Generalised Buchberger and Schreyer algorithms for strongly discrete coherent rings

Henri Lombardi[*], Stefan Neuwirth[*], Claude Quitté[**], and Ihsen Yengui[***]

[*]Université de Franche-Comté, CNRS, UMR 6623, LmB, 25000 Besançon, France,
henri.lombardi@univ-fcomte.fr, stefan.neuwirth@univ-fcomte.fr.
[**]Université de Poitiers, CNRS, UMR 7348, Laboratoire de Mathématiques et Applications, Poitiers, France, claude.quitte@orange.fr.
[***]Département de mathématiques, Faculté des sciences, Université de Sfax, 3000 Sfax, Tunisia,
ihsen.yengui@fss.rnu.tn.

11th February 2024

http://hlombardi.free.fr/Syzygy-cohfdi.tex

Contents

Abstract

Let M be a finitely generated submodule of a free module over a multivariate polynomial ring with coefficients in a discrete coherent ring. We prove that its module $\mathrm{LT}(M)$ of leading terms is countably generated and provide an algorithm for computing explicitly a generating set. This result is also useful when $\mathrm{LT}(M)$ is not finitely generated.

Suppose that the base ring is strongly discrete coherent. We provide a Buchberger-like algorithm and prove that it converges if, and only if, the module of leading terms is finitely generated. We also provide a constructive version of Hilbert's syzygy theorem by following Schreyer's method.

MSC 2020: 13D02, 13P10, 13C10, 13P20, 14Q20.

Keywords: Generalized Buchberger algorithm, syzygy theorem, free resolution, monomial order, Schreyer's monomial order, Schreyer's syzygy algorithm.

1 Introduction

This paper is written in the framework of Bishop style constructive mathematics (see Bishop 1967, Bishop and Bridges 1985, Mines, Richman, and Ruitenburg 1988, Lombardi and Quitté 2015, Yengui 2015).

It can be seen as a sequel to the paper Gamanda, Lombardi, Neuwirth, and Yengui 2020 (see also Hadj Kacem and Yengui 2010, Yengui 2006).

It generalises results in Adams and Loustaunau 1994 to suitable nonnoetherian contexts.

Our general context is the following.

General context 1.1. In this article, $\mathbf{R}$ is a commutative ring with unit, $X_1, \ldots, X_n$ are n indeterminates ($n \geq 1$), $\mathbf{R}[\underline{X}] = \mathbf{R}[X_1, \ldots, X_n]$, $\mathbf{H}_n^m \simeq \mathbb{A}^m(\mathbf{R}[\underline{X}])$ is a free $\mathbf{R}[\underline{X}]$-module with basis $(e_1, \ldots, e_m)$ ($m \geq 1$), and $>$ is a monomial order on $\mathbf{H}_n^m$ (see Definition 2.2). The case of an ideal in $\mathbf{R}[\underline{X}]$ is addressed by considering $m = 1$: $\mathbf{H}_n^1 = \mathbf{R}[\underline{X}]$ and e_1 is the unit of $\mathbf{R}$.

We shall make suitable hypotheses of coherence and discreteness. Let us consider a finitely generated submodule M of $\mathbf{H}_n^m$ and the module $\mathrm{LT}(M)$ of M with respect to our monomial order.

Our first fundamental theorem 3.10 states that $\mathrm{LT}(M)$ is countably generated and provides an algorithm for computing explicitly a generating set. This result is also useful when $\mathrm{LT}(M)$ is not finitely generated.

The second fundamental theorem 5.1 indicates a precise context in which the (generalised) Buchberger criterion and Buchberger algorithm work.

The third fundamental theorem 6.4 indicates a precise context in which the (generalised) Schreyer method works for computing a finite free resolution for M.

We shall work in four more specific contexts.

Discrete coherent context 1.2. General context 1.1 with $\mathbf{R}$ discrete and coherent.

Strongly discrete coherent context 1.3. General context 1.1 with $\mathbf{R}$ strongly discrete and coherent.

Simple division context 1.4. General context 1.1 with $\mathbf{R}$ strongly discrete.

Division with remainder context 1.5. General context 1.1 with $\mathbf{R}$ strongly discrete assuming moreover that we have a partial preorder $\leq_{\mathbf{R}}$ on elements of $\mathbf{R}$ (with $a \leq_{\mathbf{R}} b$ if $a = b$) and a generalised division algorithm Rem for $\mathbf{R}$ which computes, for given $c, c_1, \ldots, c_k \in \mathbf{R}$, a remainder $r_0 = c - \sum_j a_j c_j$ satisfying $r_0 = 0$ if, and only if, $c \in \langle c_1, \ldots, c_k \rangle$ and $r_0 \leq_{\mathbf{R}} c$, $a_j c_j \leq_{\mathbf{R}} c$ $(j = 1, \ldots, k)$ otherwise.

Simple division context 1.4 may be seen as the particular case of Division with remainder context 1.5 with equality for $\leq_{\mathbf{R}}$ and division not computing anything if $c \notin \langle c_1, \ldots, c_k \rangle$. We prefer nevertheless to treat the two contexts separately.
hum: `"equality for` $\leq_{\mathbf{R}}$`": c'est bien ça? Préciser des exemples de préordres partiels: stathme euclidien...`

2 Gröbner bases for modules over a discrete ring

We start with recalling the following constructive definitions.

Definition 2.1.

- A ring is *discrete* if it is equipped with a zero test: equality is decidable.
- Let U be an $\mathbf{R}$-module. The *syzygy* module of an n-tuple $(v_1, \ldots, v_n) \in U^n$ is

$$\mathrm{Syz}(v_1, \ldots, v_n) := \{\, (b_1, \ldots, b_n) \in \mathbf{R}^{1\times n} \; ; \; b_1 v_1 + \cdots + b_n v_n = 0 \,\}.$$

The syzygy module of a single element v is the *annihilator* $\mathrm{Ann}(v)$ of v.

- An $\mathbf{R}$-module U is *coherent* if the syzygy module of every n-tuple of elements of U is finitely generated, i.e. if there is an algorithm providing a finite system of generators for the syzygies, and an algorithm that represents each syzygy as a linear combination of the generators. The ring $\mathbf{R}$ is *coherent* if it is coherent as an $\mathbf{R}$-module. It is well-known that a module is coherent if, and only if, on the one hand any intersection of two finitely generated submodules is finitely generated, and on the other hand the annihilator of every element is a finitely generated ideal.

- A ring is *strongly discrete* if it is equipped with a membership test for finitely generated ideals, i.e. if, given $a, b_1, \ldots, b_n \in \mathbf{R}$, one can answer the question $a \in ? \langle b_1, \ldots, b_n \rangle$ and, in the case of a positive answer, one can explicitly provide $c_1, \ldots, c_n \in \mathbf{R}$ such that $a = b_1 c_1 + \cdots + b_n c_n$.

- $\mathbf{R}$ is a *Bézout ring* if every finitely generated ideal is principal, i.e. of the form $\langle a \rangle = \mathbf{R}a$ with $a \in \mathbf{R}$. A Bézout ring is strongly discrete if, and only if, it is equipped with a divisibility test; it is coherent if, and only if, the annihilator of any element is principal. To be a valuation ring is to be a Bézout local ring (see Lombardi and Quitté 2015, Lemma IV-7.1).

- A Bézout ring $\mathbf{R}$ is *strict* if for all $b_1, b_2 \in \mathbf{R}$ we can find $d, b'_1, b'_2, c_1, c_2 \in \mathbf{R}$ such that $b_1 = db'_1$, $b_2 = db'_2$, and $c_1 b'_1 + c_2 b'_2 = 1$. Valuation rings and Bézout domains are strict Bézout rings; a quotient or a localisation of a strict Bézout ring is again a strict Bézout ring (see Lombardi and Quitté 2015, Exercise IV-7 pp. 220–221, solution pp. 227–228). A zero-dimensional Bézout ring is strict (because it is a "Smith ring", see Díaz-Toca et al. 2014, Exercice XVI-9 p. 355, solution p. 526, and Lombardi and Quitté 2015, Exercise IV-8 pp. 221-222, solution p. 228).

Definition 2.2 (Monomial orders on finite-rank free $\mathbf{R}[\underline{X}]$-modules, see Adams and Loustaunau 1994, Cox, Little, and O'Shea 2005, Yengui 2021b)**.** General context 1.1.

(1) Monomials, terms.

- A *monomial* in $\mathbf{H}_n^m$ is a vector of the form $M = \underline{X}^\alpha e_i$ $(1 \leq i \leq m)$, where $\underline{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is a monomial in $\mathbf{R}[\underline{X}]$; the index i is the *position* of the monomial. The set of monomials in $\mathbf{H}_n^m$ is denoted by $\mathbb{M}_n^m$, with $\mathbb{M}_n^1 \cong \mathbb{M}_n$ (the set of monomials in $\mathbf{R}[\underline{X}]$). For example, $X_1 X_2^3 e_2$ is a monomial in $\mathbf{H}_n^m$, but $2X_1 e_3$, $(X_1 + X_2^3)e_2$ and $X_1 e_2 + X_1 e_3$ are not.

- If $M = \underline{X}^\alpha e_i$ and $N = \underline{X}^\beta e_j$, we say that M *divides* N if $i = j$ and $\underline{X}^\alpha$ divides $\underline{X}^\beta$. For example, $X_1 e_1$ divides $X_1 X_2 e_1$, but does not divide $X_1 X_2 e_2$. Note that in the case that M divides N, there exists a monomial $\underline{X}^\gamma$ in $\mathbb{M}_n$ such that $N = \underline{X}^\gamma M$: in this case we define $N/M := \underline{X}^\gamma$; for example, $(X_1 X_2 e_1)/(X_1 e_1) = X_2$.

- A *term* in $\mathbf{H}_n^m$ is a vector of the form cM, where $c \in \mathbf{R} \setminus \{0\}$ and $M \in \mathbb{M}_n^m$. We say that a term cM *divides* a term $c'M'$, with $c, c' \in \mathbf{R} \setminus \{0\}$ and $M, M' \in \mathbb{M}_n^m$, if c divides c' and M divides M'.

(2) A *monomial order* on $\mathbf{H}_n^m$ is a relation $>$ on $\mathbb{M}_n^m$ such that

- $>$ is a total order on $\mathbb{M}_n^m$;
- $\underline{X}^\alpha M > M$ for all $M \in \mathbb{M}_n^m$ and $\underline{X}^\alpha \in \mathbb{M}_n \setminus \{1\}$;
- $M > N \implies \underline{X}^\alpha M > \underline{X}^\alpha N$ for all $M, N \in \mathbb{M}_n^m$ and $\underline{X}^\alpha \in \mathbb{M}_n$.

Note that, when specialised to the case $m = 1$, this definition coincides with the definition of a monomial order on $\mathbf{R}[\underline{X}]$.

(3) Let the ring $\mathbf{R}$ be discrete.

- Any *nonzero* vector $u \in \mathbf{H}_n^m$ can be written as a sum of terms

$$u = c_t M_t + c_{t-1} M_{t-1} + \cdots + c_1 M_1,$$

with $c_i \in \mathbf{R} \setminus \{0\}$, $M_i \in \mathbb{M}_n^m$, and $M_t > M_{t-1} > \cdots > M_1$.

- We define the *leading coefficient*, *leading monomial*, and *leading term* of u as in the ring case: $\mathrm{LC}(u) = c_t$, $\mathrm{LM}(u) = M_t$, $\mathrm{LT}(u) = \mathrm{LC}(u)\,\mathrm{LM}(u)$.

- Letting $M_t = \underline{X}^\alpha e_\ell$ with $\underline{X}^\alpha \in \mathbb{M}_n$ and $1 \leq \ell \leq m$, we say that α is the *multidegree of* u and write $\mathrm{mdeg}(u) = \alpha$, and that the index ℓ is the *leading position* of u, and write $\mathrm{LPos}(u) = \ell$.

- We stipulate that $\mathrm{LC}(0) = 0$, $\mathrm{LM}(0) = 0$, and $\mathrm{mdeg}(0) = -\infty$, but we do not define $\mathrm{LPos}(0)$.

(4) A monomial order on $\mathbf{R}[\underline{X}]$ gives rise to the two following canonical monomial orders on $\mathbf{H}_n^m$. Let us consider monomials $M = \underline{X}^\alpha e_i$ and $N = \underline{X}^\beta e_j \in \mathbb{M}_n^m$.

- We say that

$$M > N \quad \text{if} \quad \left| \begin{array}{l} \text{either } \underline{X}^\alpha > \underline{X}^\beta \\ \text{or both } \underline{X}^\alpha = \underline{X}^\beta \text{ and } i < j. \end{array} \right.$$

This monomial order is called *term over position* (TOP) because it gives precedence to the monomial order on $\mathbf{R}[\underline{X}]$ over the monomial position. For example, when $X_2 > X_1$, we have

$$X_2 e_1 > X_2 e_2 > X_1 e_1 > X_1 e_2.$$

- We say that

$$M > N \quad \text{if} \quad \left| \begin{array}{l} \text{either } i < j \\ \text{or both } i = j \text{ and } \underline{X}^\alpha > \underline{X}^\beta. \end{array} \right.$$

This monomial order is called *position over term* (POT) because it gives precedence to the monomial position over the monomial order on $\mathbf{R}[\underline{X}]$. For example, when $X_2 > X_1$, we have

$$X_2e_1 > X_1e_1 > X_2e_2 > X_1e_2.$$

Definition 2.3 (list and module of leading terms, Gröbner bases)**.** Let $\mathbf{R}$ be a discrete ring and consider a list $G = g_1, \ldots, g_p$ in $\mathbf{H}_n^m$. We denote by $\mathrm{LT}(G) = \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_p)$ the list of its leading terms. Suppose now that the g_i's are nonzero and consider the finitely generated submodule $U = \langle G\rangle = \mathbf{R}[\underline{X}]g_1 + \cdots + \mathbf{R}[\underline{X}]g_p$ of $\mathbf{H}_n^m$.

(1) The *module of leading terms* of U is $\mathrm{MLT}(U) := \langle\, \mathrm{LT}(u)\ ;\ u \in U\,\rangle$.

(2) G is a *Gröbner basis* for U if $\mathrm{MLT}(U) = \langle \mathrm{LT}(G)\rangle$.

The following proposition comes from Gamanda, Lombardi, Neuwirth, and Yengui 2020. We give it as a motivating example showing that the “obvious” syzygies do not suffice to generate all of them.

Proposition 2.4. *Let $\mathbf{R}$ be a strict Bézout ring, and $a_1, \ldots, a_s \in \mathbf{R} \setminus \{0\}$. Denote by $(e_1, \ldots, e_s)$ the canonical basis of $\mathbf{R}^s$. For $j \neq i$, write $a_j = d_{i,j}a_{i,j}$ with $d_{i,j} = \gcd(a_i, a_j)$. Then $\mathrm{Syz}(a_1, \ldots, a_s)$ is generated by the $\binom{s}{2}$ vectors $a_{i,j}e_i - a_{j,i}e_j$ with $i < j$,*[1] *and all the ze_i with $z \in \mathrm{Ann}(a_i)$. In particular, $\mathbf{R}$ is coherent if and only if $\mathrm{Ann}(a)$ is finitely generated (and thus can be generated by just one element) for any $a \in \mathbf{R}$. In that case, letting $\mathrm{Ann}(a_k) = \langle b_k\rangle$ for $1 \le k \le s$, we have:*

$$\mathrm{Syz}(a_1, \ldots, a_s) = \langle\, a_{i,j}e_i - a_{j,i}e_j, b_ke_k\ ;\ 1 \le i < j \le s, 1 \le k \le s\,\rangle.$$

Proof. Let $(c_1, \ldots, c_s) \in \mathrm{Syz}(a_1, \ldots, a_s)$, and let $\mathrm{s}(a_i, a_j) := a_{i,j}e_i - a_{j,i}e_j$.
Note that $\gcd(a_{i,j}, a_{j,i}) = 1$. For each permutation $i_1, \ldots, i_s$ of $1, \ldots, s$, we shall transform the sum $a_{i_1,i_2} \cdots a_{i_{s-1},i_s}(c_1e_1 + \cdots + c_se_s)$ by replacing successively

$$\begin{array}{ccc} a_{i_1,i_2}e_{i_1} & \text{by} & \mathrm{s}(a_{i_1}, a_{i_2}) + a_{i_2,i_1}e_{i_2}, \\ \vdots & & \vdots \\ a_{i_{s-1},i_s}e_{i_{s-1}} & \text{by} & \mathrm{s}(a_{i_{s-1}}, a_{i_s}) + a_{i_s,i_{s-1}}e_{i_s}. \end{array}$$

At the end, the sum will be a linear combination of $\mathrm{s}(a_{i_1}, a_{i_2})$, $\mathrm{s}(a_{i_2}, a_{i_3})$, …, $\mathrm{s}(a_{i_{s-1}}, a_{i_s})$, and e_{i_s}; let z be the coefficient of e_{i_s} in this combination. As $(c_1, \ldots, c_s) \in \mathrm{Syz}(a_1, \ldots, a_s)$, we have $ze_{i_s} \in \mathrm{Syz}(a_1, \ldots, a_s)$ and $za_{i_s} = 0$.

[1]These are the *obvious* syzygies.

It remains to obtain a Bézout identity with respect to the products $a_{i_1,i_2}\cdots a_{i_{s-1},i_s}$, because it yields an expression of $(c_1,\dots,c_s)$ as a linear combination of the required form. For this, it is enough to develop the product of the $\binom{s}{2}$ Bézout identities with respect to $a_{i,j}$ and $a_{j,i}$, $1\le i<j\le s$: this yields a sum of products of $\binom{s}{2}$ terms, each of which is either $a_{i,j}$ or $a_{j,i}$, $1\le i<j\le s$, so that it is indexed by the tournaments on the vertices $1,\dots,s$; every such product contains a product of the above form $a_{i_1,i_2}\cdots a_{i_{s-1},i_s}$ because every tournament contains a hamiltonian path (see Rédei 1934–1935). □

Remark 2.5. The above proof results from an analysis of the following proof in the case where $\mathbf{R}$ is local, which entails in fact the general case. Since $\mathbf{R}$ is a valuation ring, we may consider a permutation $i_1,\dots,i_s$ of $1,\dots,s$ such that $a_{i_s}\mid a_{i_{s-1}}\mid\cdots\mid a_{i_1}$. Thus $\mathrm{s}(a_{i_1},a_{i_2})=e_{i_1}-a_{i_2,i_1}e_{i_2}$, …, $\mathrm{s}(a_{i_{s-1}},a_{i_s})=e_{i_{s-1}}-a_{i_s,i_{s-1}}e_{i_s}$ for some $a_{i_2,i_1},\dots,a_{i_s,i_{s-1}}$. Then, by replacing successively e_{i_k} by $\mathrm{s}(a_{i_k},a_{i_{k+1}})+a_{i_{k+1},i_k}e_{i_{k+1}}$, the syzygy $(c_1,\dots,c_s)$ may be rewritten as a linear combination of $\mathrm{s}(a_{i_1},a_{i_2})$, …, $\mathrm{s}(a_{i_{s-1}},a_{i_s})$, and e_{i_s}, with the coefficient of e_{i_s} turning out to lie in $\mathrm{Ann}(a_{i_s})$. ■

In the following, we give examples of coherent rings over which syzygy modules are not always generated by vectors with at most 2 nonzero components.

Example 2.6. Consider the (noetherian) coherent ring $\mathbb{Z}[u]$ and the syzygy module $\mathrm{Syz}(2,u,u{+}2)$. As $\mathrm{Syz}(2,u)=\langle(u,-2)\rangle$, $\mathrm{Syz}(2,u{+}2)=\langle(u+2,-2)\rangle$, and $\mathrm{Syz}(u{+}2,u)=\langle(-u,u+2)\rangle$, we conclude that if $s=(s_1,s_2,s_3)\in\mathrm{Syz}(2,u,u+2)$ can be written as a $\mathbb{Z}[u]$-linear combination of syzygies in $\mathrm{Syz}(2,u,u+2)$ with at most 2 nonzero components, then it has entries s_i in $\langle 2,u\rangle$. The sygygy $(1,1,-1)\in\mathrm{Syz}(2,u,u+2)$ does not satisfy this property.

Example 2.7. Consider the ring $\mathbf{R}=\mathbb{Z}[u]+v\,\mathbb{Q}(u)[v]_{(v)}$. It is coherent by Dobbs and Papick 1976, Theorem 3 (since $\mathrm{q.f.}(\mathbb{Z}[u])=\mathbb{Q}(u)$ and $\mathbb{Z}[u]$ is coherent) but nonnoetherian (since $\mathbb{Z}[u]$ is not a field, see Gilmer 1972, § 17, Exercise 14). As in Example 2.6, $(1,1,-1)\in\mathrm{Syz}_{\mathbf{R}}(2,u,u+2)$ cannot be written as an $\mathbf{R}$-linear combination of syzygies in $\mathrm{Syz}_{\mathbf{R}}(2,u,u+2)$ with at most 2 nonzero components (suppose so and take $v=0$).

3 Syzygies in a polynomial ring over a discrete coherent ring

Definition 3.1 (Syzygies of terms)**.** Discrete coherent context 1.2. Let $p\ge 1$ and $\mathscr{P}_p=\{\,E\,;\,\emptyset\ne E\subseteq [\![1,p]\!]\,\}$ be the set of nonempty subsets of the set of indices $[\![1,p]\!]$.

(1) Let $f_1,\dots,f_p\in\mathbf{H}_n^m$ not all zero with $\mathrm{LC}(f_j)=a_j$ and $\mathrm{LM}(f_j)=M_j$. Let $g_1,\dots,g_p\in\mathbf{R}[\underline{X}]$ with $\mathrm{LC}(g_j)=b_j$ and $\mathrm{LM}(g_j)=N_j$. The *leading monomial of the*

expression $g_1 f_1 + \cdots + g_p f_p$ *with respect to* $f_1, \ldots, f_p$ is the monomial $L = L(g) = \sup_{j \in [\![1,p]\!]} N_j M_j$, and its *leading monomial index set* is $E = \{\, j \;;\, N_j M_j = L \,\}$.

(2) Consider $M_1 = M_1' e_{i_1}, \ldots, M_p = M_p' e_{i_p}$ monomials in $\mathbf{H}_n^m$, $a_1, \ldots, a_p \in \mathbf{R}$. Let $\mathscr{P}(M_1, \ldots, M_p) \subseteq \mathscr{P}_p$ be the subset of those E which are *position level sets* of $(M_1, \ldots, M_p)$, i.e. such that $i_j = i_{j'}$ for $j, j' \in E$. Note that all singletons belong to $\mathscr{P}(M_1, \ldots, M_p) \subseteq \mathscr{P}_p$. For each position level set E of $(M_1, \ldots, M_p)$, let $s_1^E, \ldots, s_{\ell^E}^E$ be a finite number of generators of $\mathrm{Syz}((a_j)_{j \in E})$ as given by a certificate of coherence in $\mathbf{R}$; here $s_i^E = (s_{i,j}^E)_{j \in E}$. Let $M^E = \mathrm{lcm}(M_j \;;\, j \in E)$ and $S^E(a_1 M_1, \ldots, a_p M_p)$ be the list $S_1^E, \ldots, S_{\ell^E}^E$, where $S_i^E = (S_{i,1}^E, \ldots, S_{i,p}^E)$ with

$$S_{i,j}^E = \begin{cases} s_{i,j}^E \; M^E / M_j & \text{if } j \in E, \\ 0 & \text{otherwise.} \end{cases}$$

This is a syzygy for $(a_1 M_1, \ldots, a_p M_p)$: see Equation (1) below. Finally, let $S(a_1 M_1, \ldots, a_p M_p)$ be the concatenation of all the lists $S^E(a_1 M_1, \ldots, a_p M_p)$ when E ranges over the position level sets E of $(M_1, \ldots, M_p)$.

Example 3.2. Let $T_1 = (2X^2Y,\, 0) = 2M_1$, $T_2 = (XY^2,\, 0) = M_2$, $T_3 = (0,\, 4X) = 4M_3$ in $(\mathbb{Z}/8\mathbb{Z})[X,Y]^2$. We have $\mathscr{P}(M_1, M_2, M_3) = \{\{1\}, \{2\}, \{3\}, \{1,2\}\}$, $S_1^{\{1\}} = (4,0,0)$, $S_1^{\{2\}} = (0,0,0)$, $S_1^{\{3\}} = (0,0,2)$, $S_1^{\{1,2\}} = (Y, 6X, 0)$, and $\ell^{\{1\}} = \ell^{\{2\}} = \ell^{\{3\}} = \ell^{\{1,2\}} = 1$.

The following theorem generalises Gamanda, Lombardi, Neuwirth, and Yengui 2020, Theorem 4.5.

Proposition 3.3. *Discrete coherent context 1.2. The finite list* $S(a_1 M_1, \ldots, a_p M_p)$ *generates the syzygy module* $\mathrm{Syz}(a_1 M_1, \ldots, a_p M_p) \subseteq \mathbf{R}[\underline{X}]^p$.

Proof. Let us use the notation of Definition 3.1. We first check that each S_i^E is a syzygy for $(a_1 M_1, \ldots, a_p M_p)$:

$$S_{i,1}^E a_1 M_1 + \cdots + S_{i,p}^E a_p M_p = \sum\nolimits_{j \in E} s_{i,j}^E a_j M^E = \Big(\sum\nolimits_{j \in E} s_{i,j}^E a_j \Big) M^E = 0. \tag{1}$$

Conversely, let $\underline{g} = (g_1, \ldots, g_p) \in \mathrm{Syz}(a_1 M_1, \ldots, a_p M_p)$, not all g_j zero, let $L = L(\underline{g})$ be the leading monomial of the syzygy expression $g_1 a_1 M_1 + \cdots + g_p a_p M_p$, and let E be its leading monomial index set. We have $\sum_{j \in E} b_j a_j = 0$, and thus $(b_j)_{j \in E} = c_1 s_1^E + \cdots + c_{\ell^E} s_{\ell^E}^E$ for some $c_1, \ldots, c_{\ell^E} \in \mathbf{R}$. Let

$$\underline{g'} = (g_1', \ldots, g_p') = \underline{g} - \frac{L}{M^E} \sum\nolimits_{i=1}^{\ell^E} c_i S_i^E \in \mathrm{Syz}(a_1 M_1, \ldots, a_p M_p);$$

note that M^E divides L because every M_j, $j \in E$, does. We have $g'_j = g_j$ for $j \notin E$ and, for $j \in E$,

$$\begin{aligned} g'_j = g_j - \frac{L}{M^E} \sum_{i=1}^{\ell^E} c_i S^E_{i,j} &= g_j - \frac{L}{M^E} \sum_{i=1}^{\ell^E} c_i \frac{M^E}{M_j} s^E_{i,j} \\ &= g_j - \frac{L}{M_j} \sum_{i=1}^{\ell^E} c_i s^E_{i,j} = g_j - \frac{L}{M_j} b_j = g_j - \mathrm{LT}(g_j). \end{aligned}$$

Thus $L(\underline{g'}) < L(\underline{g})$. Reiterating this (with $\underline{g'}$ instead of $\underline{g}$), we reach the desired result after a finite number of steps since the set of monomials is well-ordered. □

Example 3.4 (Example 3.2 continued). In $(\mathbb{Z}/8\mathbb{Z})[X,Y]^2$, we have

$$\mathrm{Syz}(T_1, T_2, T_3) = \langle (4,0,0), (0,0,2), (Y, 6X, 0) \rangle.$$

Following in detail the first step in the preceding proof we add a useful corollary.

Proposition 3.5. *Discrete coherent context 1.2. Notation of Definition 3.1. Let*

$$u = \sum\nolimits_{j \in [\![1,p]\!]} g_j f_j, \quad L = \sup\nolimits_{j \in [\![1,p]\!]} N_j M_j, \quad \textit{and} \quad E = \{\, j \in [\![1,p]\!] \; ; \, N_j M_j = L \,\}.$$

If $\mathrm{LM}(u) < L$, *then the polynomials* $f_{p+1}, \dots, f_{p+\ell^E} \in \mathbf{R}[\underline{X}]$ *and terms* $g_{p+1}, \dots, g_{p+\ell^E} \in \mathbf{R}[\underline{X}]$ *defined by*

$$f_{p+i} = \sum\nolimits_{j \in E} S^E_{i,j} \, f_j \ \textit{ and } \ g_{p+i} = c_i \frac{L}{M^E}$$

are such that

- $u = \sum_{j \in [\![1,p+\ell^E]\!] \setminus E} g_j f_j$,
- *the leading monomial of the expression of* u *with respect to* $(f_j)_{j \in [\![1,p+\ell^E]\!] \setminus E}$ *is* $< L$.

Proof. As $\mathrm{LM}(u) < L$, the coefficient of L in $\sum_{j \in E} g_j f_j$ vanishes, so that $\sum_{j \in E} b_j a_j = 0$: we have

$$\begin{aligned} \sum\nolimits_{j \in E} g_j f_j = \sum\nolimits_{j \in E} \sum\nolimits_{1 \le i \le \ell^E} c_i s^E_{i,j} N_j f_j &= \sum\nolimits_{1 \le i \le \ell^E} c_i \sum\nolimits_{j \in E} S^E_{i,j} \frac{M_j N_j}{M^E} \, f_j \\ &= \sum\nolimits_{1 \le i \le \ell^E} g_{p+i} f_{p+i}, \end{aligned}$$

with

$$\mathrm{LM}(g_{p+i}) \, \mathrm{LM}(f_{p+i}) \le \frac{L}{M^E} \, \mathrm{LM} \Big(\sum\nolimits_{j \in E} S^E_{i,j} \, f_j \Big) < \frac{L}{M^E} M^E = L. \qquad \square$$

Syzygies of terms, examples in the case of an ideal

In this case, which is Discrete coherent context 1.2 with $m = 1$, every subset of $\mathscr{P}_p$ is a position level set.

Example 3.6. Let us consider the following syzygy of $(6XY^2, 15X^2YZ, 10Z^2)$ in $\mathbb{Z}[X, Y, Z]$:

$$\underline{g} = (g_1, g_2, g_3) = (5XZ + 10Z^2, -2Y + 2Z, -3X^2Y - 6XY^2).$$

Following the algorithm given in the proof of Proposition 3.3 and considering the graded monomial lexicographic order with $X > Y > Z$, we have $L(\underline{g}) = L = X^2Y^2Z$, $E = \{1, 2\}$, $\mathrm{Syz}(6, 15) = \langle s_1^E = \frac{1}{3}(-15, 6) = (-5, 2)\rangle$, $\ell^E = 1$, $M^E = X^2Y^2Z$, $S_1^E = (-5\frac{X^2Y^2Z}{XY^2}, 2\frac{X^2Y^2Z}{X^2YZ}, 0) = (-5XZ, 2Y, 0)$, $(b_1, b_2) = (5, -2) = (-1) \cdot s_1^E$, $\underline{g'} = (g'_1, g'_2, g'_3) = \underline{g} - \frac{L}{M^E}\sum_{i=1}^{\ell^E} c_i S_i^E = \underline{g} + \frac{X^2Y^2Z}{X^2Y^2Z} S_1^E = \underline{g} + (-5XZ, 2Y, 0) = (10Z^2, 2Z, -3X^2Y - 6XY^2) = (g_1 - \mathrm{LT}(g_1), g_2 - \mathrm{LT}(g_2), g_3)$, with $L(\underline{g'}) = L' = X^2YZ^2 < L(\underline{g})$.

Continuing with $\underline{g'}$, we obtain: $E' = \{2, 3\}$, $\mathrm{Syz}(15, 10) = \langle s_1^{E'} = \frac{1}{5}(-10, 15) = (-2, 3)\rangle$, $\ell_{E'} = 1$, $M_{E'} = X^2YZ^2$, $S_1^{E'} = (0, -2\frac{X^2YZ^2}{X^2YZ}, 3\frac{X^2YZ^2}{Z^2}) = (0, -2Z, 3X^2Y)$, $(b'_2, b'_3) = (2, -3) = (-1)\cdot s_1^{E'}$, $\underline{g''} = \underline{g'} - \frac{L'}{M_{E'}}\sum_{i=1}^{\ell_{E'}} c'_i S_i^{E'} = \underline{g'} + \frac{X^2YZ^2}{X^2YZ^2} S_1^{E'} = \underline{g'} + (0, -2Z, 3X^2Y) = (10Z^2, 0, -6XY^2) = (g'_1, g'_2 - \mathrm{LT}(g'_2), g'_3 - \mathrm{LT}(g'_3)) = -2S_1^{\{1,3\}}$. We conclude that

$$\underline{g} = -S_1^{\{1,2\}} - S_1^{\{2,3\}} - 2S_1^{\{1,3\}}.$$

Example 3.7. Let us consider the following syzygy of $(3XY, 3Y, X)$ in $\mathbb{Z}[X, Y]$:

$$\underline{g} = (g_1, g_2, g_3) = (2X + Y, -3X^2 + 2XY, 3XY - 9Y^2).$$

Following the algorithm given in the proof of Proposition 3.3 and considering the lexicographic monomial order with $X > Y$, we have $L(\underline{g}) = L = X^2Y$, $E = \{1, 2, 3\}$, $\mathrm{Syz}(3, 3, 1) = \langle s_1^E = (-1, 1, 0), s_2^E = (-1, 0, 3)\rangle$, $\ell^E = 2$, $M^E = XY$, $S_1^E = (-1, X, 0)$, $S_2^E = (-1, 0, 3Y)$, $(b_1, b_2, b_3) = (2, -3, 3) = -3s_1^E + s_2^E$, $(c_1, c_2) = (-3, 1)$, $\underline{g'} = (g'_1, g'_2, g'_3) = \underline{g} - \frac{L}{M^E}\sum_{i=1}^{\ell^E} c_i S_i^E = \underline{g} - \frac{X^2Y}{XY}(-3S_1^E + S_2^E) = \underline{g} - X(2, -3X, 3Y) = (Y, 2XY, -9Y^2) = (g_1 - \mathrm{LT}(g_1), g_2 - \mathrm{LT}(g_2), g_3 - \mathrm{LT}(g_3)) = 2YS_1^E - 3YS_2^E$, with $L(\underline{g'}) = XY^2 < L(\underline{g})$. We conclude that

$$\underline{g} = (-3X + 2Y)S_1^{\{1,2,3\}} + (X - 3Y)S_2^{\{1,2,3\}}.$$

S-lists and iterated S-lists, a fundamental theorem

Definition 3.8. Discrete coherent context 1.2. Let $f_1, \dots, f_p \in \mathbf{H}_n^m$ not all zero and consider their leading terms $a_1M_1, \dots, a_pM_p \in \mathbf{H}_n^m$.

If $S_1, \dots, S_\ell$ is the list of generators of $\mathrm{Syz}(\mathrm{LT}(f_1, \dots, f_p))$ computed in Proposition 3.3, the *S-list* of $f_1, \dots, f_p$ is

$$\mathscr{S}(f_1, \dots, f_p) = S_{1,1}f_1 + \cdots + S_{1,p}f_p, \dots, S_{\ell,1}f_1 + \cdots + S_{\ell,p}f_p.$$

By induction, we define the *iterated S-lists* by

- $\mathscr{S}^0(f_1, \dots, f_p) = f_1, \dots, f_p$;
- $\mathscr{S}^{q+1}(f_1, \dots, f_p)$ is the concatenation of $\mathscr{S}^q(f_1, \dots, f_p)$ with $\mathscr{S}(\mathscr{S}^q(f_1, \dots, f_p))$.

Note that each member of an iterated S-list is in $\langle f_1, \dots, f_p \rangle$.

Remark 3.9. If $\mathbf{R}$ is a Bézout ring then for any $a_1, \dots, a_q \in \mathbf{R}$ there exists a finite generating set for $\mathrm{Syz}(a_1, \dots, a_q)$ whose vectors have at most two nonzero components (see Proposition 2.4). Choose these generating sets of syzygies in $\mathbf{R}^q$. It follows that in the corresponding iterated S-lists of $f_1, \dots, f_p$ there are only S-pairs ($\#E = 2$) and auto-S-polynomials ($\#E = 1$), as expected. Similarly, if $\mathbf{R}$ is a Prüfer domain (e.g. $\mathbf{R} = \{f \in \mathbb{Q}[X] \ ; \ f(\mathbb{Z}) \subseteq \mathbb{Z}\}$, which has Krull dimension equal to 2, see Lombardi 2010, Ducos 2015), then for any $a_1, \dots, a_q \in \mathbf{R}$ there exists a finite generating set for $\mathrm{Syz}(a_1, \dots, a_q)$ whose vectors have at most two nonzero components: in fact, a Prüfer domain is locally a valuation domain (thus, locally a Bézout domain). So in the corresponding iterated S-lists of $f_1, \dots, f_p$ there are only S-pairs (the auto-S-polynomials vanish since the ring $\mathbf{R}$ is supposed to be integral). ■

Fundamental theorem 3.10. *Discrete coherent context 1.2. Let $f_1, \dots, f_p \in \mathbf{H}_n^m$ not all zero. For any $u \in \langle f_1, \dots, f_p \rangle$ there exists $q \in \mathbb{N}$ and items $p_1, \dots, p_t$ in the list $\mathscr{S}^q(f_1, \dots, f_p)$ such that $\mathrm{LT}(u) \in \langle \mathrm{LT}(p_1, \dots, p_t) \rangle$. In other words,*

$$\mathrm{MLT}(\langle f_1, \dots, f_p \rangle) = \bigcup_{q \in \mathbb{N}} \uparrow \langle \mathrm{LT}(\mathscr{S}^q(f_1, \dots, f_p)) \rangle.$$

Comment 3.11. Compared to Adams and Loustaunau 1994, Theorem 4.2.8, where the authors suppose that the base ring $\mathbf{R}$ is strongly discrete, coherent, and noetherian, in our Theorem 3.10 we suppose only that $\mathbf{R}$ is discrete and coherent. Moreover, we do not perform divisions. This could be useful when one tries to prove results on the structure of the leading terms ideals (see Ben Amor and Yengui 2021, Guyot and Yengui 2024, Yengui 2021a, 2022). However Theorem 3.10 does not give a termination condition when one knows that the leading terms ideal is finitely generated (such a condition is given in Theorem 5.1). Our Theorem 3.10 is also useful when the leading terms ideal is not finitely generated (see Example 3.13 (1) and the counterexample given in Yengui 2021a). ■

Proof. Write

$$u = \sum_{j=1}^{p} g_j f_j \text{ with } N_j = \mathrm{LM}(g_j) \text{ and } M_j = \mathrm{LM}(f_j). \tag{2}$$

So $\mathrm{LM}(u) \leq \sup_{1 \leq j \leq p}(N_j M_j) =: L$ (the leading monomial of the expression of u with respect to the generating set $\mathscr{S}^0(f_1, \ldots, f_p) = f_1, \ldots, f_p$).
Case 1. $\mathrm{LM}(u) = L$. Clearly, $\mathrm{LT}(u) \in \langle \mathrm{LT}(f_1, \ldots, f_p) \rangle$.
Case 2. $\mathrm{LM}(u) < L$. Let $E = \{ j \, ; \, N_j M_j = L \}$ and write

$$\begin{aligned} u &= \sum_{j \notin E} g_j f_j + \sum_{j \in E} g_j f_j \\ &= \sum_{j \notin E} g_j f_j + \sum_{j \in E} (g_j - \mathrm{LT}(g_j)) f_j + \sum_{j \in E} \mathrm{LT}(g_j) f_j. \end{aligned}$$

As the left hand side and the two first terms have leading monomials less than L, so does the third, that is, $\mathrm{LM}\left(\sum_{j \in E} \mathrm{LT}(g_j) f_j \right) < L$. Note that for every $j \in E$, we have $\mathrm{LM}(g_j)\,\mathrm{LM}(f_j) = L$.
By virtue of Proposition 3.5, we obtain another expression for $\sum_{j \in E} \mathrm{LT}(g_j) f_j$ and hence also for u:

$$u = \sum_{j \notin E} g_j f_j + \sum_{j \in E} \left(g_j - \mathrm{LT}(g_j) \right) f_j + \sum_{1 \leq i \leq \ell^E} g_{p+i} f_{p+i}$$

with f_{p+i} in $\mathscr{S}(f_1, \ldots, f_p)$, $g_{p+1}, \ldots, g_{p+\ell^E}$ terms in $\mathbf{R}[\underline{X}]$, and $\mathrm{LM}(g_{p+i})\,\mathrm{LM}(f_{p+i}) < L$. The leading monomial of this expression, now with respect to the generating set $\mathscr{S}^1(f_1, \ldots, f_p)$, is $< L$. Reiterating this, we end up with a situation like that of Case 1 because the set of monomials is well-ordered. So we reach the desired result after a finite number of steps. □

Remark 3.12. In the proof of Fundamental theorem 3.10 with $m = 1$, if the considered monomial order refines total degree (i.e. if $M > N$ whenever $\mathrm{tdeg}(M) > \mathrm{tdeg}(N)$), then, letting $d = \max_{1 \leq j \leq p}\big(\mathrm{tdeg}(g_j) + \mathrm{tdeg}(f_j)\big)$ and $\delta = \mathrm{tdeg}(u)$ (assumed ≥ 1), we have $q \leq \binom{n+d}{d} - \binom{n+\delta-1}{\delta-1}$ (the number of monomials in $X_1, \ldots, X_n$ of total degree at least δ and at most d). ■

Example 3.13. Let $\mathbf{V}$ be a nonarchimedean valuation domain, i.e. a valuation domain $\mathbf{V}$ such that there exist nonunits $a, b \in \mathbf{V}$ with a^q dividing b for every $q \in \mathbb{N}$.

(1) Let $f_1 = aX + 1$, $f_2 = b \in \mathbf{V}[X]$. Then $\mathrm{MLT}(\langle f_1, f_2 \rangle)$ is not finitely generated (see Yengui 2015, Example 253): $\mathrm{LT}(\mathscr{S}^q(f_1, f_2)) = \left\langle aX, b, \frac{b}{a}, \ldots, \frac{b}{a^q} \right\rangle$ and $\mathrm{MLT}(\langle f_1, f_2 \rangle) = \left\langle aX, b, \frac{b}{a}, \frac{b}{a^2}, \ldots \right\rangle$.

(2) Let $f_1 = a^2 + aXY$, $f_2 = bY^2 \in \mathbf{V}[X,Y]$. We have

$$\begin{aligned}\left\langle \mathrm{LT}(\mathscr{S}^0(f_1,f_2)\right\rangle = aY\left\langle X, \frac{b}{a}Y\right\rangle \subsetneq \left\langle \mathrm{LT}(\mathscr{S}^1(f_1,f_2)\right\rangle = aY\left\langle X, \frac{b}{a}Y, b\right\rangle \\ \subsetneq \left\langle \mathrm{LT}(\mathscr{S}^2(f_1,f_2)\right\rangle = \langle aXY, bY^2, abY, a^2b\rangle = \mathrm{MLT}(\langle f_1,f_2\rangle).\end{aligned}$$

Corollary 3.14. *Discrete coherent context 1.2. Let $I = \langle f_1,\ldots,f_p\rangle$ be a nonzero finitely generated submodule of $\mathbf{H}_n^m$. Suppose that $\mathrm{MLT}(I)$ is finitely generated, i.e. that there exist $u_1,\ldots,u_t \in I$ such that $\mathrm{LT}(I) = \langle \mathrm{LT}(u_1,\ldots,u_t)\rangle$. Then there exists $q \in \mathbb{N}$ such that $\mathrm{MLT}(I) = \langle \mathrm{LT}(\mathscr{S}^q(f_1,\ldots,f_p))\rangle$.*

Remark 3.15. In Corollary 3.14 with $m = 1$, if the considered monomial order refines total degree, then, writing $u_k = \sum_{j=1}^p g_{k,j} f_j$ with $g_{k,j} \in \mathbf{R}[\underline{X}]$ and letting $d = \max_{1\le k\le t, 1\le j\le p}(\mathrm{tdeg}(g_{k,j}) + \mathrm{tdeg}(f_j))$ and $\delta = \min_{1\le k\le t} \mathrm{tdeg}(u_k)$ (assumed to be ≥ 1), we have $q \le \binom{n+d}{d} - \binom{n+\delta-1}{\delta-1}$. ■

4 Basic algorithms

The division algorithms

These algorithms in General context 1.1 need $\mathbf{R}$ to be strongly discrete; note that coherence is not used here. We present two algorithms, one for Simple division context 1.4 and another one for Division with remainder context 1.5.

Like the classical division algorithm for $\mathbf{F}[\underline{X}]^m$ with $\mathbf{F}$ a discrete field (see Yengui 2015, Algorithm 211), these algorithms have the following goal.

Input $u \in \mathbf{H}_n^m$, $h_1,\ldots,h_p \in \mathbf{H}_n^m \setminus \{0\}$.
Output $q_1,\ldots,q_p \in \mathbf{R}[\underline{X}]$ and $r \in \mathbf{H}_n^m$ such that

$$\begin{cases} u = q_1h_1 + \cdots + q_ph_p + r, \\ \mathrm{LM}(u) \geq \mathrm{LM}(q_j)\,\mathrm{LM}(h_j) \text{ whenever } q_j \neq 0, \\ T \notin \langle \mathrm{LT}(h_1,\ldots,h_p)\rangle \text{ for each term } T \text{ of } r. \end{cases}$$

Definition 4.1. The vector r is called *a remainder of u on division by the list $H = h_1,\ldots,h_p$* and is denoted by $r = \overline{u}^H$.

Algorithms 4.2 and 4.3 provide a suitable answer: a suitable remainder r and suitable quotients q_j. Nevertheless, there are a priori many different possible answers.

For the definition of the leading monomial $\mathrm{LM}(f)$ and of the divisibility $M \mid N$ in the case of monomials, see Definition 2.2.

Division algorithm 4.2 (Simple division context 1.4).

Division $(u, h_1, \ldots, h_p)$
local variables $j : [\![1,p]\!]$, D : subset of $[\![1,p]\!]$,
$c, c_1, \ldots, c_p, a_1, \ldots, a_p : \mathbf{R}$, $u', M, M_1, \ldots, M_p : \mathbf{H}_n^m$;
$r \leftarrow 0$; $u' \leftarrow u$;
for j **from** 1 **to** p **do**
  $q_j \leftarrow 0$; $M_j \leftarrow \mathrm{LM}(h_j)$; $c_j \leftarrow \mathrm{LC}(h_j)$ **od** ;
while $u' \neq 0$ **do**
  $M \leftarrow \mathrm{LM}(u')$; $c \leftarrow \mathrm{LC}(u')$; $D \leftarrow \{\, j \,;\, M_j \mid M \,\}$;
  if $c \in \langle c_j ; j \in D \rangle$ **then**
    find $(a_j)_{j \in D}$ **such that** $\sum_{j \in D} a_j c_j = c$;
    $u' \leftarrow u' - \sum_{j \in D} a_j (M/M_j) h_j$;
    for $j \in D$ **do** $q_j \leftarrow q_j + a_j (M/M_j)$ **od** ;
  else
    $r \leftarrow r + \mathrm{LT}(u')$; $u' \leftarrow u' - \mathrm{LT}(u')$;
  fi
od ;
return $(r, q_1, \ldots, q_p)$;

One sees easily by induction that $\mathrm{LM}(q_j)\,\mathrm{LM}(h_j) \leq \mathrm{LM}(u)$ and $u = q_1 h_1 + \cdots + q_p h_p + r$ at the end.

Division algorithm 4.3 (Division with remainder context 1.5).

Division2 $(u, h_1, \ldots, h_p)$
local variables $j : [\![1,p]\!]$, D : subset of $[\![1,p]\!]$,
$c, r_0, c_1, \ldots, c_p, a_1, \ldots, a_p : \mathbf{R}$, $u', M, M_1, \ldots, M_p : \mathbf{H}_n^m$;
$r \leftarrow 0$; $u' \leftarrow u$;
for j **from** 1 **to** p **do**
  $q_j \leftarrow 0$; $M_j \leftarrow \mathrm{LM}(h_j)$; $c_j \leftarrow \mathrm{LC}(h_j)$;
od ;
while $u' \neq 0$ **do**
  $M \leftarrow \mathrm{LM}(u')$; $c \leftarrow \mathrm{LC}(u')$; $D \leftarrow \{\, j \,;\, M_j \mid M \,\}$;
  $(r_0, (a_j)_{j \in D}) \leftarrow \mathsf{Rem}(c, (c_j)_{j \in D})$;
  $u' \leftarrow u' - \sum_{j \in D} a_j (M/M_j) h_j - r_0\,\mathrm{LM}(u')$; $r \leftarrow r + r_0\,\mathrm{LM}(u')$;
  for $j \in D$ **do** $q_j \leftarrow q_j + a_j (M/M_j)$ **od** ;
od ;
return $(r, q_1, \ldots, q_p)$

Syzygy algorithms

Notation 4.4. We denote by List(A) the set of (finite) lists of elements of A.

These algorithms take place in Discrete coherent context 1.2. They are a key tool for constructing a Gröbner basis and have been introduced by Buchberger (1965) for the case where the base ring is a discrete field.

We begin with the basic syzygy algorithm giving $S^E(a_1M_1, \dots, a_pM_p) = S_1^E, \dots, S_\ell^E$ for $a_1M_1, \dots, a_pM_p \in \mathbf{H}_n^m$ and a subset $E \subseteq \mathscr{P}(M_1, \dots, M_p)$ (see Definition 3.1). Let us recall that $\mathbf{H}_n^m = \mathbf{R}[\underline{X}]$ if $m = 1$.

Input $a_1M_1, \dots, a_pM_p$ terms in $\mathbf{H}_n^m$, $E \subseteq \mathscr{P}(M_1, \dots, M_p)$.
Output A list of syzygies $S_1^E, \dots, S_\ell^E$ for $(a_1M_1, \dots, a_pM_p)$ such that, writing $S_i^E = (S_{i,j}^E)_{j \in [\![1,p]\!]}$, we have $S_{i,j}^E = 0$ for $j \notin E$ and, for every syzygy $(g_j)_{j \in [\![1,p]\!]}$ with leading monomial index set E with respect to $a_1M_1, \dots, a_pM_p$, $(\mathrm{LT}(g_j))_{j \in E} \in \langle (S_{1,j}^E)_{j \in E}, \dots, (S_{\ell,j}^E)_{j \in E} \rangle$.

Basic syzygy algorithm for terms 4.5 (Basic syzygies of terms, Discrete coherent context 1.2, Definition 3.1)**.**

BasicSyzygiesOfTerms$(a_1M_1, \dots, a_pM_p, E)$
local variables $j : [\![1,p]\!]$, $\ell, i : \mathbb{N}$, $s_1, \dots, s_\ell : \mathbf{R}^E$, $M^E : \mathbf{H}_n^m$;
find $\ell \in \mathbb{N}$ and $s_1, \dots, s_\ell \in \mathbf{R}^E$ **such that** $\mathrm{Syz}((a_j)_{j \in E}) = \langle s_1, \dots, s_\ell \rangle$;
for i **from** 1 **to** ℓ **do**
  for j **from** 1 **to** p **do**
    $M^E \leftarrow \mathrm{lcm}(M_j \,;\, j \in E)$;
    if $j \in E$ **then** $S_{i,j}^E \leftarrow s_{i,j}(M^E/M_j)$ **else** $S_{i,j}^E \leftarrow 0$ **fi**
  od ;
od ;
return $(S_{1,j}^E)_{j \in [\![1,p]\!]}, \dots, (S_{\ell,j}^E)_{j \in [\![1,p]\!]}$;

We now give an algorithm whose goal is to provide a generating set of syzygies for a vector of terms in $\mathbf{H}_n^m$; see Definition 3.1 and Proposition 3.3.

Input $a_1M_1 = a_1e_{i_1}M_1', \dots, a_pM_p = a_pe_{i_p}M_p'$ terms in $\mathbf{H}_n^m$.
Output a list of lists of syzygies $S_i^E \in \mathbf{R}[\underline{X}]^p$ such that the S_i^E's generate $\mathrm{Syz}(a_1M_1, \dots, a_pM_p)$.

In the algorithm, we construct the syzygies S_i^E by successive concatenations of the lists obtained by the previous algorithm.

Syzygy algorithm for terms 4.6 (Syzygies of terms, Discrete coherent context 1.2, see Definition 3.1)**.**

SyzygiesOfTerms ($a_1M_1, \dots, a_pM_p$)
local variables E : subset of $[\![1,p]\!]$, S^E : $\mathrm{List}(\mathbf{R}[\underline{X}]^p)$;
$S \leftarrow$;
for $E \in \mathscr{P}(M_1, \dots, M_p)$ **do**
  $S^E \leftarrow$ BasicSyzygiesOfTerms ($a_1M_1, \dots, a_pM_p, E$)
  $S \leftarrow S, S^E$
od ;
return S ;

In the case of an ideal ($m = 1$), one may forget about the basis vectors $e_{i_1}, \dots, e_{i_p}$ and one has $\mathscr{P}(M_1, \dots, M_p) = \mathscr{P}_p$.

S-list algorithms

We have the following goal corresponding to the S-list $\mathscr{S}(f_1, \dots, f_p)$ in Definition 3.8 (Discrete coherent context 1.2).

Input $f_1, \dots, f_p \in \mathbf{H}_n^m$ not all zero,
Output $\mathscr{S}(f_1, \dots, f_p)$ in $\langle f_1, \dots, f_p \rangle$ as in Definition 3.8.

S-list algorithm 4.7 (First S-list algorithm, Discrete coherent context 1.2, Definition 3.8)**.**

FirstSlist ($f_1, \dots, f_p$)
local variables $Si, Ss : \mathbf{R}[\underline{X}]^p$;
$Slist \leftarrow$;
$S \leftarrow$ SyzygiesOfTerms ($\mathrm{LT}(f_1, \dots, f_p)$) ;
for Si **in** S **do**
  $Ss \leftarrow Si_1 f_1 + \cdots + Si_p f_p$;
  if $Ss \neq 0$ **do** $Slist \leftarrow Slist, Ss$ **fi**
od ;
return $Slist$;

hum: `Le test` $Ss \neq 0$ `est-il important ? Il n'est pas spécifié dans Definition 3.8 !`

We have the following goal corresponding to the S-list $\mathscr{S}^q(f_1, \dots, f_p)$ in Definition 3.8 (Discrete coherent context 1.2.)

Input $q \in \mathbb{N}$, $f_1, \dots, f_p \in \mathbf{H}_n^m$ not all zero,
Output $\mathscr{S}^q(f_1, \dots, f_p)$ in $\langle f_1, \dots, f_p \rangle$ as in Definition 3.8.

S-list algorithm 4.8 (Iterated S-list algorithm: Discrete coherent context 1.2, Definition 3.8)**.**

IteratedSlist ($q, f_1, \ldots, f_p$)
local variables r : $\mathbb{N}$, $Si, Ss : \mathbf{R}[\underline{X}]^p$, $ItSlist : \mathrm{List}(\mathbf{R}[\underline{X}]^p)$;
$ItSlist \leftarrow f_1, \ldots, f_p$;
for r **from** 1 **to** q **do**
    $ItSlist \leftarrow ItSlist$, FirstSlist ($ItSlist$)
od ;
return $ItSlist$;

Rewriting algorithms

The next algorithm corresponds to Proposition 3.5.

Input $f_1, \ldots, f_p \in \mathbf{H}_n^m$ not all zero, with $\mathrm{LC}(f_j) = a_j$ and $\mathrm{LM}(f_j) = M_j$, $g_1, \ldots, g_p \in \mathbf{R}[\underline{X}]$ with $\mathrm{LC}(g_j) = b_j$ and $\mathrm{LM}(g_j) = N_j$, such that the leading monomial L of the expression $\sum_{j=1}^{p} g_j f_j = u$ with respect to $f_1, \ldots, f_p$ (let E be the corresponding leading monomial index set) is $> \mathrm{LT}(u)$.

Output $f_{p+1}, \ldots, f_{p+\ell^E}$ in $\langle f_1, \ldots, f_p \rangle \subseteq \mathbf{H}_n^m$ and terms $g_{p+1}, \ldots, g_{p+\ell^E} \in \mathbf{R}[\underline{X}]$ such that each $f_{p+i} \in \mathscr{S}(f_1, \ldots, f_p)$, $u = \sum_{j \in [\![1,p+\ell^E]\!] \setminus E} g_j f_j$ and the leading monomial of this expression of u with respect to $(f_j)_{j \in [\![1,p+\ell^E]\!] \setminus E}$ is $< L$. In fact, the output is a list of pairs of the same pattern as the input.

Rewriting algorithm 4.9 (Rewriting a linear combination: Discrete coherent context 1.2, Proposition 3.5)**.**

Rewriting ($(g_j, f_j)_{j \in [\![1,p]\!]}$)
local variables $j : [\![1,p]\!]$, $k, \ell, i : \mathbb{N}$, E : subset of $[\![1,p]\!]$, $N_1, \ldots, N_p : \mathbf{R}[\underline{X}]$,
    $L, M^E, M_1, \ldots, M_p : \mathbf{H}_n^m$, $c_1, \ldots, c_\ell : \mathbf{R}$, $s_1, \ldots, s_\ell : \mathbf{R}^E$,
    $(S^E_{1,j})_{j \in [\![1,p]\!]}, \ldots, (S^E_{\ell,j})_{j \in [\![1,p]\!]} : \mathbf{R}[\underline{X}]^p$;
for $j \in [\![1,p]\!]$ **do**
    $a_j \leftarrow \mathrm{LC}(f_j)$; $M_j \leftarrow \mathrm{LM}(f_j)$; $b_j \leftarrow \mathrm{LC}(g_j)$; $N_j \leftarrow \mathrm{LM}(g_j)$ **od** ;
    $L = \sup\{ N_j M_j \; ; 1 \leq j \leq p \}$; $E = \{ j \in [\![1,p]\!] \; ; N_j M_j = L \}$;
    $M^E = \mathrm{lcm}(M_j \; ; j \in E)$;
$k \leftarrow 0$; **for** $j \in [\![1,p]\!] \setminus E$ **do** $k \leftarrow k+1$; $g'_k = g_j$; $f'_k \leftarrow f_j$; **od** ;
$(S^E_{1,j})_{j \in [\![1,p]\!]}, \ldots, (S^E_{\ell,j})_{j \in [\![1,p]\!]} \leftarrow$ BasicSyzygiesOfTerms ($a_1 M_1, \ldots, a_p M_p, E$)
for $i \in [\![1,\ell]\!]$ **do**
    $s_i \leftarrow (\mathrm{LC}(S^E_{i,j}))_{j \in E}$ **od** ;
find $(c_i)_{i \in [\![1,\ell]\!]}$ **such that** $(b_j)_{j \in E} = \sum_{i \in [\![1,\ell]\!]} c_i s_i$;

for $i \in [\![1,\ell]\!]$ **do**
  $g'_{k+i} \leftarrow c_i \frac{L}{M^E}$; $f'_{k+i} \leftarrow \sum_{j\in E} S^E_{i,j} f_j$ **od** ;
return $(g'_i, f'_i)_{i\in[\![1,k+\ell]\!]}$;

We have the following goal corresponding to Fundamental theorem 5.1 in Discrete coherent context 1.2. This is an iteration of the previous one. We add an information concerning q for $\mathscr{S}^q$.

Input $f_1, \dots, f_p \in \mathbf{H}_n^m \setminus \{0\}$, $g_1, \dots, g_p \in \mathbf{R}[\underline{X}]$; we let $u = \sum_{j=1}^p g_j f_j$.
Output $q \in \mathbb{N}$ and $h_1, \dots, h_\ell \in \mathscr{S}^q(f_1, \dots, f_p)$ such that $\mathrm{LT}(u) \in \langle \mathrm{LT}(h_1, \dots, h_\ell)\rangle$.

Rewriting algorithm 4.10 (Iterated rewriting of a linear combination: Discrete coherent context 1.2, Fundamental theorem 5.1)**.**

FullRewriting($(g_j, f_j)_{j\in[\![1,p]\!]}$)
local variables $L, M_0, f : \mathbf{H}_n^m$; $g : \mathbf{R}[\underline{X}]$, $S : \mathrm{List}(\mathbf{R}[\underline{X}] \times \mathbf{H}_n^m)$;
$M_0 \leftarrow \mathrm{LM}(\sum_{j\in[\![1,p]\!]} g_j f_j)$; $q \leftarrow 0$; $S \leftarrow (g_j, f_j)_{j\in[\![1,p]\!]}$;
while $M_0 < \sup\{\, \mathrm{LM}(g)\,\mathrm{LM}(f) \;;\; (g, f)$ in $S \,\}$ **do**
  $S \leftarrow$ Rewriting(S); $q \leftarrow q + 1$ **od** ;
return q, S ;

5 Buchberger's algorithm

The proof of the following theorem parallels exactly the proof of the analogue Theorem 4.2.3 in Adams and Loustaunau 1994.

Fundamental theorem 5.1. *Strongly discrete coherent context 1.3.*

(1) Buchberger's criterion. *Let $f_1, \dots, f_p \in \mathbf{H}_n^m$ not all zero, and denote by $S_1, \dots, S_\ell$ the generators of* $\mathrm{Syz}(\mathrm{LT}(f_1, \dots, f_p))$ *computed in Proposition 3.3. Then $G = f_1, \dots, f_p$ is a Gröbner basis for $\langle f_1, \dots, f_p\rangle$ if and only if for every $1 \le i \le \ell$, we have*

$$\overline{S_{i,1} f_1 + \cdots + S_{i,p} f_p}^{G} = 0.$$

(2) Buchberger's algorithm works. *Let $g_1, \dots, g_q \in \mathbf{H}_n^m \setminus \{0\}$ and $M = \langle g_1, \dots, g_q\rangle$. If the module of leading terms* $\mathrm{MLT}(M)$ *of the module M is finitely generated, the (generalised) Buchberger algorithm 5.2 computes a Gröbner basis for $\langle g_1, \dots, g_q\rangle$.*

The (generalised) Buchberger algorithm has the following goal.

Input $g_1, \dots, g_q \in \mathbf{H}_n^m \setminus \{0\}$.
Output a Gröbner basis $g_1, \dots, g_q, \dots, g_t$ for $\langle g_1, \dots, g_q\rangle$.

Buchberger's algorithm 5.2.

```
Buchberger(g_1, ..., g_q)
local variables S : List(H_n^m); f : H_n^m; L : List(R[X]);
G ← g_1, ..., g_q;
repeat
   S ← 𝒮(G);
   for f in S do
      (f, L) ← Division(f, G);
      if f ≠ 0 then replace f by FullRewriting else delete f fi;
   od;
   if S ≠ ∅ then G ← G, S fi;
until S = ∅;
return G;
```

Remark 5.3. If the algorithm terminates, then we can transform the obtained Gröbner basis into a Gröbner basis $h_1, \dots, h_{p'}$ such that no term of an element h_ℓ lies in $\langle \mathrm{LT}(h_k) \; ; \; k \neq \ell \rangle$ by replacing each element of the Gröbner basis with a remainder of it on division by the other nonzero elements and by repeating this process until it stabilises. Such a Gröbner basis is called a *pseudo-reduced Gröbner basis*. ■

6 Schreyer's syzygy algorithm

Definition 6.1 (Schreyer's monomial order)**.** Let $\mathbf{R}$ be a discrete ring. Consider a list $G = g_1, \dots, g_p$ in $\mathbf{H}_n^m \setminus \{0\}$ and the finitely generated submodule $U = \langle g_1, \dots, g_p \rangle = \mathbf{R}[\underline{X}]g_1 + \cdots + \mathbf{R}[\underline{X}]g_p$ of $\mathbf{H}_n^m$. Let $(\epsilon_1, \dots, \epsilon_p)$ be the canonical basis of $\mathbf{R}[\underline{X}]^p$. *Schreyer's monomial order induced by* $>$ *and* $g_1, \dots, g_p$ on $\mathbf{R}[\underline{X}]^p$ is the order denoted by $>_{g_1,\dots,g_p}$, or again by $>$, defined as follows:

$$\underline{X}^\alpha \epsilon_\ell > \underline{X}^\beta \epsilon_k \quad \text{if} \quad \left| \begin{array}{l} \text{either } \mathrm{LM}(\underline{X}^\alpha g_\ell) > \mathrm{LM}(\underline{X}^\beta g_k) \\ \text{or both } \mathrm{LM}(\underline{X}^\alpha g_\ell) = \mathrm{LM}(\underline{X}^\beta g_k) \text{ and } \ell < k. \end{array} \right.$$

Schreyer's monomial order is defined on $\mathbf{R}[\underline{X}]^p$ in the same way as when $\mathbf{R}$ is a discrete field (see Ene and Herzog 2012, p. 66).

Now we shall follow closely the ingenious proof by Schreyer (1980) of Hilbert's syzygy theorem via Gröbner bases, but with a strongly discrete coherent ring instead of a field. Schreyer's proof is very well explained in Ene and Herzog 2012, §§ 4.4.1–4.4.3.

The following syzygy algorithm à la Schreyer takes also place in Strongly discrete coherent context 1.3 for $\mathbf{R}$. It has the following goal.

Input a Gröbner basis $g_1, \ldots, g_p$ for a submodule of $\mathbf{H}_n^m$.
Output a Gröbner basis $(u_i^E)_{E \in \mathscr{P}(\mathrm{LM}(g_1),\ldots,\mathrm{LM}(g_p)),1 \leq i \leq \ell^E}$ for $\mathrm{Syz}(g_1, \ldots, g_p)$ with respect to Schreyer's monomial order induced by $>$ and $g_1, \ldots, g_p$.

Schreyer's syzygy algorithm 6.2.

1 **local variables** $Slist$, Si^E, $q_\ell : \mathbf{R}[\underline{X}]$;
2 $Slist \leftarrow$ FirstSlist$(g_1, \ldots, g_p)$
3 **for** S^E **in** $Slist$ **do**
4   **for** S_i^E **in** S^E **do**
5   **compute** $q_1, \ldots, q_p$ **such that**
6         $S_{i,1}^E g_1 + \cdots + S_{i,p}^E g_p = q_1 g_1 + \cdots + q_p g_p$ **by** Algorithm 4.2 (note that
7             $\mathrm{LM}(S_{i,1}^E g_1 + \cdots + S_{i,p}^E g_p) \geq \mathrm{LM}(q_\ell g_\ell)$ whenever $q_\ell g_\ell \neq 0$);
8         $u_i^E \leftarrow S_{i,1}^E \epsilon_1 + \cdots + S_{i,p}^E \epsilon_p - q_1 \epsilon_1 - \cdots - q_p \epsilon_p$
9   **od**
10 **od**

Note that the polynomials $q_1, \ldots, q_p$ of lines 5–7 may have been computed while constructing the Gröbner basis.

Remark 6.3. For an arbitrary system of generators $h_1, \ldots, h_p$ for a submodule U of $\mathbf{H}_n^m$, the syzygy module of $h_1, \ldots, h_p$ is easily obtained from the syzygy module of a Gröbner basis for U (see Yengui 2015, Theorem 296). ■

Fundamental theorem 6.4 (Schreyer's algorithm for a strongly discrete coherent ring)**.** *Strongly discrete coherent context 1.3. Let U be a submodule of $\mathbf{H}_n^m$ with Gröbner basis $g_1, \ldots, g_p$. Then the relations u_i^E computed by Schreyer's syzygy algorithm 6.2 form a Gröbner basis for the syzygy module* $\mathrm{Syz}(g_1, \ldots, g_p)$ *with respect to Schreyer's monomial order induced by $>$ and $g_1, \ldots, g_p$. Moreover, for E an position level subset of $[\![1, p]\!]$ and $1 \leq i \leq \ell^E$,*

$$\mathrm{LT}(u_i^E) = s_{i,r}^E \; M^E/M_r \; \epsilon_r \text{ with } r = \min\{\, j \in E \; ; \; s_{i,j}^E \neq 0 \,\}. \tag{3}$$

Schreyer's monomial order is a tailor-made term over position monomial order which changes at each iteration, i.e. after each computation of a Gröbner basis of the syzygy module of the considered Gröbner basis. Schreyer's trick is, for $v = \sum_{k=1}^p v_k \epsilon_k \in \mathrm{Syz}(g_1, \ldots, g_p)$, to prioritise (by deciding that they are greater) the $\mathrm{LM}(v_\ell \epsilon_\ell)$ such that $\mathrm{LM}(v_\ell \epsilon_\ell) = \max\{\mathrm{LM}(v_1 g_1), \ldots, \mathrm{LM}(v_p g_p)\}$, and to order the obtained generators $u_1, \ldots, u_t$ of $Syz(g_1, \ldots, g_p)$ in such a way that X_n does not appear in the leading terms of the u_i (when computing a Gröbner basis for the first syzygy module), and to iterate this process until exhausting all the X_i from the leading terms of the Gröbner basis of the syzygy module. Once we reach this situation, we continue the resolution over the base ring $\mathbf{R}$.

hum: `expliquer que la base des epsilon change à chaque étape`

`dire que la longueur des résolutions libres finies augmente de` n `en passant de` R `à` $R[X_1, \ldots, X_n]$

`les exemples donnés dans les corolaires sont trop restrictifs on doit citer le cas d'un anneau R où les idéaux de type fini ont tous une résolution projective finie et celui où la longueur de cette résolution est bornée indépendamment de l'idéal`

Proof (a slight modification of the proof of Ene and Herzog 2012, Theorem 4.16). Let us use the notation of Schreyer's syzygy algorithm 6.2. Recall that $u_i^E = (S_{i,k}^E - q_k)_{1 \le k \le p}$, with $\sum_{k=1}^p S_{i,k}^E g_k = \sum_{s=1}^p q_s g_s$, and $\mathrm{LM}(q_s g_s) \le \mathrm{LM}(\sum_{k=1}^p S_{i,k}^E g_k) < \mathrm{LM}(g_j)(M^E/M_j) = M^E$ for any $j \in E$. So $\mathrm{LT}(u_i^E) = \mathrm{LT}(S_i^E) = s_{i,r}^E\ M^E/M_r\ \epsilon_r$ where $r = \min\{\, j \in E\ ;\ s_{i,j}^E \neq 0\,\}$.

Let us show now that the relations u_i^E form a Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, \ldots, g_p)$. For this, let $v = \sum_{k=1}^p v_k \epsilon_k \in \mathrm{Syz}(g_1, \ldots, g_p)$ and let us show that $\mathrm{LT}(v) \in \langle\, \mathrm{LT}(u_i^E)\ ;\ E \in \mathscr{P}(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_p)), 1 \le i \le \ell^E\,\rangle$. Let us write $\mathrm{LM}(v_k \epsilon_k) = N_k \epsilon_k$ and $\mathrm{LC}(v_k \epsilon_k) = c_k$ for $1 \le k \le p$. Then $\mathrm{LM}(v) = N_j \epsilon_j$ for some $1 \le j \le p$. Now let $v' = \sum_{k \in \mathcal{S}} c_k N_k \epsilon_k$, where $\mathcal{S}$ is the set of those k for which $N_k\,\mathrm{LM}(g_k) = N_j\,\mathrm{LM}(g_j)$. By definition of Schreyer's monomial order, we have $k \ge j$ for all $k \in \mathcal{S}$. Substituting each ϵ_k in v' by $T_k = \mathrm{LT}(g_k)$, the sum becomes zero. Therefore v' is a relation of the terms T_k with $k \in \mathcal{S}$. By virtue of Proposition 3.3, v' is a linear combination of elements in $S((T_k)_{k \in \mathcal{S}})$ of the form S_i^E with $E \subseteq \mathcal{S}$ and $1 \le i \le \ell^E$. By inspecting the j^{th} component of v', we deduce that there exist $w_1, \ldots, w_t \in \mathbf{R}[\underline{X}]$, position level subsets $E_1, \ldots, E_t$ of $\mathcal{S}$ with $j \in E_1 \cap \cdots \cap E_t$, nonnegative integers $1 \le i_1 \le \ell_{E_1}, \ldots, 1 \le i_t \le \ell_{E_t}$, such that $c_j N_j = w_1 s_{E_1,i_1,j} M_{E_1}/M_j + \cdots + w_t s_{E_t,i_t,j} M_{E_t}/M_j$, and $s_{E_1,i_1,j} \neq 0, \ldots, s_{E_t,i_t,j} \neq 0$. As $k > j$ for all $k \in \mathcal{S}$ with $k \neq j$, it follows that $\mathrm{LT}(v') \in \langle \mathrm{LT}(S_{E_1,i_1}, \ldots, S_{E_t,i_t}) \rangle$. The desired result follows since $\mathrm{LT}(v) = \mathrm{LT}(v')$ and $\mathrm{LT}(u_i^E) = \mathrm{LT}(S_i^E)$. □

As a consequence of Theorem 6.4, we obtain the following constructive versions of Hilbert's syzygy theorem for a strongly discrete coherent ring.

Theorem 6.5 (Syzygy theorem for a strongly discrete coherent ring)**.** *Let* $\mathbf{R}$ *be a strongly discrete coherent ring,* $\mathbf{H}_n^m$ *a free* $\mathbf{R}[\underline{X}]$*-module with basis* $(e_1, \ldots, e_m)$*, and* $>$ *a monomial order on* $\mathbf{H}_n^m$*. Let* U *be a finitely generated submodule of* $\mathbf{H}_n^m$ *such that*

MLT(U) *is finitely generated according to some monomial order. Then* $M = \mathbf{H}_n^m/U$ *admits an* $\mathbf{R}[\underline{X}]$*-resolution*

$$0 \to F_p/\mathcal{S} \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

such that $p \leq n+1$*,* $F_0, \ldots, F_p$ *are finitely generated free* $\mathbf{R}[\underline{X}]$*-modules, and* $\mathcal{S}$ *is generated by finitely many iterated syzygies whose leading terms with respect to Schreyer's induced monomial order do not depend on the indeterminates* $X_n, \ldots, X_1$*.*

Proof. Let $(g_1, \ldots, g_s)$ be a Gröbner basis for U with respect to the considered order. We can reorder the g_i's so that whenever $\mathrm{LM}(g_i)$ and $\mathrm{LM}(g_j)$ involve the same basis element for some $i < j$, say $\mathrm{LM}(g_i) = N_i\epsilon_k$ and $\mathrm{LM}(g_j) = N_j\epsilon_k$, then $\deg_{X_n}(N_i) \geq \deg_{X_n}(N_j)$. It follows that the indeterminate X_n cannot appear in the leading terms of the u_i^E computed by Schreyer's syzygy algorithm 6.2. Thus, after at most n computations of the iterated syzygies, we reach the desired situation. □

Corollary 6.6 (Syzygy theorem for a Bézout domain with a divisibility test, Gamanda, Lombardi, Neuwirth, and Yengui 2020, Theorem 6.2)**.** *Let* $M = \mathbf{H}_n^m/U$ *be a finitely presented* $\mathbf{R}[\underline{X}]$*-module, where* $\mathbf{R}$ *is a Bézout domain with a divisibility test. Assume that* MLT(U) *is finitely generated according to some monomial order. Then* M *admits a finite free* $\mathbf{R}[\underline{X}]$*-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n+1$*.*

Corollary 6.7 (Syzygy theorem for a one-dimensional Bézout domain with a divisibility test, Gamanda, Lombardi, Neuwirth, and Yengui 2020, Corollary 6.3)**.** *Let* $M = \mathbf{H}_n^m/U$ *be a finitely presented* $\mathbf{R}[\underline{X}]$*-module, where* $\mathbf{R}$ *is a one-dimensional Bézout domain with a divisibility test. Then* M *admits a finite free* $\mathbf{R}[\underline{X}]$*-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n+1$*.*

References

William W. Adams and Philippe Loustaunau. *An introduction to Gröbner bases.* American Mathematical Society, Providence, 1994. (pp. 2, 4, 11, and 18)

Faten Ben Amor and Ihsen Yengui. The trailing terms ideal. *J. Algebra Appl.*, 20(9): Paper No. 2150153, 6, 2021. doi:10.1142/S021949882150153X. (p. 11)

Errett Bishop. *Foundations of constructive analysis.* McGraw-Hill, New York, 1967. (p. 2)

Errett Bishop and Douglas Bridges. *Constructive analysis.* Grundlehren der mathematischen Wissenschaften, 279. Springer-Verlag, Berlin, 1985. (p. 2)

Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D. thesis, Mathematisches Institut, Universität Innsbruck, 1965. Translation by Michael P. Abramson: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *J. Symbolic Comput.*, 41(3–4):475–511, 2006. doi:10.1016/j.jsc.2005.09.007. (p. 15)

David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry.* Graduate Texts in Mathematics, 185. Springer, New York, second edition, 2005. (p. 4)

Gema-Maria Díaz-Toca, Henri Lombardi, and Claude Quitté. *Modules sur les anneaux commutatifs: cours et exercices.* Calvage & Mounet, Paris, 2014. (p. 4)

David E. Dobbs and Ira J. Papick. When is $D + M$ coherent? *Proc. Amer. Math. Soc.*, 56:51–54, 1976. doi:10.2307/2041572. (p. 7)

Lionel Ducos. Polynômes à valeurs entières : un anneau de Prüfer de dimension 2. *Comm. Algebra*, 43(3):1146–1155, 2015. doi:10.1080/00927872.2013.865040. (p. 11)

Viviana Ene and Jürgen Herzog. *Gröbner bases in commutative algebra.* Graduate Studies in Mathematics, 130. American Mathematical Society, Providence, 2012. (pp. 19 and 21)

Maroua Gamanda, Henri Lombardi, Stefan Neuwirth, and Ihsen Yengui. The syzygy theorem for Bézout rings. *Math. Comput.*, 89(322):941–964, 2020. `arXiv:1905.08117`. (pp. 2, 6, 8, and 22)

Robert Gilmer. *Multiplicative ideal theory.* Pure and Applied Mathematics, 12. Marcel Dekker, New York, 1972. (p. 7)

Luc Guyot and Ihsen Yengui. The multivariate Serre conjecture ring. *J. Algebra*, 640: 385–400, 2024. doi:10.1016/j.jalgebra.2023.10.032. (p. 11)

Amina Hadj Kacem and Ihsen Yengui. Dynamical Gröbner bases over Dedekind rings. *J. Algebra*, 324(1):12–24, 2010. doi:10.1016/j.jalgebra.2010.04.014. (p. 2)

Henri Lombardi. Un anneau de Prüfer. *Actes Rencontres C.I.R.M.*, 2(2):59–69, 2010. ISSN 2105-0597. doi:10.5802/acirm.35. (p. 11)

Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods. Finite projective modules.* Algebra and applications, 20. Springer, Dordrecht, 2015. Translated from the French (Calvage & Mounet, Paris, 2011, revised and extended by the authors) by Tania K. Roblot. (pp. 2 and 4)

Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra.* Universitext. Springer-Verlag, New York, 1988. (p. 2)

László Rédei. Ein kombinatorischer Satz. *Acta Sci. Math. (Szeged)*, 7:39–43, 1934–1935. URL `http://acta.bibl.u-szeged.hu/13432`. (p. 7)

Frank-Olaf Schreyer. Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz und eine Anwendung auf analytische Cohen-Macaulay Stellenalgebren minimaler Multiplizität. Master's thesis, Universität Hamburg, 1980. (p. 19)

Ihsen Yengui. Dynamical Gröbner bases. *J. Algebra*, 301(2):447–458, 2006. doi:10.1016/j.jalgebra.2006.01.051. (p. 2)

Ihsen Yengui. *Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.* Lecture Notes in Mathematics, 2138. Springer, Cham, 2015. (pp. 2, 12, 13, and 20)

Ihsen Yengui. A counterexample to the Gröbner ring conjecture. *J. Algebra*, 586:526–536, 2021a. doi:10.1016/j.jalgebra.2021.07.009. (p. 11)

Ihsen Yengui. *Computational algebra: course and exercises with solutions.* World Scientific Publishing, 2021b. (p. 4)

Ihsen Yengui. The trailing terms ideal over a valuation domain. *Comm. Algebra*, 50(6): 2290–2295, 2022. doi:10.1080/00927872.2021.2005080. (p. 11)