



Contents lists available at ScienceDirect

Journal of Algebra

[www.elsevier.com/locate/jalgebra](http://www.elsevier.com/locate/jalgebra)



# Computing syzygies over $\mathbf{V}[X_1, \dots, X_k]$ , $\mathbf{V}$ a valuation domain



Lionel Ducos<sup>a</sup>, Annick Valibouze<sup>b,c</sup>, Ihsen Yengui<sup>d,\*</sup>

<sup>a</sup> *Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 Futuroscope Cedex, France*

<sup>b</sup> *Sorbonne Université, UPMC Univ. Paris 06, UMR 7606, LIP6 & LSTA, F-75005, Paris, France*

<sup>c</sup> *CNRS, UMR 7606, LIP6, F-75005, Paris, France*

<sup>d</sup> *Département de Mathématiques, Faculté des Sciences de Sfax, Université de Sfax, 3000 Sfax, Tunisia*

## ARTICLE INFO

### Article history:

Received 6 March 2014

Available online xxxx

Communicated by Steven Dale Cutkosky

### Keywords:

Saturation

Coherence

Echelon matrix

Syzygies

Valuation domains

## ABSTRACT

We give an algorithm for computing the  $\mathbf{V}$ -saturation of any finitely-generated submodule of  $\mathbf{V}[X_1, \dots, X_k]^m$  ( $k \in \mathbb{N}$ ,  $m \in \mathbb{N}^*$ ), where  $\mathbf{V}$  is a valuation domain. Our algorithm is based on a notion of “echelon form” which ensures its correctness. The proposed algorithm terminates when two (Hilbert) series on the quotient field and the residue field of  $\mathbf{V}$  coincide. As application, our algorithm computes syzygies over  $\mathbf{V}[X_1, \dots, X_k]$ .

© 2014 Elsevier Inc. All rights reserved.

## Introduction

It is folklore (see for example Theorem 7.3.3 in [5]) that if  $\mathbf{V}$  is a valuation domain, then  $\mathbf{V}[X_1, \dots, X_k]$  ( $k \in \mathbb{N}$ ) is coherent: that is, syzygy modules of finitely-generated ideals of  $\mathbf{V}[X_1, \dots, X_k]$  are finitely-generated. The proof in the above-mentioned reference relies

\* Corresponding author.

E-mail addresses: [ducos@math.univ-poitiers.fr](mailto:ducos@math.univ-poitiers.fr) (L. Ducos), [annick.valibouze@upmc.fr](mailto:annick.valibouze@upmc.fr) (A. Valibouze), [ihsen.yengui@fss.rnu.tn](mailto:ihsen.yengui@fss.rnu.tn) (I. Yengui).

on a profound and difficult result published in a huge paper by Gruson and Raynaud [6]. There is nevertheless no known general algorithm for this remarkable result, and it seems difficult to compute the syzygy module even for small polynomials. An exception is the case of Noetherian valuation rings (not necessarily integral), which can be settled by adapting the notion of Gröbner basis originally introduced by Buchberger for polynomials with coefficients in a field to the case where the base ring is a valuation ring (see for example [1,7,16,17]).

In [12], an algorithm for computing Gröbner bases over  $\mathbf{V}[X]$ , with  $\mathbf{V}$  a valuation domain of Krull dimension 1, is given. This was generalized in [14] to the nonintegral case and in [18] to the multivariate case. As a consequence, one can deduce an algorithm for computing a finite generating set for the syzygies of any finitely-generated submodule of  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain of Krull dimension 1.

The main objective of this paper is to give a general algorithm for computing a finite generating set for the syzygies of any finitely-generated ideal of  $\mathbf{V}[X_1, \dots, X_k]$  ( $\mathbf{V}$  a valuation domain of any Krull dimension) which neither relies on Noetherianity nor on Krull dimension. We will in fact give an algorithm for computing a finite generating set for the  $\mathbf{V}$ -saturation of any finitely-generated submodule of  $\mathbf{V}[X_1, \dots, X_k]^n$ . This algorithm is based on a notion of “echelon form” which ensures its correctness. The proposed algorithm terminates when two (Hilbert) series on the quotient field of  $\mathbf{V}$  and the residue field of  $\mathbf{V}$  coincide. Computing syzygies over  $\mathbf{V}[X_1, \dots, X_k]$  is one important application of the saturation algorithm we give.

It is worth pointing out that an algorithm for the univariate case was given originally in [11] and then revisited in [3].

## 1. Preliminary tools

**Terminology.** In this paper we use the terminology of constructive algebra as in [9,10,13]. For an arbitrary ring  $\mathbf{R}$ , we denote by  $\mathbf{R}^\times$  its group of units. The ring  $\mathbf{R}$  is said to be *discrete* if there is an algorithm deciding if  $x = 0$  or  $x \neq 0$  for an arbitrary element of  $\mathbf{R}$ . A ring  $\mathbf{R}$  is said to be *local* if we have explicitly the implication

$$\forall x, y \in \mathbf{R}, x + y \in \mathbf{R}^\times \implies (x \in \mathbf{R}^\times \vee y \in \mathbf{R}^\times).$$

A local ring  $\mathbf{R}$  has as unique maximal ideal its *Jacobson radical*  $\text{Rad}(\mathbf{R}) = \{x \in \mathbf{R} \mid 1 + x\mathbf{R} \subseteq \mathbf{R}^\times\}$ . The quotient ring  $\mathbf{k} = \mathbf{R}/\text{Rad}(\mathbf{R})$  is a field, called *residual field* of  $\mathbf{R}$ . The local ring  $\mathbf{R}$  is said to be *residually discrete* if we have explicitly the disjunction  $\forall x \in \mathbf{R} (x \in \mathbf{R}^\times \vee x \in \text{Rad}(\mathbf{R}))$ . In that case, the residual field is discrete. We have an algorithm deciding the disjunction “ $x = 0$  or  $x$  is invertible” for all  $x \in \mathbf{k}$ .

We need the following series of definitions.

**Definition 1.** Let  $\mathbf{R}$  be a residually discrete local ring, and fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ .

1. A polynomial  $f \in \mathbf{R}[X_1, \dots, X_k]$  is said to be *primitive* if it has an invertible coefficient.
2. A vector  $u = (u_1, \dots, u_m) \in \mathbf{R}[X_1, \dots, X_k]^m$  is said to be *primitive* if it has a primitive component. The position  $i$  of the last (from left to right) primitive  $u_i$  will be denoted by  $\text{index}(u)$ , the last monomial (i.e., the one with the highest multi-degree) of  $u_{\text{index}(u)}$  which has an invertible coefficient will be denoted by  $\text{PrimMon}(u)$ , and the coefficient of this monomial will be denoted by  $\text{PrimCoeff}(u)$ . For example, if  $\mathbf{R} = \mathbb{Z}_{2\mathbb{Z}}$  and  $u = (-4 + 2XY, 1 - 6X^3, 5X^7 - 3X^4Y + 6XY^4)$ , fixing the lexicographic order with  $X < Y$  as monomial order, we have  $\text{index}(u) = 3$ ,  $\text{PrimMon}(u) = X^4Y$ , and  $\text{PrimCoeff}(u) = -3$ .
3. We suppose that  $\mathbf{R}$  is a valuation ring (i.e., a ring  $\mathbf{V}$  in which for all  $a, b \in \mathbf{V}$ , either  $a$  divides  $b$  or  $b$  divides  $a$ ). For a vector  $u = (u_1, \dots, u_m) \in \mathbf{R}[X_1, \dots, X_k]^m \setminus \{0\}$ , as all the coefficients of the  $u_i$ 's are comparable under division, denoting by  $a$  the right-most coefficient (components from left to right and then accordingly to increasing multi-degrees) of  $u$  dividing all the others, the primitive vector  $\frac{1}{a}u$  is called *the primitive version* of  $u$  and denoted by  $\text{Prim}(u)$ . For example, if  $\mathbf{R} = \mathbb{Z}_{2\mathbb{Z}}$  and  $u = (8X - 4, 14 - 18X^2, 2 - 6X + 4X^2)$ , then  $\text{Prim}(u) = -\frac{1}{6}u$ .
4. For a primitive vector  $u = (u_1, \dots, u_m) \in \mathbf{R}[X_1, \dots, X_k]^m$ , we denote by  $\mathcal{I}(u)$  the couple  $(\text{index}(u), \text{mdeg}(\text{PrimMon}(u))) \in \llbracket 1, m \rrbracket \times \mathbb{N}^k$  (where  $\text{mdeg}$  denotes the multi-degree). It will be called the *height* of  $u$ .
5. Let  $u, v$  be two primitive vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$ . By the result of *the reduction of  $v$  by  $u$*  we mean the vector  $w = v + \alpha u$  where  $\alpha \in \mathbf{R}$  is chosen such that the term of multi-degree  $\text{mdeg}(\text{PrimMon}(u))$  and in position  $\text{index}(u)$  does not appear in  $w$  (we denote  $v \xrightarrow{u} w$ ). Let us take again the example seen in item 2 above with  $\text{index}(u) = 3$  and  $\text{PrimMon}(u) = X^4Y$  and consider the vector  $v = (0, X + X^2Y, 2XY^2 + 5X^4Y)$ . The term  $5X^4Y$  in  $v$  disappears with  $\alpha = \frac{5}{3}$  as follows:

$$v \xrightarrow{u} v + \frac{5}{3}u = \left( -\frac{20}{3} + \frac{10}{3}XY, \frac{5}{3} - 10X^3, \frac{25}{3}X^7 + 10XY^4 + 10XY^2 \right).$$

6. For a list  $S = [s_1, s_2, \dots]$  of vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$ , by  $MS$ , where  $M$  is a monomial, we mean the list  $[Ms_1, Ms_2, \dots]$ . Moreover, if  $\mathcal{N}$  is a totally ordered set of monomials  $N_0 < N_1 < \dots$  in  $\mathbf{R}[X_1, \dots, X_k]$ , by  $\mathcal{N}S$  we mean the list  $[N_0S, N_1S, \dots]$ .
7. The total degree of a vector  $u \in \mathbf{R}[X_1, \dots, X_k]^m$  is the maximum of the total degrees of its entries. It will be denoted by  $\text{tdeg}(u)$ .

**Definition 2.** Let  $\mathbf{R}$  be a residually discrete local ring,  $L := [L_1, L_2, \dots]$  a list of vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ), and fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ .

1. We say that  $L$  is *primitive triangular* if all the  $L_i$ 's are primitive vectors and for each  $i \geq 1$ , denoting by  $\text{PrimMon}(L_i) = M_i$  and  $\text{index}(L_i) = n_i$ ,  $M_i$  does not appear (i.e., has coefficient 0) in the  $n_i$ th component of  $L_j$  for all  $j > i$ .

2. We say that  $L$  is *in an echelon form* if all the  $L_i$ 's are primitive vectors and the  $\mathcal{I}(L_i)$ 's are pairwise different (we disregard the  $L_i$ 's which are null). Of course, if  $L$  is primitive triangular then it is in an echelon form.

**Definition 3.** Let  $\mathbf{R}$  be a residually discrete local ring, fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ , and consider  $u, v \in \mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ).

1. By an operations of type 1 we mean an operation of type

$$v \leftarrow v + \alpha u,$$

(reduction of  $v$  by  $u$ , where  $\alpha \in \mathbf{R}$  is such that the term of multidegree  $\text{mdeg}(\text{PrimMon}(u))$  and in position  $\text{index}(u)$  disappears from  $v$ ).

2. By an operations of type 2 we mean an operation of type

$$v \leftarrow \text{Prim}(v).$$

The following simple but precious three lemmas will be at the heart of the proposed algorithm.

**Lemma 4.** Let  $\mathbf{R} \subseteq \mathbf{T}$  be an extension of rings where  $\mathbf{R}$  is a residually discrete local ring, and consider a submodule  $\mathcal{M}$  of  $\mathbf{T}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ). Fixing a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ , if  $S = [u_1, u_2, \dots]$  is a primitive triangular list of vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$  generating  $\mathcal{M}$  as a  $\mathbf{T}$ -module then it also generates  $\mathcal{M} \cap \mathbf{R}[X_1, \dots, X_k]^m$  as an  $\mathbf{R}$ -module.

**Proof.** Let  $u \in \mathcal{M} \cap \mathbf{R}[X_1, \dots, X_k]^m$ . There exist  $a_1, \dots, a_s \in \mathbf{T}$  such that

$$u = a_1 u_1 + \dots + a_s u_s.$$

Thus, for each  $1 \leq i \leq s$ , by identifying the coefficient in component number  $\text{index}(u_i)$  and of multidegree  $\text{mdeg}(\text{PrimMon}(u_i))$  and denoting  $c_i = \text{PrimCoeff}(u_i)$ , we have:

$$\begin{cases} c_1 a_1 \in \mathbf{R} \\ b_{2,1} a_1 + c_2 a_2 \in \mathbf{R} \\ \vdots \\ b_{s,1} a_1 + b_{s,2} a_2 + \dots + b_{s,s-1} a_{s-1} + c_s a_s \in \mathbf{R} \end{cases}$$

for some  $b_{i,j} \in \mathbf{R}$ . As  $c_1, \dots, c_s \in \mathbf{R}^\times$ , this triangular system yields to  $a_1, \dots, a_s \in \mathbf{R}$ , as desired.  $\square$

**Lemma 5.** Let  $\mathbf{R}$  be a residually discrete local ring, fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ , and consider two primitive vectors  $u, v$  in  $\mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ) such that  $\mathcal{I}(u) \neq \mathcal{I}(v)$ . Then the result  $w$  of the reduction of  $v$  by  $u$  is primitive and  $\mathcal{I}(w) = \mathcal{I}(v)$ .

**Proof.** First, suppose that  $\text{index}(u) \neq \text{index}(v)$ . It suffices to deal with the following two subcases:

- $\text{index}(u) = 1$  and  $\text{index}(v) = 2$ : write  $u = (u_1, u_2, \dots)$  and  $v = (v_1, v_2, \dots)$  where  $u_1, v_2$  are primitive polynomials and  $v_1 \in \text{Rad}(\mathbf{R})[X_1, \dots, X_k]$ . We have  $w = (v_1 + \alpha u_1, v_2 + \alpha u_2, \dots)$  for some  $\alpha \in \text{Rad}(\mathbf{R})$  and the result clearly follows.
- $\text{index}(u) = 2$  and  $\text{index}(v) = 1$ : write  $u = (u_1, u_2, \dots)$  and  $v = (v_1, v_2, \dots)$  where  $u_2, v_1$  are primitive polynomials and  $u_1 \in \text{Rad}(\mathbf{R})[X_1, \dots, X_k]$ . We have  $w = (v_1 + \beta u_1, v_2 + \beta u_2, \dots)$  for some  $\beta \in \mathbf{R}$  and the result clearly follows.

The case  $\text{mdeg}(\text{PrimMon}(u)) \neq \text{deg}(\text{PrimMon}(v))$  is analogous.  $\square$

**Lemma 6.** Let  $\mathbf{R}$  be a residually discrete local ring, fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ , and consider a list  $L = [u_1, u_2, \dots]$  of primitive vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ) which is in an echelon form. Then we can (theoretically) transform  $L$  into a primitive triangular list  $L' = [u'_1, u'_2, \dots]$  only by means of operations of type 1.

**Proof.** As in the gaussian algorithm, this can be done with operations of type 1 and 2. But Lemma 5 guaranties that all the vectors computed when reducing  $L$  to  $L'$  are primitive and so there is no need of operations of type 2.  $\square$

**Definition 7.** Let  $\mathbf{R}$  be a domain with quotient field  $\mathbf{K}$  and consider vectors  $s_1, s_2, \dots \in \mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ). By the  $\mathbf{R}$ -saturation of  $\mathcal{S} := \sum_{i=1}^{\infty} \mathbf{R}s_i$  we mean

$$\begin{aligned} \text{Sat}(\mathcal{S}) &:= \{s \in \mathbf{R}[X_1, \dots, X_k]^m \mid \alpha s \in \mathcal{S} \text{ for some } \alpha \in \mathbf{R} \setminus \{0\}\} \\ &= (\mathcal{S} \otimes_{\mathbf{R}} \mathbf{K}) \cap \mathbf{R}[X_1, \dots, X_k]^m. \end{aligned}$$

If  $\text{Sat}(\mathcal{S}) = \mathcal{S}$ , we say that  $\mathcal{S}$  is  $\mathbf{R}$ -saturated.

Now we reach the main result our saturation algorithm will be based on.

**Proposition 8.** Let  $\mathbf{R}$  be a residually discrete local domain, fix a monomial order on  $\mathbf{R}[X_1, \dots, X_k]$ , and consider a list  $L = [u_1, u_2, \dots]$  of primitive vectors in  $\mathbf{R}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ). If  $L$  is in an echelon form then  $\sum_{i=1}^{\infty} \mathbf{R}u_i$  is  $\mathbf{R}$ -saturated.

**Proof.** On the one hand, by virtue of Lemma 6, we can (theoretically) transform the list  $L$  into a primitive triangular list  $L' = [u'_1, u'_2, \dots]$  only with the help of operations of type 1, and thus  $\sum_{i=1}^{\infty} \mathbf{R}u_i = \sum_{i=1}^{\infty} \mathbf{R}u'_i$ . On the other hand, using Lemma 4 with

$S = L'$  and  $\mathbf{T}$  being the quotient field of  $\mathbf{R}$ , we infer that  $\sum_{i=1}^{\infty} \mathbf{R}u'_i$  is  $\mathbf{R}$ -saturated. The result clearly follows.  $\square$

From now on, by a valuation domain we mean a residually discrete valuation domain (i.e., a valuation domain with an invertibility test).

**Algorithm 9** (*Saturation algorithm for a finitely-generated sub- $\mathbf{V}$ -module of  $\mathbf{V}[X_1, \dots, X_k]^m$* ).

**Input:** A finite list  $S = [s_1, \dots, s_n]$  of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain and  $m \geq 1$ .

**Output:** A generating list for  $\text{Sat}(\mathbf{V}s_1 + \dots + \mathbf{V}s_n)$ .

Start by fixing a monomial order on  $\mathbf{V}[X_1, \dots, X_k]$ . As in the gaussian algorithm, put  $S$  in an echelon form by performing operations of type 1 and 2 so that the updated list  $S$  will be formed by primitive vectors in an echelon form. By virtue of Proposition 8, it forms a generating set for  $\text{Sat}(\mathbf{V}s_1 + \dots + \mathbf{V}s_n)$ .

## 2. The $\mathbf{V}$ -saturation of finitely-generated submodules of $\mathbf{V}[X_1, \dots, X_k]^m$

### 2.1. The saturation defect series

**Notation 10.** Let  $\mathbf{V}$  be a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ . Consider a list  $L = [u_1, \dots, u_s]$  ( $s \geq 1$ ) of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$  ( $m \geq 1$ ). We denote by  $\langle L \rangle_{\mathbf{K}}$  (resp.  $\langle L \rangle_{\mathbf{k}}$ ) the  $\mathbf{K}$ -vector space (resp. the  $\mathbf{k}$ -vector space) generated by  $u_1, \dots, u_s$  (resp. by the classes  $\bar{u}_1, \dots, \bar{u}_s$  of  $u_1, \dots, u_s$  modulo  $\text{Rad}(\mathbf{V})[X_1, \dots, X_k]^m$ ), and

$$\dim_{\mathbf{K}} L := \dim_{\mathbf{K}} \langle L \rangle_{\mathbf{K}} \quad \text{and} \quad \dim_{\mathbf{k}} L := \dim_{\mathbf{k}} \langle L \rangle_{\mathbf{k}}.$$

We also denote by  $\langle L \rangle_{\mathbf{V}}$  the  $\mathbf{V}$ -module generated by  $u_1, \dots, u_s$ , and by  $\langle L \rangle_{\mathbf{V}[X_1, \dots, X_k]}$  (resp.  $\langle L \rangle_{\mathbf{K}[X_1, \dots, X_k]}$ ) the  $\mathbf{V}[X_1, \dots, X_k]$ -submodule of  $\mathbf{V}[X_1, \dots, X_k]^m$  (resp. the  $\mathbf{K}[X_1, \dots, X_k]$ -submodule of  $\mathbf{K}[X_1, \dots, X_k]^m$ ) generated by  $u_1, \dots, u_s$ .

**Lemma 11.** *Let  $\mathbf{V}$  be a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ . If  $L$  is a finite list of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$  then  $\dim_{\mathbf{K}} L \geq \dim_{\mathbf{k}} L$ .*

**Proof.** Denote by  $L = [u_1, \dots, u_s]$ ,  $d = \dim_{\mathbf{k}} L$  and suppose that  $\bar{u}_1, \dots, \bar{u}_d$  are  $\mathbf{k}$ -linearly independent. Then, necessarily,  $u_1, \dots, u_d$  are  $\mathbf{K}$ -linearly independent. To see this, let  $\alpha_1, \dots, \alpha_d \in \mathbf{V}$  such that  $\alpha_1 u_1 + \dots + \alpha_d u_d = 0$ . As  $\mathbf{V}$  is a valuation domain, there exists  $1 \leq i_0 \leq d$  such that  $\alpha_{i_0}$  divides all the  $\alpha_i$ 's. Necessarily  $\alpha_{i_0} = 0$  because otherwise

we would have  $\bar{u}_{i_0} \in \sum_{1 \leq i \leq d; i \neq i_0} \mathbf{k} \bar{u}_i$ , and thus  $\alpha_1 = \cdots = \alpha_d = 0$ . We conclude that  $\dim_{\mathbf{K}} L \geq d = \dim_{\mathbf{k}} L$ .  $\square$

Now we give a necessary and sufficient condition for a finitely-generated sub- $\mathbf{V}$ -module of  $\mathbf{V}[X_1, \dots, X_k]^m$  to be  $\mathbf{V}$ -saturated using its corresponding dimensions as  $\mathbf{K}$ -vector space and  $\mathbf{k}$ -vector space.

**Theorem 12.** *Let  $L$  be a finite list of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ . Then,  $\langle L \rangle_{\mathbf{V}}$  is  $\mathbf{V}$ -saturated if and only if  $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L$ .*

**Proof.** Denote by  $L = [u_1, \dots, u_s]$ .

“ $\Leftarrow$ ” We proceed by induction on  $s$ .

For  $s = 1$ , two cases may arise:

- Case 1:  $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L = 0$ . In this case, we have  $L = [0]$  and of course  $\{0\}$  is  $\mathbf{V}$ -saturated as  $\mathbf{V}$  is a domain.
- Case 2:  $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L = 1$ . Necessarily,  $u_1$  is primitive and thus  $\mathbf{V}u_1$  is  $\mathbf{V}$ -saturated.

Suppose now that  $s > 1$ . Two cases may arise:

- Case 1:  $u_1$  is not primitive (i.e., belongs to  $\text{Rad}(\mathbf{V})[X_1, \dots, X_k]^m$ ). Let us denote by  $L' = [u_2, \dots, u_s]$ . Necessarily,  $u_1 \in \langle L' \rangle_{\mathbf{K}}$  as otherwise we would have

$$\dim_{\mathbf{k}} L' = \dim_{\mathbf{k}} L = \dim_{\mathbf{K}} L = 1 + \dim_{\mathbf{K}} L' \geq 1 + \dim_{\mathbf{k}} L'.$$

As  $\dim_{\mathbf{K}} L = \dim_{\mathbf{K}} L'$ ,  $\dim_{\mathbf{k}} L = \dim_{\mathbf{k}} L'$ , and  $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L$ , we infer that  $\dim_{\mathbf{K}} L' = \dim_{\mathbf{k}} L'$ . The  $\mathbf{V}$ -module  $\langle L' \rangle_{\mathbf{V}}$  is  $\mathbf{V}$ -saturated by the induction hypothesis. Now, since  $u_1 \in \langle L' \rangle_{\mathbf{K}}$ , there exist  $\beta_1 \in \mathbf{V} \setminus \{0\}$  and  $\beta_2, \dots, \beta_s \in \mathbf{V}$  such that  $\beta_1 u_1 = \beta_2 u_2 + \cdots + \beta_s u_s$ , and hence  $u_1 \in \langle L' \rangle_{\mathbf{V}}$ . It follows that  $\langle L \rangle_{\mathbf{V}} = \langle L' \rangle_{\mathbf{V}}$ , and thus  $\langle L \rangle_{\mathbf{V}}$  is  $\mathbf{V}$ -saturated as desired.

- Case 2:  $u_1$  is primitive. For  $2 \leq i \leq s$ , we set  $v_i := u_i + \alpha_i u_1$ , where  $\alpha_i \in \mathbf{V}$  is such that the term of degree  $\deg(\text{PrimMon}(u_1))$  and in position  $\text{index}(u_1)$  does not appear in  $v_i$ . Denoting by  $S := [v_2, \dots, v_s]$ , we have  $\langle L \rangle_{\mathbf{V}} = \mathbf{V}u_1 \oplus \langle S \rangle_{\mathbf{V}}$ ,  $\dim_{\mathbf{K}} L = \dim_{\mathbf{K}} S + 1$ , and  $\dim_{\mathbf{k}} L = \dim_{\mathbf{k}} S + 1$ . As  $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L$ , we infer that  $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S$ . As  $\langle S \rangle_{\mathbf{V}}$  is  $\mathbf{V}$ -saturated (by the induction hypothesis) and so is  $\mathbf{V}u_1$  (by virtue of the case  $s = 1$ ), the desired conclusion follows.

“ $\Rightarrow$ ” Fixing a monomial order on  $\mathbf{V}[X_1, \dots, X_k]$ , we can put  $L$  in an echelon form by means of operations of type 1 and 2. Of course, an operation of type 1 does not affect the  $\mathbf{V}$ -module generated by the current list. Also, so does an operation of type 2 as  $\langle L \rangle_{\mathbf{V}}$

is  $\mathbf{V}$ -saturated. Denoting by  $U$  the new list obtained after putting  $L$  in an echelon form, we get

$$\dim_{\mathbf{K}} L = \dim_{\mathbf{K}} U = \dim_{\mathbf{k}} U = \dim_{\mathbf{k}} L. \quad \square$$

**Definition and notation 13.** Let  $L = [u_1, \dots, u_s]$  ( $s \geq 1$ ) be a list of  $s$  polynomial vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ .

1. For  $i \in \mathbb{N}$ , we denote by  $L_i$  the  $\mathbf{K}$ -vector space generated by the  $Mu_j$ 's where  $1 \leq j \leq s$  and  $M$  is a monomial at  $X_1, \dots, X_k$  of total degree at most  $i$ .
2. We denote by

$$h_{L, \mathbf{K}}(t) = \sum_{i \geq 0} (\dim_{\mathbf{K}} L_i) t^i,$$

a series (it is in fact a Hilbert series, see [Lemma 14](#) below) that we associate to  $L$  over  $\mathbf{K}$ . On the other hand, we associate to  $L$  a series

$$h_{L, \mathbf{k}}(t) = \sum_{i \geq 0} (\dim_{\mathbf{k}} \bar{L}_i) t^i$$

over the residue field  $\mathbf{k}$ , where  $\bar{L}_i$  is the list obtained from  $L_i$  by passing modulo  $\text{Rad}(\mathbf{V})[X_1, \dots, X_k]^m$ .

As  $\dim_{\mathbf{k}} \bar{L}_i \leq \dim_{\mathbf{K}} L_i$  ([Lemma 11](#)), the series

$$\delta_L(t) := h_{L, \mathbf{K}}(t) - h_{L, \mathbf{k}}(t)$$

has nonnegative coefficients. This series will be called the (*saturation*) *defect series* of the list  $L$ .

**Lemma 14.** *We have*

$$h_{U, \mathbf{K}}(t) = \text{HS}_{\text{Syz}_{\mathbf{K}}(u_1, \dots, u_s)}(t),$$

where  $\text{HS}$  denotes the classical Hilbert series.

**Proof.** This follows from the exact sequence

$$\begin{aligned} 0 \rightarrow \text{Syz}_{\mathbf{K}}(u_1, \dots, u_s) \rightarrow \mathbf{K}[X_1, \dots, X_k]^s \rightarrow \langle u_1, \dots, u_s \rangle \rightarrow 0 \\ (p_1, \dots, p_s) \mapsto p_1 u_1 + \dots + p_s u_s. \quad \square \end{aligned}$$

It is worth pointing out that classical Hilbert series can be computed effectively (see for example [\[15\]](#)).



**Example 15.** Consider the list  $U = [u_1 = 1 + 2X, u_2 = 1 + 2Y]$  with  $u_i \in \mathbb{Z}_{2\mathbb{Z}}[X, Y]$ . We have:

$$h_{U, \mathbb{Q}}(t) = \sum_{i=0}^{\infty} \frac{i^2 + 5i + 4}{2} t^i = \sum_{i=0}^{\infty} \left( \binom{2+i}{2} + \binom{1+i}{1} \right) t^i = \frac{1}{(1-t)^3} + \frac{1}{(1-t)^2},$$

$$h_{U, \mathbb{Z}/2\mathbb{Z}}(t) = \sum_{i=0}^{\infty} \frac{i^2 + 3i + 2}{2} t^i = \sum_{i=0}^{\infty} \binom{2+i}{2} t^i = \frac{1}{(1-t)^3},$$

and thus the defect series of  $U$  is

$$\delta_U(t) = \frac{1}{(1-t)^2}.$$

Now we are in position to state that a finite list of vectors  $\mathbf{V}[X_1, \dots, X_k]^m$  ( $\mathbf{V}$  a valuation domain) whose defect is null generates a  $\mathbf{V}$ -saturated sub- $\mathbf{V}[X_1, \dots, X_k]$ -module of  $\mathbf{V}[X_1, \dots, X_k]^m$ . This result will be used as a termination condition in our [Algorithm 18](#).

**Theorem 16.** *Let  $L$  be a finite list of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ . If  $\delta_L = 0$  then  $\langle L \rangle_{\mathbf{V}[X_1, \dots, X_k]}$  is  $\mathbf{V}$ -saturated.*

**Proof.** We keep the notation of [Definition and notation 13](#). As  $\delta_L = 0$ , we have  $\dim_{\mathbf{K}} L_i = \dim_{\mathbf{k}} L_i$ , and thus, by virtue of [Theorem 12](#),  $\langle L_i \rangle_{\mathbf{V}}$  is  $\mathbf{V}$ -saturated for each  $i \in \mathbb{N}$ . The desired result follows since  $\langle L \rangle_{\mathbf{V}[X_1, \dots, X_k]} = \bigcup_{i \in \mathbb{N}} \uparrow \langle L_i \rangle_{\mathbf{V}}$ .  $\square$

**Remark 17.** The converse of [Theorem 16](#) does not hold. To see this, let  $\mathbf{V} = \mathbb{Z}_{2\mathbb{Z}}$  and consider the list  $L = [X, 2X^2]$  of polynomials in  $\mathbf{V}[X]$ . We have:

$$h_{L, \mathbb{Q}}(t) = 2 + 2t + 2t^2 + \dots = \frac{2}{1-t},$$

$$h_{L, \mathbb{Z}/2\mathbb{Z}}(t) = 1 + t + t^2 + \dots = \frac{1}{1-t},$$

and thus the defect series of  $L$  is

$$\delta_L(t) = \frac{1}{1-t} \neq 0$$

despite that  $\langle L \rangle_{\mathbf{V}[X]} = \langle X \rangle$  is  $\mathbf{V}$ -saturated.

## 2.2. A saturation algorithm in the multivariate case

Considering a finite list  $S = [s_1, \dots, s_n]$  of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$  where  $\mathbf{V}$  is a valuation domain of quotient field  $\mathbf{K}$  and residue field  $\mathbf{k}$ , the following algorithm

computes a finite list of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$  generating  $\text{Sat}(\langle s_1, \dots, s_n \rangle)$  as a  $\mathbf{V}[X_1, \dots, X_k]$ -module. During the execution of the algorithm, the  $\mathbf{V}[X_1, \dots, X_k]$ -module (generated by the current list) grows every time a nonprimitive vector is created by the “triangulation” and then replaced by its primitive version (for the saturation). While the generated  $\mathbf{K}[X_1, \dots, X_k]$ -module (by the current list) does not change, the generated  $\mathbf{k}[X_1, \dots, X_k]$ -module grows, and one is gradually approximating the saturation.

**Algorithm 18** (*Saturation algorithm in the multivariate case*).

**Input:** A finite list  $S = [s_1, \dots, s_n]$  of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$ , where  $\mathbf{V}$  is a valuation domain and  $m \geq 1$ .

**Output:** A finite list  $G$  of vectors in  $\mathbf{V}[X_1, \dots, X_k]^m$  generating  $\text{Sat}(\langle s_1, \dots, s_n \rangle)$  as a  $\mathbf{V}[X_1, \dots, X_k]$ -module.

Start by fixing a monomial order on  $\mathbf{V}[X_1, \dots, X_k]$ .

Initialization:  $G := S$ . All along the algorithm described below, if a nonprimitive vector  $u$  is encountered during the computations, then  $\text{Prim}(u)$  must be added to  $G$ .

Let us fix some notation. We denote by  $S_0$  the list  $S$  put in an echelon form, and by induction  $T_j = [S_0, \dots, S_j]$  where  $S_{j+1}$  denotes  $[X_1 S_j, \dots, X_k S_j]$  put in an echelon form with respect to  $T_j$  and then put in an echelon form, with the initialization  $T_0 = S_0$ .

We begin by putting  $S$  in an echelon form (it becomes  $S_0$ ) and then compute its defect series  $\delta_{S_0}(t)$ . If  $\delta_{S_0}(t) = 0$  then stop; else compute  $S_1$ . If  $\delta_{S_1}(t) = 0$  then stop; else compute  $S_2$ , and so on.

**Theorem 19.** *Algorithm 18 terminates and is correct.*

**Proof.** We denote by  $\mathbf{K}$  the quotient field of  $\mathbf{V}$  and by  $\mathbf{k}$  its residue field.

First note that the primitive monomial of a primitive vector  $v \in \mathbf{V}[X_1, \dots, X_k]^m$  is nothing but the leading monomial (accordingly to a “position-over-term” monomial order on  $\mathbf{V}[X_1, \dots, X_k]^m$  obtained from the monomial order on  $\mathbf{V}[X_1, \dots, X_k]$ , see page 201 of [2]) of its class modulo the radical of  $\mathbf{V}$ . So, the computed primitive monomials are those of a nondecreasing sequence of submodules of  $\mathbf{k}[X_1, \dots, X_k]^m$ . As  $\mathbf{k}[X_1, \dots, X_k]^m$  is Noetherian, this sequence must stabilize and we obtain the classical behavior of Hilbert series over a field saying that, after the regularity, the leading monomials obtained at total degree  $k+1$  are obtained by simple translation of those obtained at degree  $k$ . Thus, the process described above will not add any new entry to  $G$  and a fortiori we ultimately obtain a defect which is zero.

Why  $G$  is a generating set for  $\text{Sat}(\langle s_1, \dots, s_n \rangle)$  as a  $\mathbf{V}[X_1, \dots, X_k]$ -module?

This is a direct consequence of Theorem 16.  $\square$

**Theorem 20.** Let  $\mathbf{V}$  be a valuation domain. Then the  $\mathbf{V}$ -saturation of any finitely-generated submodule of  $\mathbf{V}[X_1, \dots, X_k]^m$  ( $k \in \mathbb{N}$ ,  $m \in \mathbb{N}^*$ ) is finitely-generated.

**Proof.** This is a direct consequence of Algorithm 18.  $\square$

**Example 21** (Example 15 continued). As  $\delta_U(t) = \frac{1}{(1-t)^2} \neq 0$ , one has to put  $U$  in an echelon form. This can be done as follows:

$$U = [u_1 = 1 + 2X, u_2 = 1 + 2Y] \rightarrow U_0 := \left[ u_1, \frac{1}{2}(u_2 - u_1) \right] = [1 + 2X, Y - X].$$

As  $h_{U_0, \mathbb{Q}}(t) = h_{U_0, \mathbb{Z}/2\mathbb{Z}}(t) = \frac{1}{(1-t)^3} + \frac{1}{(1-t)^2}$ , we have  $\delta_{U_0}(t) = 0$ . We conclude that

$$\text{Sat}(\langle u_1, u_2 \rangle) = \langle 1 + 2X, Y - X \rangle.$$

### 3. The case of a Prüfer domain

We borrow the following definition and notation from [8].

**Definition and notation 22.** Let  $I$  and  $U$  be two subsets of a ring  $\mathbf{R}$ . We denote by  $\mathcal{M}(U)$  the monoid generated by  $U$ ,  $\mathcal{I}_{\mathbf{R}}(I)$  or  $\mathcal{I}(I)$  the ideal generated by  $I$  and  $\mathcal{S}(I; U)$  the monoid  $\mathcal{M}(U) + \mathcal{I}(I)$ . If  $I = \{a_1, \dots, a_k\}$  and  $U = \{u_1, \dots, u_\ell\}$ , we denote  $\mathcal{M}(U)$ ,  $\mathcal{I}(I)$  and  $\mathcal{S}(I; U)$  by  $\mathcal{M}(u_1, \dots, u_\ell)$ ,  $\mathcal{I}(a_1, \dots, a_k)$  and  $\mathcal{S}(a_1, \dots, a_k; u_1, \dots, u_\ell)$ , respectively. The localization  $\mathcal{S}(I; U)^{-1}\mathbf{R}$  will be denoted by  $\mathbf{R}_{(I; U)}$ .

#### Definition 23.

- A ring  $\mathbf{R}$  is *arithmetical* if each finitely-generated ideal is locally principal. A constructive characterization of arithmetical rings [4] is the following:

$$\forall x, y \in \mathbf{R} \exists s, t, a, b \in \mathbf{R} \begin{cases} sx = ay \\ bx = ty \\ s + t = 1 \end{cases} \quad (1)$$

In fact property (1) amounts to saying that each finitely-generated ideal becomes principal after localization at a finite family of comaximal monoids.

- An integral ring is called a *Prüfer domain* if it is arithmetical.
- A ring  $\mathbf{R}$  is *coherent* if each finitely-generated ideal is finitely presented, or equivalently, if for any  $a_1, \dots, a_n \in \mathbf{R}$ , the syzygy module  $\text{Syz}_{\mathbf{R}}(a_1, \dots, a_n)$  is finitely-generated.

**Theorem 24.** Let  $\mathbf{R}$  be a Prüfer domain and  $m \geq 1$ . Then the  $\mathbf{R}$ -saturation of any finitely-generated submodule of  $\mathbf{R}[X_1, \dots, X_k]^m$  is finitely-generated.

**Proof.** Let  $s_1, \dots, s_n \in \mathbf{R}[X_1, \dots, X_k]^m$ . The proof (algorithm) works in the same way as the case in which the base ring is a valuation domain ([Theorem 20](#)). The only difference occurs when one has to handle two incomparable (under division) elements  $a, b$  in  $\mathbf{T} = \mathbf{R}_{(I;U)}$  ( $T$  is the current ring with the initialization  $\mathbf{R}_{(0;1)} = \mathbf{R}$ ). In that situation, one should first compute  $u, v, w \in \mathbf{T}$  such that

$$\begin{cases} ub = va \\ wb = (1 - u)a. \end{cases}$$

More precisely, one has to open two branches  $\mathbf{R}_{(I;u,U)}$  and  $\mathbf{R}_{(I;(1-u),U)}$ . In the first,  $a$  divides  $b$ , and in the second  $b$  divides  $a$ . In the latter branch (the same holds for the first branch), one has to open two sub-branches  $\mathbf{R}_{(I;(1-u),w,U)}$  and  $\mathbf{R}_{(I,w;(1-u),U)}$ . In the first,  $a$  and  $b$  are associated and  $a$  divides  $b$ , while in the second  $b$  divides strictly  $a$  (i.e.,  $\frac{a}{b}$  is in the Jacobson radical), and this situation will be preserved in the whole opened sub-branches.

At the end of this dynamical computation, one finds a generating set for  $\text{Sat}(\langle s_1, \dots, s_\ell \rangle)$  at each leaf of the constructed binary tree (the leaves correspond to comaximal localizations of the ring  $\mathbf{R}$ ). To obtain a generating set for  $\text{Sat}(\langle s_1, \dots, s_\ell \rangle)$  over  $\mathbf{R}$  one has only to collect all together the generating sets at the leaves and to clear denominators (exactly as in Theorem 10 of [\[7\]](#)).  $\square$

**Theorem 25.** *If  $\mathbf{R}$  is a Prüfer domain then  $\mathbf{R}[X_1, \dots, X_k]$  is coherent.*

**Proof.** As in the proof of [Theorem 24](#), it suffices to prove the result locally, i.e., one can suppose that  $\mathbf{R}$  is a valuation domain. Let  $p_1, \dots, p_m \in \mathbf{R}[X_1, \dots, X_k]$ , and consider  $n$  vectors  $s_1, \dots, s_n \in \mathbf{R}[X_1, \dots, X_k]^m$  generating the syzygy module of  $p_1, \dots, p_m$  over the quotient field  $\mathbf{K}$  of  $\mathbf{R}$  as a  $\mathbf{K}[X_1, \dots, X_k]$ -module ( $s_1, \dots, s_n$  can be computed using Gröbner bases techniques [\[1,2\]](#)). Then, the syzygy module of  $p_1, \dots, p_m$  over  $\mathbf{R}$  is nothing but the  $\mathbf{R}$ -saturation of  $\langle s_1, \dots, s_n \rangle$  which is finitely-generated by [Theorem 20](#).  $\square$

At the end of this paper, it is worth pointing one important issue we will try to address in a future work: to prove the termination of [Algorithm 18](#) in such an effective way that a bound could be deduced for the number of steps in the algorithm. In fact, we were obligated to utilize a Noetherianity argument to prove the termination of [Algorithm 18](#), which defeats all hope of computing a complexity bound.

## References

- [1] W.-W. Adams, P. Loustau, *An Introduction to Gröbner Bases*, Grad. Stud. Math., vol. 3, American Mathematical Society, Providence, RI, 1994.
- [2] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties and Algorithms*, 2nd edition, Springer-Verlag, New York, 1997.
- [3] L. Ducos, S. Monceur, I. Yengui, Computing the  $\mathbf{V}$ -saturation of finitely-generated submodules of  $\mathbf{V}[X]^m$  where  $\mathbf{V}$  is a valuation domain, preprint, 2013.

- [4] L. Ducos, C. Quitté, H. Lombardi, M. Salou, Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind, *J. Algebra* 281 (2004) 604–650.
- [5] S. Glaz, *Commutative Coherent Rings*, second edition, Lecture Notes in Math., vol. 1371, Springer-Verlag, Berlin–Heidelberg–New York, 1990.
- [6] L. Gruson, M. Raynaud, Critères de platitude et de projectivité. Techniques de “platification” d’un module, *Invent. Math.* 13 (1971) 1–89.
- [7] A. Hadj Kacem, I. Yengui, Dynamical Gröbner bases over Dedekind rings, *J. Algebra* 324 (2010) 12–24.
- [8] H. Lombardi, C. Quitté, Constructions cachées en algèbre abstraite (2) Le principe local-global, dans, in: M. Fontana, S.-E. Kabbaj, S. Wiegand (Eds.), *Commutative Ring Theory and Applications*, in: *Lect. Notes Pure Appl. Math.*, vol. 131, M. Dekker, 2002, pp. 461–476.
- [9] H. Lombardi, C. Quitté, *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices*, Calvage et Mounet, 2011.
- [10] H. Lombardi, C. Quitté, *Commutative Algebra. Constructive Methods. Finite projective modules*, Springer, in press.
- [11] H. Lombardi, C. Quitté, I. Yengui, Un algorithme pour le calcul des syzygies sur  $\mathbf{V}[X]$  dans le cas où  $\mathbf{V}$  est un domaine de valuation, *Comm. Algebra* 42 (2014) 3768–3781.
- [12] H. Lombardi, P. Schuster, I. Yengui, The Gröbner ring conjecture in one variable, *Math. Z.* 270 (2012) 1181–1185.
- [13] R. Mines, F. Richman, W. Ruitenburg, *A Course in Constructive Algebra*, Universitext, Springer-Verlag, 1988.
- [14] S. Monceur, I. Yengui, On the leading terms ideals of polynomial ideals over a valuation ring, *J. Algebra* 351 (2012) 382–389.
- [15] C. Traverso, Hilbert functions and the Buchberger algorithm, *J. Symbolic Comput.* 22 (1997) 355–376.
- [16] I. Yengui, Dynamical Gröbner bases, *J. Algebra* 301 (2006) 447–458.
- [17] I. Yengui, Corrigendum to Dynamical Gröbner bases [*J. Algebra* 301 (2) (2006) 447–458] and to Dynamical Gröbner bases over Dedekind rings [*J. Algebra* 324 (1) (2010) 12–24], *J. Algebra* 339 (2011) 370–375.
- [18] I. Yengui, The Gröbner ring conjecture in the lexicographic order case, *Math. Z.* 276 (2014) 261–265.