

On the computation of parametric Gröbner bases for modules and syzygies

Katsusuke Nabeshima

Received: 22 January 2008 / Revised: 17 April 2009 / Published online: 15 May 2010
© The JJIAM Publishing Committee and Springer 2010

Abstract This paper presents algorithms to compute parametric Gröbner bases for modules and parametric syzygies. The theory of Gröbner basis is by far the most important tool for computations in commutative algebra and algebraic geometry. The theory of parametric Gröbner basis is also important to solve problems of ideals generated by parametric polynomials and submodule generated by parametric vectors. Several algorithms are known for computing parametric Gröbner bases in polynomial rings. However, nobody has studied the extension of parametric Gröbner bases to modules yet. In this paper we extend the theory of parametric Gröbner bases to modules, and we describe an algorithm for computing syzygies of parametric polynomials (vectors). These algorithms have been implemented in the computer algebra system *Risa/Asir*.

Keywords Gröbner bases · Comprehensive · Syzygies · Modules

1 Introduction

Nowadays it is common knowledge that Gröbner bases and Buchberger's algorithm [2] are key ingredients in computational commutative algebra, and are hence fundamental tools for applications in several fields both inside and outside mathematics (see [3,4]). For every concept and construction in computer algebra the question of uniformity in the input parameters, is crucial both from a theoretical and a practical viewpoint. This applies in particular to the concept of Gröbner bases.

Parametric polynomial systems have been studied by many researchers. Mainly, we have two kinds of parametric polynomials

K. Nabeshima (✉)
Graduate School of Information Science and Technology,
Osaka University, Machikaneyama 1-1, Toyonaka, Osaka, 560-0043, Japan
e-mail: nabeshima@math.sci.osaka-u.ac.jp

- (1) polynomials with parametric *coefficients*, and
- (2) polynomials with parametric *exponents*.

Recently, Gröbner bases for parametric polynomials have been actively investigated. For example, one can see several papers for Gröbner bases of a polynomial ideal with parametric coefficients in [12, 14, 20, 23, 25, 29], and for Gröbner bases of a polynomial ideal with parametric exponents in [17, 26, 28, 30].

In this paper, we treat parametric vector systems like the case (1). In detail, this paper describes algorithms for computing parametric Gröbner bases for modules and parametric syzygies. Parametric Gröbner bases (comprehensive Gröbner bases) for parametric ideals were introduced, constructed, and studied by Weispfenning in 1992 [25]. Since then parametric Gröbner bases were studied and implemented in several computer algebra systems including REDUCE [6], Maple [12, 14, 23], Mathematica [23], Risa/Asir [23] and Singular [23]. Roughly speaking, a parametric Gröbner basis is a finite subset G of a parametric polynomial ideal I such that $\sigma(G)$ constitutes a Gröbner basis of the ideal generated by $\sigma(I)$ under all specializations σ of the parameters. Since it is well-known that Gröbner bases are key ingredients in computational commutative algebra, the concept of parametric Gröbner bases has a lot of applications [25] for parametric polynomials (or vectors).

Several algorithms [12, 14, 21, 23, 25] are known for computing parametric Gröbner bases in polynomial rings. In this paper, we consider the problems of computing parametric Gröbner bases for modules. Theoretically, Gröbner basis algorithms admit natural extensions to modules. However, especially in the parametric situation, complexity is an important issue. An efficient algorithm for computation of parametric Gröbner bases over polynomial rings, was proposed recently by Suzuki and Sato [23]. We describe the generalization of the Suzuki–Sato algorithm [23] to the module case. In order to generalize the Suzuki–Sato algorithm, we need the special hybrid orders to compute parametric Gröbner bases for modules. This is the key for constructing the algorithms. We describe the special hybrid orders in Sect. 3.

By studying parametric Gröbner bases for modules we can solve a lot of parametric problems. For example, consider the problem of syzygy computations. In the ordinary setting, computing a Gröbner basis over a module is closely related to the computation of syzygies [9, 27]. In parametric setting, by computing a parametric Gröbner basis we can obtain parametric syzygies. We illustrate a method of computing parametric syzygies in Sect. 4. All algorithms of this paper have been implemented in the computer algebra system Risa/Asir by the author, and the implementation has been published on the web pages <http://www.math.sci.osaka-u.ac.jp/~nabeshima/PGB/>.

The outline of the paper is as follows: Sect. 2 presents the basic definitions for module structure and notations for polynomial rings over a field and polynomial rings over a polynomial ring. Section 3 describes the algorithms for the construction of parametric Gröbner bases (comprehensive Gröbner bases and systems) for modules and their examples. Section 4 describes an algorithm for computing modules of syzygies of parametric polynomials (or vectors) and examples.

In this paper, we set the following notations. Let K and L be fields such that L is an extension of K . $\bar{X} = \{X_1, \dots, X_n\}$ and $\bar{A} = \{A_1, \dots, A_m\}$ denote finite sets of

variables such that $\bar{X} \cap \bar{A} = \emptyset$. \mathbb{N} , \mathbb{Q} and \mathbb{C} are defined as the set of natural numbers, the field of rational numbers and the field of complex numbers, respectively. Note that in this paper, the set of natural numbers \mathbb{N} includes zero. $\text{pp}(\bar{X})$, $\text{pp}(\bar{A})$ and $\text{pp}(\bar{A}, \bar{X})$ denote the sets of power products of \bar{X} , \bar{A} and $\bar{X} \cup \bar{A}$, respectively. In this paper, we often use a block order on $\text{pp}(\bar{A}, \bar{X})$ for computing Gröbner bases. The definition of block orders on $\text{pp}(\bar{A}, \bar{X})$ is the following.

Definition 1 (*block orders*) Let \succ_1 and \succ_2 be term orders on $\text{pp}(\bar{A})$ and $\text{pp}(\bar{X})$, respectively, and $t_1, s_1 \in \text{pp}(\bar{A})$. Then, a term order $\succ_{\bar{X}, \bar{A}}$ on $\text{pp}(\bar{A}, \bar{X})$ is defined as follows; $t_2, s_2 \in \text{pp}(\bar{X})$, $t_1 t_2 \succ_{\bar{X}, \bar{A}} s_1 s_2 \iff t_2 \succ_2 s_2$ or $(t_2 = s_2, \text{ and } t_1 \succ_1 s_1)$. This order $\succ_{\bar{X}, \bar{A}}$ is called a *block order* and written as $\succ_{\bar{X}, \bar{A}} := (\succ_2, \succ_1)$.

In several papers and books [5, 7, 9, 13], an algorithm for computing Gröbner bases for $K[\bar{X}]$ -modules and its properties have been introduced. In this paper we consider parametric Gröbner bases for $K[\bar{X}]$ -modules. We apply the following notations and definitions for the module structure. (Let A be a matrix. In this paper, the transposed matrix of A is written as A^T .)

Let e_1, \dots, e_r be the canonical basis of the free module $K[\bar{X}]^r = \bigoplus_{i=1}^r K[\bar{X}]e_i$. i.e., for each $i = 1, \dots, r$,

$$e_i = \begin{matrix} i\text{th} \\ (0, \dots, 0, \quad 1, \quad 0, \dots, 0)^T \in K[\bar{X}]^r \end{matrix}$$

denotes the i -th canonical basis vector of $K[\bar{X}]^r$ with 1 at the i -th place. We call

$$x^\alpha e_i = \begin{matrix} i\text{th} \\ (0, \dots, 0, \quad x^\alpha, \quad 0, \dots, 0)^T \in K[\bar{X}]^r \end{matrix}$$

a *module power product* (involving component i) where $\alpha \in \mathbb{N}^n$ and $x^\alpha \in \text{pp}(\bar{X})$. The set of module power product with respect to \bar{X} is defined as $\text{pp}(\bar{X})^r$. (I.e., $x^\alpha e_i \in \text{pp}(\bar{X})^r$.)

Definition 2 (*Module orders*) Let \succ be a term order on $\text{pp}(\bar{X})$. A module order on $\text{pp}(\bar{X})^r$ is a total order \succ_m on the set of power products $\{x^\alpha e_i | \alpha \in \mathbb{N}^n, i = 1, \dots, r\}$, which is compatible with the module structure including the order \succ , that is, satisfying, for all $\alpha, \beta, \gamma \in \mathbb{N}^n, i, j = 1, \dots, r$,

- (1) $x^\alpha e_i \succ_m x^\beta e_j \Rightarrow x^{\alpha+\gamma} e_i \succ_m x^{\beta+\gamma} e_j$,
- (2) $x^\alpha \succ x^\beta \Rightarrow x^\alpha e_i \succ_m x^\beta e_i$.

Two module orders are of particularly practical interest: position-over-term (POT) and term-over-position (TOP) which are the following.

Definition 3 Let \succ be a term order on $\text{pp}(\bar{X})$ and \succ_m be a module order on $K[\bar{X}]^r$ with \succ .

1. A module order \succ_m is called POT if \succ_m satisfies

$$x^\alpha e_i \succ_m x^\beta e_j \Leftrightarrow i < j \quad \text{or} \quad (i = j \text{ and } x^\alpha \succ x^\beta).$$

This module order is written as (POT, \succ).

2. A module order \succ_m is called TOP if \succ_m satisfies

$$x^\alpha e_i \succ_m x^\beta e_j \Leftrightarrow x^\alpha \succ x^\beta \quad \text{or} \quad (x^\alpha = x^\beta \text{ and } i < j).$$

This module order is written as (TOP, \succ).

In this paper, we define $K[\bar{A}, \bar{X}]$ as a polynomial ring over a field K and $K[\bar{A}][\bar{X}] := (K[\bar{A}])[\bar{X}]$ as a polynomial ring over a polynomial ring $K[\bar{A}]$. Furthermore, $K[\bar{A}, \bar{X}]^r := \bigoplus_{i=1}^r K[\bar{A}, \bar{X}]e_i$, and $K[\bar{A}][\bar{X}]^r := \bigoplus_{i=1}^r K[\bar{A}][\bar{X}]e_i$. We use the following notations for the two polynomial rings.

For the notations of $K[\bar{A}, \bar{X}]^r$, we use the following. Let f be a non-zero vector in $K[\bar{A}, \bar{X}]^r$ and \succ_m be an arbitrary module order on $\text{pp}(\bar{A}, \bar{X})^r$. The leading power product of f w.r.t. \succ_m is written as $\text{lpp}(f)$. The leading coefficient of f w.r.t. \succ_m is written as $\text{lc}(f)$. The leading monomial of f w.r.t. \succ_m is written as $\text{lm}(f) := \text{lc}(f) \text{lpp}(f)$. The set of monomials of f is denoted by $\text{Mono}(f)$.

For the notation of $K[\bar{A}][\bar{X}]^r$, if a non-zero vector f is in $K[\bar{A}][\bar{X}]^r$, then we apply the subscript \bar{A} as follows. Let \succ_m be an arbitrary module order on $\text{pp}(\bar{X})^r$. The leading power product of f w.r.t. \succ_m is written as $\text{lpp}_{\bar{A}}(f)$. The leading coefficient of f w.r.t. \succ_m is written as $\text{lc}_{\bar{A}}(f)$. The leading monomial of f w.r.t. \succ_m is written as $\text{lm}_{\bar{A}}(f) := \text{lc}_{\bar{A}}(f) \text{lpp}_{\bar{A}}(f)$. The set of monomials of f is denoted by $\text{Mono}_{\bar{A}}(f)$. If $\text{lpp}(f) = A_1^{\alpha_1} \cdots A_m^{\alpha_m} X_1^{\beta_1} \cdots X_n^{\beta_n} e_i \in \text{pp}(\bar{A}, \bar{X})^r$, then $\deg_{\bar{A} \cup \bar{X}}(\text{lpp}(f)) := (\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n) \in \mathbb{N}^{m+n}$, and $\deg_{\bar{X}}(\text{lpp}(f)) := (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. Note that the subscripts are $\bar{A} \cup \bar{X}$ and \bar{X} . If $r = 1$, we apply $K[\bar{X}]^1$, $\text{pp}(\bar{X})^1$ as $K[\bar{X}]$, $\text{pp}(\bar{X})$.

Example 1 Let a, b, x, y be variables and $f = \begin{pmatrix} 2ax - bx + y^2 \\ axy + 3 \end{pmatrix}$ be a vector.

Let us consider f as a vector of $\mathbb{Q}[a, b, x, y]^2$ with a module order $\succ_m := (\text{POT}, \succ_{\{x, y\}, \{a, b\}}) = (\text{POT}, (x \succ_{\text{lex}} y, a \succ_{\text{lex}} b))$ where \succ_{lex} is the lexicographic order. Then we have the following: $\text{lpp}(f) = axe_1$, $\text{lc}(f) = 2$, $\text{lm}(f) = 2axe_1$, $\deg(\text{lpp}(f)) = (1, 0, 1, 0) \in \mathbb{N}^4$, $\deg_{\{a\}}(\text{lpp}(f)) = 1$, $\text{Mono}(f) = \{2axe_1, bxe_1, y^2e_1, axye_2, 3e_2\}$.

Let us consider f as a vector of $\mathbb{Q}[a, b][x, y]^2$ with a module order $\succ_m := (\text{POT}, x \succ_{\text{lex}} y)$. Then we have the following: $\text{lpp}_{\{a, b\}}(f) = xe_1$, $\text{lc}_{\{a, b\}}(f) = 2a - b$, $\text{lm}_{\{a, b\}}(f) = (2a - b)xe_1$, $\deg_{\{x, y\}}(\text{lpp}_{\bar{A}}(f)) = (1, 0) \in \mathbb{N}^2$, $\deg_{\{y\}}(\text{lpp}_{\bar{A}}(f)) = 0$, $\text{Mono}_{\{a, b\}}(f) = \{(2a - b)xe_1, y^2e_1, axye_2, 3e_2\}$.

Let f_1, \dots, f_s be polynomials in $K[\bar{X}]$. Then we set $\mathbb{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in K^n \mid f_i(a_1, \dots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}$. We call $\mathbb{V}(f_1, \dots, f_s)$ the affine variety defined by f_1, \dots, f_s over K . In this paper, angle brackets $\langle \cdot \rangle$ are defined as follows: let $g_1, \dots, g_l \in R[\bar{X}]^r$ where R is a Noetherian ring with identity. Then, $\langle g_1, \dots, g_l \rangle := \left\{ \sum_{i=1}^l h_i g_i \mid h_1, \dots, h_l \in R[\bar{X}] \right\}$.

2 Parametric Gröbner bases for modules

In this section we present algorithms for computing parametric Gröbner bases for modules. There are two kinds of parametric Gröbner bases, “comprehensive Gröbner

bases” and “comprehensive Gröbner systems”. That is, in this section, we present algorithms for computing comprehensive Gröbner bases and systems. In fact, these algorithms are the generalization of the Suzuki–Sato algorithms [23] to modules. In several papers [12, 14, 19, 22–25], parametric Gröbner bases were studied in polynomial rings over a field. We extend the concept of parametric Gröbner bases to modules. First we describe stabilities of submodules under specializations for modules. Second we treat the theory of comprehensive Gröbner systems. Third, we illustrate the theory of comprehensive Gröbner bases.

2.1 Stability of submodules

Here we describe the stability of submodules under specialization in $K[\bar{A}][\bar{X}]^r$. In order to describe the theory, we introduce a definition of Gröbner bases in $K[\bar{A}][\bar{X}]^r$, and an algorithm for computing them.

Definition 4 Let \succ_m be a module order on $\text{pp}(\bar{X})^r$. A finite set $G = \{g_1, \dots, g_s\}$ of a submodule M in $K[\bar{A}][\bar{X}]^r$ is said to be a *Gröbner basis* with respect to \succ_m if $\text{lm}_{\bar{A}}(M) = \langle \text{lm}_{\bar{A}}(g_1), \dots, \text{lm}_{\bar{A}}(g_s) \rangle$ where $\text{lm}_{\bar{A}}(M) = \{\text{lm}_{\bar{A}}(f) | f \in M\}$.

In order to compute a Gröbner basis for a submodule, we need to introduce the following special module order. By the following special order, we can construct a “simple” algorithm for computing parametric Gröbner bases. In fact, this special order is one of the key tools for computing parametric Gröbner bases.

Definition 5 (*Hybrid module order 1*) Let \succ_m be a module order on $\text{pp}(\bar{X})^r$ and \succ_1 a term order on $\text{pp}(\bar{A})$. Let $A_1 X_1 e_i, A_2 X_2 e_j \in \text{pp}(\bar{A}, \bar{X})^r$ for $1 \leq i, j \leq r$ where $A_1, A_2 \in \text{pp}(\bar{A})$ and $X_1, X_2 \in \text{pp}(\bar{X})$. Then a hybrid module order $1 \succ_{hm1}$ on $\text{pp}(\bar{A}, \bar{X})^r$ is defined as follows

$$A_1 X_1 e_i \succ_{hm1} A_2 X_2 e_j \iff X_1 e_i \succ_m X_2 e_j \quad \text{or} \quad (X_1 e_i = X_2 e_j \text{ and } A_1 \succ_1 A_2).$$

This hybrid module order 1 is written as $\succ_{hm1} := (\succ_m, \succ_1)$.

Remark If \succ_m is TOP, then we have to consider the following order: $\bar{X} \succ e_1 \succ e_2 \succ \dots \succ e_r \succ \bar{A}$. Note that, this order is *not* TOP or POT. If \succ_m is POT, then we have to consider the following order: $e_1 \succ e_2 \succ \dots \succ e_r \succ \bar{X} \succ \bar{A}$. This order is still POT.

The following lemma tells us how to compute Gröbner bases in $K[\bar{A}][\bar{X}]^r$.

Lemma 1 Let F be a set of vectors in $K[\bar{A}][\bar{X}]^r$. Clearly, F can be seen as a set of vectors in $K[\bar{A}, \bar{X}]^r$. Let $G = \{g_1, \dots, g_s\}$ be the reduced Gröbner basis for $\langle F \rangle$ in $K[\bar{A}, \bar{X}]^r$ with respect to a hybrid module order $1 \succ_{hm1} := (\succ_m, \succ_1)$ where \succ_m is a module order on $\text{pp}(\bar{X})^r$ and \succ_1 is a term order on $\text{pp}(\bar{A})$. Then, G can be also seen as a set of vectors in $K[\bar{A}][\bar{X}]^r$. This set G is a Gröbner basis for $\langle F \rangle$ in $K[\bar{A}][\bar{X}]^r$ with respect to a module order \succ_m .

Proof For all $h \in \langle F \rangle \subseteq K[\bar{A}][\bar{X}]^r$, we prove that $\text{lm}_{\bar{A}}(h)$ is generated by $\{\text{lm}_{\bar{A}}(g) \mid g \in G\}$. The element h can be seen as an element of $K[\bar{A}, \bar{X}]^r$, and h can be written as $h = h_1 g_1 + \cdots + h_s g_s$ where $h_1, \dots, h_s \in K[\bar{A}, \bar{X}]$. Since G is the reduced Gröbner basis for $\langle F \rangle$ with respect to \succ_{hm1} in $K[\bar{A}, \bar{X}]^r$, there exists $g_{i_1}, g_{i_2} \in G$ such that $\text{lm}(h) = q_1 \cdot \text{lm}(g_{i_1})$, $\text{lm}(h - \text{lm}(h)) = q_2 \cdot \text{lm}(g_{i_2})$ where $q_1, q_2 \in \text{pp}(\bar{A}, \bar{X})^r$ and $1 \leq i_1, i_2 \leq s$. That is, $q_1 \cdot \text{lm}(g_{i_1}) \succ_{hm1} q_2 \cdot \text{lm}(g_{i_2})$. As G is the reduced Gröbner basis, no element in $\text{lm}(G) \setminus \{g_{i_1}\}$ divides g_{i_1} , and no element in $\text{lm}(G) \setminus \{g_{i_2}\}$ divides g_{i_2} . Therefore, w.l.o.g., we consider

$$\text{lm}(h) \succ_{hm1} \text{lm}(h_1 g_1) \succ_{hm1} \cdots \succ_{hm1} \text{lm}(h_s g_s) \quad (*1)$$

on $\text{pp}(\bar{A}, \bar{X})^r$.

Here, we define a notation “ \succeq_m ” a module order on $\text{pp}(\bar{X})^r$ as follows; $p_1 \succeq_m p_2 \iff p_1 \succ_m p_2$ or $p_1 = p_2$, where $p_1, p_2 \in \text{pp}(\bar{X})^r$ and \succ_m is a module order on $\text{pp}(\bar{X})^r$.

Now, we see h as a member of $K[\bar{A}][\bar{X}]^r$ (the main variables are \bar{X}). As we know the ordering $(*1)$ with respect to $\succ_{hm1} = (\succ_m, \succ_1)$, by Definition 5 and \succeq_m , we have

$$\text{lpp}_{\bar{A}}(h) \succeq_m \text{lpp}_{\bar{A}}(h_1 g_1) \succeq_m \cdots \succeq_m \text{lpp}_{\bar{A}}(h_s g_s) \quad (*2)$$

on $\text{pp}(\bar{X})^r$. Since $h = h_1 g_1 + \cdots + h_s g_s$ in $K[\bar{A}, \bar{X}]^r$, $\text{lm}_{\bar{A}}(h) = \text{lm}_{\bar{A}}(h_1 g_1 + \cdots + h_s g_s)$ in $K[\bar{A}][\bar{X}]^r$. W.l.o.g., $h_1 g_1, \dots, h_k g_k$ have the same leading power product $\text{lpp}_{\bar{A}}(h)$ with respect to \succeq_m , where $k \leq s$. That is, by $(*2)$,

$$\begin{aligned} \text{lm}_{\bar{A}}(h) &= \text{lc}_{\bar{A}}(h_1 g_1) \text{lpp}_{\bar{A}}(h_1 g_1) + \cdots + \text{lc}_{\bar{A}}(h_k g_k) \text{lpp}_{\bar{A}}(h_k g_k) \\ &= \text{lm}_{\bar{A}}(h_1 g_1) + \text{lm}_{\bar{A}}(h_2 g_2) + \cdots + \text{lm}_{\bar{A}}(h_k g_k). \end{aligned}$$

Obviously, $\text{lm}_{\bar{A}}(h_i g_i) = \text{lm}_{\bar{A}}(h_i) \cdot \text{lm}_{\bar{A}}(g_i)$, hence $\text{lm}_{\bar{A}}(h) = \text{lm}_{\bar{A}}(h_1) \cdot \text{lm}_{\bar{A}}(g_1) + \cdots + \text{lm}_{\bar{A}}(h_k) \cdot \text{lm}_{\bar{A}}(g_k)$. Therefore, $\text{lm}_{\bar{A}}(h) \in \langle \{\text{lm}_{\bar{A}}(g) \mid g \in G\} \rangle$ in $K[\bar{A}][\bar{X}]^r$. G is a Gröbner basis for $\langle F \rangle$ with respect to \succ_m in $K[\bar{A}][\bar{X}]^r$.

Algorithm 21 GröbnerBasisM(F, \succ_m)

Input F : a finite set of vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,

Output G : a Gröbner basis of $\langle F \rangle$ w.r.t. \succ_m in $K[\bar{A}][\bar{X}]^r$.

1. Consider F as a set of vectors in $K[\bar{A}, \bar{X}]^r$.
 2. Compute the **reduced Gröbner basis** G for $\langle F \rangle$ with respect to a **hybrid module order** $\mathbf{1} \succ_{hm1} = (\succ_m, \succ_1)$ where \succ_1 is a term order on $\text{pp}(\bar{A})$.
 3. Consider G as a set of vectors in $K[\bar{A}][\bar{X}]^r$. Then, by Lemma 1, G is a Gröbner basis for $\langle F \rangle$ with respect to \succ_m in $K[\bar{A}][\bar{X}]^r$.
-

Every ring homomorphism $\pi : K[\bar{A}] \rightarrow L$ extends naturally to a homomorphism $\pi : K[\bar{A}][\bar{X}] \rightarrow L[\bar{X}]$. Moreover, we extend the homomorphism $\pi : K[\bar{A}][\bar{X}]^r \rightarrow L[\bar{X}]^r$ for modules. The image under π of a submodule $I \subseteq K[\bar{A}][\bar{X}]^r$ generates the extension submodule $\pi(I) := \{\pi(f) \mid f \in I\} \subseteq L[\bar{X}]^r$.

Definition 6 We call a submodule $I \subseteq K[\bar{A}][\bar{X}]^r$ stable under the ring homomorphism π and an order \succ_m if for each $i = 1, \dots, r$, it satisfies $\pi(\text{lm}_{\bar{A}}(I)) = \text{lm}(\pi(I))$ where $\pi(\text{lm}_{\bar{A}}(I)) := \{\pi(\text{lm}_{\bar{A}}(f)) \mid f \in I\}$ and $\text{lm}(\pi(I)) := \{\text{lm}(f) \mid f \in \pi(I)\}$.

In several papers [1, 8, 10, 11, 18], the stability of ideals under specialization has been studied in polynomial rings. We can easily extend the concept of stability of ideals under specialization to submodules. Then, in $K[\bar{A}][\bar{X}]$, the generalization of “Kalkbrener [11] Theorem 3.1” also holds. This theorem is the key theorem of this paper which is the following.

Theorem 1 Let π be a ring homomorphism from $K[\bar{A}]$ to L , I a submodule of $K[\bar{A}][\bar{X}]^r$ and $G = \{g_1, \dots, g_s\}$ a Gröbner basis for I with respect to a module order \succ_m where $r \in \mathbb{N}$.

We assume that the g_i 's are ordered in such a way that there exists an $q \in \{1, \dots, s\}$ with $\pi(\text{lc}_{\bar{A}}(g_i)) \neq 0$ for $i \in \{1, \dots, q\}$ and $\pi(\text{lc}_{\bar{A}}(g_i)) = 0$ for $i \in \{q+1, \dots, s\}$. Then the following three conditions are equivalent.

1. I is stable under π and \succ_m .
2. $\{\pi(g_1), \dots, \pi(g_q)\}$ is a Gröbner basis for $\pi(I)$ in $L[\bar{X}]^r$ with respect to a module order \succ_m .
3. For every $i \in \{q+1, \dots, s\}$ the polynomial $\pi(g_i)$ is reducible to 0 modulo $\{\pi(g_1), \dots, \pi(g_q)\}$ in $L[\bar{X}]^r$.

Proof Obviously, $\{\pi(g_1), \dots, \pi(g_q)\}$ is a Gröbner basis of $\langle \pi(I) \rangle$ in $L[\bar{X}]^r$ if and only if $\langle \{\pi(\text{lm}_{\bar{A}}(g)) \mid g \in G\} \rangle = \langle \text{lm}(\pi(I)) \rangle$. Since $\langle \{\pi(\text{lm}_{\bar{A}}(g)) \mid g \in G\} \rangle = \langle \pi(\text{lm}_{\bar{A}}(I)) \rangle$, (1) and (2) are equivalent. If $\{\pi(g_1), \dots, \pi(g_q)\}$ is a Gröbner basis for $\langle \pi(I) \rangle$ then the condition (3) holds. It remains to show that (3) implies (1). Since $\{g_1, \dots, g_s\}$ is a Gröbner basis of I , we can write $\langle \text{lm}_{\bar{A}}(I) \rangle = \langle \text{lm}_{\bar{A}}(g_1), \dots, \text{lm}_{\bar{A}}(g_s) \rangle$. We prove $\langle \pi(\text{lm}_{\bar{A}}(I)) \rangle = \langle \text{lm}(\pi(I)) \rangle$.

(\subseteq) Take a non-zero vector $f \in \langle \pi(\text{lm}_{\bar{A}}(I)) \rangle$, then f can be written as

$$\begin{aligned} f &= \pi(c_1 \text{lm}_{\bar{A}}(g_1) + \dots + c_s \text{lm}_{\bar{A}}(g_s)) \quad (c_1, \dots, c_s \in K[\bar{A}][\bar{X}]) \\ &= \pi(c_1)\pi(\text{lm}_{\bar{A}}(g_1)) + \dots + \pi(c_s)\pi(\text{lm}_{\bar{A}}(g_s)) \cdots (*) \quad (\pi: \text{homo.}) \end{aligned}$$

By the assumption, for each $i \in \{q+1, \dots, s\}$, $\pi(\text{lm}_{\bar{A}}(g_i)) = \pi(\text{lc}_{\bar{A}}(g_i)) \text{lpp}_{\bar{A}}(g_i) = 0$, then we have

$$\begin{aligned} (*) &= \pi(c_1)\pi(\text{lm}_{\bar{A}}(g_1)) + \dots + \pi(c_q)\pi(\text{lm}_{\bar{A}}(g_q)) \\ &= \pi(c_1) \text{lm}(\pi(g_1)) + \dots + \pi(c_q) \text{lm}(\pi(g_q)) \\ &\quad (\text{for each } j \in \{1, \dots, q\}, \pi(\text{lm}(g_j)) = \text{lm}(\pi(g_j))) \end{aligned}$$

As $\text{lm}(\pi(g_1)), \dots, \text{lm}(\pi(g_q)) \in \text{lm}(\pi(I))$ and $\pi(c_1), \dots, \pi(c_q) \in L[\bar{X}]$, hence $f \in \text{lm}(\pi(I))$.

(\supseteq) Take a non-zero vector $f \in \langle \text{Im}(\pi(I)) \rangle$, then f can be written as

$$\begin{aligned} f &= \text{Im}(\pi(f_1)) \quad (f_1 \in I) \\ &= \text{Im}(\pi(c_1 g_1 + \cdots + c_s g_s)) \quad (c_1, \dots, c_s \in K[\bar{A}][\bar{X}]) \\ &= \text{Im}(\pi(c_1)\pi(g_1) + \cdots + \pi(c_s)\pi(g_s)) \quad (\pi: \text{homo.}) \\ &= (*1) \end{aligned}$$

By the assumption (3), $i \in \{q+1, \dots, s\}$, $\pi(g_i)$ is reducible to 0 modulo $\{\pi(g_1), \dots, \pi(g_q)\}$.

$$\begin{aligned} (*1) &= \text{Im}(R_1\pi(g_1) + \cdots + R_q\pi(g_q)) \quad (\exists R_1, \dots, R_q \in K[\bar{X}]) \\ &= (*2) \end{aligned}$$

There exist $\pi(g_k)$ in $L[\bar{X}]^r$ such that $\text{lpp}(L_k\pi(g_k)) = \text{lpp}(f)$ where $k \in \{1, \dots, q\}$.

W.o.l.g, $R_1\pi(g_1), \dots, R_b\pi(g_b)$ have the leading power product $\text{lpp}(f)$ where $b \in \{1, \dots, q\}$. Then, we can write (*2) as

$$\begin{aligned} (*2) &= \text{Im}(L_1\pi(g_1) + \cdots + L_b\pi(g_b)) \\ &= \text{Im}(L_1)\text{Im}(\pi(g_1)) + \cdots + \text{Im}(L_b)\text{Im}(\pi(g_b)) \\ &= \text{Im}(L_1)\pi(\text{Im}_{\bar{A}}(g_1)) + \cdots + \text{Im}_{\bar{A}}(L_b)\pi(\text{Im}(g_b)). \\ &\quad (\text{For each } j \in \{1, \dots, q\}, \pi(\text{Im}_{\bar{A}}(g_j)) = \text{Im}(\pi(g_j)).) \end{aligned}$$

Since $\text{Im}(R_1), \dots, \text{Im}(R_b) \in L[\bar{X}]$ and $\pi(\text{Im}_{\bar{A}}(g_1)), \dots, \pi(\text{Im}_{\bar{A}}(g_b)) \in \langle \pi(\text{Im}_{\bar{A}}(I)) \rangle$, we have $f \in \langle \pi(\text{Im}_{\bar{A}}(I)) \rangle$. Therefore $\langle \pi(\text{Im}_{\bar{A}}(I)) \rangle = \langle \text{Im}(\pi(I)) \rangle$.

2.2 Comprehensive Gröbner systems for modules

Here we present comprehensive Gröbner systems for modules. Roughly speaking, a comprehensive Gröbner system is a parametric Gröbner basis with parameters' spaces for a parametric polynomial ideal. If we take a parameters' space \mathbb{P} and its set of parametric polynomials G from a comprehensive Gröbner systems for a parametric polynomial ideal I , then $\sigma(G)$ constitutes a Gröbner basis of the ideal generated by $\sigma(I)$ under the specialization σ with respect to the parameters' space \mathbb{P} of the parameters.

In this paper, for arbitrary $\bar{a} \in L^m$, we define the canonical specialization homomorphism $\sigma_{\bar{a}}: K[\bar{A}] \rightarrow L$ induced by \bar{a} , and we can naturally extend it to $\sigma_{\bar{a}}: (K[\bar{A}])[\bar{X}] \rightarrow L[\bar{X}]$. Moreover, we extend the homomorphism to $\sigma_{\bar{a}}: K[\bar{A}][\bar{X}]^r \rightarrow L[\bar{X}]^r$ for modules. For h_1, \dots, h_l in $K[\bar{A}]$, we define $\text{LCM}(h_1, \dots, h_l)$ as the least common multiple of h_1, \dots, h_l .

The next theorem is the direct consequences of Theorem 1, and this is the main theorem of this paper. By the next theorem, we can construct the algorithm for computing parametric Gröbner bases.

Theorem 2 *Let \succ_m be a module order on $\text{pp}(\bar{X})^r$, $F = \{f_1, \dots, f_l\}$ be a set of vectors in $K[\bar{A}][\bar{X}]^r$, S a set of polynomials in $K[\bar{A}]$ and $T = \{se_i | s \in S, 1 \leq i \leq r\}$.*

Furthermore, G be a Gröbner basis of a submodule $\langle F \cup T \rangle \subseteq K[\bar{A}][\bar{X}]^r$ with respect to \succ_m . Suppose that $B =: \{g \mid g \in G \cap K[\bar{A}]e_i, \text{lc}_{\bar{A}}(g) \in \langle S \rangle, 1 \leq i \leq r\}$, $\{h_1, \dots, h_l\} = \{\text{lc}_{\bar{A}}(g) \mid g \in G \setminus B\} \subseteq K[\bar{A}]$ and $h = \text{LCM}(h_1, \dots, h_l)$.

Then, for $\bar{a} \in \mathbb{V}(S) \setminus \mathbb{V}(h)$, $\sigma_{\bar{a}}(G)$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F) \rangle$ with respect to \succ_m in $L[\bar{X}]^r$.

Proof For all $q \in B \cap G$ and $\bar{a} \in \mathbb{V}(S) \setminus \mathbb{V}(h)$, we have $\sigma_{\bar{a}}(q) = 0$. Thus, $\langle G \setminus B \rangle$ is stable under $\sigma_{\bar{a}}$. Therefore, $\sigma_{\bar{a}}(G) = \sigma_{\bar{a}}(G \setminus B)$. Clearly, for each $g \in G \setminus B$, we have $\sigma_{\bar{a}}(\text{lc}_{\bar{A}}(g)) \neq 0$. By Theorem 1, $\sigma_{\bar{a}}(G) \setminus \{0\}$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F) \rangle$ with respect to \succ_m in $L[\bar{X}]^r$.

By this theorem, we are able to construct an algorithm for computing comprehensive Gröbner systems in $K[\bar{A}][\bar{X}]^r$. Before describing the algorithm, we have to define comprehensive Gröbner systems for modules.

Definition 7 Let F be a set of vectors in $K[\bar{A}][\bar{X}]^r$, $\mathcal{A}_1, \dots, \mathcal{A}_l$ algebraically constructible subsets of L^m and G_1, \dots, G_l subsets of $K[\bar{A}][\bar{X}]^r$. Let \mathcal{S} be a subset of L^m such that $\mathcal{S} \subseteq \mathcal{A}_1 \cup \dots \cup \mathcal{A}_l$. A finite set $\mathcal{G} = \{(\mathcal{A}_1, G_1), \dots, (\mathcal{A}_l, G_l)\}$ of pairs is called a comprehensive Gröbner system (CGS) on \mathcal{S} for $\langle F \rangle$ if $\sigma_{\bar{a}}(G_i)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$ in $L[\bar{X}]^r$ for each $i = 1, \dots, l$ and $\bar{a} \in \mathcal{A}_i$. Each (\mathcal{A}_i, G_i) is called a segment of \mathcal{G} . We simply say \mathcal{G} is a comprehensive Gröbner system for $\langle F \rangle$ if $\mathcal{S} = L^m$.

Example 2 Let $F = \{ax^2y + y, bx^2y^2 + ax + y\} \subset \mathbb{Q}[a, b][x, y]^1$, a, b parameters, x, y variables and \succ the lexicographic order such that $x \succ y$. Then, a comprehensive Gröbner system for $\langle F \rangle$ with respect to \succ is

$$\mathcal{G}_1 = \left\{ \left(\mathbb{Q}^2 \setminus \mathbb{V}(a, b), \{a^2x - by^2 + ay, -b^2y^5 + 2bay^4 - a^2y^3 - a^3y\} \right), (\mathbb{V}(a, b), \{y\}) \right\}.$$

This meaning is the following:

- if parameters a, b belong to $\mathbb{Q}^2 \setminus \mathbb{V}(a, b)$ (i.e., $a \neq 0, b \neq 0$), then $\{a^2x - by^2 + ay, -b^2y^5 + 2bay^4 - a^2y^3 - a^3y\}$ is a Gröbner basis for $\langle F \rangle$ in $\mathbb{Q}[x, y]$,
- if parameters a, b belong to $\mathbb{V}(a, b)$ (i.e., $a = b = 0$), then $\{y\}$ is a Gröbner basis for $\langle F \rangle$ in $\mathbb{Q}[x, y]$.

In the comprehensive Gröbner system \mathcal{G}_1 , the parameters' spaces $\mathbb{Q}^2 \setminus \mathbb{V}(a, b)$ and $\mathbb{V}(a, b)$ are disjoint, i.e., $(\mathbb{Q}^2 \setminus \mathbb{V}(a, b)) \cap \mathbb{V}(a, b) = \emptyset$. The following set \mathcal{G}_2 is also a comprehensive Gröbner system for $\langle F \rangle$ with respect to \succ ;

$$\mathcal{G}_2 = \left\{ \left(\mathbb{Q}^2 \setminus \mathbb{V}(ab), \{-b^2y^5 + 2bay^4 - a^2y^3 - a^3y, a^2x - by^2 + ay\} \right), \left(\mathbb{V}(b) \setminus \mathbb{V}(a), \{-y^2x + y, ax + y, y^3 + ay\} \right), (\mathbb{V}(a), \{y\}) \right\}.$$

In the comprehensive Gröbner system \mathcal{G}_2 , the parameters' spaces are not disjoint, however \mathcal{G}_2 is a comprehensive Gröbner systems, too.

Now we can compute comprehensive Gröbner systems by the following algorithm. In algorithms of this paper, we use an algorithm `factorize` which outputs a set of all irreducible factors of an input in $K[\bar{A}]$.

Algorithm 22 CGSM(F, \succ_m) (CGS for Modules)**Input** F : a finite set of vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,**Output** H : comprehensive Gröbner system for $\langle F \rangle$ w.r.t. \succ_m in $K[\bar{A}][\bar{X}]^r$.**begin** $G \leftarrow \text{GröbnerBasisM}(F, \succ_m)$ **if** $e_1, \dots, e_r \in G$ **then return** $(\{\emptyset, \{1\}, G\})$ **end-if** $S \leftarrow \{h_1, \dots, h_l\} := \{q \mid q \in \text{factorize}(\text{lc}_{\bar{A}}(g)), \text{lc}_{\bar{A}}(g) \notin K, g \in G\}$ **if** $S \neq \emptyset$ **then** $h \leftarrow \text{LCM}(h_1, \dots, h_l)$ $H \leftarrow \{(\emptyset, h, G)\} \cup \text{CGSMMainM}(G \cup \{h_1 e_1, \dots, h_l e_r\}, \{h_1\}, \succ_m) \cup \dots \cup \text{CGSMMainM}(G \cup \{h_l e_1, \dots, h_l e_r\}, \{h_l\}, \succ_m)$ **else** $H \leftarrow \{(\emptyset, \{1\}, G)\}$ **end-if****return**(H)**end****Algorithm 23** CGSMMainM(F, Z, \succ_m) (CGS Main for Modules)**Input** F : a set of vectors in $K[\bar{A}][\bar{X}]^r$, Z : a set of polynomials in $K[\bar{A}]$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,**Output** H : comprehensive Gröbner system for $\langle F \rangle$ w.r.t. \succ_m on $\mathbb{V}(Z)$ in $K[\bar{A}][\bar{X}]^r$.**begin** $G \leftarrow \text{GröbnerBasisM}(F, \succ_m)$ **if** $e_1, \dots, e_r \in G$ **then** $C \leftarrow$ the reduced Gröbner basis for $\langle Z \rangle$ in $K[\bar{A}]$ **if** $1 \in C$ **then** $H \leftarrow \emptyset$ **else** $H \leftarrow \{(C, \{1\}, \{e_1, \dots, e_r\})\}$ **end-if****else** $B \leftarrow \{g \mid g \in G \cap K[\bar{A}]e_i, \text{lc}_{\bar{A}}(g) \in \langle Z \rangle, \text{ for some } i \in \{1, \dots, r\}\}$ $S \leftarrow \{h_1, \dots, h_l\} := \{q \mid q \in \text{factorize}(\text{lc}_{\bar{A}}(g)), g \in G \setminus B\}$ **if** $S \neq \emptyset$ **then** $h \leftarrow \text{LCM}(h_1, \dots, h_l)$ $H \leftarrow \{(Z, h, G \setminus B)\} \cup \text{CGSMMainM}(G \cup \{h_1 e_1, \dots, h_l e_r\}, Z \cup \{h_1\}, \succ_m) \cup \dots \cup \text{CGSMMainM}(G \cup \{h_l e_1, \dots, h_l e_r\}, Z \cup \{h_l\}, \succ_m)$ **else** $H \leftarrow \{(Z, \{1\}, G \setminus B)\}$ **end-if****end-if****return**(H)**end**

Remark We are able to apply a lot of optimization techniques to obtain small and nice outputs comprehensive Gröbner systems. For instance, we can compute a radical ideal of $\langle Z \rangle$ for getting small and nice outputs, however, with respect to speed, this is not always good. In the algorithms CGSM and CGSMMainM, we applied the algorithm GröbnerBasisB for computing Gröbner bases in $K[\bar{A}][\bar{X}]$. The Gröbner bases computed w.r.t. a block order with $\bar{X} \gg \bar{A}$ in $K[\bar{A}, \bar{X}]^r$ are not always reduced Gröbner bases in $K[\bar{A}][\bar{X}]^r$. There sometimes exist some unnecessary polynomials in

the outputs. Therefore, we can also apply the technique of reduced Gröbner bases in $K[\bar{A}][\bar{X}]^r$ for getting nice comprehensive Gröbner systems [15]. In [16], an efficient criterion for computing comprehensive Gröbner systems have been studied in polynomial rings. We are able to extend this criterion to modules. In the algorithms **CGSM** and **CGSMmainM**, we can use these techniques for computing comprehensive Gröbner systems. Note that conditions of segments (of a comprehensive Gröbner system) produced by the algorithm **CGSM** may not be disjoint, i.e. $(\mathbb{V}(Z) \setminus \mathbb{V}(h)) \cap (\mathbb{V}(Z') \setminus \mathbb{V}(h'))$ could be non-empty for distinct elements $(Z, h, G), (Z', h', G') \in H$. Though this fact looks a serious disadvantage, it enables us to avoid producing unnecessary inequations (which is h in the algorithm **CGSMmainM**). In the algorithm we do not even check if $(\mathbb{V}(Z) \setminus \mathbb{V}(h)) = \emptyset$. Of course, we can check it after the algorithm terminates and omit it from the segments in case it is empty. We can also make the constructible sets of segments pairwise disjoint [23]. Since a leading coefficient of each polynomial of a segment does not vanish by the specialization, we can apply reductions of $K(\bar{A})[\bar{X}]^r$ where $K(\bar{A})$ is the field of rational functions. This is also one of optimization techniques.

Theorem 3 *The algorithm **CGSM** terminates for any input in $K[\bar{A}][\bar{X}]^r$. If H is the output of **CGSM**(F, \succ_m), then H is a comprehensive Gröbner system for $\langle F \rangle$ with respect to \succ_m on L^m .*

Proof First we show the termination. Obviously, the algorithms **GröbnerBasisM** and **factorize** terminate. We have to prove the termination of **CGSMmainM**. We suppose that **CGSMmainM**(F, Z, \succ_m) does not terminate, then there exists an infinite sequence F_0, F_1, \dots , such that $F_0 = F$ and $F_i \neq F_{i+1}$ for $i \in \mathbb{N}$. By the algorithm, $F_{s+1} = F_s \cup \{h_s\}$ for some $h_s \in K[\bar{A}]$ such that $h_s \notin \langle F_s \rangle$ where $s \in \mathbb{N}$. Hence we have $\langle F_s \rangle \subsetneq \langle F_{s+1} \rangle$ for each s . We know that every infinite ascending chain $M_1 \subseteq M_2 \subseteq \dots$ of submodules of $K[\bar{A}][\bar{X}]^r$ stabilizes. That is, there exists $N \in \mathbb{N}$ such that $M_N = M_{N+1} = \dots = M_{N+l} = \dots$ for all $0 \leq l$. Therefore, $\langle F_s \rangle \subsetneq \langle F_{s+1} \rangle$ for each s contradicts by the fact. **CGSMmainM** terminates. We next show that, if $(Z, h, G) \in H$, then the triple (Z, h, G) forms a segment of a comprehensive Gröbner system for $\langle F \rangle$, i.e., $\sigma_{\bar{a}}(G)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$ for each $\bar{a} \in \mathbb{V}(Z) \setminus \mathbb{V}(h)$. Let G be a Gröbner basis of the ideal $\langle F' \rangle$ with respect to \succ_m in $K[\bar{A}][\bar{X}]^r$, $B := \{g | g \in G \cap K[\bar{A}]e_i, \text{lc}_{\bar{A}}(g) \in \langle Z \rangle, \text{ for some } i \in \{1, \dots, r\}\}$ and $\{h_1, \dots, h_l\} := \{q | q \in \text{factorize}(\text{lc}_{\bar{A}}(g)), g \in G \setminus B\}$ and $h = \text{LCM}(h_1, \dots, h_l)$. Then by Theorem 2, $\sigma_{\bar{a}}(G)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F') \rangle$ for each $\bar{a} \in \mathbb{V}(Z) \setminus \mathbb{V}(h)$. In fact $\bar{a} \in \mathbb{V}(Z) \setminus \mathbb{V}(h)$ implies $\sigma_{\bar{a}}(G \setminus B) = \sigma_{\bar{a}}(G)$ and $\sigma_{\bar{a}}(F') = \sigma_{\bar{a}}(F)$. This means that $\sigma_{\bar{a}}(G)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$. We have to finally prove that the conditions in H covers the entire L^m , i.e., $L^m = \bigcup_{(P, h, G) \in H} \mathbb{V}(P) \setminus \mathbb{V}(h)$. In the algorithm, if the first “if” of **CGSM** is true, then the output is $\{(\emptyset, \{1\}, G)\}$. The condition is $\mathbb{V}(\emptyset) \setminus \mathbb{V}(1) = L^m$. If the second “if” of **CGSM** is false, then the output is $\{(\emptyset, \{1\}, G)\}$. The condition is L^m . If the second “if” of **CGSM** is true, then we have to consider $\{(\emptyset, h, G)\} \cup \text{CGSMmainM}(G \cup \{h_1e_1, \dots, h_1e_r\}, \{h_1\}, \succ_m) \cup \dots \cup \text{CGSMmainM}(G \cup \{h_1e_1, \dots, h_1e_r\}, \{h_l\}, \succ_m)$. Let us consider **CGSMmainM**(F, Z, \succ_m). Let G' be a Gröbner basis of $\langle F \rangle$ with respect to \succ_m in $K[\bar{A}][\bar{X}]^r$ and let $h' = h'_1 \cdots h'_l$ in $K[\bar{A}]$. Then, the equation $\mathbb{V}(Z) = (\mathbb{V}(Z) \setminus \mathbb{V}(h')) \cup \bigcup_{i=1}^l \mathbb{V}(Z \cup h'_i)$ always holds.

By the induction on the well-founded tree of the algorithm, this equation follows. Therefore, the condition of $\{(\emptyset, h', G)\} \cup \text{CGSMMainM}(G \cup \{h'_1 e_1, \dots, h'_l e_r\}, \{h'_1\}, \succ_m) \cup \dots \cup \text{CGSMMainM}(G \cup \{h'_l e_1, \dots, h'_l e_r\}, \{h'_l\}, \succ_m)$ is L^m .

This algorithm CGSM has been implemented in the computer algebra system Risa/Asir by the author. This program have been published on the following web pages <http://www.math.sci.osaka-u.ac.jp/~nabeshima/PGB/>.

Example 3 Let x, y be variables, a, b parameters and \succ_{lex} the lexicographic order on $\text{pp}(x, y)$. We consider $f_1 = \begin{pmatrix} ax - bx + 1 \\ ax^2y + ax + b \end{pmatrix}$ and $f_2 = \begin{pmatrix} by + a \\ bx^2 + bx + 2 \end{pmatrix}$ in $\mathbb{Q}[a, b][x, y]^2$. Then, our program outputs the following list which is a comprehensive Gröbner system for $\langle f_1, f_2 \rangle$ w.r.t. (POT, \succ_{lex}) s.t. $x \succ_{lex} y$.

```
[a-b]==0,    (b) !=0,
[0, (b^2*y^2+b^2*y-b) *x^2+(b^2*y+b^2-b) *x+b^2*y+b^2-2]
[1, b*y*x^2+b*x+b]
```

```
[b, a]==0,    (1) !=0,
[0, 1]
[1, 0]
```

```
[b]==0,    (a) !=0,
[0, -a^2*y*x^2+(-a^2+2*a) *x+2]
[1, a*y*x^2+(a-2) *x]
```

```
[0]==0,    (b) *(a-b) !=0,
[0, (-b*a+b^2) *x^3+(b*a*y^2+a^2*y-b*a+b^2-b) *x^2
  +(b*a*y+a^2-2*a+b) *x+b^2*y+b*a-2]
[b*y+a, b*x^2+b*x+2]
[(a-b) *x+1, a*y*x^2+a*x+b]
```

The output means the following:

If $\mathbb{V}(a-b) \setminus \mathbb{V}(b)$, then $\left\{ \begin{pmatrix} 0 \\ (*1) \end{pmatrix}, \begin{pmatrix} 1 \\ byx^2 + bx + b \end{pmatrix} \right\}$.

If $\mathbb{V}(a, b)$, then $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.

If $\mathbb{V}(b) \setminus \mathbb{V}(a)$, then $\left\{ \begin{pmatrix} 0 \\ -a^2yx^2 + (-a^2 + 2a)x + 2 \end{pmatrix}, \begin{pmatrix} 1 \\ ayx^2 + (a-2)x \end{pmatrix} \right\}$.

If $\mathbb{C}^2 \setminus \mathbb{V}((a-b)b)$, then $\left\{ \begin{pmatrix} 0 \\ (*2) \end{pmatrix}, \begin{pmatrix} by + a \\ bx^2 + bx + 2 \end{pmatrix}, \begin{pmatrix} (a-b)x + 1 \\ ayx^2 + ax + b \end{pmatrix} \right\}$,

where $(*1) = (b^2y^2 + b^2y - b)x^2 + (b^2y + b^2 - b)x + b^2y + b^2 - 2$ and $(*2) = (-ba + b^2)x^3 + (bay^2 + a^2y - ba + b^2 - b)x^2 + (bay + a^2 - 2a + b)x + b^2y + ba - 2$.

2.3 Comprehensive Gröbner bases for modules

Here we present an algorithm that provides an explicit construction of a comprehensive Gröbner basis for $\langle F \rangle$ from any finite set $F \subset K[\bar{A}][\bar{X}]^r$ via the intermediate concept of a Gröbner system.

Definition 8 (*Comprehensive Gröbner Bases*) Let F and G be sets of vectors in $K[\bar{A}][\bar{X}]^r$ and \succ_m a module order on $\text{pp}(\bar{X})^r$. $G \subset \langle F \rangle$ is called a comprehensive Gröbner basis (CGB) for $\langle F \rangle$ with respect to \succ_m if for all $\bar{a} \in L^m$, $\sigma_{\bar{a}}(G)$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F) \rangle$ with respect to \succ_m in $L[\bar{X}]^r$.

Example 4 Let $F = \{ax^2y + y, bx^2y^2 + ax + y\} \subset \mathbb{Q}[a, b][x, y]^1$, a, b parameters, x, y variables and \succ the lexicographic order s.t. $x \succ y$. Then, a comprehensive Gröbner basis for $\langle F \rangle$ w.r.t. \succ , is $G = \{bxy^3 - axy^2 + ay, a^2x - by^2 + ay, -b^2y^5 + 2aby^4 - a^2y^3 - a^3y, -bx^3y^3 - xy^2 + y, bx^2y^2 + ax + y, bx^2y^4 + bxy^3 + y^3 + ay, ax^2y + y\}$. Even if we substitute arbitrary values for the parameter a, b of the set G , the set $\{\sigma(G)\}$ is always a Gröbner basis for $\langle \sigma(F) \rangle$ with respect to \succ where σ is a specialization.

We already saw comprehensive Gröbner systems in the previous subsection, which has conditions of parameters (cells of the parameter space). However, comprehensive Gröbner bases don't have conditions of parameters (cells of the parameter space). A comprehensive Gröbner basis is a set of vectors. In this point, comprehensive Gröbner bases are different from comprehensive Gröbner systems. In this subsection we consider an algorithm for computing comprehensive Gröbner bases. We need the following concept for constructing an algorithm for computing them.

Definition 9 Let F be a set of vectors in $K[\bar{A}][\bar{X}]^r$, $s_1, \dots, s_l, t_1, \dots, t_l \subset K[\bar{A}]$ and $G_1, \dots, G_l \subset K[\bar{A}][\bar{X}]^r$. Then a comprehensive Gröbner system $\{(\mathbb{V}(s_1) \setminus \mathbb{V}(t_1), G_1), \dots, (\mathbb{V}(s_l) \setminus \mathbb{V}(t_l), G_l)\}$ for $\langle F \rangle$ is called *faithful* if $G_i \subset \langle F \rangle$ for each $i = 1, \dots, l$.

In fact, in this subsection we describe an algorithm for computing *faithful* comprehensive Gröbner systems. If $\{(\mathbb{V}(s_1) \setminus \mathbb{V}(t_1), G_1), \dots, (\mathbb{V}(s_l) \setminus \mathbb{V}(t_l), G_l)\}$ is a faithful comprehensive Gröbner system for $\langle F \rangle$, then by Definition 8, $G_1 \cup \dots \cup G_l$ is a comprehensive Gröbner basis for $\langle F \rangle$. Hence, we modify the algorithm **CGSMaInM** to compute faithful comprehensive Gröbner systems. The key idea which is from [23], is to apply a new auxiliary variable U besides \bar{X} and \bar{A} . We follow this technique to compute comprehensive Gröbner bases for modules.

We define homomorphisms σ^0 and σ^1 from $K[\bar{A}][U, \bar{X}]^r$ to $K[\bar{A}][\bar{X}]^r$ as a specialization of U with 0 and 1, respectively, i.e. $\sigma^0(f(U, \bar{A}, \bar{X})) = f(0, \bar{A}, \bar{X})$ and $\sigma^1(f(U, \bar{A}, \bar{X})) = f(1, \bar{A}, \bar{X})$. Before we describing the algorithm for computing comprehensive Gröbner bases, we need the following lemma which is also from [23].

Lemma 2 [23, Lemma 3.1] *Let F and S be subsets of $K[\bar{A}][\bar{X}]^r$. For any $g \in \langle (U \cdot F) \cup (U - 1) \cdot S \rangle \subseteq K[\bar{A}][U, \bar{X}]^r$, then $\sigma^0(g) \in \langle S \rangle \subseteq K[\bar{A}][\bar{X}]^r$ and $\sigma^1(g) \in \langle F \rangle \subseteq K[\bar{A}][\bar{X}]^r$.*

In order to construct an algorithm for computing comprehensive Gröbner bases in $K[\bar{A}][\bar{X}]^r$, we need the following special hybrid order. This order is the key for our

main result of this subsection. In fact, this special order and the new variable U always tell us what the leading monomial of a vector under specializations. Moreover, even if we apply the special order for computing Gröbner bases, our algorithm for computing comprehensive Gröbner bases, is still simple like the algorithm CGSM.

Definition 10 (Hybrid module order 2) Let \succ_m be a module order on $K[\bar{X}]^r$. Then, a hybrid module order 2 \succ_{hm2} on $\text{pp}(U, \bar{X})^r$ is defined as follows

$$U^{\alpha_1} x^{\alpha_2} e_i \succ_{hm2} U^{\beta_1} x^{\beta_2} e_j \iff \alpha_1 > \beta_1 \quad \text{or} \quad (\alpha_1 = \beta_1 \text{ and } x^{\alpha_2} e_i \succ_m x^{\beta_2} e_j),$$

for all $\alpha_1, \beta_1 \in \mathbb{N}$, $\alpha_2, \beta_2 \in \mathbb{N}^n$, $i, j = 1, \dots, r$. This hybrid module order 2 with respect to a variable U is written as $\succ_{hm2} := (U, \succ_m)$.

Remark If \succ_m is TOP, then we have to consider the following order: $U \succ \bar{X} \succ e_1 \succ e_2 \succ \dots \succ e_r$. Actually, this order is still TOP. If \succ_m is POT, then we have to consider the following order: $U \succ e_1 \succ e_2 \succ \dots \succ e_r \succ \bar{X}$. This order is not POT or TOP. In fact, when we compute a comprehensive Gröbner basis, we need two special module orders “hybrid module order 1” and “hybrid module order 2”. Since these hybrid orders are very complicated, we have to be careful when we compute a comprehensive Gröbner basis.

The next theorem is the main result of this subsection. By the following theorem, we can construct an algorithm for computing comprehensive Gröbner bases.

Theorem 4 Let F be a subset of $K[\bar{A}][\bar{X}]^r$, S' a subset of $K[\bar{A}]$, $S := \{se_i | s \in S', 1 \leq i \leq r\}$ and \succ_m a module order on $\text{pp}(\bar{X})^r$. Let G be a Gröbner basis of $\langle (U \cdot F) \cup (U - 1) \cdot S \rangle$ in $K[\bar{A}][U, \bar{X}]^r$ with respect to a “hybrid module order 2” $\succ_{hm2} = (U, \succ_m)$. Suppose that $B_1 := \{g | g \in G \cap K[\bar{A}][U]e_i, \text{lc}_{\bar{A}}(g) \in \langle S' \rangle, \text{ for some } i \in \{1, \dots, r\}\}$, $B_2 := \{g | g \in G, \deg_U(\text{lpp}_{\bar{A}}(g)) = 0\}$, $G' := \{g | g \in G \setminus (B_1 \cup B_2)\}$ and $\{h_1, \dots, h_l\} := \{\text{lc}_{\bar{A}}(g) | g \in G'\} \subseteq K[\bar{A}]$. Then, for all $\bar{a} \in \mathbb{V}(S') \setminus \mathbb{V}(h)$, $\sigma_{\bar{a}}(\sigma^1(G))$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F) \rangle$ with respect to \succ_m in $L[\bar{X}]^r$ where $h = \text{LCM}(h_1, \dots, h_l)$. (In fact, $\sigma_{\bar{a}}(\sigma^1(G)) = \sigma_{\bar{a}}(\sigma^1(G'))$.)

Proof Note that any vector of G' has a linear form of U , i.e., the degree of U is at most 1. It is clearly that $\sigma^1(G)$ is a basis of $\langle F \rangle$ by Lemma 2. We prove that $\sigma_{\bar{a}}(\sigma^1(G))$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$. For all $\bar{a} \in \mathbb{V}(S') \setminus \mathbb{V}(h)$ and $g \in G'$, we have $\sigma_{\bar{a}}(\text{lc}_{\bar{A}}(g)) \neq 0$. By the definition of G' , B_1 and B_2 , we have $G = G' \cup B_1 \cup B_2$. For each $f \in B_1$, f can be written as $f = U \cdot f_1 e_i + f_2 e_i$ where $f_1, f_2 \in K[\bar{A}]$ for some $i \in \{1, \dots, r\}$. By Lemma 2, $\sigma^0(f) = f_2 e_i \in \langle S \rangle$, thus $\sigma_{\bar{a}}(f_2 e_i) = 0$. By the definition of B_1 , $\text{lc}_{\bar{A}}(f) = f_1 \in \langle S' \rangle$, so $\sigma_{\bar{a}}(f_1) = 0$. Hence, $\sigma_{\bar{a}}(f) = 0$. For all $q \in B_2$, by Lemma 2, $\sigma^0(q) = q \in \langle S \rangle$. Thus $\sigma_{\bar{a}}(q) = 0$. Even if we change a module order \succ_m into a “hybrid module order 2” \succ_{hm2} in Theorem 1, the properties of Theorem 1 hold. Thus, $\sigma_{\bar{a}}(G) = \sigma_{\bar{a}}(G \setminus (B_1 \cup B_2)) = \sigma_{\bar{a}}(G')$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(U \cdot F \cup (U - 1) \cdot S) \rangle$ with respect to \succ_{hm2} in $L[U, \bar{X}]^r$. For each $g \in G'$, g can be written as $g = U \cdot g_1 + g_2$ where $g_1, g_2 \in K[\bar{A}][\bar{X}]^r$. By Lemma 2, we have $\sigma^0(g) = g_2 \in \langle S \rangle$, thus $\sigma_{\bar{a}}(g_2) = 0$. Namely, we have $\sigma_{\bar{a}}(g) = \sigma_{\bar{a}}(U \cdot g_1)$. Since every power product of $\sigma_{\bar{a}}(G')$ has the new variable U whose degree is 1 and $U \gg \bar{X}$, $\sigma^1(\sigma_{\bar{a}}(G'))$ is a Gröbner basis of $\langle \sigma^1(\sigma_{\bar{a}}(U \cdot F) \cup (U - 1) \cdot S) \rangle = \langle \sigma^1(\sigma_{\bar{a}}(U \cdot F)) \rangle = \langle \sigma_{\bar{a}}(F) \rangle$. Therefore, it follows that $\sigma_{\bar{a}}(\sigma^1(G))$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F) \rangle$ in $L[\bar{X}]^r$.

Remark In Theorem 4, we need to compute a Gröbner basis for $\langle (U \cdot F) \cup (U - 1) \cdot S \rangle$ in $K[\bar{A}][U, \bar{X}]^r$ with respect to \succ_{hm2} . Probably, one has the following question: “How do we compute this Gröbner basis?” In fact, we consider two kinds of module orders POT and TOP as \succ_m . If \succ_m is a POT in Theorem 4, by the hybrid module order $2 \succ_{hm2}$, we have to consider the following order: $U \succ e_1 \succ e_2 \succ \cdots \succ e_r \succ \bar{X}$. Now, we consider a “hybrid module order 1” (\succ_{hm2}, \succ_1) on $\text{pp}(\bar{A}, U, \bar{X})^r$ where \succ_1 is a term order on $\text{pp}(\bar{A})$, i.e. $U \succ e_1 \succ \cdots \succ e_r \succ \bar{X} \succ \bar{A}$. (Obviously, $K[\bar{A}][U, \bar{X}]^r$ can be seen as $K[\bar{A}, U, \bar{X}]^r$.) We know the algorithm GröbnerBasisM for computing Gröbner bases. Therefore, by the algorithm GröbnerBasisM and the hybrid module order 1 (\succ_{hm2}, \succ_1), we can compute a Gröbner basis for $\langle (U \cdot F) \cup (U - 1) \cdot S \rangle$ in $K[\bar{A}][U, \bar{X}]^r$ with respect to \succ_{hm2} . (I.e. GröbnerBasisM(F, \succ_{hm2}).)

If \succ_m is a TOP in Theorem 4, by the hybrid module order $2 \succ_{hm2}$, we have to consider the following order: $U \succ \bar{X} \succ e_1 \succ e_2 \succ \cdots \succ e_r$. We consider a “hybrid module order 1” (\succ_{hm2}, \succ_1) on $\text{pp}(\bar{A}, U, \bar{X})^r$ where \succ_1 is a term order on $\text{pp}(\bar{A})$, i.e. $U \succ \bar{X} \succ e_1 \succ \cdots \succ e_r \succ \bar{A}$. Therefore, by the algorithm GröbnerBasisM and the hybrid module order 1 (\succ_{hm2}, \succ_1), we can compute a Gröbner basis for $\langle (U \cdot F) \cup (U - 1) \cdot S \rangle$ in $K[\bar{A}][U, \bar{X}]^r$ with respect to \succ_{hm2} .

Theorem 4 leads us to have the following algorithm which outputs a faithful comprehensive Gröbner system for $\langle F \rangle$ on L^m .

Algorithm 24 FCGSM(F, \succ_m) (Faithful CGS for Modules)

Input F : a finite set of vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,
Output G : a faithful comprehensive Gröbner system for $\langle F \rangle$ w.r.t. \succ_m on L^m .
begin
 $H \leftarrow \text{GröbnerBasisM}(F, \succ_m)$
if $e_1, \dots, e_r \in H$ **then** $G \leftarrow \{(\emptyset, \{1\}, H)\}$ **end-if**
 $S \leftarrow \{h_1, \dots, h_l\} := \{q \mid q \in \text{factorize}(\text{lc}_{\bar{A}}(g)), \text{lc}_{\bar{A}}(g) \notin K, g \in H\}$
if $S \neq \emptyset$ **then**
 $h \leftarrow \text{LCM}(h_1, \dots, h_l)$
 $G \leftarrow \{(\emptyset, h, H)\} \cup \text{CGBMainM}(H, \{h_1 e_1, \dots, h_l e_r\}, \{h_1\}, \succ_m) \cup$
 $\quad \dots \cup \text{CGBMainM}(H, \{h_l e_1, \dots, h_l e_r\}, \{h_l\}, \succ_m)$
else $G \leftarrow \{(\emptyset, \{1\}, H)\}$
end-if
return(G)
end

Algorithm 25 CGBMainM(F, S, Z, \succ_m)

Input F : a finite set of $K[\bar{A}][\bar{X}]^r$, Z : a finite set of polynomials in $K[\bar{A}]$,
 $S = \{q \mid q = p e_i, p \in Z, \text{ for each } i \in \{1, \dots, r\}\}$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,
Output G : a faithful comprehensive Gröbner system for $\langle F \rangle$ w.r.t. \succ_m on $\mathbb{V}(Z)$.
begin
 $H \leftarrow \text{GröbnerBasisM}(U \cdot F \cup ((U - 1) \cdot S, \succ_{hm2}))$ where $\succ_{hm2} := (U, \succ_m)$
 $C \leftarrow$ the reduced Gröbner basis for $\langle Z \rangle$ in $K[\bar{A}]$

```

if  $1 \in C$  then  $G \leftarrow \emptyset$  end-if
   $B_1 \leftarrow \{g \mid g \in H \cap K[\bar{A}][U]e_i, \text{lc}_{\bar{A}}(g) \in \langle Z \rangle, \text{ for some } i \in \{1, \dots, r\}\}$ 
   $B_2 \leftarrow \{g \mid g \in H, \deg_U(\text{lpp}_A(g)) = 0\}; H' \leftarrow H \setminus (B_1 \cup B_2)$ 
   $M \leftarrow \{\text{lc}_{\bar{A}}(g) \mid g \in H'\}$ 
   $L \leftarrow \{\beta_1, \dots, \beta_l\} := \{q \mid q \in \text{factorize}(g), g \notin K, g \in M\}$ 
if  $L \neq \emptyset$  then
   $\beta \leftarrow \text{LCM}(\beta_1, \dots, \beta_l)$ 
   $G \leftarrow \{(Z, \beta, \sigma^1(H'))\} \cup \text{CGBMainM}(F, S \cup \{\beta_1 e_1, \dots, \beta_l e_r\}, Z \cup \{\beta_1\}, \succ_m) \cup$ 
     $\dots \cup \text{CGBMainM}(F, S \cup \{\beta_l e_1, \dots, \beta_l e_r\}, Z \cup \{\beta_l\}, \succ_m)$ 
else  $G \leftarrow \{(Z, \{1\}, \sigma^1(H'))\}$ 
end-if
return( $G$ )
end

```

Remark Like the remark of Algorithm 22, we are also able to apply a lot of optimization techniques for getting small and nice outputs.

Theorem 5 *The algorithm $\text{FCGSM}(F, \succ_m)$ terminates, and the output of FCGSM is a faithful comprehensive Gröbner system for $\langle F \rangle$ w.r.t. \succ_m on L^m .*

Proof All notations of this proof is from Algorithm 24 and 25. In order to show the termination of the algorithm, it suffices to show that any of $\{\beta_j e_1, \dots, \beta_j e_r\}$ is not in the submodule $\langle S \rangle$ where $j \in \{1, \dots, l\}$ because this algorithm is almost same as the algorithm CGSM (see Theorem 3) (and we have $\sigma_{\bar{a}}(B_1) = \sigma_{\bar{a}}(B_2) = 0$ where $\bar{a} \in \mathbb{V}(S') \setminus \mathbb{V}(h)$). By the construction of β_j , there exists $g \in H$ such that $\beta_j = \text{lc}_{\bar{A}}(g)$, $\text{lpp}_{\bar{A}}(g) \notin \text{pp}(\bar{X})^r$. Therefore g can be written as $g = \beta_j U T + g_1$, where $T \in \text{pp}(\bar{X})^r$, $\text{lpp}_{\bar{A}}(g) = U \cdot T$ and $g_1 \in K[\bar{A}][U, \bar{X}]^r$. If $\beta_j e_1, \dots, \beta_j e_r \in \langle S \rangle$, then $\beta_j e_i \cdot (U - 1) \in \langle G \rangle$ where $1 \leq i \leq r$. Hence, $\text{lm}_{\bar{A}}(\beta_j e_i \cdot (U - 1)) = \text{lm}_{\bar{A}}(\beta_j e_i \cdot U)$ must be reduced by G . In the algorithm GröbnerBasisM, we need to compute the reduced Gröbner basis for $\langle U \cdot F \cup (U - 1) \cdot S \rangle$ in $K[\bar{A}, U, \bar{X}]^r$ with respect to a hybrid module order 2 “ $\succ_{hm2} = (U, \succ_{hm1})$ ” where $\succ_{hm1} = (\succ_m, \succ_1)$ is a hybrid module order 1. Since G is the reduced Gröbner basis in $K[\bar{A}, U, \bar{X}]^r$, this is the contradiction. Therefore, $\beta_j e_i$ is not in the submodule $\langle S \rangle$. It is an easy consequence of Theorem 3 and Lemma 2 that the output of FCGSM is a faithful comprehensive Gröbner system for $\langle F \rangle$ on L^m .

Now, it is clear that the following algorithm outputs a comprehensive Gröbner bases for modules.

Algorithm 26 $\text{CGBM}(F, \succ_m)$ (CGB for Modules)

Input F : a finite set of vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,

Output G : a comprehensive Gröbner basis for $\langle F \rangle$ w.r.t. \succ_m .

begin

$G \leftarrow \emptyset; H \leftarrow \text{FCGSM}(F, \succ_m)$

while $H \neq \emptyset$


```

    Select  $(h_1, h_2, G_1)$  from  $H$ ;  $H \leftarrow H \setminus \{(h_1, h_2, G_1)\}$ ;  $G \leftarrow G \cup G_1$ 
end-while
return( $G$ )
end

```

This algorithm has been implemented in the computer algebra system Risa/Asir by the author. This program have been published on the following web pages <http://www.math.sci.osaka-u.ac.jp/~nabeshima/PGB/>.

Example 5 Let x, y be variables and a, b parameters and \succ_{lex} the lexicographic order. We consider $f_1 = \begin{pmatrix} ax - bx + 1 \\ ax^2y + ax + b \end{pmatrix}$ and $f_2 = \begin{pmatrix} by + a \\ bx^2 + bx + 2 \end{pmatrix}$ in $\mathbb{Q}[a, b][x, y]^2$. Then, our program outputs the following list which is a comprehensive Gröbner bases for $\langle f_1, f_2 \rangle$ w.r.t. (POT, \succ_{lex}) such that $x \succ_{lex} y$.

```

[ 0, (-b*a+b^2) *x^3+(b*a*y^2+a^2*y-b*a+b^2-b) *x^2
  +(b*a*y+a^2-2*a+b) *x+b^2*y+b*a-2]
[b*y+a, b*x^2+b*x+2]
[(a-b) *x+1, a*y*x^2+a*x+b]
[(-b*y-b) *x+1, -b*x^3+(a*y-b) *x^2+(a-2) *x+b]

```

This means

$$\left\{ \begin{pmatrix} 0 \\ (*1) \end{pmatrix}, \begin{pmatrix} by + a \\ bx^2 + bx + 2 \end{pmatrix}, \begin{pmatrix} (a-b)x + 1 \\ ayx^2 + ax + b \end{pmatrix}, \begin{pmatrix} (-by-b)x + 1 \\ (*2) \end{pmatrix} \right\},$$

where $(*1) := (-ba + b^2)x^3 + (bay^2 + a^2y - ba + b^2 - b)x^2 + (bay + a^2 - 2a + b)x + b^2y + ba - 2$ and $(*2) = -bx^3 + (ay - b)x^2 + (a - 2)x + b$.

3 Parametric syzygies

Here we treat an algorithm for computing parametric syzygies of parametric vectors (or polynomials). In general, there are close relations between Gröbner bases and syzygies. In this section, we see the relations for parametric vectors (or polynomials), and construct an algorithm for computing parametric syzygies.

Let $f_1, \dots, f_l \in K[\bar{X}]^r$. Then, a module of syzygies of (f_1, \dots, f_l) is written as $\text{syz}(f_1, \dots, f_l)$, i.e., $\text{syz}(f_1, \dots, f_l) := \{(g_1, \dots, g_l) \in K[\bar{X}]^l \mid g_1, \dots, g_l \in K[\bar{X}], \sum_{i=1}^l g_i f_i = 0\}$.

Definition 11 (*Parametric Syzygy systems*) Let f_1, \dots, f_k be vectors in $K[\bar{A}][\bar{X}]^r$, $\mathcal{A}_1, \dots, \mathcal{A}_l$ be algebraically constructible subsets of L^m and G_1, \dots, G_l be subsets of $K[\bar{A}][\bar{X}]^r$. Let \mathcal{S} be a subset of L^m such that $\mathcal{S} \subseteq \mathcal{A}_1 \cup \dots \cup \mathcal{A}_l$. A finite set $\mathcal{G} = \{(\mathcal{A}_1, G_1), \dots, (\mathcal{A}_l, G_l)\}$ of pairs is called a *parametric syzygy system* on \mathcal{S} of (f_1, \dots, f_k) if for each $i \in \{1, \dots, l\}$ and $\bar{a} \in \mathcal{A}_i$, $\sigma_{\bar{a}}(G_i)$ is a basis of a module of syzygies of $(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$, i.e. $\langle \sigma_{\bar{a}}(G_i) \rangle = \text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$ on \mathcal{A}_i . Each (\mathcal{A}_i, G_i) is called a segment of \mathcal{G} . We simply say \mathcal{G} is a parametric syzygy system of F if $\mathcal{S} = L^m$.

Suppose that \mathcal{G} is a comprehensive syzygy of $\{f_1, \dots, f_k\} \subset K[\bar{A}][\bar{X}]^r$. Then, for $(\mathcal{A}_i, G_i) \in \mathcal{G}$ and $\bar{a} \in \mathcal{A}_i$, $(g_1, \dots, g_k)^T \in \langle G_i \rangle \subseteq K[\bar{A}][\bar{X}]^k$ satisfies $\sum_{j=1}^k \sigma_{\bar{a}}(g_j) \sigma_{\bar{a}}(f_j) = 0$.

The following lemma and theorem tell us how to compute a parametric syzygy system of a set of vectors.

Lemma 3 *Let $F = \{f_1, \dots, f_k\}$ be a set of vectors in $K[\bar{A}][\bar{X}]^r$, S a set of polynomials in $K[\bar{A}]$ and $T = \{se_i | s \in S, 1 \leq i \leq r\}$. Furthermore, $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of a submodule $\langle F \cup T \rangle \subseteq K[\bar{A}][\bar{X}]^r$ with respect to $\succ_m := (\text{POT}, \succ)$ where \succ is a term order on $\text{pp}(\bar{X})$. Let that $B =: \{g | g \in G \cap K[\bar{A}]e_i, \text{lc}_{\bar{A}}(g) \in \langle S \rangle, 1 \leq i \leq r\}$, $\{h_1, \dots, h_l\} = \{\text{lc}_{\bar{A}}(g) | g \in G \setminus B\} \subseteq K[\bar{A}]$ and $h = \text{LCM}(h_1, \dots, h_l)$, and fix $s = 0, \dots, r-1$ arbitrary. Then, set $G' := G \cap \bigoplus_{i=s+1}^r K[\bar{A}][\bar{X}]e_i$, and $F' := \langle F \rangle \cap \bigoplus_{i=s+1}^r K[\bar{A}][\bar{X}]e_i$. Then, for all $\bar{a} \in \mathbb{V}(S) \setminus \mathbb{V}(h)$, $\sigma_{\bar{a}}(G')$ is a Gröbner basis for $\langle \sigma_{\bar{a}}(F') \rangle$ with respect to \succ_m in $L[\bar{X}]^r$.*

Proof By Theorem 1 and Theorem 2, for all $\bar{a} \in \mathbb{V}(S) \setminus \mathbb{V}(h)$, $\sigma_{\bar{a}}(G)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$. Let $b \in \langle F' \rangle$, then we have to prove that there exists $f \in G'$ such that $\text{lm}(\sigma_{\bar{a}}(f)) | \text{lm}(\sigma_{\bar{a}}(b))$. Since $\sigma_{\bar{a}}(G \setminus B)$ is a Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$ in $K[\bar{A}]^r$, there exists $f \in \sigma_{\bar{a}}(G \setminus B)$ such that $\text{lm}(f)$ divides $\sigma_{\bar{a}}(b)$. In particular, $\text{lm}(\sigma_{\bar{a}}(f)) \in \bigoplus_{i=s+1}^r K[\bar{X}]e_i$. Actually, by the assumption, we have $\text{lm}(\sigma_{\bar{a}}(f)) = \sigma_{\bar{a}}(\text{lm}(f))$ and $\sigma_{\bar{a}}(f) \neq 0$. Therefore, by these facts and the definition of the module order \succ_m , we obtain $f \in \bigoplus_{i=s+1}^r K[\bar{X}]e_i$. In particular, $f \in G'$.

Theorem 6 *Let $F = \{f_1, \dots, f_k\}$ be a set of vectors in $K[\bar{A}][\bar{X}]^r$. Consider the canonical embedding $K[\bar{A}][\bar{X}]^r \subseteq K[\bar{A}][\bar{X}]^{r+k}$ and the canonical projection $\pi: K[\bar{A}][\bar{X}]^{r+k} \rightarrow K[\bar{A}][\bar{X}]^k$. Let S be a set of polynomials in $K[\bar{A}]$ and $T = \{se_i | s \in S, 1 \leq i \leq r\}$. Furthermore, $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of a submodule $\langle \{f_1 + e_{r+1}, f_2 + e_{r+2}, \dots, f_k + e_{r+k}\} \cup T \rangle \subseteq K[\bar{A}][\bar{X}]^{r+k}$ with respect to $\succ_m := (\text{POT}, \succ)$, $B =: \{g | g \in G \cap K[\bar{A}]e_i, \text{lc}_{\bar{A}}(g) \in \langle S \rangle, 1 \leq i \leq r\}$, $\{h_1, \dots, h_l\} = \{\text{lc}_{\bar{A}}(g) | g \in G \setminus B\} \subseteq K[\bar{A}]$ and $h = \text{LCM}(h_1, \dots, h_l)$ where \succ is a term order on $\text{pp}(\bar{X})$. Suppose that $\{g_1, \dots, g_l\} = \{G \setminus B\} \cap \bigoplus_{i=r+1}^{r+k} K[\bar{A}][\bar{X}]e_i$, then for all $\bar{a} \in \mathbb{V}(S) \setminus \mathbb{V}(h)$, $\text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k)) = \langle \sigma_{\bar{a}}(\pi(g_1)), \dots, \sigma_{\bar{a}}(\pi(g_l)) \rangle$.*

Proof We know that $\sigma_{\bar{a}}(\{f_1 + e_{r+1}, f_2 + e_{r+2}, \dots, f_k + e_{r+k}\} \cup T) = \{\sigma_{\bar{a}}(f_1) + e_{r+1}, \dots, \sigma_{\bar{a}}(f_k) + e_{r+k}\}$. Let us define $F' := \langle \sigma_{\bar{a}}(f_1) + e_{r+1}, \dots, \sigma_{\bar{a}}(f_k) + e_{r+k} \rangle$. First, we prove that $\pi(F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i) = \text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$.

(\subseteq) Let $h \in F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i$, that is, $h = \sum_{v=r+1}^{r+k} h_v e_v = \sum_{j=1}^k b_j (\sigma_{\bar{a}}(f_j) + e_{r+j})$, for suitable $b_j \in K[\bar{X}]$. This implies that $\sum_{j=1}^k b_j \sigma_{\bar{a}}(f_j) = 0$ and $b_j = h_{r+j}$. Therefore, $\pi(h) \in \text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$.

(\supseteq) Let $h = (h_1, \dots, h_k) \in \text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$, that is, we have $\sum_{v=1}^k h_v \sigma_{\bar{a}}(f_v) = 0$. Then, $h' = \sum_{v=1}^k h_v (\sigma_{\bar{a}}(f_v) + e_{r+v}) \in F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i$. Obviously, $h = \pi(h') \in \pi(F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i)$. Therefore, $\pi(F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i) = \text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$.

Next, we have to consider generators of $\text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k))$. By Lemma 3, $\sigma_{\bar{a}}(G \setminus B) \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i$ is a Gröbner basis of $\langle F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i \rangle$.

Therefore, $\text{syz}(\sigma_{\bar{a}}(f_1), \dots, \sigma_{\bar{a}}(f_k)) = \pi(F' \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i) = \pi(\langle \sigma_{\bar{a}}(G) \rangle \cap \bigoplus_{i=r+1}^{r+k} K[\bar{X}]e_i) = \langle \pi(\sigma_{\bar{a}}(g_1)), \dots, \pi(\sigma_{\bar{a}}(g_l)) \rangle = \langle \sigma_{\bar{a}}(\pi(g_1)), \dots, \sigma_{\bar{a}}(\pi(g_l)) \rangle$.

By the algorithm CGSM, we already know how to compute a parametric Gröbner system. Now we can construct an algorithm for computing parametric syzygy systems.

Algorithm 31 PSS($\{f_1, \dots, f_k\}, \succ_m$) (Parametric Syzygy Systems)

Input: f_1, \dots, f_k : vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m : a module order on $\text{pp}(\bar{X})^r$,

Output: H : a parametric syzygy system of f_1, \dots, f_k on L^m .

begin

$H \leftarrow \emptyset$; $F \leftarrow \{f_1 + e_{r+1}, \dots, f_k + e_{r+k}\}$; $D \leftarrow \text{CGSM}(F, \succ_m)$

while $D \neq \emptyset$ **do**

Select $(h1, h2, G)$ from D ; $D \leftarrow D \setminus \{(h1, h2, G1)\}$

$H \leftarrow H \cup \left\{ \left(h1, h2, \pi \left(G \cap \bigoplus_{i=r+1}^{r+k} K[\bar{A}][\bar{X}]e_i \right) \right) \right\}$ (see below (*))

end-while

return(H)

end

(*) π is the canonical projection

$\pi : K[\bar{A}][\bar{X}]^{r+k} \rightarrow K[\bar{A}][\bar{X}]^k, (a_1, \dots, a_r, a_{r+1}, \dots, a_{r+k}) \mapsto (a_1, \dots, a_r)$.

Theorem 7 The algorithm PSS terminates for any input of a finite subset F of $K[\bar{A}][\bar{X}]^r$. If H is the output of PSS(F, \succ_m), then H is a parametric syzygy system of F on L^m .

Proof Since the algorithm CGSM terminates by Theorem 3, the algorithm PSS terminates. By Theorem 6 and algorithm CGSM, H is a parametric syzygy system of F on L^m .

The algorithm PSS has been implemented in the computer algebra system Risa/Asir by the author. This program have been published on the following web pages <http://www.math.sci.osaka-u.ac.jp/~nabeshima/PGB/>.

Example 6 Let $f_1 = x^2 + ay$, $f_2 = x + b$, $f_3 = bx + y$ be polynomials in $\mathbb{C}[a, b][x, y]$, a, b parameters and x, y variables. We consider the lexicographic order \succ s.t. $x \succ y$. Then, the program outputs the following as a parametric syzygy system of (f_1, f_2, f_3) (w.r.t. \succ).

```
[0]==0,      (b)*(a+1)!=0,
[-x-b, x^2+a*y, 0]
[-y+b^2, y*x-b*a*y, -b*x+a*y]
[0, b*x+y, -x-b]
```

```
[b]==0,      (1)!=0,
[1, -x, -a]
```

$[0, y, -x]$

$[a+1] == 0, \quad (b) != 0,$

$[1, -x, 1]$

$[0, b*x+y, -x-b]$

This output means the following

$$\left\{ \begin{array}{ll} \left(\begin{pmatrix} -x-b \\ x^2+ay \\ 0 \end{pmatrix}, \begin{pmatrix} -y+b^2 \\ yx-bay \\ -bx+ay \end{pmatrix}, \begin{pmatrix} 0 \\ bx+y \\ -x-b \end{pmatrix} \right), & \text{if } \mathbb{C}^2 \setminus \mathbb{V}(b(a+1)), \\ \left(\begin{pmatrix} 1 \\ -x \\ -a \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ -x \end{pmatrix} \right), & \text{if } \mathbb{V}(b), \\ \left(\begin{pmatrix} 1 \\ -x \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ bx+y \\ -x-b \end{pmatrix} \right), & \text{if } \mathbb{V}(a+1) \setminus \mathbb{V}(b). \end{array} \right.$$

Probably, one has the following question.

Question: Can we change algorithm CGSM into CGBM (or FCGS) in the algorithm PSS for computing global syzygies (not system) like comprehensive Gröbner bases as follows?

Algorithm 32 PSB($\{f_1, \dots, f_k\}, \succ_m$)

Input: f_1, \dots, f_k : vectors in $K[\bar{A}][\bar{X}]^r$, \succ_m a module order on $\text{pp}(\bar{X})^r$,

begin

$F \leftarrow \{f_1 + e_{r+1}, \dots, f_k + e_{r+k}\}$

$H \leftarrow \text{CGBM}(F, \succ_m) \leftarrow ?$

$G \leftarrow \pi(H \cap \bigoplus_{i=r+1}^{r+k} K[\bar{A}][\bar{X}]e_i)$

end-while

return(G)

end

The answer is “NO”. In fact, we can obtain a basis of parametric syzygies from the algorithm PSB. However, the output of the algorithm can not cover all syzygies of the input F under specialization $\sigma_{\bar{a}}$ for any $a \in L^m$.

The computation of parametric syzygies cannot be computed by an immediate generalization to modules of a comprehensive Gröbner basis algorithm for syzygies. Syzygies for a special case cannot be deduced from global syzygies, is straightforward. Consider any generic system, such that the generic element is regular (hence the global syzygies are the trivial ones), and a special case is non-regular (hence the

trivial syzygies are a proper submodule). The additional syzygies have support in a proper non-dense subset of the parameters' space, hence cannot be computed globally. The non-extensibility of syzygies is why comprehensive Gröbner bases are non-trivial (and would be useful in case that they could be computed in practice).

4 Concluding remarks

In this paper we presented algorithms for computing parametric Gröbner bases for module and parametric syzygies. In the algorithms for computing parametric Gröbner bases for modules, since we applied the two kinds of hybrid module orders for computing Gröbner bases in $K[\tilde{A}][\tilde{X}]^r$ and $K[\tilde{A}][U, \tilde{X}]$, the algorithms are still simple. The key tools of the algorithms for computing parametric Gröbner bases, are the theory of the stability of submodules and the these special hybrid orders.

In general, as parametric Gröbner bases are huge in $K[\tilde{A}][\tilde{X}]^1$, parametric Gröbner bases in $K[\tilde{A}][\tilde{X}]^r$ are huge, too. This means that we need high speed machines and a lot of memory (RAM) in the machines. However, our programs in the both the computer algebra system **Risa/Asir** still work for a lot of (easy) examples in $K[\tilde{A}][\tilde{X}]^r$ where $r \leq 3$, $|\tilde{X}| \leq 3$ and $|\tilde{A}| \leq 3$ (OS: WindowsXP, CPU: Pentium M 1.73GHz, Memory: 512MB RAM).

References

1. Becker, T.: On Gröbner bases under specialization. *Appl. Algebra Eng. Commun. Comput.* **5**, 1–8 (1994)
2. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Ph.D. thesis, Universität Innsbruck, Austria (1965)
3. Buchberger, B.: Gröbner bases: an algorithmic method in polynomial ideal theory. In: Bose, N. (ed.) *Multidimensional Systems Theory*, pp. 184–232. Reidel, Dordrecht (1985)
4. Buchberger, B., Winkler, F. (eds.): *Gröbner Bases and Applications*. Cambridge University Press, Cambridge (1998)
5. Cox, D., Little, J., O'Shea, D.: *Using Algebraic Geometry*. Springer, New York (1997)
6. Dolzmann, A., Sturm, T.: Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bull.* **31**(2), 2–9 (1997)
7. Furukawa, A., Sasaki, T., Kobayashi, H.: Gröbner basis of a module over $K[x_1, \dots, x_n]$ and polynomial solutions of a system of linear equations. In: SYMSAC, pp. 222–224. ACM Press, New York (1986)
8. Gianni, P.: Properties of Gröbner bases under specializations. In: Davenport, J.H. (ed.) *EUROCAL'87*, pp. 293–297. ACM Press, New York (1987)
9. Greuel, G.-M., Pfister, G.: *A Singular Introduction to Commutative Algebra*. Springer, New York (2002)
10. Kalkbrener, M.: Solving systems of algebraic equations by using Gröbner bases. In: Davenport, J. (ed.), *EUROCAL 87*, pp. 282–292. Springer, New York (1987)
11. Kalkbrener, M.: On the stability of Gröbner bases under specializations. *J. Symb. Comput.* **24**, 51–58 (1997)
12. Manubens, M., Montes, A.: Improving DISPGB algorithm using the discriminant ideal. *J. Symb. Comput.* **41**, 1245–1263 (2006)
13. Möller, M., Mora, F.: New constructive methods in classical ideal theory. *J. Algebra* **100**, 138–178 (1986)
14. Montes, A.: A new algorithm for discussing Gröbner basis with parameters. *J. Symb. Comput.* **33**(1–2), 183–208 (2002)

15. Nabeshima, K.: Reduced Gröbner bases in polynomial rings over a polynomial ring. *Math. Comput. Sci.* **2**, 587–599 (2009)
16. Nabeshima, K.: A speed-up of the algorithm for computing comprehensive Gröbner systems. In: Brown, C. (ed.) *International Symposium on Symbolic and Algebraic Computation*, pp. 299–306. ACM Press, New York (2007)
17. Pan, W., Wang, D.: Uniform Gröbner bases for ideals generated by polynomials with parametric exponents. In: Dumas, J-G. (ed.) *International Symposium on Symbolic and Algebraic Computation*, pp. 269–276. ACM Press, New York (2006)
18. Sato, Y.: Stability of Gröbner basis and ACGB. In: Dlozmann, A., Seidl, A., Sturm, T. (eds.) *The A3L 2005, Conference in Honor of the 60th Birthday of Volker Weispfenning*, pp. 223–228. BOD Norderstedt (2005)
19. Sato, Y., Suzuki, A.: Discrete comprehensive Gröbner bases. In: Mourrain, B. (ed.) *International Symposium on Symbolic and Algebraic Computation*, pp. 292–296. ACM Press, New York (2001)
20. Suzuki, A., Sato, Y.: An alternative approach to comprehensive Gröbner bases. In: Mora, T. (ed.) *International Symposium on Symbolic and Algebraic Computation*, pp. 255–261. ACM Press, New York (2002)
21. Suzuki, A., Sato, Y.: An alternative approach to Comprehensive Gröbner bases. *J. Symb. Comput.* **36**(3–4), 649–667 (2003)
22. Suzuki, A., Sato, Y.: Comprehensive Gröbner Bases via ACGB. In: Tran, Q.-N. (ed.) *The 10th International Conference on Applications of Computer Algebra*, pp. 65–73. Lamar University (2004)
23. Suzuki, A., Sato, Y.: A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In: *International Symposium on Symbolic and Algebraic Computation*, pp. 326–331. ACM Press, New York (2006)
24. Suzuki, A.: Computation of full comprehensive Gröbner bases. In: Ganzha, V.F., Mayr, E.W., Vorozhtsov, E.V. (eds.) *International Workshop on Computer Algebra in Scientific Computing (CASC)*, LNCS, vol. 3718, pp. 431–444. Springer, New York (2005)
25. Weispfenning, V.: Comprehensive Gröbner bases. *J. Symb. Comput.* **14**(1), 1–29 (1992)
26. Weispfenning, V.: Gröbner bases for binomials with parametric exponents. In: Ganzha, V.F., Mayr, E.W., Vorozhtsov, E.V. (eds.) *International Workshop on Computer Algebra in Scientific Computing (CASC)*, pp. 467–478. Technische Universität München (2004)
27. Winkler, F.: Solution of equations I: polynomial ideals and Gröbner bases. In: Jenks, R.D., Chudnovsky, D., Dekker, M. (eds.) *Computers Mathematics, Lecture Notes in Pure and Applied Mathematics*, vol. 125, pp. 383–407 (1986)
28. Yokoyama, K.: On systems of algebraic equations with parametric exponents. In: Gutierrez, J. (ed.) *International Symposium on Symbolic and Algebraic Computation*, pp. 312–317. ACM Press, New York (2004)
29. Yokoyama, K.: Stability of parametric decomposition. In: Iglesias, A., Takayama, N. (eds.) *International Congress on Mathematical Software*, LNCS, vol. 4151, pp. 391–402. Springer, Berlin (2006)
30. Yokoyama, K.: On systems of algebraic equations with parametric exponents II. In: *Applicable Algebra in Engineering Communication and Computing*, pp. 603–630 (2008)