Journal of Mathematical Sciences: Advances and Applications
Volume 5, Number 2, 2010, Pages 289-306

TESTING FREENESS OVER HERMITE RINGS

VERÓNICA CIFUENTES and OSWALDO LEZAMA

Escuela de Matemáticas y Estadística
UPTC, Tunja
Colombia

Departamento de Matemáticas
Grupo de Álgebra Conmutativa Computacional-SAC[2]
Universidad Nacional de Colombia
Bogotá
Colombia
e-mail: jolezamas@unal.edu.co

Abstract

In this paper, we present some matrix and constructive results that check freeness for a given finitely generated projective S-module M of constant rank, where S is a Hermite commutative ring. In particular, we give a matrix characterization of PF rings (a commutative ring S is PF is every f.g projective S-module is free). In addition, following the ideas in [3], we will exhibit an easy procedure for computing the module $\mathrm{Hom}_S(M, N)$, where S is an arbitrary Noetherian commutative ring with some natural computational conditions.

1. Introduction

It is well known that, if S is a principal ideal domain and M is a finitely generated (f.g) projective S-module, then M is free; the same is true, if S is a local ring. A less trivial situation is when

2010 Mathematics Subject Classification: Primary: 13C10; Secondary: 13B25, 13E15.

Keywords and phrases: free modules, syzygies, Hermite rings, commutative Noetherian rings, constructive algebra.

Received June 15, 2010

$S = K[x_1, \ldots, x_n]$, K is a field, but the famous Quillen-Suslin's theorem shows that any f.g projective module over S is also free (see [20] and [22]). However, if S is a Dedekind domain, then not any f.g projective module over S is free (see [6]). Thus, given a ring S and a concrete f.g projective module M, it is interesting to have a method for checking, if M is free. In this paper, we present some matrix and constructive results that checks freeness for a given finitely generated projective S-module M of constant rank, where S is a Hermite commutative ring (compare with [8], [9], [15] and [19]). A commutative ring S is *Hermite*, if each stably free module over S is free. Some well known examples of Hermite rings are semilocal rings and principal ideal domains; $R[x_1, \ldots, x_n]$ is Hermite, if R a *PID*.

In addition, we will exhibit in the last section a procedure for computing the module $\mathrm{Hom}_S(M, N)$, where S is an SC commutative ring (see the Definition 7) and M, N are f.g modules over S. The Hom modules were computed in [12] for the special case when $S := R[x_1, \ldots, x_n]$, with R is a commutative Noetherian Gröbner soluble ring. Gröbner soluble rings are defined as follows (see [11]); we say that a ring S is *Gröbner soluble* (GS), if:

(i) Given elements $a, a_1, \ldots, a_r \in S$, there exists a procedure to decide, if $a \in < a_1, \ldots, a_r >$ and if it is, to compute $c_1, \ldots, c_r \in S$ such that $a = a_1c_1 + \cdots + a_rc_r$.

(ii) Given $a_1, \ldots, a_r \in S$, there exists a procedure to find a set of generators for the S-module

$$Syz_S[a_1 \ldots a_r] := \{(c_1, \ldots, c_r) \in S^r | a_1c_1 + \cdots + a_rc_r = 0\}.$$

From now on, S represents an arbitrary commutative ring, $S[x_1, \ldots, x_n]$ is the polynomial ring over S in $n \geq 1$ variables; for $s, r \geq 1$, $M_{s\times r}(S)$ is the set of rectangular matrices of size $s \times r$, and $GL_r(S)$ is the general linear group of invertible matrices over S of size $r \times r$. S^s is the free S-module of rank s consisting of columns vectors of size $s \times 1$ with entries in S. If $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_r \in S^s$, then $Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_r) := \{(b_1, \ldots, b_r) \in S^r | b_1\boldsymbol{f}_1 + \cdots + b_r\boldsymbol{f}_r = 0\}$, and for $F \in M_{s\times r}(S)$, $Syz(F)$ is the module of syzygies of the columns of F. For a matrix U, $\langle U \rangle$ represents the module generated by its columns. In general, we will use the habitual notation and terminology of matrix and constructive methods over commutative rings (see, for example, [6], [8], [9], [15]-[17]).

2. Main Result

We recall that a commutative ring S is *Hermite* (H) is every stably free S-module is free. The following theorem and the Corollaries 2 and 5 are the main results of the paper.

Theorem 1. *Let S be a Hermite ring. Then,*

(i) *Let M be a finitely generated projective S-module of constant rank r with presentation* $S^l \xrightarrow{F_1} S^s \xrightarrow{F_0} M \to 0$. *M is free, if and only if there exists a matrix* $U \in GL_s(S)$ *such that*

$$UF_1 = \begin{bmatrix} I_{s-r} & 0 \\ 0 & 0 \end{bmatrix}. \tag{2.1}$$

In such case, a basis of M is given by the last r columns of U^{-1}.

(ii) *Let M be a direct summand of* S^s *and* $F_0 : S^s \to M$ *be the canonical projection on M. M is free with* $rank(M) = r$, *if and only if there exists a matrix* $P \in GL_s(S)$ *such that*

$$PF_0P^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}. \tag{2.2}$$

In such case, a basis of M is given by the last r columns of P^{-1}.

Proof. (i) $\Rightarrow$) Since M is free and has constant rank r, then M has a basis of r elements; moreover, since r coincides with the minimal number of generators of M, then $r \leq s$. Let $G_0 : S^s \to S^r$ be the canonical projection given by $G_0(\boldsymbol{e}_j) = \mathbf{0}$, if $1 \leq j \leq s - r$ and $G_0(\boldsymbol{e}_{s-r+i}) = \boldsymbol{e}_i$, if $1 \leq i \leq r$; note that the matrix of G_0 in the canonical bases is

$$G_0 = [0 \quad I_r].$$

Let $H : M \to S^r$ be an isomorphism, then we have the following diagram with first row exact

$$\begin{tikzcd}
S^l \arrow[r, "F_1"] \arrow[d, "i_{S^l}"'] & S^s \arrow[r, "F_0"] \arrow[d, "U"] & M \arrow[r] \arrow[d, "H"] & 0 \\
S^l \arrow[r, "G_1"] & S^s \arrow[r, "G_0"] & S^r \arrow[r] & 0
\end{tikzcd} \tag{2.3}$$

where U and G_1 are defined as follows: since M is projective, there exists $F_0' : M \to S^s$ such that $F_0 F_0' = i_M$ and $S^s = \ker(F_0) \oplus F_0'(M)$; let $H(\boldsymbol{v}_i) = \boldsymbol{e}_i$, $1 \leq i \leq r$, then $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ is a basis of M. Let $F_0'(\boldsymbol{v}_i) = \boldsymbol{z}_i$, then $\{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r\}$ is a basis of $F_0'(M)$. Note that $\ker(F_0)$ is stably free of constant rank $s - r \leq l$. By the hypothesis, $\ker(F_0)$ has a basis $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{s-r}\}$ of size $s - r$, and then $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{s-r}; \boldsymbol{z}_1, \ldots, \boldsymbol{z}_r\}$ is a basis for S^s. With this, we define U in the following way:

$$U(\boldsymbol{w}_j) = \boldsymbol{e}_j, \text{ for } 1 \leq j \leq s - r,$$

$$U(\boldsymbol{z}_i) = \boldsymbol{e}_{s-r+i}, \text{ for } 1 \leq i \leq r.$$

We observe that U is an isomorphism and moreover, $G_0 U = HF_0$. We define $G_1 = UF_1$, thus the diagram (2.3) is commutative. We will prove that the second row of (2.3) is exact. By the construction, G_0 is surjective; $G_0 UF_1 = HF_0 F_1 = 0$, and then $\mathrm{Im}(UF_1) \subseteq \ker(G_0)$. Moreover, $\ker(G_0) \subseteq \mathrm{Im}(UF_1)$: in fact, let $x \in \ker(G_0)$, so $x = U(z)$ and hence $G_0(U(z)) = 0 = HF_0(z)$, i.e., $F_0(z) = 0$ since H is injective; from this, we get that $z \in \ker(F_0) = \mathrm{Im}(F_1)$, so $z = F_1(w)$ and $x = U(F_1(w))$, i.e., $x \in \mathrm{Im}$

(UF_1). Thus, $\mathrm{Im}(G_1) = \mathrm{Im}(UF_1) = \ker(G_0)$ and hence the second row of (2.3) is exact. Finally, $\ker(G_0) = \langle \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{s-r} \rangle$, and then

$$UF_1 = \begin{bmatrix} I_{s-r} & 0 \\ 0 & 0 \end{bmatrix}.$$

$\Leftarrow$) Now, we assume that there exists a matrix $U \in GL_s(S)$ that satisfies (2.1). As in the previous part, we consider again the canonical projection G_0, so $\ker(G_0) = \mathrm{Im}(UF_1)$; we have the diagram

$$\begin{tikzcd} S^s \arrow[r, "F_0"] \arrow[d, "U"] & M \arrow[r] \arrow[d, "H"] & 0 \\ S^s \arrow[r, "G_0"] & S^r \arrow[r] & 0 \end{tikzcd} \tag{2.4}$$

where H is defined as follows: let $m \in M$, there exists $x \in S^s$ such that $F_0(x) = m$. We define $H(m) := G_0U(x)$; if $x' \in S^s$ is such that $F_0(x') = m$, then $x - x' \in \ker(F_0) = \mathrm{Im}(F_1)$, so $x - x' = F_1(z)$, with $z \in S^l$; from this, we get $U(x - x') = UF_1(z) \in \mathrm{Im}(UF_1) = \ker(G_0)$, so $G_0U(x) = G_0U(x')$, this means that H is well defined. Note that H is an S-homomorphism such that $HF_0 = G_0U$. From this, we get that H is surjective and hence $M \cong S^r \oplus N$, but since M has constant rank r, then $N_P = 0$ for each prime ideal of S, i.e., $N = 0$ and M is free.

Finally, we note that a basis of $F_0'(M) \cong M$ is $\boldsymbol{z}_i = U^{-1}(\boldsymbol{e}_{s-r+i})$, $1 \le i \le r$, i.e., the last r columns of U^{-1}.

(ii) $\Rightarrow$) Let M be free with rank r being a direct summand of S^s, then $r \le s$ and $S^s = M' \oplus M$; we can repeat the reasoning of the first part of (i): let F_0 be the canonical projection on M and $H : M \to S^r$ be an isomorphism, let $\{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r\} \subset M$ such that $H(\boldsymbol{z}_i) = \boldsymbol{e}_i$, $1 \le i \le r$, then

$\{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r\}$ is a basis of M. Since S is a Hermite ring, M' is free, let $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{s-r}\}$ be a basis of M'. Then $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{s-r}; \boldsymbol{z}_1, \ldots, \boldsymbol{z}_r\}$ is a basis for S^s. With this, we define U as above, then U is an isomorphism and we get the following commutative diagram

$$\begin{tikzcd} S^s \arrow[r, "F_0"] \arrow[d, "U"'] & S^s \arrow[d, "U"] \\ S^s \arrow[r, "T_0"] & S^s \end{tikzcd}$$

where T_0 is given by $T_0(\boldsymbol{e}_j) = \mathbf{0}$, if $1 \leq j \leq s-r$ and $T_0(\boldsymbol{e}_{s-r+i}) = \boldsymbol{e}_{s-r+i}$, if $1 \leq i \leq r$, i.e.,

$$T_0 = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}.$$

Thus, we set $P = U \in GL_s(S)$ and we get $PF_0P^{-1} = T_0$.

$\Leftarrow$) We observe that $M = \operatorname{Im}(F_0) = \operatorname{Im}(F_0P^{-1}) =$ *module generated by the last r columns of* P^{-1}. This means that a basis for M is given by the last r columns of P^{-1}. □

An interesting consequence of the previous theorem is the following matrix characterization of *PF* rings (a commutative ring S is *PF* is every f.g projective S-module is free, see [13]). In the proof, we will use a well known matrix interpretation of f.g projective modules: let S be a commutative ring and M be an S-module. Then, M is an f.g projective module, if and only if there exists an idempotent matrix F over S such that $M \cong \operatorname{Im}(F)$.

Corollary 2. *Let S be a commutative ring. S is PF, if and only if for each* $s \geq 1$ *and every idempotent matrix* $F \in M_s(S)$, *there exist an invertible matrix* $P \in GL_s(S)$ *and some* $0 \leq r \leq s$ *such that*

$$PFP^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}.$$

Proof. $\Rightarrow$) Let $F \in M_s(S)$ be an idempotent matrix and let M be the R-module generated by the columns of F. We have $S^s \xrightarrow{F} S^s$ with $M = \mathrm{Im}(F)$ and $F^2 = F$, so $S^s = M \oplus M'$, i.e., M is a finitely generated projective module, then by the hypothesis, M is free. Since S is H, we can apply the Theorem 1 (ii).

$\Leftarrow$) Let M be a finitely generated projective R-module, so there exists $s \geq 1$ such that $S^s = M \oplus M'$; let $S^s \xrightarrow{F} S^s$ be the canonical projection on M, so F is idempotent and, by the hypothesis, we have the following commutative diagram

$$\begin{array}{ccc} S^s & \xrightarrow{F} & S^s \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle P} \\ S^s & \xrightarrow{D} & S^s \end{array}$$

with

$$D = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}.$$

Then, $M = \mathrm{Im}(F) \cong \mathrm{Im}(D) \cong S^r$. □

3. Equivalent Matrices and Free Modules

According to (2.1), for the matrix presentation F_1 of the free S-module M, there exists $U \in GL_s(S)$ such that $UF_1 = G_1$, with

$$G_1 = \begin{bmatrix} I_{s-r} & 0 \\ 0 & 0 \end{bmatrix},$$

i.e., F_1 is equivalent to G_1. In a similar way, we have a similarity relationship in (2.2). From this arises, the problem about to have a procedure for computing the matrices U and P, or more general, to study the equivalence of matrices over commutative rings from a constructive point of view. Next, we present some results in such direction, see the Corollary 5. We will exhibit also a procedure for computing the module $\mathrm{Hom}_S(M, N)$, where S is an SC commutative ring (see the Definition 7) and M, N are finitely generated modules over S. The Hom modules were computed in [12] for the special case when $S = R[x_1, \ldots, x_n]$, with R is a commutative Noetherian GS ring. Some ideas behind the results have been taken from [2], where similar problems have been considered for certain special class of computable Ore algebras.

We start with some beautiful results that involve Kronecker product of matrices.

Definition 3. Let S be a commutative ring and $E = [e_{ij}] \in M_{r\times s'}(S)$ be a matrix. $\mathrm{col}(E)$ is the column vector obtained concatenating the columns of E,

$$\mathrm{col}(E) := (e_{11}, \ldots, e_{r1}; \ldots; e_{1s'}, \ldots, e_{rs'})^t \in S^{rs'}.$$

Proposition 4. *Let S be a commutative ring. Then*:

(i) *If* $E \in M_{r\times s'}(S), U \in M_{s'\times s}(S)$, *and* $F \in M_{s\times l}(S)$ *are matrices, then*

$$\mathrm{col}(EUF) = (F^t \otimes E)\mathrm{col}(U).$$

(ii) *Let* $F \in M_{s\times l}(S), G \in M_{s'\times l'}(S), U \in M_{s'\times s}(S)$, *and* $V \in M_{l'\times l}(S)$. *Then*,

$$UF = GV, \textit{ if and only if } [I_{s'} \otimes F^t \quad G \otimes I_l]\begin{bmatrix}\mathrm{col}(U^t) \\ -\mathrm{col}(V)\end{bmatrix} = 0,$$

i.e.,

$$UF = GV, \textit{ if and only if } [\mathrm{col}(U^t) \quad -\mathrm{col}(V)]^t \in Syz[I_{s'} \otimes F^t \quad G \otimes I_l].$$

(iii) *With the notation of* (ii), *let* $\mathcal{P}_{F,G} := \{(U, V) | UF = GV\}$. *Then* $\mathcal{P}_{F,G}$ *is an S-module and* $\mathcal{P}_{F,G} \cong Syz[I_{s'} \otimes F^t \quad G \otimes I_l]$.

(iv) *Let* $s' = s$ *and* $l' = l$. *F and G are equivalent*, *if and only if there exists a vector* $[\operatorname{col}(U^T) \quad -\operatorname{col}(V)]^T \in Syz[I_s \otimes F^T \quad G \otimes I_l]$, *with* $U \in GL_s(S)$ *and* $V \in GL_l(S)$.

Proof. (i) This follows from a direct computation of product and Kronecker product of matrices:

$$\operatorname{col}(EUF) = \begin{bmatrix} \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{1z}u_{zw}f_{w1} \\ \vdots \\ \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{rz}u_{zw}f_{w1} \\ \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{1z}u_{zw}f_{w2} \\ \vdots \\ \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{rz}u_{zw}f_{w2} \\ \vdots \\ \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{1z}u_{zw}f_{wl} \\ \vdots \\ \sum_{w=1}^{s}\sum_{z=1}^{s'} e_{rz}u_{zw}f_{wl} \end{bmatrix};$$

$$(F^t \otimes E)\operatorname{col}(U) = \begin{bmatrix} f_{11}e_{11} & \cdots & f_{11}e_{1s'} & \cdots & f_{s1}e_{11} & \cdots & f_{s1}e_{1s'} \\ \vdots & & \vdots & & \vdots & & \vdots \\ f_{11}e_{r1} & \cdots & f_{11}e_{rs'} & \cdots & f_{s1}e_{r1} & \cdots & f_{s1}e_{rs'} \\ \vdots & & \vdots & & \vdots & & \vdots \\ f_{1l}e_{11} & \cdots & f_{1l}e_{1s'} & \cdots & f_{sl}e_{11} & \cdots & f_{sl}e_{1s'} \\ \vdots & & \vdots & & \vdots & & \vdots \\ f_{1l}e_{r1} & \cdots & f_{1l}e_{rs'} & \cdots & f_{sl}e_{r1} & \cdots & f_{sl}e_{rs'} \end{bmatrix} \begin{bmatrix} u_{11} \\ \vdots \\ u_{s'1} \\ \vdots \\ u_{1s} \\ \vdots \\ u_{s's} \end{bmatrix}.$$

(ii) Note that

$$UF - GV = \begin{bmatrix} \sum_{z=1}^{s} u_{1z}f_{z1} - \sum_{w=1}^{l'} g_{1w}v_{w1} & \cdots & \sum_{z=1}^{s} u_{1z}f_{zl} - \sum_{w=1}^{l'} g_{1w}v_{wl} \\ \vdots & & \vdots \\ \sum_{z=1}^{s} u_{s'z}f_{z1} - \sum_{w=1}^{l'} g_{s'w}v_{w1} & \cdots & \sum_{z=1}^{s} u_{s'z}f_{zl} - \sum_{w=1}^{l'} g_{s'w}v_{wl} \end{bmatrix},$$

and for $[I_{s'} \otimes F^t \quad G \otimes I_l]\begin{bmatrix} \operatorname{col}(U^t) \\ -\operatorname{col}(V) \end{bmatrix}$, we have

$$\begin{bmatrix} f_{11} & \cdots & f_{s1} & \cdots & 0 & \cdots & 0 & g_{11} & \cdots & 0 & \cdots & g_{1l'} & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ f_{1l} & \cdots & f_{sl} & \cdots & 0 & \cdots & 0 & 0 & \cdots & g_{11} & \cdots & 0 & \cdots & g_{1l'} \\ & \vdots & & \ddots & & \vdots & & & \vdots & & \ddots & & \vdots & \\ 0 & \cdots & 0 & \cdots & f_{11} & \cdots & f_{s1} & g_{s'1} & \cdots & 0 & \cdots & g_{s'l'} & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & f_{1l} & \cdots & f_{sl} & 0 & \cdots & g_{s'1} & \cdots & 0 & \cdots & g_{s'l'} \end{bmatrix} \begin{bmatrix} u_{11} \\ \vdots \\ u_{1s} \\ \vdots \\ u_{s'1} \\ \vdots \\ u_{s's} \\ -v_{11} \\ \vdots \\ -v_{l'1} \\ \vdots \\ -v_{1l} \\ \vdots \\ -v_{l'l} \end{bmatrix}.$$

Thus, $\operatorname{col}((UF - GV)^t) = 0$, if and only if $[I_{s'} \otimes F^t \quad G \otimes I_l] \begin{bmatrix} \operatorname{col}(U^t) \\ -\operatorname{col}(V) \end{bmatrix} = 0$,

i.e., $UF = GV$, if and only if $[I_{s'} \otimes F^t \quad G \otimes I_l] \begin{bmatrix} \operatorname{col}(U^t) \\ -\operatorname{col}(V) \end{bmatrix} = 0.$

(iii) This follows from (ii), if we define $(U, V) + (U', V') := (U + U', V + V')$ and $a.(U, V) := (aU, aV)$, with $a \in S$.

(iv) This is a direct consequence of (ii) and the fact that a square matrix U over a commutative ring S of size $s \times s$ is invertible, if and only if its columns generate S^s. □

From Proposition 4, we can complement the Theorem 1 with the following matrix constructive result.

Corollary 5. *Let S be a Hermite ring and M be an S-module.*

(i) *Let M be a finitely generated projective S-module of constant rank r given by the finite presentation*

$$S^l \xrightarrow{F_1} S^s \xrightarrow{F_0} M \to 0,$$

and let

$$G_1 = \begin{bmatrix} I_{s-r} & 0 \\ 0 & 0 \end{bmatrix}$$

of size $s \times l$. *M is free, if and only if there exists* $[\operatorname{col}(U^T) \;\; -\operatorname{col}(I_l)]^T \in Syz\;[I_s \otimes F_1^T \;\; G_1 \otimes I_l]$, *with* $U \in GL_s(S)$. *In such case, a basis of M is given by the last r columns of* U^{-1}.

(ii) *Let M be a direct summand of* S^s *and* $F_0 : S^s \to M \subseteq S^s$ *be the canonical projection on M. Let*

$$T_0 = \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}$$

of size $s \times s$. *Then, M is free with* $\dim(M) = r$, *if and only if there exists* $[\operatorname{col}(P^T) \;\; -\operatorname{col}(P)]^T \in Syz[I_s \otimes F_0^T \;\; T_0 \otimes I_s]$, *with* $P \in GL_s(S)$. *In such case, a basis of M is given by the last r columns of* P^{-1}.

Another interesting result valid for arbitrary commutative rings is the following proposition that gives a procedure for computing the Hom modules in a more simple and general way (compare with [12]).

Proposition 6. *Let S be a commutative ring,* M, M' *modules over S and let*

$$S^l \xrightarrow{F_1} S^s \xrightarrow{F_0} M \to 0,$$

$$S^{l'} \xrightarrow{G_1} S^{s'} \xrightarrow{G_0} M' \to 0$$

be finite presentations of M and M'. *With the notation of Proposition* 4, *if* $H \in \operatorname{Hom}_S(M, M')$, *then there exists* $(U, V) \in \mathcal{P}_{F_1, G_1}$ *such that the following diagram is commutative*:

$$\begin{array}{ccccccc} S^l & \xrightarrow{F_1} & S^s & \xrightarrow{F_0} & M & \longrightarrow & 0 \\ {\scriptstyle V}\downarrow & & \downarrow{\scriptstyle U} & & \downarrow{\scriptstyle H} & & \\ S^{l'} & \xrightarrow{G_1} & S^{s'} & \xrightarrow{G_0} & M' & \longrightarrow & 0. \end{array} \quad (3.1)$$

Conversely, if $(U, V) \in \mathcal{P}_{F_1, G_1}$, *then there exists* $H \in \operatorname{Hom}_S(M, M')$ *such that the previous diagram is commutative.*

Additionally, if $\ker(G_1)$ *is finitely generated, then there exists a matrix* G_2 *of size* $l' \times t'$ *(for some* t'*) such that*

$$\operatorname{Hom}_S(M, M') \cong \mathcal{P}_{F_1, G_1} / \mathcal{K},$$

where

$$\mathcal{K} := \{(U, V) | U = G_1 Z_1, V = Z_1 F_1 + G_2 Z_2, \text{ with } Z_1 \in M_{l' \times s}(S), Z_2 \in M_{t' \times l}(S)\}.$$

Proof. The proof of the first part is classical and can be found also in [21]. Let $H \in \operatorname{Hom}_S(M, M')$, since S^s is projective, there exists $U : S^s \to S^{s'}$ such that $HF_0 = G_0 U$; moreover, $G_0 U F_1 = HF_0 F_1 = 0$, so $\operatorname{Im}(UF_1) \subseteq \ker(G_0) = \operatorname{Im}(G_1)$. Then, since S^l is projective, there exists $V : S^l \to S^{l'}$ such that $UF_1 = G_1 V$. This shows that the diagram (3.1) is commutative.

Conversely, let $(U, V) \in \mathcal{P}_{F_1, G_1}$, i.e., $UF_1 = G_1 V$; let $x \in M$, then there exists $y \in S^s$ such that $F_0(y) = x$, so we define $H : M \to M'$, $H(x) := G_0 U(y)$. Note that H is well defined: in fact, if $F_0(y') = x = F_0(y)$, then $y' - y \in \ker(F_0) = \operatorname{Im}(F_1)$ and there exists $z \in S^l$ such that $F_1(z) = y' - y$, so $G_0 U(y' - y) = G_0 U(F_1(z)) = G_0 G_1 V(z) = 0$ and hence $G_0 U(y) = G_0 U(y')$. Moreover, H is an homomorphism and satisfies $HF_0 = G_0 U$, i.e., the diagram (3.1) is commutative.

Now, we will prove the second part. We define

$$\mathcal{P}_{F_1, G_1} \xrightarrow{\alpha} \operatorname{Hom}_S(M, M'),$$

$$(U, V) \mapsto H_{U, V},$$

where $H_{U, V}$ is defined as above, i.e.,

$$H_{U,V}(x) := G_0U(y), \tag{3.2}$$

with $F_0(y) = x$, $x \in M$, and $y \in S^s$. It is easy to check that α is an S-homomorphism, moreover, as we saw, α is surjective. Let $\mathcal{K} := \ker(\alpha)$ and $(U, V) \in \mathcal{K}$, then $H_{U,V} = 0$, and we have the following commutative diagram

$$\begin{tikzcd}
S^l \arrow[r, "F_1"] \arrow[d, "V"'] & S^s \arrow[r, "F_0"] \arrow[d, "U"] & M \arrow[r] \arrow[d, "H_{U,V}=0"] & 0 \\
S^{l'} \arrow[r, "G_1"] & S^{s'} \arrow[r, "G_0"] & M' \arrow[r] & 0
\end{tikzcd}$$

note that $\operatorname{Im}(U) \subseteq \ker(G_0) = \operatorname{Im}(G_1)$, hence there exists an homomorphism $Z_1 : S^s \to S^{l'}$ such that $G_1Z_1 = U$. By the hypothesis, there exists an homomorphism $S^{t'} \xrightarrow{G_2} S^{l'}$ such that $G_2 := Syz(G_1) = \ker(G_1)$, where t' is the size of some set of generators of $\ker(G_1)$. We observe that $\operatorname{Im}(V - Z_1F_1) \subseteq \operatorname{Im}(G_2)$: in fact, for $w \in S^l$, we have $G_1(V - Z_1F_1)(w) = G_1V(w) - G_1Z_1F_1(w) = UF_1(w) - UF_1(w) = 0$, thus, $(V - Z_1F_1)(w) \in \ker(G_1) = \operatorname{Im}(G_2)$ and there exists $w' \in S^t$ such that $G_2(w') = (V - Z_1F_1)(w)$. So, there exists an homomorphism $Z_2 : S^l \to S^{t'}$ such that $G_2Z_2 = V - Z_1F_1$, i.e., $V = Z_1F_1 + G_2Z_2$.

Conversely, let $(U, V) \in \mathcal{P}_{F_1, G_1}$ such that $U = G_1Z_1$ and $V = Z_1F_1 + G_2Z_2$ for some matrices $Z_1 \in M_{l' \times s}(S)$, $Z_2 \in M_{t' \times l}(S)$, then $H_{U,V}(x) = G_0U(y) = G_0G_1Z_z(y) = 0$, with $x = F_0(y)$. This means that $H_{U,V} = 0$, i.e., $(U, V) \in \ker(\alpha)$ (note that the condition on V was not used). $\square$

According to the previous proposition, given $H \in \operatorname{Hom}_S(M, M')$, the matrices U, V for H in general are not unique, however, by Proposition 4 (ii), any generator of $[I_{s'} \otimes F_1^t \quad G_1 \otimes I_l]$ gives a such pair of matrices computed by the following algorithm:

Computation of matrices U and V

Input: Matrices F_1 and G_1 as in (3.1).

Output: Matrices U and V as in (3.1) given by $\operatorname{col}(U^t)$ and $\operatorname{col}(V)$.

Initialization: Define the matrix

$$K := [I_{s'} \otimes F_1^t \quad G_1 \otimes I_l].$$

Compute $Syz(K)$.

Choose any generator of $Syz(K)$ presented as

$[\operatorname{col}(U^t) \ \ -\operatorname{col}(V)]^t$, where $\operatorname{col}(U^t)$ is a column vector conformed by the first ss' entries of the chosen generator and $\operatorname{col}(V)$ is a column vector conformed by the next $l'l$ entries.

Conform U and V with the entries of $\operatorname{col}(U^t)$ and $\operatorname{col}(V)$.

The previous algorithm is effective, if we know how to compute syzygies of matrices over S, this holds, for example, if $S = R[x_1, \ldots, x_n]$, where R is a Noetherian Gröbner soluble ring, see [5] and [12].

Definition 7. A commutative ring S is syzygy computable (SC), if there exists an effective procedure for computing $Syz(F)$ for any matrix F over S.

Corollary 8. *Let S be a Noetherian SC commutative ring. If M, M' are finitely generated S-modules, then* $\operatorname{Hom}_S(M, M')$ *is effective computable.*

Proof. Finite presentations for M and M' as in the Proposition 6, and a finite set of generators of $Syz[I_{s'} \otimes F_1^t \quad G_1 \otimes I_l]$ can be effective computed since S is a Noetherian SC ring:

$$Syz[I_{s'} \otimes F_1^t \quad G_1 \otimes I_l] = \langle [\mathrm{col}(U_1^t) \ \ -\mathrm{col}(V_1)]^t, \ldots, [\mathrm{col}(U_t^t) \ \ -\mathrm{col}(V_t)]^t \rangle;$$

from the above algorithm and the proof of Proposition 6, we get that

$$\mathrm{Hom}_S(M, M') = \langle H_{U_1,V_1}, \ldots, H_{U_t,V_t} \rangle. \qquad \square$$

Example 9. We will repeat the example presented in the Section 3 of [12], but using the previous algorithm. Let $S := \mathbb{Z}_{10}[x, y]$, we want to compute $\mathrm{Hom}_S(M, N)$, where $M =< \boldsymbol{f}_1, \boldsymbol{f}_2 >\subseteq S^2$ and $N =< \boldsymbol{g}_1, \boldsymbol{g}_2, \boldsymbol{g}_3 >\subseteq S^2$, with $\boldsymbol{f}_1 = (3x^2y + 3x, xy - 2y)$, $\boldsymbol{f}_2 = (7xy^2 + y, y^2 - 4x)$, $\boldsymbol{g}_1 = (0, x)$, $\boldsymbol{g}_2 = (y, x)$, and $\boldsymbol{g}_3 = (2x, x)$. We choose the monomial order POTREV on $\mathrm{Mon}(S^2)$ and deglex on $\mathrm{Mon}(S)$, with $x > y$ (see [11]).

Step 1. We compute finite presentations for M and N:

$$A \xrightarrow{F_1} A^2 \xrightarrow{F_0} M, \qquad A^2 \xrightarrow{G_1} A^3 \xrightarrow{G_0} N,$$

with

$$F_0 = \begin{bmatrix} 3x^2y + 3x & 7xy^2 + y \\ xy - 2y & y^2 - 4x \end{bmatrix}, \quad F_1 = Syz(F_0) = \begin{bmatrix} 5y \\ 5x \end{bmatrix},$$

$$G_0 = \begin{bmatrix} 0 & y & 2x \\ x & x & x \end{bmatrix}, \quad G_1 = Syz(G_0) = \begin{bmatrix} 5 & 2x + 9y \\ 0 & 8x \\ 5 & y \end{bmatrix}.$$

Step 2. With the notation of the above algorithm, we have $s = 2$, $l = 1$, $s' = 3$, $l' = 2$, and we must compute $Syz(K)$, with

$$K = \left[\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 5y & 5x \end{bmatrix} \quad \begin{bmatrix} 5 & 2x + 9y \\ 0 & 8x \\ 5 & y \end{bmatrix} \otimes \begin{bmatrix} 1 \end{bmatrix} \right],$$

i.e.,

$$K = \begin{bmatrix} 5y & 5x & 0 & 0 & 0 & 0 & 5 & 2x + 9y \\ 0 & 0 & 5y & 5x & 0 & 0 & 0 & 8x \\ 0 & 0 & 0 & 0 & 5y & 5x & 5 & y \end{bmatrix}.$$

With the procedure described in [12], we get a system of generators of $Syz(K)$:

$$(0, 0, 0, 0, 0, 0, 2, 0)^T, (-1, 0, 0, 0, -1, 0, y, 0)^T, (0, -1, 0, 0, 0, -1, x, 0)^T,$$

$$(0, 0, 0, 0, 0, 0, -y, 5)^T, (0, 0, 0, 0, x, -y, 0, 0)^T, (0, 0, 2, 0, 0, 0, 0, 0)^T,$$

$$(0, 0, 0, 2, 0, 0, 0, 0)^T, (0, 0, x, -y, 0, 0, 0, 0)^T, (0, 0, 0, 0, 2, 0, 0, 0)^T,$$

$$(0, 0, 0, 0, 0, 2, 0, 0)^T.$$

Step 3. From the above generators, we obtain the pair of matrices (U_i, V_i), $1 \leq i \leq 10$:

$$U_1 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, V_1 := \begin{bmatrix} -2 \\ 0 \end{bmatrix}; U_2 := \begin{bmatrix} -1 & 0 \\ 0 & 0 \\ -1 & 0 \end{bmatrix}, V_2 := \begin{bmatrix} -y \\ 0 \end{bmatrix};$$

$$U_3 := \begin{bmatrix} 0 & -1 \\ 0 & 0 \\ 0 & -1 \end{bmatrix}, V_3 := \begin{bmatrix} -x \\ 0 \end{bmatrix}; U_4 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, V_4 := \begin{bmatrix} y \\ -5 \end{bmatrix};$$

$$U_5 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ x & -y \end{bmatrix}, V_5 := \begin{bmatrix} 0 \\ 0 \end{bmatrix}; U_6 := \begin{bmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 0 \end{bmatrix}, V_6 := \begin{bmatrix} 0 \\ 0 \end{bmatrix};$$

$$U_7 := \begin{bmatrix} 0 & 0 \\ 0 & 2 \\ 0 & 0 \end{bmatrix}, V_7 := \begin{bmatrix} 0 \\ 0 \end{bmatrix}; U_8 := \begin{bmatrix} 0 & 0 \\ x & -y \\ 0 & 0 \end{bmatrix}, V_8 := \begin{bmatrix} 0 \\ 0 \end{bmatrix};$$

$$U_9 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 2 & 0 \end{bmatrix}, V_9 := \begin{bmatrix} 0 \\ 0 \end{bmatrix}; U_{10} := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 2 \end{bmatrix}, V_{10} := \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

We checked that $U_i F_1 = G_1 V_i$, for each $1 \leq i \leq 10$.

Step 4. With (3.2), we get the homomorphisms H_{U_i, V_i}, i.e., a system of generators of $\mathrm{Hom}_S(M, N)$. Note that $H_{U_1, V_1} = 0 = H_{U_4, V_4}$, thus, we have only 8 generators:

$$H_{U_2, V_2}(\boldsymbol{f}_1) = \begin{bmatrix} 0 & y & 2x \\ x & x & x \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 0 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2x \\ -2x \end{bmatrix} = -(\boldsymbol{g}_1 + \boldsymbol{g}_3);$$

$$H_{U_2, V_2}(\boldsymbol{f}_2) = \begin{bmatrix} 0 & y & 2x \\ x & x & x \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 0 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \mathbf{0}.$$

In a similar way, we get

$$H_{U_3, V_3}(\boldsymbol{f}_1) = \mathbf{0},\ H_{U_3, V_3}(\boldsymbol{f}_2) = -(\boldsymbol{g}_1 + \boldsymbol{g}_3);$$

$$H_{U_5, V_5}(\boldsymbol{f}_1) = x\boldsymbol{g}_3,\ H_{U_5, V_5}(\boldsymbol{f}_2) = -y\boldsymbol{g}_3;$$

$$H_{U_6, V_6}(\boldsymbol{f}_1) = 2\boldsymbol{g}_2,\ H_{U_6, V_6}(\boldsymbol{f}_2) = \mathbf{0};$$

$$H_{U_7, V_7}(\boldsymbol{f}_1) = \mathbf{0},\ H_{U_7, V_7}(\boldsymbol{f}_2) = 2\boldsymbol{g}_2;$$

$$H_{U_8, V_8}(\boldsymbol{f}_1) = x\boldsymbol{g}_2,\ H_{U_8, V_8}(\boldsymbol{f}_2) = -y\boldsymbol{g}_2;$$

$$H_{U_9, V_9}(\boldsymbol{f}_1) = 2\boldsymbol{g}_3,\ H_{U_9, V_9}(\boldsymbol{f}_2) = \mathbf{0};$$

$$H_{U_{10}, V_{10}}(\boldsymbol{f}_1) = \mathbf{0},\ H_{U_{10}, V_{10}}(\boldsymbol{f}_2) = 2\boldsymbol{g}_3.$$

We observe that these results coincide with those of Section 3 in [12]. In fact, using the notation of [12], we have $H_{U_2, V_2} = -\phi_1$, $H_{U_3, V_3} = -\phi_6$, $H_{U_5, V_5} = \phi_4 - y\phi_6$, $H_{U_6, V_6} = \phi_3$, $H_{U_7, V_7} = \phi_7$, $H_{U_8, V_8} = \phi_2$, $H_{U_9, V_9} = \phi_5$, and $H_{U_{10}, V_{10}} = \phi_8$.

References

[1] F. Chyzak, A. Quadrat and D. Robertz, Effective algorithms for parametrizing linear control systems over Ore algebras, AAECC 16 (2005), 319-376.

[2] T. Cluzeau and A. Quadrat, Factoring and decomposing a class of linear functional systems, Lin. Alg. and its Appl. 428 (2008), 324-381.

[3] A. Fabiańska and A. Quadrat, Applications of the Quillen-Suslin theorem to multirankal systems theory, INRIA, Rapport de Recherche $n°$ 6126 (2007).

[4] J. Gago-Vargas, On Suslin's Stability Theorem for $R[x_1, \ldots, x_m]$, Ring Theory and Algebraic Geometry, Lecture Notes in Pure and Applied Mathematics, Vol. 221, Marcel Dekker, New York, (2001), 203-210.

[5] G. Greuel and G. Pfister, A Singular Introduction to Commutative Algebra, 2nd edition, Springer, 2007.

[6] T. Y. Lam, Serre's Problem on Projective Modules, Springer Monographs in Mathematics, Springer, 2006.

[7] S. Lang, Algebra, Springer, 2004.

[8] R. C. Laubenbacher and C. Woodburn, An algorithm for the Quillen-Suslin theorem for monoid rings, J. Pure Appl. Algebra 117-118 (1997), 395-429.

[9] R. C. Laubenbacher and K. Schlauch, An algorithm for the Quillen-Suslin theorem for quotients of polynomial rings by monomial ideals, J. Symb. Comp. 30 (2000), 555-571.

[10] R. C. Laubenbacher and C. Woodburn, A new algorithm for the Quillen-Suslin theorem, Contributions to Algebra and Geometry 41 (2000), 23-31.

[11] O. Lezama, Gröbner bases for modules over Noetherian polynomial commutative rings, Georgian Mathematical Journal 15 (2008), 121-137.

[12] O. Lezama, Some applications of Gröbner bases in homological algebra, S*ão* Paulo Journal of Mathematical Sciences 3(1) (2009), 25-59.

[13] O. Lezama et al., Quillen-Suslin rings, Extracta Mathematicae 24(1) (2009).

[14] A. Logar and B. Sturmfels, Algorithms for the Quillen-Suslin theorem, J. Algebra 145(1) (1992).

[15] H. Lombardi, Le contenu constructif d'un principe local-global avec une application á la structure d'un module projectif de type fini, Laboratoire de Mathématiques de Besançon, Université de Franche-Comté, 1997.

[16] H. Lombardi and Quitté, Algèbre Commutative, Méthodes Constructives, Modules Projectifs de Type Fini, 2009:
http://hlombardi.free.fr/

[17] B. MacDonald, Linear Algebra over Commutative Rings, Marcel Dekker, 1984.

[18] H. Park and C. Woodburn, An algorithmic proof of Suslin's stability theorem for polynomial rings, J. Algebra 178 (1995), 277-298.

[19] A. Quadrat and D. Robertz, Computation of bases of free modules over the Weyl algebras, Journal of Symbolic Computation (2007), doi:10.1016/j.jsc.2007.06.005.

[20] D. Quillen, Projective modules over polynomial rings, Invent. Math. 36 (1976), 167-171.

[21] J. J. Rotman, An Introduction to Homological Algebra, Academic Press, 1979.

[22] A. A. Suslin, Projective modules over polynomial rings are free, Soviet Math. Dokl. 17 (1976), 1160-1164.

■