mathcal{N}(k)B : 1 \le k \le n\};$$

   $A\mathfrak{M}$, $\mathfrak{M}B$ will have similar meaning.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

2. *For each* $j, l: 1 \le j < l \le n$ *and* $c \in K$, $c \neq 0$ *let* $E(j, l; c) := (\epsilon_{\alpha,\beta})_{\alpha,\beta}$ *be the* s*-square matrix defined by*

$$\epsilon_{\alpha,\beta} := \begin{cases} -c & \text{if } \alpha = l, \beta = j \\ \delta_{ij} & \textit{otherwise} \end{cases}.$$

□

Remark 4.13. Let $\mathfrak{M} := \{\mathrm{N}(k) : 1 \le k \le n\}$ be a set of s-square matrices, $\mathrm{N}(k) := (a_{ij}^k)$.

$E(j, l; c)\cdot\mathrm{N}(k)$ is the matrix $(b_{ih}^k)_{ih}$ whose elements are

$$b_{ih} := \begin{cases} a_{ij}^k - c a_{il}^k & \text{if } h = j \\ a_{ih}^k & \text{if } h \neq j \end{cases}$$

□

Algorithm 4.14 (Traverso)**.**

$List := \{\mathsf{c}^1, \ldots, \mathsf{c}^h\}$, $I := \{1, \ldots, s\}$

While $List \neq \emptyset$ **do**

Choose $(c_1, \ldots, c_s) \in List$

$List := List \setminus \{(c_1, \ldots, c_s)\}$

$List := List \cup \{(c_1, \ldots, c_s)\mathrm{M} : \mathrm{M} \in \mathfrak{M}\}$

Let $l := \max\{i \in I : c_i \neq 0\}$

$I := I \setminus \{l\}$

For all $j \in I$, $k = 1..n$ **do**

$\mathfrak{M} := E(j, l; c_l^{-1} c_j)\mathfrak{M}$

$\Lambda\iota\sigma\tau := List$, $List := \emptyset$

For all $(d_1, \ldots, d_s) \in \Lambda\iota\sigma\tau$ **do**

For $j := 1..s$ **let** $e_j := d_j - d_l c_l^{-1} c_j$

If $(e_1, \ldots, e_s) \neq (0, \ldots, 0)$ **do** $List := List \cup \{(e_1, \ldots, e_s)\}$

$\mathfrak{M} :=$ **Extract**$(\mathfrak{M}, I)$

where **Extract**$(\mathfrak{M}, I)$ substitutes each matrix $M \in \mathfrak{M}$ with its minor containing the rows and columns indexed by I. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

5. HIS SIBLINGS

5.1. Duality (1)

Our presentation of Möller Algorithm produces a sequence $\mathbf{q}$ which is *triangular* to $\mathbb{L}'$. In order to get $\mathbf{q}' = \{q'_1, \ldots, q'_s\}$ *biorthogonal* to $\mathbb{L}'$, apply the usual Gram-Schmidt procedure to $\mathbf{q}'$ amounts here to Gauss-reduce by row the matrix $(\ell'_i(q_j))_{ij}$, performing the same operations on the q_i's.

Of course, in order to preserve the multiplication structure, the matrices $M(k)$ must be updated accordingly.

Example 5.1. Continuing the computation of Example 3.3 we have

$$\left(\ell'_i(q_j)\right)_{ij} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and it is therefore sufficient to define

$$\begin{aligned} q'_1 &:= q_1 - q_2 - q_3 - q_4 - 2q_5 = 1 - X - XY - Y^2, \\ q'_2 &:= q_2 - q_4 = X + XY, \\ q'_3 &:= q_3 + q_4 + q_5 = \tfrac{1}{2}Y + \tfrac{1}{2}Y^2, \\ q'_4 &:= q_4 = -XY, \\ q'_5 &:= q_5 = -\tfrac{1}{2}Y + XY + \tfrac{1}{2}Y^2, \end{aligned}$$

in order to obtain $\ell'_i(q'_j) = \delta_{ij}$, $\forall i, j$. □

This dualization has interesting applications to the case in which the linear functionals ℓ_i are point evaluations, i.e., when points $P_i = (x_{1i}, \ldots, x_{ni}) \in K^n$ are given s.t. $\ell_i(f) = f(x_{1i}, \ldots, x_{ni})$.

In this case, in fact, it holds

$$q'_i(P_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

and $\mathbf{q}'$ is naturally related with Lagrange interpolation (see Theorem 2.7). In this case the polynomials q'_i, which are easy to compute, are called *separators*. A set of points $\{P_j : 1 \le j \le s\}$ are said to be *in Cayley-Bacharach*

position when the separators have the same degree $deg(q_i') = \max(deg(t) : t \in N(W))$, which can be easily tested as it was firstly remarked in Marinari et al. (1993).

5.2. Duality (2)

Above we diagonalized the matrix $(\ell_i'(q_j))_{ij}$ by operating on rows; of course we could have done it on columns, performing the same operations on the set $\mathbb{L}'$; thus we would have obtained a set $\mathbf{\Lambda} := \{\lambda_1, \ldots, \lambda_s\}$ biorthogonal to $\mathbf{q}$. We will see below that also this approach through columns has interesting applications (see next Lemma 5.3, see also Sec. 5.4).

Example 5.2. In our example, performing column Gaussian reduction on

$$\left(\ell_i'(q_j)\right)_{ij} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

we obtain

$$\begin{aligned} \lambda_1 &:= \ell_1, \\ \lambda_2 &:= \ell_2 - \ell_1, \\ \lambda_3 &:= \ell_3 - \ell_1, \\ \lambda_4 &:= \ell_4 + \ell_3 - \ell_2 - \ell_1, \\ \lambda_5 &:= \ell_5 + \ell_3 - 2\ell_1. \end{aligned}$$

□

5.3. Right Multiplication by X_i

Recalling that the matrices $M(k) := (a_{ij}^k)_{ij}$ produced by Möller Algorithm satisfy $\forall i,\ 1 \le i \le s$, $\mathfrak{X}_k(q_i) = \sum_j a_{ij}^k q_j$, we see now that the multiplicative structure of the $\mathscr{P}$-module L is described via $\mathbf{\Lambda}$ in a somehow optimal way, as shown by:

Lemma 5.3. *Let* $\mathbf{\Lambda} = \{\lambda_1, \ldots, \lambda_s\} \subset V^*$ *and* $\mathbf{q} = \{q_1, \ldots, q_s\} \subset V$ *be biorthogonal. Then,* $\forall k = 1..n$, $\forall j = 1..s$, $\forall i = 1..s$, *it holds*

$$\lambda_j \circ \mathfrak{X}_k(q_i) = (\lambda_j X_k)(q_i) = \lambda_j(X_k q_i) = \lambda_j(\mathfrak{X}_k(q_i)) = a_{ij}^k.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Proof. $\lambda_j(\mathfrak{X}_k(q_i)) = \lambda_j(\sum_{l=1}^{s} a_{il}^k q_l) = \sum_{l=1}^{s} a_{il}^k \lambda_j(q_l) = a_{ij}^k$. □

Corollary 5.4. *Under the same assumptions: Then:*

- $\forall k = 1..n,\ \forall j = 1..s,\ \lambda_j \circ \mathfrak{X}_k = \sum_j a_{ij}^k \lambda_i$.
- $v(X_k q_i) := (a_{i1}^k, \ldots, a_{is}^k)$.

Example 5.5. In our example, by the previous computation reading the rows of $\mathfrak{M}(k)$ gives directly $w_i := v(f_i, \mathbf{\Lambda})$:

$$
\begin{aligned}
w_1 &= (1,0,0,0,0), \\
w_2 &= (0,1,0,0,0), \qquad w_3 = (0,0,1,0,0), \\
w_4 &= (0,1,0,0,0), \qquad w_5 = (0,0,0,-1,0), \\
w_6 &= (0,0,0,-1,0), \qquad w_7 = (0,0,1,2,2), \\
w_8 &= (0,0,0,1,0), \qquad w_9 = (0,0,0,-1,0), \\
w_{10} &= (0,0,0,0,0), \qquad w_{11} = (0,0,0,0,-1).
\end{aligned}
$$

□

5.4. The Canonical Module

In Alonso (2000) we have expanded a footnote of Gröbner (1967–1968) in which Gröbner (following in this Macaulay (1913)) outlined an algorithm to decompose a $(X_1, \ldots, X_n)$-primary ideal $\mathsf{I} \subset \mathscr{P}$ (commutative) into minimal components, proposing to apply Möller algorithm in order to obtain the $\mathscr{P}-$module structure of $Hom_K(\mathscr{P}/\mathsf{I}, K)$ with $\mathsf{I} \subset \mathscr{P}$ a 0-dimensional ideal (for a similar algorithm in the case in which I is a homogeneous ideal defined by simple points, cf. Beck Kreuzer, 1996).

The same idea allows to explicitly describe the right $\mathscr{P}$-module structure of $Hom_K(W, K)$ for a left $\mathscr{P}$-module W, $L := \mathrm{Span}_K \mathbb{L} = \mathrm{Span}_K \mathbf{\Lambda}$ by giving

- An integer ν.
- ν functionals $\lambda_{j_i} \in \mathbf{\Lambda}$, $1 \le i \le \nu$.
- A well-ordering $<_\nu$ on $\mathbb{T}^\nu$ compatible with $<$.
- A module $\mathscr{U} \subset \mathscr{P}^\nu$, by producing $\mathbf{N}(\mathscr{U})$ and its border basis $\mathscr{B}(\mathscr{U})$.
- An explicit vector space isomorphism

$$\sigma : \mathrm{Span}_K(\mathbf{\Lambda}) \mapsto \mathrm{Span}_K(\mathbf{N}(\mathscr{U})) \subset \mathscr{P}^\nu,$$

s.t., denoting

$$\Sigma : \mathscr{P}^{\nu} \mapsto \mathrm{Span}_K(\mathbf{\Lambda})$$

the projection $\mathbf{\Sigma}(\sum_{i=1}^{\nu} f_i e_i) = \sum_{i=1}^{\nu} \lambda_j f_i$, it holds

- $\mathscr{U} := \ker(\mathbf{\Sigma})$, and
- σ is a splitting homomorphism for $\mathbf{\Sigma}$.

Once the linear algebra structure of $\mathfrak{Q}(L)$ is known, in order to deduce the one of L it is only needed to use the obvious duality $(V^*)^* = V$ and to dualize Möller algorithm: the original algorithm deduces the structure of $\mathfrak{Q}(L)$ as a submodule of $\mathscr{P}$ performing linear algebra on the vectors of the evaluation of its polynomials at the functionals in $\mathbb{L}$; in the same way, linear algebra on the vectors of the evaluation of the functionals of $\mathrm{Span}_K(\mathbb{L})$ at a linear basis of $\mathfrak{Q}(L)$ provides the module structure and the border basis of $\mathrm{Span}_K(\mathbb{L}) \cong (\mathfrak{Q}(L))^*$.

Recall that if we look to the jth column of $M(k)$ setting $\mu := \mathsf{c}(k, j)$, we get

$$(a^k_{\mu j})^{-1} \lambda_j X_k = \lambda_\mu + \sum_{i>\mu} (a^k_{\mu j})^{-1} a^k_{ij} \lambda_i.$$

Therefore if $\mu < j$, λ_μ can be defined, in terms of λ_i, $i > \mu$, as

$$\lambda_\mu = (a^k_{\mu j})^{-1} \lambda_j X_k - \sum_{i>\mu} (a^k_{\mu j})^{-1} a^k_{ij} \lambda_i.$$

Remark that, setting $I := \{j_1, \ldots, j_\nu\} = \{1, \ldots, s\} \backslash \{\mathsf{c}(k,j), \forall\, k,j\}$ ordered so that $j_1 > j_2 > \cdots > j_\nu$, we can choose the $\nu := \mathrm{Card}(I)$ functionals λ_{j_i}, $1 \le i \le \nu$ as the generators of the module L.

We then impose a well-ordering on $\mathbb{T}^\nu$ and we will choose the easy:

$$\omega_1 e_{i_1} <_\nu \omega_2 e_{i_2} \Longleftrightarrow i_1 < i_2 \quad \text{or} \quad i_1 = i_2 \quad \text{and} \quad \omega_1 < \omega_2.$$

Algorithm 5.6.

$N := \emptyset$; $H := \emptyset$; $\mu := s$; $\nu := 0$;

While $\mu > 0$ **do**

If $\nexists\, k, j : \mathsf{c}(k, j) = \mu$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$\nu := \nu + 1$,

$\sigma(\lambda_\mu) := e_\nu$, $\mathbf{\Sigma}(e_\nu) := \lambda_\mu$,

$T(\lambda_\mu) := e_\nu$, $N := N \cup \{T(\lambda_\mu)\}$,

else

Let k, j be s.t.

- $\mathsf{c}(k, j) = \mu$
- $\mathsf{c}(\kappa, \imath) = \mu \Longrightarrow k \leq \kappa$
- $\mathsf{c}(k, \imath) = \mu \Longrightarrow j > \imath$

$\sigma(\lambda_\mu) := (a^k_{\mu j})^{-1}\sigma(\lambda_j)X_k - \sum_{i=\mu+1}^{s} (a^k_{\mu j})^{-1} a^k_{ij}\sigma(\lambda_i)$,

$T(\lambda_\mu) := T(\lambda_j)X_k$, $N := N \cup \{T(\lambda_\mu)\}$,

$List := List \cup \{(\lambda_\mu, X_k) : 1 \leq k \leq n\}$;

For all κ, $\imath$ s.t. $\mathsf{c}(\kappa, \imath) = \mu$, $k < \kappa$ **or** $k = \kappa$, $j > \imath$ **do**

$p := \sigma(\lambda_\imath)X_\kappa - \sum_i a^\kappa_{i\imath}\sigma(\lambda_i)$;

$p := \mathbf{B} - \mathbf{reduce}(p, H)$

$H := H \cup \{p\}$

$\mu := \mu - 1$;

For all k, j s.t. $\mathsf{c}(k, j) = 0$ **do**

$p := \sigma(\lambda_j)X_k - \sum_i a^k_{ij}\sigma(\lambda_i)$;

$p := \mathbf{B} - \mathbf{reduce}(p, H)$

$H := H \cup \{p\}$

$\mathscr{B}(\mathscr{U}) := H$, $\mathbf{N}(\mathscr{U}) := N = \{T(\lambda_i) : 1 \leq i \leq s\}$. □

Here **B-reduce** is the procedure discussed in Marinari et al. (1993). Each element $f \in H$, when called, satisfies $f - T(f)$ is a linear combination of terms in N and p is such that $p - T(p)$ is a linear combination of terms in $N \cup \mathbf{T}(H)$. $\mathbf{B} - \mathbf{reduce}(p, H)$ substitutes in p each occurrence of a term $T(f) \in \mathbf{T}(H)$ with $f - T(f)$. As a consequence, $f := \mathbf{B} - \mathbf{reduce}(p, H)$ satisfies that $f - T(f)$ is a linear combination of terms in N.

Example 5.7. In our example, where we have $\nu = 2$, $I = \{5, 4\}$ and $T(\cdot)$ is

indicated in **bold**, the computation will give:

$$
\begin{array}{ll}
\mu = 5 & \\
\sigma(\lambda_5) = (\mathbf{1}, 0) & N = \{e_1\} \\
\mu = 4 & \\
\sigma(\lambda_4) = (0, \mathbf{1}) & N = \{e_1, e_2\} \\
\mu = 3 & \lambda_5 Y = 2\lambda_3 - \lambda_5 \\
\sigma(\lambda_3) = (\tfrac{1}{2}\mathbf{Y} + \tfrac{1}{2}, 0) & N = \{e_1, e_2, Ye_1\} \\
\lambda_4 X = -\lambda_3 + \lambda_4 & H = H \cup \{(\tfrac{1}{2} Y + \tfrac{1}{2}, \mathbf{X} - 1)\} \\
\mu = 2 & \lambda_4 Y = -\lambda_2 + 2\lambda_3 - \lambda_4 \\
\sigma(\lambda_2) = (Y + 1, -\mathbf{Y} - 1) & N = \{e_1, e_2, Ye_1, Ye_2\} \\
\mu = 1 & \lambda_3 Y = \lambda_3 + \lambda_1 \\
\sigma(\lambda_1) = (\tfrac{1}{2}\mathbf{Y^2} - \tfrac{1}{2}, 0) & N = \{e_1, e_2, Ye_1, Ye_2, Y^2 e_1\} \\
\lambda_2 X = \lambda_2 + \lambda_1 & H = H \cup \{(\tfrac{1}{2} Y^2 + \tfrac{1}{2} Y, \mathbf{XY} - Y)\} \\
X\sigma(\lambda_5) = (X, 0) & H = H \cup \{(\mathbf{X}, 0)\} \\
X\sigma(\lambda_3) = (\tfrac{1}{2} XY + \tfrac{1}{2} X, 0) & H = H \cup \{(\mathbf{XY}, 0)\} \\
Y\sigma(\lambda_2) = (Y^2 + Y, -Y^2 - Y) & H = H \cup \{(-Y^2 - Y, \mathbf{Y^2} + Y) \\
X\sigma(\lambda_1) = (\tfrac{1}{2} XY^2 - \tfrac{1}{2} X, 0) & H = H \cup \{(\mathbf{XY^2}, 0)\} \\
Y\sigma(\lambda_1) = (\tfrac{1}{2} Y^3 - \tfrac{1}{2} Y, 0) & H = H \cup \{(\mathbf{Y^3} - Y, 0)\}
\end{array}
$$

□

5.5. A Vandermonde Criterium

In our setting it is worthwhile to remark the following result:

Theorem 5.8 (Möller). *Let* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset V^*$ *and* $w = \{w_1, \ldots, w_s\} \subset \mathscr{P}$ *be two linearly independent sets. Denoting*

$$L := \mathrm{Span}_K(\mathbb{L}), \quad W := \mathrm{Span}_K(\mathbf{w}),$$

the following conditions are equivalent:

1. $W = \mathfrak{Q}(L)$.
2. $\det(\ell_i(w_j)) \neq 0$.
3. $L = \mathfrak{L}(W)$.

Proof. $1 \Longrightarrow 2$: Let $\mathbf{q} = \{q_1, \ldots, q_s\}$ be biorthogonal to $\mathbb{L}$. Therefore

$$W = \mathfrak{Q}(L) \Longleftrightarrow \mathrm{Span}_K(\mathbf{w}) = \mathrm{Span}_K(\mathbf{q}).$$

Denoting (c_{ij}) the invertible matrix s.t. $w_j = \sum_i c_{ij} q_i$, we have

$$\ell_i(w_j) = \sum_l c_{lj} \ell_i(q_l) = c_{ij}, \quad \forall i, j$$

and $\det(\ell_i(w_j)) = \det(c_{ij}) \neq 0$.

$2\Rightarrow 1$: Let (a_{jk}) be the inverse of the matrix (c_{ij}), $c_{ij} := \ell_i(w_j)$, so that $\sum_j \ell_i(w_j)a_{jk} = \delta_{ik}$, and let $q_k := \sum_j a_{jk}w_j$, $\forall k$ and $\mathbf{q} := \{q_1, \ldots, q_s\}$; then we have $W = \mathrm{Span}_K(\mathbf{q})$ and $\ell_i(q_k) = \sum_j a_{jk}\ell_i(w_j) = \delta_{ik}$ so that $\mathbf{q}$ is biorthogonal to $\mathbb{L}$ and that $\mathrm{Span}_K(\mathbf{q}) = \mathfrak{Q}(L)$.

$1\Rightarrow 3$: $L = \mathfrak{L}\mathfrak{Q}(L) = \mathfrak{L}(W)$.

$3\Rightarrow 1$: $W = \mathfrak{Q}\mathfrak{L}(P) = \mathfrak{Q}(L)$. □

Remark 5.9. In the "classical" case in which $\mathscr{P} = K[X]$, ℓ_i is evaluation at an α_i algebraic over K, $\ell_i(f) := f(\alpha_i)$ and $\mathbf{p} := \{1, X, X^2, \ldots, X^{s-1}\}$, $(\ell_i(p_j))_{ij}$ is exactly the Vandermonde matrix

$$(\ell_i(p_j))_{ij} = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{s-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{s-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & \alpha_s & \alpha_s^2 & \cdots & \alpha_s^{s-1} \end{vmatrix}$$

□

6. AND HIS GENERATION

6.1. Computing a Gröbner Representation from a Relaxed One

Let $W \subset \mathscr{P}^\nu$ be a left $\mathscr{P}$-module s.t. $\dim_K(\mathscr{P}^\nu/W) := s < \aleph_0$ which is given by a relaxed Gröbner representation, i.e., by the assignment of a set $\mathfrak{M} := \{N(k): 1 \le k \le n\}$, where $N(k)$ represents the effect of $\mathfrak{X}_k$ w.r.t. some unknown K-basis $\mathbf{q} = \{q_1, \ldots, q_s\}$.

Our aim is to show how to explicitly produce such a basis $\mathbf{q} = \{q_1, \ldots, q_s\}$. In order to do that we dualize again the dual of Möller Algorithm; that algorithm worked by reading a K-basis and the border basis of L from the columns of the multiplication matrices, using the fact that $a^k_{ij} = 0$, $\forall i < \mu$. "Vice versa", we read a K-basis and the border basis of W from the rows of the multiplication matrices, using the fact that $a^k_{\mu l} = 0$, $\forall l > j$.

Namely, recall that if we read the μth row of $M(k)$, and we set $j := \mathsf{r}(k, \mu)$ we get

$$(a^k_{\mu j})^{-1} X_k q_\mu = q_j + \sum_{i<j} (a^k_{\mu j})^{-1} a^k_{\mu i} q_i,$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

i.e.,

$$q_j = (a^k_{\mu j})^{-1} X_k q_\mu - \sum_{i<j} (a^k_{\mu j})^{-1} a^k_{\mu i} q_i.$$

Finally when extracting information from the columns, we look for entries $\mathsf{c}(k,j) = \mu$ in decreasing order of μ; contrariwise we look the entries $\mathsf{r}(k,\mu)$ in the rows, in increasing order of j.

Algorithm 6.1.

$H := \emptyset$; $j := 1$; $\nu := 0$;

While $j < s$ **do**

If $\nexists k, \mu$: $\mathsf{r}(k, \mu) = j \neq 0$

$\nu := \nu + 1$,

$q_j := e_\nu$

$T(q_\nu) := e_\nu$, $N := N \cup \{T(q_j)\}$,

else

Let k, μ be s.t.

– $\mathsf{r}(k, \mu) = j$

– $\mathsf{r}(\kappa, \sigma) = j \Longrightarrow k \leq \kappa$

– $\mathsf{r}(k, \sigma) = j \Longrightarrow \mu < \sigma$

$q_j = (a^k_{\mu j})^{-1} X_k q_\mu - \sum_{i<\mu} (a^k_{\mu j})^{-1} a^k_{\mu i} q_i$

$T(q_j) := X_k T(q_\mu)$, $N := N \cup \{T(q_j)\}$,

$j = j + 1$;

For all κ, σ s.t. $\mathsf{r}(\kappa, \sigma) = j$, $k < \kappa$ **or** $k = \kappa$, $\mu < \sigma$ **do**

$p := X_\kappa q_\sigma - \sum_i a^\kappa_{\sigma i} q_i$;

$p := \mathbf{B} - \mathbf{reduce}(p, H)$

$H := H \cup \{p\}$

For all k, μ s.t. $\mathsf{r}(k, \mu) = 0$ **do**

$p := X_k q_\mu - \sum_i a^k_{\mu i} q_i$;

$p := \mathbf{B} - \mathbf{reduce}(p, H)$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$H := H \cup \{p\}$$

$$\mathbf{q} = \{q_1, \ldots, q_s\}$$

$$\mathscr{B}(W) := H,\ \mathbf{N}(W) := N = \{T(q_i)\colon 1 \le i \le s\}. \qquad \square$$

Remark 6.2. It is worthwhile to remark that if we apply the algorithms 5.6 and 6.1, instead of to the module V/W, directly to the module $V/\mathbf{T}(W)$ (thus obtaining the canonical module structure of $\mathfrak{Q}(\mathbf{T}(W))$) computations are essentially the same, except that at each **While**-loop instead of producing p (resp. $\sigma(\lambda_j)$) the algorithm produces $T(p)$ (resp. $T(\lambda_j)$), so that

$$\mathfrak{Q}(\mathbf{T}(W)) = \mathbf{T}(\mathfrak{Q}(W)).$$

This is another, unexpected, instance of the usual general pattern in which Gröbner technology, in order to obtain information on $\mathscr{P}^\nu/\mathscr{U}$, computes the information on $\mathscr{P}^\nu/T(\mathscr{U})$ and "lifts" it from $\mathscr{P}^\nu/T(\mathscr{U})$ to $\mathscr{P}^\nu/\mathscr{U}$. $\square$

6.2. Stetter Problem

The result above was stimulated by a question posed to us by H. Stetter in 1999: whether it was possible to describe the structure of the quotient ring A of $\mathscr{P}$ (commutative) by a 0-dimensional ideal I in case we were given just the matrices representing the multiplication of A w.r.t. an (unknown) K-basis of A.

We have shown a positive answer under the following restrictions:

(A) $q_1 := 1$.
(B) The matrices in $\mathfrak{M}$ commute.
(C) For each $j > 1$, $\exists k, \mu$: $\mathsf{r}(k, \mu) = j$, $\mu < j$.

About condition (**A**), let us start by presenting an

Example 6.3. Let us consider $V := K[X]$, $\mathsf{I} := (X^3 - 1) \subset K[X]$. $K[X]/\mathsf{I}$ can be represented by giving

- $s = 1$.
- $\mathbf{N} := \{1, X, X^2\}$.
- $g_1 := 1$, $g_X := X$, $g_{X^2} := X^2$, $g_{X^3} := X^3 - 1$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

- $M(1) := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
- $\mathbf{q} := \{1, X, X^2\}$.

The point is that $\{M(1)\}$ represents the structure of $K[X]/\mathsf{I}$ over a lot of other bases, e.g. $\{X, X^2, 1\}, \{1+X, X+X^2, 1+X^2\}$ and, in general, $\{p(X), p(X)X, p(X)X^2\} \bmod \mathsf{I}$ for any $p(X)$ s.t. $\gcd(p, X^3-1) = 1$. This restriction must be added, since, for instance, taking $p(X) := 1-X$ we would have $\{p(X), p(X)X, p(X)X^2\} = (1-X, X-X^2, X^2-1) \bmod \mathsf{I}$ which is not a basis of $K[X]/\mathsf{I}$. □

Namely, Möller Algorithm works over $K[X]/\mathsf{I}$ only as a *module* "forgetting" its algebra structure. Condition (A) has the effect to forcing the condition that the module $K[X]/\mathsf{I}$ is in fact a ring:

Lemma 6.4. *Let A be a finite dimensional K-algebra. For each $a \in A$ consider the morphism $\phi_a : A \mapsto A$, $\phi_a(b) = ab$, $\forall b \in A$. Then:*

1. *ϕ_a is a K-module isomorphism iff a is invertible.*
2. *ϕ_a is a ring isomorphism iff $a = 1$.*

Corollary 6.5 (Marinari and Mora, 1999)**.** *Let $\mathscr{P} := K[X_1, \ldots, X_n]$ and let A be a left $\mathscr{P}$-module s.t. $s := \dim_K(\mathsf{A})$ is finite. Let $\mathfrak{M} := \{M(k) : 1 \le k \le n\}$ be a relaxed Gröbner representation of A.*

Then Algorithm 6.1 *computes the unique K-basis $\mathbf{q}$ of A such that $(\mathbf{q}, \mathfrak{M})$ is a Gröbner representation of A satisfying $q_1 = 1$.*

If $\mathbf{p} := \{p_1, \ldots, p_s\}$ is any other K-basis of A such that $(\mathbf{q}, \mathfrak{M})$ is a Gröbner representation of A, then

- *p_1 is invertible.*
- *$p_i = p_1 q_i$ $\forall i$.*

Once we have forced, via condition (A), that the module A is a ring, we must be guaranteed that this ring is actually a commutative one (we notice in fact that the results of Corollary 6.5 hold also in the non-commutative case) and this is obviously equivalent to condition (B) (cf. Moritzugu and Kuriyama, 1999); we remark that Mourrain (1999) proved that (B) is equivalent (when A is commutative) to the assumption that A is given by the relaxed Gröbner representation $\mathfrak{M}$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Now we clarify the meaning of condition (C): the discussion above allow us to assume that there is a basis $\mathbf{q}$ with $q_1 = 1$, under which $\mathfrak{M}$ represents the multiplications of A.

Given $\mathbf{q} := \{1 = q_1, \ldots, q_s\}$, we let

$$t_i := T(q_i),\ \forall i, \quad \mathbf{N} := \{t_1, t_2, \ldots, t_s\}$$

Then, clearly, if it holds

(D) $\mathbf{q} := \{1 = q_1, \ldots, q_s\}$ is such that:

- $\mathrm{Span}_K(\mathbf{q}) = \mathrm{Span}_K(\mathbf{N})$
- $1 = t_1 < t_2 < \cdots < t_s$,
- $\forall \tau_1, \tau_2 \in \mathbf{T},\ \tau_1\tau_2 \in \mathbf{N} \Longrightarrow \tau_1, \tau_2 \in \mathbf{N}$.

$\mathbf{q}$ and $\mathfrak{M}$ would be the result of re-applying Möller Algorithm to compute the border basis (Sec. 4.2) and so it would satisfy Lemma 4.3.

In particular $\forall j > 1,\ \exists k,\ \mu : t_j = X_k t_\mu,\ \mu < j$ and, by Lemma 4.3, $\mathsf{r}(k, \mu) = j$. As a consequence (D) $\Longrightarrow$ (C).

Remark 6.6. As we already remarked in Remark 6.2, Algorithm 5.3 can be directly applied to compute the basis $\mathbf{N}(W)$:

$t_1 = 1$; $j := 2$;

While $j < s$ **do**

Let $i := \min\{\mathsf{r}(j, k) \neq 0\}$, k s.t. $\mathsf{r}(j, k) = i$;

$t_j := X_k t_i$;

$j := j + 1$. □

The question posed to us by Stetter was prompted by the result of Moritzugu and Kuriyama (1999). We recall the Auzinger-Stetter Algorithm

Theorem 6.7 (Auzinger and Stetter, 1988; Möller and Stetter, 1995)**.** *Let* A *be the quotient of the polynomial ring* $\mathscr{P} := K[X_1, \ldots, X_n]$ *by a* 0*-dimensional ideal* I *and let* $\mathbf{q} := \{q_1, \ldots, q_s\}$ *be s.t.* $\mathsf{A} \cong \mathrm{Span}_K(\mathbf{q})$*. For each* $g \in K[X_1, \ldots, X_n]$ *let* $M(g) := (a_{ij})$ *be the matrix s.t.* $gq_i = \sum_j a_{ij} q_j$, $\forall i$.

Assume that $P_1, \ldots, P_s \in K^s$ *are the roots of* I *and that* $g(P_i) \neq g(P_j)$, $\forall i, j$ *then the eigenvalues of* $M(g)$ *are* $g(P_1), \ldots, g(P_s)$ *each having the same multiplicity than the corresponding root.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

If the eigenspace corresponding to $g(P_i)$ has dimension one, then a corresponding eigenvector is $(q_1(P_i), \ldots, q_s(P_i))$. □

In Moritzugu and Kuriyama (1999), under the assumptions of Theorem 6.7 for $g = X_1$, it was proposed an algorithm which computes an invertible matrix S s.t. $S^{-1}\mathfrak{M}S$ consists of upper triangular block diagonal forms, having the same dimension; i.e., representing the primary component p of I corresponding to each of the roots, via the (upper triangular) matrices representing the multiplication of $\mathscr{P}/\mathsf{p}$ w.r.t. an (unknown) K-basis of $\mathscr{P}/\mathsf{p}$.

We remark also that Mourrain (1997, 1999), given a 0-dimensional ideal $\mathsf{I} \subset \mathscr{P}$, provides a Gröbner relaxed representation of $\mathsf{A} = \mathscr{P}/\mathsf{I}$; Algorithm 6.1 then allows to produce a Gröbner representation of A and a Gröbner basis of I within the FGLM complexity.

ACKNOWLEDGMENTS

The first author is partially supported by PB98-0756-C02-01, and the second and third authors are partially supported by GNSGA and MURST.

This paper has been written while the third author was visiting Florida State University, Tallahassee; he wants to thank friends there for the nice hospitality.

The authors thank Prof. Borges-Trenard for his useful comments, Prof. Stetter for the stimulating discussions, Dr. Reinhert for her encouragement, and Prof. Mauceri for an essential suggestion.

REFERENCES

Abbott, J., Bigatti, A., Kreuzer, M., Robbiano, L. (2000). Computing ideals of points. *J. Symb. Comp.* 30:341–356.

Alonso, M. E., Marinari, M. G., Mora, T. (2000). Gröbner-Kreuzer Algorithm, or: how to compute the canonical module of a 0-dimensional ideal. Preprint.

Alonso, M. E., Mora, T., Niesi, G., Raimondo, M. (1992). An Algorithm for computing analytic branches of space curves at singular points. In: Proc. 1992 Int. Workshop on Mathematics Mechanization. Pekin: International Academic Publishers, pp. 135–166.

Auzinger, W., Stetter, H. J. (1988). An elimination algorithm for the computation of all zeros of a system of multivariate polynomial

equations In: *Internationale Schriftenreihe zur Numerischem Mathmatrio 86.* Birkhäuser, pp. 11–30.

Beck, S., Kreuzer, M. (1996). How to compute the canonical module of a set of points. *Algorithms in Algebraic Geometry and its Applications.* Progress in Mathematics 143. Birkhäuser, pp. 51–78.

Borges-Trenard, M. A., Borges-Quintana, M., Mora, T. (2000). Computing Gröbner Bases by FGLM techniques in a noncommutative settings. *J. Symb. Comp.* 30:429–449.

Buchberger, B., Möller, H. M. (1982). The construction of multivariate polynomials with preassigned zeros. EUROCAM'82, LNCS 144, Springer-Verlag, pp. 24–31.

Cerlienco, L., Mureddu, M. (1990). Algoritmi combinatori per l'interpolazione polinomiale in dimensione ≥ 2 In: Actes de la 24^{me} Session du Seminaire Lotharingien de Combinatoire. Univ. de Strasbourg, pp. 39–76.

Cioffi, F. (1999). Minimally generating ideals of fat points in polynomial time using linear algebra. *Ricerche di Matematica XLVII* 1:55–63.

Cioffi, F., Orecchia, F. (2001). Computation of minimal generators of ideals of fat points. In: Proc. ISSAC'01*,* ACM. pp. 72–76.

Faugère, J. C. (1999). A new efficient algorithm for computing Gröbner bases (F4). *J. Pure and Applied Algebra* 139:61–88.

Faugère, J. C., Gianni, P., Lazard, D., Mora, T. (1993). Efficient computation of zero-dimensional Gröbner Bases by change of ordering. *J. Symb. Comp.* 16:329–344.

Gianni, P., Mora, T. (1989). Algebraic solution of systems of polynomial equations using Gröbner Bases In: Proc. AAECC-5, LNCS 356. Springer-Verlag, pp. 247–257.

Gröbner, W. (1967–1968). *Algebraische Geometrie (2 Teil).* Bibliographisches Institut Mannheim.

Labonté, G. (1990). An algorithm for the construction of matrix representations for finite presented non-commutative algebras. *J. Symb. Comp.* 9:27–38.

Lakshmann, Y. (1991). A single exponential bound on the complexity of computing Gröbner Bases of zero dimensional ideals In: Effective Methods in algebraic Geometry: papers of Symp. MEGA-90. Progress in Mathematics 94. Birkhäuser, pp. 227–234.

Lazard, D. (1985). Ideal basis and primary decomposition: Case of two variables. *J. Symb. Comp.* 1:261–270.

Macaulay, F. S. (1913). On the resolution of a given modular system into primary systems including some properties of Hilbert numbers. *Math. Ann.* 74:66–121.

Marinari, M. G., Mora, T. (1999). The linear structure of a primary ring. Preprint.
Marinari, M. G., Möller, H. M., Mora, T. (1993). Gröbner Bases of ideals defined by functionals with an application to ideals of projective points. *AAECC* 4:103–145.
Marinari, M. G., Möller, H. M., Mora, T. (1996). On multiplicities in polynomial system solving. *Trans. AMS* 348:3283–3321.
Möller, H. M., Stetter, H. J. (1995). Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numer. Math.* 70:311–329.
Mora, T. (1994). An introduction to commutative and noncommutative Gröbner Bases. *Th. Comp. Sci.* 134:131–173.
Mora, T. (1996). Solving Polynomial Equation System. *Tutorial of ISSAC'96.* Zurich.
Mora, T. (1999). De Nugis Groebnerialium 4: Around Hartshorne Theorem. Preprint. //ftp.disi.unige.it/persons/MoraF/NG1.ps.gz.
Moritzugu, S., Kuriyama, K. (1999). On multiple zero of systems of algebraic equations. Proc. ISSAC 99, ACM. New York, pp. 23–30.
Mourrain, B. (1997). Isolated points, duality and residues. *J. of Pure and Applied Algebra* 117,118:469–493.
Mourrain, B. (1999). A new criterion for normal forms algorithm. In: AAECC-13, LNCS 1719. Springer-Verlag, pp. 430–443.
Reinhert, B., Madlener, K., Mora, T. (1999). A note on Nielsen reduction and coset enumeration. In: Proc. ISSAC'98, ACM. pp. 171–178.
Traverso, C. (1992). Natural representation of algebraic numbers. *Informal talk at MEGA-92.* Nice.

Received May 12, 2001
Revised April 25, 2002