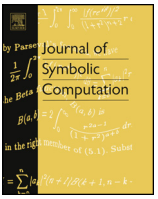
Journal of Symbolic Computation 127 (2025) 102370

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc



# Signature-based standard basis algorithm under the framework of GVW algorithm

Dong Lu [a], Dingkang Wang [b,c], Fanghui Xiao [d], Xiaopeng Zheng [e]

[a] School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China
[b] KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China
[c] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
[d] MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, China
[e] College of Mathematics and Computer Science, Shantou University, Shantou 515821, China

ARTICLE INFO

*Article history:*
Received 28 September 2022
Received in revised form 16 March 2024
Accepted 17 July 2024
Available online 19 July 2024

*Keywords:*
Signature-based algorithms
Standard bases
Semigroup orders
Mora normal form algorithm
Cover theorem

ABSTRACT

The GVW algorithm, one of the most important so-called signature-based algorithms, is designed to eliminate a large number of useless polynomial reductions from Buchberger's algorithm. The cover theorem serves as the theoretical foundation of the GVW algorithm, and up to now, it applies only to a certain class of monomial orders, namely global orders and a special class of local orders. In this paper we extend this theorem to any semigroup order, which can be either global, local or even mixed. Building upon the pioneering idea of the Mora normal form algorithm, we propose a more comprehensive and general proof for the cover theorem while bypassing the need to choose a minimal element from an infinite set of monomials in all the existing proofs. Therefore, the algorithm for signature-based standard bases is presented for any semigroup order under the framework of the GVW algorithm, and an example is given to provide an illustration of the algorithm.



*E-mail addresses:* donglu@swjtu.edu.cn (D. Lu), dwang@mmrc.iss.ac.cn (D. Wang), xiaofanghui@hunnu.edu.cn (F. Xiao), zhengxiaopeng@amss.ac.cn (X. Zheng).

https://doi.org/10.1016/j.jsc.2024.102370
0747-7171/

## 1. Introduction

Hironaka (1964) proposed the concept of standard bases for solving the problem of singularity resolution of algebraic varieties. Buchberger (1965) presented Gröbner bases, which are bases with special properties of ideals in a polynomial ring, and gave the first algorithm to compute them. Generally, the definition of standard bases is more extensive. In particular, they can be called Gröbner bases in a polynomial ring but for a local ring, they are always called standard bases. Based on the groundbreaking work of Buchberger in Gröbner bases, many researchers have devoted themselves to studying Gröbner basis algorithms and obtained excellent works (see, e.g., Buchberger (1979, 1985); Lazard (1983); Gebauer and Möller (1986); Möller et al. (1992); Faugère (1999, 2002)).

One of the most important breakthroughs is the F5 algorithm proposed by Faugère (2002). The F5 algorithm follows the same underlying structure of Buchberger's algorithm, which functions by performing polynomial reductions on a series of so-called S-polynomials. By the introduction of "signature", Faugère has given rewriting rules to detect and discard many useless S-polynomials without performing any reduction, which greatly improves the efficiency of the algorithm. Along with that, several variants of the F5 algorithm have been presented (see, e.g., Ars and Hashemi (2010); Eder and Perry (2010, 2011); Arri and Perry (2011); Sun and Wang (2011a,b); Gerdt et al. (2013), and Eder and Faugère (2017) for a comprehensive survey). Among them, Gao et al. (2010, 2016) presented a new framework for computing Gröbner bases, i.e., the GVW algorithm, which is the foundation of the paper.

Due to the high efficiency of the signature-based algorithm, many researches began to generalize signature-based Gröbner basis algorithms to different rings. For example, Eder et al. (2017) generalized signature-based Gröbner basis algorithms to the polynomial ring with coefficients in a Euclidean ring. However, they have just used signature-based computation as a pre-reduction step for a classical Gröbner bases computation over the Euclidean ring. Caruso et al. (2020) introduced two signature-based Gröbner basis algorithms for Tate algebras, which play a major role in the context of analytic geometry over the $p$-adics, in order to avoid many reductions. Francis and Verron (2021) extended signature-based Gröbner basis algorithms to the polynomial ring with coefficients in a principal ideal domain. They dealt with gcd-polynomials by taking into account the different combination coefficients, and then choose the appropriate combination coefficients to realize that the signature does not drop.

Based on the framework of the GVW algorithm, Lu et al. (2018) extended the signature-based Gröbner basis algorithm to local rings. As is well known, any global order implies that any non-trivial monomial is greater than 1. This can guarantee that any nonempty subset of monomials has a minimal element by Dickson lemma. However, any local order corresponding to computations in local rings indicates that any non-trivial monomial is less than 1. This leads to the possibility that there are no minimal elements in nonempty infinite sets of monomials in local rings. Signatures inherit an order from the chosen monomial orders, and until 2018, all known proofs of the cover theorem rely on choosing a minimal signature from an infinite set of monomials. In order to get a minimal signature in local rings, Lu et al. (2018) restricted a local order to an antigraded order and constructed a special set, then generalized the cover theorem, the theoretical foundation of the GVW algorithm, to local rings in order to discard useless J-pairs which are analogous to S-polynomials in Buchberger's algorithm.

In this paper, we extend the cover theorem to any semigroup order, which can be either global, local or even mixed. To ensure the termination of reductions for polynomials in local rings, Mora (1982) proposed a famous algorithm called the Mora normal form algorithm. Inspired by the idea of the Mora normal form algorithm, we give a more essential proof for the cover theorem, and remove the restriction for global orders and antigraded orders. More importantly, we generalize the Mora normal form algorithm for polynomials to the case of polynomials with signatures in order to perform a sequence of successive regular top-reductions. This crucial step serves two purposes. First, it guarantees the preservation of the polynomial's signature throughout the entire reduction process. Second, it enables the reduction process to conclude within a finite number of steps. Based on these, we propose a signature-based algorithm to compute standard bases with respect to any semigroup order.

The paper is organized as follows. Some basic concepts about semigroup orders, localization, standard bases and the Mora normal form algorithm are introduced in Section 2. Based on the idea of the Mora normal form algorithm, we prove the cover theorem with respect to any semigroup order in Section 3 and propose a signature-based algorithm to compute standard bases in Section 4. In Section 5, an example is given to illustrate the effectiveness of the algorithm. We end with some concluding remarks in Section 6.

## 2. Preliminaries

Let $k$ be a field, $n$ a positive integer, $X$ the $n$ variables $x_1, \ldots, x_n$, $k[X]$ the polynomial ring in $X$ over $k$ and $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$ the set of monomials in $k[X]$. For any given positive integer $m$, we write $k[X]^{1\times m}$ as $k[X]^m$ which is a free module of rank $m$ over $k[X]$.

### 2.1. Semigroup orders

**Definition 1** *(Cox et al. (2005)).* An order $\succ$ on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$ is said to be a semigroup order if it satisfies:

1. $\succ$ is a total order, i.e., for any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, exactly one of the following is true:
$$X^\alpha \succ X^\beta,\ X^\alpha = X^\beta,\ \text{or}\ X^\alpha \prec X^\beta.$$
2. $\succ$ is compatible with multiplication of monomials, i.e., for any $\gamma \in \mathbb{Z}^n_{\geq 0}$, we have
$$X^\alpha \succ X^\beta \Longrightarrow X^\gamma X^\alpha \succ X^\gamma X^\beta.$$

Semigroup orders include global orders, which have the additional well-ordering property, as well as local orders and other orders which do not.

**Definition 2** *(Cox et al. (2005)).* Let $\succ$ be a semigroup order on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$, then

1. $\succ$ is called a global order if $X^\alpha \succ 1$ for all $\alpha \neq (0, \ldots, 0)$.
2. $\succ$ is called a local order if $1 \succ X^\alpha$ for all $\alpha \neq (0, \ldots, 0)$.
3. $\succ$ is called a mixed order if it is neither global nor local.

For instance, the lexicographic order, graded lexicographic order and graded reverse lexicographic order are global orders; the antigraded lexicographic order and antigraded reverse lexicographic order are local orders. Please refer to Cox et al. (2005) for specific definitions.

**Example 3.** Let $\succ_1$ be the lexicographic order on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$, and $\succ_2$ be the antigraded lexicographic order on $\left\{Y^\beta \mid \beta \in \mathbb{Z}^l_{\geq 0}\right\}$, where $Y$ is the $l$ variables $y_1, \ldots, y_l$. Then we define a semigroup order $\succ_3$ by $X^\alpha Y^\beta \succ_3 X^{\alpha'} Y^{\beta'}$ if either $X^\alpha \succ_1 X^{\alpha'}$, or $X^\alpha = X^{\alpha'}$ and $Y^\beta \succ_2 Y^{\beta'}$. It is easy to verify that $\succ_3$ is a mixed order.

We denote elements in $k[X]^m$ by the bold letters $\mathbf{f}$, $\mathbf{u}$, and so on. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ be the standard basis of $k[X]^m$, where $\mathbf{e}_i$ is the $i$-th unit vector of $k[X]^m$, and $i = 1, \ldots, m$. In this paper, we will always use the "downward" ordering on the entries in a vector, i.e., $\mathbf{e}_1 \succ \mathbf{e}_2 \succ \cdots \succ \mathbf{e}_m$, although any other ordering could be used as well. Given a semigroup order $\succ$ on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$, it can be extended to $k[X]^m$ to obtain $\succ_m$.

**Definition 4** *(Cox et al. (2005)).* Let $\succ$ be a semigroup order on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$. A module order is a total order $\succ_m$ on the set of monomials $\left\{X^\alpha \mathbf{e}_i \mid \alpha \in \mathbb{Z}^n_{\geq 0},\ i = 1, \ldots, m\right\}$ in $k[X]^m$, which is compatible with the $k[X]$-module structure and the order $\prec$ in the following senses:

1. $X^\alpha \succ X^\beta \Longrightarrow X^\alpha \mathbf{e}_i \succ_m X^\beta \mathbf{e}_i$,
2. $X^\alpha \mathbf{e}_i \succ_m X^\beta \mathbf{e}_j \Longrightarrow X^{\alpha+\gamma} \mathbf{e}_i \succ_m X^{\beta+\gamma} \mathbf{e}_j$,

for all $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, $i, j = 1, \ldots, m$.

**Convention 5.** *The statements "$\prec$ be a semigroup order" and "$\succ_m$ be a module order" in the following represent "$\prec$ be a semigroup order on $\left\{X^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\right\}$" and "$\succ_m$ be a module order on $\left\{X^\alpha \mathbf{e}_i \mid \alpha \in \mathbb{Z}^n_{\geq 0},\ i = 1, \ldots, m\right\}$", respectively. In addition, we should point out that $\prec_m$ is always assumed to be compatible with $\prec$.*

The most common module orders are position over term (POT) order and term over position (TOP) order. The definitions are as follows.

**Definition 6** *(Cox et al. (2005)).* Let $\prec$ be a semigroup order, and $\succ_m$ be a module order. Then

1. (POT) we say that $X^\alpha \mathbf{e}_i \succ_m X^\beta \mathbf{e}_j$ if $i < j$, or if $i = j$ and $X^\alpha \succ X^\beta$.
2. (TOP) we say that $X^\alpha \mathbf{e}_i \succ_m X^\beta \mathbf{e}_j$ if $X^\alpha \succ X^\beta$, or if $X^\alpha = X^\beta$ and $i < j$.

### 2.2. Standard bases

Let $\succ$ be a semigroup order, and $f \in k[X] \setminus \{0\}$ be written in a unique way as a sum of nonzero terms

$$f = a_\alpha X^\alpha + a_\beta X^\beta + \cdots + a_\gamma X^\gamma,$$

where $X^\alpha \succ X^\beta \succ \cdots \succ X^\gamma$ and $a_\alpha, a_\beta, \ldots, a_\gamma \in k \setminus \{0\}$. Then the leading monomial, leading coefficient and leading term of $f$ w.r.t. $\succ$ are $X^\alpha$, $a_\alpha$ and $a_\alpha X^\alpha$, and denoted by $\mathrm{lm}(f)$, $\mathrm{lc}(f)$ and $\mathrm{lt}(f)$, respectively.

**Definition 7** *(Greuel and Pfister (2002)).* Let $S_\succ = \left\{h \in k[X] \mid \mathrm{lt}(h) = 1\right\}$, where $\succ$ is a semigroup order. We define the localization of $k[X]$ w.r.t. $\succ$ as follows

$$k[X]_\succ := \left\{ \frac{f}{h} \;\middle|\; f \in k[X] \text{ and } h \in S_\succ \right\},$$

and call $k[X]_\succ$ the ring associated to $k[X]$ and $\succ$.

**Remark 8.** Every ideal in $k[X]_\succ$ has a generating set consisting of polynomials in $k[X]$, please refer to Greuel and Pfister (2002) for details. Based on this fact, limiting our study to ideals generated by polynomials for the remainder of the paper does not result in any loss of generality when studying ideals in $k[X]_\succ$.

In the following, we use $R$ to denote $k[X]_\succ$. It is easy to prove that $R = k[X]$ if and only if $\succ$ is a global order, $R = k[X]_{\langle x_1, \ldots, x_n \rangle}$ if and only if $\succ$ is a local order, where $k[X]_{\langle x_1, \ldots, x_n \rangle}$ is the collection of all rational functions $p/q$ with $p, q \in k[X]$ and $q(0, \ldots, 0) \neq 0$. Let $g = \frac{f}{h} \in R$, where $f \in k[X]$ and $h \in S_\succ$. Then the leading monomial, leading coefficient and leading term of $g$ w.r.t. $\succ$ are defined as $\mathrm{lm}(g) = \mathrm{lm}(f)$, $\mathrm{lc}(g) = \mathrm{lc}(f)$, and $\mathrm{lt}(g) = \mathrm{lt}(f)$, respectively.

If $\succ$ is a local order or a mixed order, then the classical division algorithm in Cox et al. (2007) may not terminate. This is because a local order or a mixed order is not a well-ordering. In order to solve

this problem, Mora (1982) proposed a new division algorithm in $R$ to guarantee the termination of computation.

**Proposition 9** *(Mora (1982)). Let $g, g_1, \ldots, g_s \in k[X] \setminus \{0\}$, and $\succ$ be a semigroup order. Then there is an algorithm for producing polynomials $h, a_1, \ldots, a_s, r \in k[X]$ such that*

$$hg = a_1 g_1 + \cdots + a_s g_s + r,$$

*where $\mathrm{lt}(h) = 1$, $\mathrm{lm}(g) \succeq \mathrm{lm}(a_i g_i)$ for all $a_i \neq 0$, and either $r = 0$, or $\mathrm{lm}(g) \succeq \mathrm{lm}(r)$ and $\mathrm{lm}(r)$ is not divisible by any $\mathrm{lm}(g_i)$.*

The algorithm in Proposition 9 is called the Mora normal form algorithm. On the correctness and termination of the algorithm, please refer to Mora (1982) for details. Based on Proposition 9, we can now compute a standard basis of an ideal $I$ in $R$ using Buchberger's algorithm, substituting the Mora normal form algorithm for the classical division algorithm.

**Definition 10.** Let $I$ be an ideal in $R$, and $\succ$ be a semigroup order. A finite set $\{g_1, \ldots, g_s\} \subset I$ is called a standard basis of $I$ w.r.t. $\succ$ if for every $g$ in $I$, $\mathrm{lm}(g)$ is divisible by some $\mathrm{lm}(g_i)$.

Let $\mathbf{f} \in R^m$ and $\succ_m$ be a module order. $\mathbf{f}$ can be written as $\mathbf{f} = \frac{\mathbf{u}}{h}$ with $h \in S_\succ$ and $\mathbf{u} \in k[X]^m$. Then the leading monomial, leading coefficient and leading term of $\mathbf{f}$ are defined as $\mathrm{lm}(\mathbf{f}) = \mathrm{lm}(\mathbf{u})$, $\mathrm{lc}(\mathbf{f}) = \mathrm{lc}(\mathbf{u})$ and $\mathrm{lt}(\mathbf{f}) = \mathrm{lt}(\mathbf{u})$, respectively. We say that $X^\alpha \mathbf{e}_i \mid X^\beta \mathbf{e}_j$ if and only if $i = j$ and $X^\alpha \mid X^\beta$. If $X^\alpha \mathbf{e}_i \mid X^\beta \mathbf{e}_j$, then we define the quotient $\frac{X^\beta \mathbf{e}_j}{X^\alpha \mathbf{e}_i}$ to be $X^{\beta-\alpha} \in k[X]$. That is, $\frac{X^\beta \mathbf{e}_j}{X^\alpha \mathbf{e}_i} = X^{\beta-\alpha}$. Greuel and Pfister (2002) extended the Mora normal form algorithm to the case of $R^m$.

**Proposition 11** *(Greuel and Pfister (2002)). Let $\boldsymbol{u}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_s \in k[X]^m \setminus \{\mathbf{0}\}$, and $\succ_m$ be a module order. Then there is an algorithm for producing polynomials $h, a_1, \ldots, a_s \in k[X]$ and a vector $\boldsymbol{r} \in k[X]^m$ such that*

$$h\boldsymbol{u} = a_1 \boldsymbol{u}_1 + \cdots + a_s \boldsymbol{u}_s + \boldsymbol{r},$$

*where $\mathrm{lt}(h) = 1$, $\mathrm{lm}(\boldsymbol{u}) \succeq_m \mathrm{lm}(a_i \boldsymbol{u}_i)$ for all $a_i \neq 0$, and either $\boldsymbol{r} = \mathbf{0}$, or $\mathrm{lm}(\boldsymbol{u}) \succeq_m \mathrm{lm}(\boldsymbol{r})$ and $\mathrm{lm}(\boldsymbol{r})$ is not divisible by any $\mathrm{lm}(\boldsymbol{u}_i)$.*

A standard basis for a submodule $W$ of $R^m$ can be defined similar to Definition 10, and we can use Proposition 11 to compute it.

**Definition 12.** Let $W$ be a submodule in $R^m$, and $\succ_m$ be a module order. A finite set $\{\mathbf{u}_1, \ldots, \mathbf{u}_s\} \subset W$ is called a standard basis of $W$ w.r.t. $\succ_m$ if for every $\mathbf{u}$ in $W$, $\mathrm{lm}(\mathbf{u})$ is divisible by some $\mathrm{lm}(\mathbf{u}_i)$.

### 2.3. Strong standard bases

Let $\mathbf{f} = (f_1, \ldots, f_m) \in k[X]^m \setminus \{\mathbf{0}\}$, and $I = \langle f_1, \ldots, f_m \rangle \subset R$. We define a subset $M$ of $R^m \times R$:

$$M := \left\{ (\mathbf{u}, v) \in R^m \times R \;\middle|\; \mathbf{u} \cdot \mathbf{f}^{\mathrm{T}} = v \right\}.$$

It is easy to verify that $M$ is a $R$-submodule of $R^m \times R$ generated by $(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$. If $(\mathbf{u}, 0) \in M$, then $\mathbf{u}$ is called a *syzygy* of $\mathbf{f}$. Let $p = (\mathbf{u}, v) \in M$, then $\mathrm{lm}(\mathbf{u})$ is called the *signature* of $p$.

The definition of top-reduction in $M$ is as follows.

**Definition 13** *(Gao et al. (2016)).* Let $p_1 = (\mathbf{u}_1, v_1)$ and $p_2 = (\mathbf{u}_2, v_2)$ be two pairs in $M$. We say that $p_1$ is top-reducible by $p_2$, if it satisfies:

1. when $v_1 v_2 \neq 0$, then $\mathrm{lm}(v_2) \mid \mathrm{lm}(v_1)$ and $t\,\mathrm{lm}(\mathbf{u}_2) \preceq_m \mathrm{lm}(\mathbf{u}_1)$, where $t = \frac{\mathrm{lm}(v_1)}{\mathrm{lm}(v_2)}$; and

2. when $v_1 = 0$, then $v_2 = 0$ and $\mathrm{lm}(\mathbf{u}_2) \mid \mathrm{lm}(\mathbf{u}_1)$; and
3. when $v_2 = 0$, then $\mathrm{lm}(\mathbf{u}_2) \mid \mathrm{lm}(\mathbf{u}_1)$.

When $v_1 v_2 \neq 0$, the one-step top-reduction of $p_1$ and $p_2$ is defined as

$$\mathrm{OneRed}(p_1, p_2) := p_1 - ctp_2 = (\mathbf{u}_1 - ct\mathbf{u}_2, v_1 - ctv_2),$$

where $c = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}$. Such a one-step top-reduction is called *regular* if $\mathrm{lm}(\mathbf{u}_1 - ct\mathbf{u}_2) = \mathrm{lm}(\mathbf{u}_1)$, and *super* otherwise. When $v_2$ is zero, the corresponding top-reduction is always called super.

**Definition 14.** Let $G = \{(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_s, v_s)\}$ be a finite subset of $M$, where $(\mathbf{u}_i, v_i) \in k[X]^m \times k[X]$ for all $i$. Then $G$ is called a strong standard basis for $M$, if every nonzero pair $(\mathbf{u}, v)$ in $M$ is top-reducible by some pair $(\mathbf{u}_i, v_i)$ in $G$.

Clearly, the above definition is similar to that of standard bases. Now, we establish a relationship between strong standard bases and standard bases. The proof of the following proposition is slightly different from Proposition 2.8 in Lu et al. (2018), and we relax the restriction of the local order $\prec$ to any semigroup order.

**Proposition 15.** *Let $\prec$ be a semigroup order and $\prec_m$ be a module order. Suppose that $G = \{(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_s, v_s)\}$ is a strong standard basis for $M$, then*

1. $\mathbf{G}_0 = \{\mathbf{u}_i \mid v_i = 0, 1 \leq i \leq s\}$ *is a standard basis for the syzygy module of $\{f_1, \ldots, f_m\}$, and*
2. $G_1 = \{v_i \mid v_i \neq 0, 1 \leq i \leq s\}$ *is a standard basis for $I = \langle f_1, \ldots, f_m \rangle$ in $R$.*

**Proof.** The proof of the first conclusion is the same as that of Proposition 2.2 in Gao et al. (2016), so we only prove the second assertion.

Without loss of generality, let $\mathbf{G}_0 = \{\mathbf{u}_i \mid v_i = 0, 1 \leq i \leq l\}$ and $G_1 = \{v_i \mid v_i \neq 0, l+1 \leq i \leq s\}$, where $1 \leq l < s$. We select a polynomial $v \in I$ such that $v \neq 0$, then there exists a vector $\mathbf{u} \in R^m$ such that $\mathbf{u} \cdot \mathbf{f}^{\mathrm{T}} = v$. Since leading monomials of $\mathbf{u}$ and $v$ do not change by multiplying any unit in $R$, we assume that $(\mathbf{u}, v) \in k[X]^m \times k[X]$. According to Proposition 11, there exist polynomials $h, a_1, \ldots, a_l \in k[X]$ and a vector $\mathbf{r} \in k[X]^m$ such that

$$h\mathbf{u} = a_1\mathbf{u}_1 + \cdots + a_l\mathbf{u}_l + \mathbf{r},$$

where $\mathrm{lt}(h) = 1$, $\mathrm{lm}(\mathbf{u}) \succeq_m \mathrm{lm}(a_i\mathbf{u}_i)$ for all $a_i \neq 0$, and either $\mathbf{r} = \mathbf{0}$ or $\mathrm{lm}(\mathbf{u}) \succeq_m \mathrm{lm}(\mathbf{r})$ and $\mathbf{r} \notin \langle \mathbf{G}_0 \rangle$, where $\langle \mathbf{G}_0 \rangle$ is a submodule of $R^m$ generated by $\mathbf{G}_0$. It follows from $v \neq 0$ that $\mathbf{r} \neq \mathbf{0}$. Hence, we get

$$(\mathbf{r}, hv) = (h\mathbf{u}, hv) - \sum_{i=1}^{l} a_i(\mathbf{u}_i, 0) \in M$$

and $\mathrm{lm}(hv) = \mathrm{lm}(v)$. As $(\mathbf{r}, hv) \in M$ and $\mathbf{r} \notin \langle \mathbf{G}_0 \rangle$, it can be top-reduced by some pair $(\mathbf{u}_i, v_i) \in G$ with $v_i \in G_1$. Then, $v_i \neq 0$ and $\mathrm{lm}(v_i) \mid \mathrm{lm}(v)$. Therefore, $G_1$ is a standard basis for $I$. □

### 2.4. Regular Mora normal form algorithm

Let $G$ be any finite subset of $M$, we say that $p = (\mathbf{u}, v) \in M$ is regular (resp. super) top-reducible by $G$ if it is regular (resp. super) top-reducible by at least one pair in $G$. We call $p$ *eventually super top-reducible* by $G$ if there is a sequence of regular top-reductions of $p$ by pairs in $G$ that reduce $p$ to a pair $(\mathbf{u}', v') \in M$ that is no longer regular top-reducible by $G$ but is super top-reducible by $G$. However, Example 3.5 in Lu et al. (2018) shows that a sequence of regular top-reductions may not terminate. In order to guarantee that regular top-reductions w.r.t. any semigroup order terminate in a finite number of steps, we need to propose a new division algorithm to regularly top-reduce pairs in $R^m \times R$. Based on the idea of the Mora normal form algorithm, we obtain the following result.

**Proposition 16.** *Let* $(\boldsymbol{u}, v), (\boldsymbol{u}_1, v_1), \ldots, (\boldsymbol{u}_s, v_s) \in k[X]^m \times k[X]$ *be nonzero,* $\prec$ *be a semigroup order and* $\succ_m$ *be a module order. Then there is an algorithm for producing polynomials* $h, a_1, \ldots, a_s \in k[X]$ *and a pair* $(\mathbf{w}, r) \in k[X]^m \times k[X]$ *such that*

$$h(\boldsymbol{u}, v) = a_1(\boldsymbol{u}_1, v_1) + \cdots + a_s(\boldsymbol{u}_s, v_s) + (\mathbf{w}, r), \tag{1}$$

*where* $\mathrm{lt}(h) = 1$, $\mathrm{lm}(v) \succeq \mathrm{lm}(a_i v_i)$ *for all* $a_i \neq 0$, *and* $\mathrm{lm}(v) \succeq \mathrm{lm}(r)$. *Moreover,* $\mathrm{lm}(\boldsymbol{w}) = \mathrm{lm}(\boldsymbol{u})$, $\mathrm{lm}(\boldsymbol{u}) \succeq_m \mathrm{lm}(a_i \boldsymbol{u}_i)$ *for all* $a_i \neq 0$, *and* $(\mathbf{w}, r)$ *is not regular top-reducible by any pair* $(\boldsymbol{u}_i, v_i)$.

Before presenting the algorithm in Proposition 16, we need to introduce the following important concept which first proposed by Mora (1982).

**Definition 17** *(Mora (1982)).* Let $v \in k[X] \setminus \{0\}$, then the écart of $v$ is defined as

$$\text{écart}(v) := \deg(v) - \deg(\mathrm{lm}(v)),$$

where $\deg(v)$ is the total degree of $v$.

**Proposition 18.** *Let* $v_1, v_2, v_3 \in k[X] \setminus \{0\}$ *such that* $\mathrm{lm}(v_1) \mid \mathrm{lm}(v_2)$ *and* $v_3 = v_2 - \frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)} v_1$. *If écart*$(v_1) \leq$ *écart*$(v_2)$, *then* $\deg(v_3) \leq \deg(v_2)$.

**Proof.** Since écart$(v_1) \leq$ écart$(v_2)$, we have $\deg(v_1) - \deg(\mathrm{lm}(v_1)) \leq \deg(v_2) - \deg(\mathrm{lm}(v_2))$. It is easy to see that $\deg\left(\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)}\right) = \deg(\mathrm{lm}(v_2)) - \deg(\mathrm{lm}(v_1))$. Then, $\deg\left(\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)} v_1\right) = \deg(\mathrm{lm}(v_2)) - \deg(\mathrm{lm}(v_1)) + \deg(v_1) \leq \deg(v_2)$. Thus, $\deg(v_3) \leq \max\left\{\deg(v_2), \deg\left(\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)} v_1\right)\right\} \leq \deg(v_2)$. □

The algorithm mentioned in Proposition 16 is as follows.

**Algorithm 1:** Regular Mora normal form algorithm.

**Input :** $(\mathbf{u}, v) \in k[X]^m \times k[X]$ and $G = \{(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_s, v_s)\} \subset k[X]^m \times k[X]$, any semigroup order $\succ$ and a module order $\succ_m$.
**Output:** $(\mathbf{w}, r)$ as the statement in Proposition 16.

**begin**
  $(\mathbf{w}_0, r_0) := (\mathbf{u}, v)$;
  $T_0 := G$;
  $i := 1$;
  **while** $(\mathbf{w}_{i-1}, r_{i-1})$ is regular top-reducible by $T_{i-1}$ **do**
    $T_{reg}^{(i-1)} := \left\{(\bar{\mathbf{u}}, \bar{v}) \in T_{i-1} \;\middle|\; (\mathbf{w}_{i-1}, r_{i-1}) \text{ is regular top-reducible by } (\bar{\mathbf{u}}, \bar{v})\right\}$;
    choose $(\bar{\mathbf{u}}_{i-1}, \bar{v}_{i-1}) \in T_{reg}^{(i-1)}$ with écart$(\bar{v}_{i-1})$ minimal;
    **if** $(\mathbf{w}_{i-1}, r_{i-1}) \notin G$ and écart$(\bar{v}_{i-1}) >$ écart$(r_{i-1})$ **then**
      $T_i := T_{i-1} \cup \{(\mathbf{w}_{i-1}, r_{i-1})\}$;
    **else**
      $T_i := T_{i-1}$;
    $(\mathbf{w}_i, r_i) := \mathrm{OneRed}((\mathbf{w}_{i-1}, r_{i-1}), (\bar{\mathbf{u}}_{i-1}, \bar{v}_{i-1}))$;
    $i := i + 1$;
  $(\mathbf{w}, r) := (\mathbf{w}_{i-1}, r_{i-1})$;
  **return** $(\mathbf{w}, r)$.

**Remark 19.** For Theorem 3.6 in Lu et al. (2018), it contains the condition that "$(\mathbf{u}, v)$ is not covered by $G$" which is used for the termination proof of the algorithm based on Theorem 3.6. In contrast to Theorem 3.6 in Lu et al. (2018), Proposition 16 eliminates the constraint and we offer a new termination proof for Algorithm 1.

**Lemma 20.** *Let* $L_i = \left\langle \mathrm{lm}(v)x_{n+1}^{\acute{e}cart(v)} \mid (\boldsymbol{u}, v) \in T_i \setminus G \right\rangle \subset k[X, x_{n+1}]$, *where* $x_{n+1}$ *is a new variable and* $T_i$ *is the set in Algorithm 1. If the conditions in Step 8 hold, then* $L_{i-1} \subsetneq L_i$.

**Proof.** If the conditions in Step 8 of Algorithm 1 hold, then $T_i = T_{i-1} \cup \{(\mathbf{w}_{i-1}, r_{i-1})\}$. We claim that $\mathrm{lm}(r_{i-1})x_{n+1}^{\acute{e}cart(r_{i-1})}$ is not divisible by any element in $L_{i-1}$. Otherwise, there exists a pair $(\tilde{\mathbf{u}}, \tilde{v}) \in T_{i-1} \setminus G$ such that $\mathrm{lm}(\tilde{v})x_{n+1}^{\acute{e}cart(\tilde{v})} \mid \mathrm{lm}(r_{i-1})x_{n+1}^{\acute{e}cart(r_{i-1})}$. It is easy to see that

$$\mathrm{lm}(\tilde{v}) \mid \mathrm{lm}(r_{i-1}) \tag{2}$$

and

$$\acute{e}cart(\tilde{v}) \leq \acute{e}cart(r_{i-1}). \tag{3}$$

Because we only perform regular top-reductions throughout the entire calculation process, we have

$$\mathrm{lm}(r_{i-1}) \prec \mathrm{lm}(\tilde{v}) \tag{4}$$

and

$$\mathrm{lm}(\tilde{\mathbf{u}}) = \mathrm{lm}(\mathbf{w}_{i-1}) = \mathrm{lm}(\mathbf{u}). \tag{5}$$

Combining Equations (2) and (4), we get

$$\frac{\mathrm{lm}(r_{i-1})}{\mathrm{lm}(\tilde{v})} \prec 1. \tag{6}$$

It follows from Equations (5) and (6) that

$$\frac{\mathrm{lm}(r_{i-1})}{\mathrm{lm}(\tilde{v})}\mathrm{lm}(\tilde{\mathbf{u}}) \prec_m \mathrm{lm}(\mathbf{w}_{i-1}). \tag{7}$$

According to Equations (2) and (7), $(\mathbf{w}_{i-1}, r_{i-1})$ is regular reducible by $(\tilde{\mathbf{u}}, \tilde{v})$. Based on Steps 6 to 8 of Algorithm 1, we have $(\tilde{\mathbf{u}}, \tilde{v}) \in T_{reg}^{(i-1)}$ and $\acute{e}cart(\tilde{v}) \geq \acute{e}cart(\bar{v}_{i-1}) > \acute{e}cart(r_{i-1})$. This contradicts Equation (3). Consequently, we can now derive that $L_{i-1} \subsetneq L_i$. □

**Theorem 21.** *Algorithm 1 outputs as specified within a finite number of steps.*

**Proof.** *Termination*. For each set $T_i$, we construct the following ideal in $k[X, x_{n+1}]$:

$$L_i = \left\langle \mathrm{lm}(v)x_{n+1}^{\acute{e}cart(v)} \mid (\mathbf{u}, v) \in T_i \setminus G \right\rangle,$$

where $x_{n+1}$ is a new variable. Based on Steps 9 and 11 of Algorithm 1, we can obtain a chain

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_{i-1} \subseteq L_i \subseteq \cdots \tag{8}$$

Since $k[X, x_{n+1}]$ is Noetherian, there exists some positive integer $N_1$ such that the chain (8) becomes stable for $i \geq N_1$, i.e., $L_{i-1} = L_i$ for all $i \geq N_1$. By Lemma 20, for each $i$ with $i \geq N_1$ we have $(\mathbf{w}_{i-1}, r_{i-1}) \in G$ or $\acute{e}cart(\bar{v}_{i-1}) \leq \acute{e}cart(r_{i-1})$. When $i \geq N_1$, Algorithm 1 generates the following intermediate products

$$(\mathbf{w}_{N_1-1}, r_{N_1-1}), (\mathbf{w}_{N_1}, r_{N_1}), (\mathbf{w}_{N_1+1}, r_{N_1+1}), \ldots \tag{9}$$

Based on Step 12 of Algorithm 1, we have $(\mathbf{w}_i, r_i) = \mathrm{OneRed}((\mathbf{w}_{i-1}, r_{i-1}), (\bar{\mathbf{u}}_{i-1}, \bar{v}_{i-1}))$ for all $i$. It follows that $\mathrm{lm}(r_i) \prec \mathrm{lm}(r_{i-1})$ for all $i$. This means that the pairs in the sequence (9) are all different from each other. Since $G$ is a finite set, the first case $(\mathbf{w}_{i-1}, r_{i-1}) \in G$ for $i \geq N_1$ can only occur a limited number of times. That is, there is another positive integer $N_2$ such that $(\mathbf{w}_{i-1}, r_{i-1}) \notin G$ for all $i \geq N_2$, where $N_2 \geq N_1$. Therefore, we have $\acute{e}cart(\bar{v}_{i-1}) \leq \acute{e}cart(r_{i-1})$ for all $i \geq N_2$. It follows from

Proposition 18 that $\deg(r_i) \leq \deg(r_{i-1})$ for all $i \geq N_2$. Thus, we obtain the following non-increasing sequence

$$\deg(r_{N_2-1}) \geq \deg(r_{N_2}) \geq \deg(r_{N_2+1}) \geq \cdots \tag{10}$$

In addition, the leading monomial of $r_{N_2-1}$ strictly decreases in each successive iteration. That is, we have the following strictly decreasing sequence

$$\mathrm{lm}(r_{N_2-1}) \succ \mathrm{lm}(r_{N_2}) \succ \mathrm{lm}(r_{N_2+1}) \succ \cdots \tag{11}$$

By the fact that the set of monomials in $k[X]$ whose total degrees are limited by $\deg(r_{N_2-1})$ is finite, the strictly decreasing sequence (11) will be terminated within a finite number of steps. As a consequence, Algorithm 1 terminates within a finite number of steps.

*Correctness*. We will prove by induction on $i \geq 0$ that we have the form

$$h_k(\mathbf{w}_0, r_0) = \sum_{j=1}^{s} a_j^{(k)}(\mathbf{u}_j, v_j) + (\mathbf{w}_k, r_k) \tag{12}$$

for all $k$ with $0 \leq k \leq i$, where $\mathrm{lt}(h_k) = 1$, $\mathrm{lm}(r_0) \succeq \mathrm{lm}(a_j^{(k)} v_j)$ for all $a_j^{(k)} \neq 0$, and $\mathrm{lm}(r_0) \succeq \mathrm{lm}(r_k)$. Moreover, $\mathrm{lm}(\mathbf{w}_k) = \mathrm{lm}(\mathbf{w}_0)$, and $\mathrm{lm}(\mathbf{w}_0) \succeq_m \mathrm{lm}(a_j^{(k)}\mathbf{u}_j)$ for all $a_j^{(k)} \neq 0$.

Setting $h_0 = 1$ and $a_j^{(0)} = 0$ for all $j$, everything works for $i = 0$. Suppose the form (12) holds true for $0 \leq k \leq i$. Now we need to prove that the pair $(\mathbf{w}_{i+1}, r_{i+1})$ produced by the $(i+1)$-th pass through the **while** loop satisfies the form (12) for $k = i+1$.

Since $(\mathbf{w}_{i+1}, r_{i+1}) = \mathrm{OneRed}((\mathbf{w}_i, r_i), (\bar{\mathbf{u}}_i, \bar{v}_i))$, where $(\bar{\mathbf{u}}_i, \bar{v}_i) \in T_{reg}^{(i)}$ with écart$(\bar{v}_i)$ minimal. Then there exists some term $m_i \in k[X]$ such that

$$(\mathbf{w}_{i+1}, r_{i+1}) = (\mathbf{w}_i, r_i) - m_i(\bar{\mathbf{u}}_i, \bar{v}_i), \tag{13}$$

where $m_i = \frac{\mathrm{lt}(r_i)}{\mathrm{lt}(\bar{v}_i)}$, $\mathrm{lm}(r_{i+1}) \prec \mathrm{lm}(r_i)$, $\mathrm{lm}(\mathbf{w}_i) \succeq_m \mathrm{lm}(m_i\bar{\mathbf{u}}_i)$ and $\mathrm{lm}(\mathbf{w}_{i+1}) = \mathrm{lm}(\mathbf{w}_i)$. There are two possibilities to consider:

(a) $(\bar{\mathbf{u}}_i, \bar{v}_i) = (\mathbf{u}_l, v_l) \in G$ for some integer $l$, or
(b) $(\bar{\mathbf{u}}_i, \bar{v}_i) \in T_i \setminus G \subset \{(\mathbf{w}_0, r_0), (\mathbf{w}_1, r_1), \ldots, (\mathbf{w}_{i-1}, r_{i-1})\}$.

In case (a), combining the form (12) for $k = i$ and Equation (13), we obtain

$$h_i(\mathbf{w}_0, r_0) = \sum_{1 \leq j \neq l \leq s} a_j^{(i)}(\mathbf{u}_j, v_j) + (a_l^{(i)} + m_i)(\mathbf{u}_l, v_l) + (\mathbf{w}_{i+1}, r_{i+1}). \tag{14}$$

Setting $h_{i+1} = h_i$, $a_j^{(i+1)} = a_j^{(i)}$ for all $j$ with $j \neq l$, and $a_l^{(i+1)} = a_l^{(i)} + m_i$. By the fact that $\mathrm{lm}(a_l^{(i+1)}) \preceq \max\{\mathrm{lm}(a_l^{(i)}), \mathrm{lm}(m_i)\}$ and $\mathrm{lm}(m_i v_l) = \mathrm{lm}(r_i)$, we have

$$\mathrm{lm}(a_l^{(i+1)} v_l) \preceq \mathrm{lm}(r_0) \text{ and } \mathrm{lm}(a_l^{(i+1)}\mathbf{u}_l) \preceq_m \mathrm{lm}(\mathbf{w}_0).$$

Therefore, we get an expression of the form (12) for $k = i+1$.

In case (b), we assume that $(\bar{\mathbf{u}}_i, \bar{v}_i) = (\mathbf{w}_d, r_d)$ for some integer $d$, where $0 \leq d \leq i-1$. Since $(\mathbf{w}_d, r_d) = h_d(\mathbf{w}_0, r_0) - \sum_{j=1}^{s} a_j^{(d)}(\mathbf{u}_j, v_j)$ and $(\mathbf{w}_i, r_i) = h_i(\mathbf{w}_0, r_0) - \sum_{j=1}^{s} a_j^{(i)}(\mathbf{u}_j, v_j)$, we substitute them into Equation (13) to get

$$(h_i - m_i h_d)(\mathbf{w}_0, r_0) = \sum_{j=1}^{s} (a_j^{(i)} - m_i a_j^{(d)})(\mathbf{u}_j, v_j) + (\mathbf{w}_{i+1}, r_{i+1}). \tag{15}$$

Setting $h_{i+1} = h_i - m_i h_d$, and $a_j^{(i+1)} = a_j^{(i)} - m_i a_j^{(d)}$ for all $j$. Since $\mathrm{lm}(m_i r_d) = \mathrm{lm}(r_i) \prec \mathrm{lm}(r_d)$, we have $\mathrm{lm}(m_i) \prec 1$. Therefore, $\mathrm{lt}(h_{i+1}) = \mathrm{lt}(h_i - m_i h_d) = 1$. It follows from $\mathrm{lm}(a_j^{(i+1)}) \preceq \max\{\mathrm{lm}(a_j^{(i)}),$

$\mathrm{lm}(m_i a_j^{(d)})\}$ that $\mathrm{lm}(a_j^{(i+1)} v_j) \preceq \mathrm{lm}(r_0)$ for all $a_j^{(i+1)} \neq 0$ and $\mathrm{lm}(r_{i+1}) \prec \mathrm{lm}(r_0)$. In addition, we obtain $\mathrm{lm}(\mathbf{w}_{i+1}) = \mathrm{lm}(\mathbf{w}_0)$, and $\mathrm{lm}(a_j^{(i+1)} \mathbf{u}_j) \preceq_m \mathrm{lm}(\mathbf{w}_0)$ for all $a_j^{(i+1)} \neq 0$. Thus, the form (12) holds true for $k = i+1$. This concludes the induction.

Suppose the algorithm terminates after the $N$-th pass through the **while** loop. This means that $(\mathbf{w}_N, r_N)$ is not regular top-reducible by $T_N$, and we do not need to execute the $(N+1)$-th **while** loop. Therefore, it follows from $G \subseteq T_N$ that $(\mathbf{w}_N, r_N)$ is not regular top-reducible by any pairs in $G$. □

Suppose $p \in M$ can be eventually super top-reducible by $G$. According to Theorem 21, we can infer the following fact: when we perform regular top-reductions to $p$ by Algorithm 1, we can obtain the pair $(\mathbf{w}, r)$ proposed in Proposition 16 within a finite number of steps, which is not regular but super top-reducible by $G$.

## 3. Cover theorem

To compute a strong standard basis of $M$, we first recall the concept of J-pair proposed by Gao et al. (2016). Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in M$ with $v_1 v_2 \neq 0$, $t = \mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))$, $t_1 = \frac{t}{\mathrm{lm}(v_1)}$, $t_2 = \frac{t}{\mathrm{lm}(v_2)}$, $c = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}$, and $\tilde{\mathbf{t}} = \max\{t_1 \mathrm{lm}(\mathbf{u}_1), t_2 \mathrm{lm}(\mathbf{u}_2)\}$. Without loss of generality, we assume that $\tilde{\mathbf{t}} = t_1 \mathrm{lm}(\mathbf{u}_1)$. If

$$\tilde{\mathbf{t}} = \mathrm{lm}(t_1 \mathbf{u}_1 - c t_2 \mathbf{u}_2),$$

then $t_1 p_1$ is called the *J-pair* of $p_1$ and $p_2$, and $\tilde{\mathbf{t}}$ is called the *J-signature* of the J-pair. It is obvious that $t_1 p_1$ is regular top-reducible by $p_2$.

We say that a pair $(\mathbf{u}, v) \in M$ is *covered* by $G \subset M$, if there is a pair $(\mathbf{u}_0, v_0) \in G$ such that $\mathrm{lm}(\mathbf{u}_0) \mid \mathrm{lm}(\mathbf{u})$ and $t\mathrm{lm}(v_0) \prec \mathrm{lm}(v)$, where $t = \frac{\mathrm{lm}(\mathbf{u})}{\mathrm{lm}(\mathbf{u}_0)}$. With this definition, Gao et al. (2016) computed a strong standard basis by repeatedly regular top-reductions of J-pairs, which is analogous to Buchberger's algorithm. Moreover, the cover theorem proposed by Gao et al. (2016) is used in this computation to eliminate a large number of J-pairs that need to be reduced. Before generalizing their result to cases with any semigroup order, we first establish some necessary results.

Let $\mathbf{u} = (u_1, \ldots, u_m) \in k[X]^m$, then the écart of $\mathbf{u}$ is defined as

$$\text{écart}(\mathbf{u}) := \deg(\mathbf{u}) - \deg(\mathrm{lm}(\mathbf{u})),$$

where $\deg(\mathbf{u}) = \max_{1 \leq i \leq m}\{\deg(u_i)\}$.

**Proposition 22.** *Let $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3 \in k[X]^m \setminus \{\mathbf{0}\}$ such that $\mathrm{lm}(\boldsymbol{u}_1) \mid \mathrm{lm}(\boldsymbol{u}_2)$ and $\boldsymbol{u}_3 = \boldsymbol{u}_2 - \frac{\mathrm{lt}(\boldsymbol{u}_2)}{\mathrm{lt}(\boldsymbol{u}_1)} \boldsymbol{u}_1$. If écart$(\boldsymbol{u}_1) \leq$ écart$(\boldsymbol{u}_2)$, then $\deg(\boldsymbol{u}_3) \leq \deg(\boldsymbol{u}_2)$.*

**Proof.** The proof is similar to that of Proposition 18, and is omitted here. □

It follows from Proposition 22 that $\deg(\mathbf{u}_3)$ is bounded by $\deg(\mathbf{u}_2)$ after reducing $\mathbf{u}_2$ by $\mathbf{u}_1$. This property will play a significant role in the proof of our main theorem.

For the convenience of description, in the following we always assume that $G \subset k[X]^m \times k[X]$ and $(\tilde{\mathbf{u}}, \tilde{v}) \in k[X]^m \times k[X]$. In addition, $\prec$ is a semigroup order and $\prec_m$ is a module order.

**Lemma 23** *(Gao et al. (2016)). Let $p_1 = (\boldsymbol{u}_1, v_1), p_2 = (\boldsymbol{u}_2, v_2) \in k[X]^m \times k[X]$, and $t$ be a monomial in $k[X]$. If $tp_1$ is regular top-reducible by $p_2$, then $t_1 p_1$ is a J-pair of $p_1$ and $p_2$, where $t_1 = \frac{\mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}{\mathrm{lm}(v_1)}$ is a divisor of $t$. Furthermore, $t_1 p_1$ is regular top-reducible by $p_2$.*

According to the proof of Lemma 23 proposed by Gao et al. (2016), this conclusion holds true for any semigroup order. By Lemma 23, we can obtain the following result that reveals an important property if every J-pair of $G$ is covered by $G$, where $G$ is a finite subset of $M$.

**Lemma 24.** *Let $G \subset M$ be a finite set such that $\{(\boldsymbol{e}_i, f_i)\}_{i=1}^m \subset G$, and $(\tilde{\mathbf{u}}, \tilde{v}) \in M$ with $\tilde{\mathbf{u}} \neq 0$. If every J-pair of $G$ is covered by $G$, then there is a pair $(\mathbf{u}_1, v_1) \in G$ such that $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\tilde{\mathbf{u}})$ and $\frac{\mathrm{lm}(\tilde{\mathbf{u}})}{\mathrm{lm}(\mathbf{u}_1)}(\mathbf{u}_1, v_1)$ is not regular top-reducible by $G$.*

**Proof.** Since $\{(\mathbf{e}_i, f_i)\}_{i=1}^m \subset G$, there is at least a pair $(\mathbf{u}, v) \in G$ such that $\mathrm{lm}(\mathbf{u}) \mid \mathrm{lm}(\tilde{\mathbf{u}})$. Let

$$T_{\tilde{\mathbf{u}}} = \left\{(\mathbf{u}, v) \in G \;\middle|\; \mathrm{lm}(\mathbf{u}) \mid \mathrm{lm}(\tilde{\mathbf{u}})\right\},$$

then $T_{\tilde{\mathbf{u}}}$ is nonempty. As $G$ is a finite set, we can select a pair $p_1 = (\mathbf{u}_1, v_1)$ from $T_{\tilde{\mathbf{u}}}$ such that $t\mathrm{lm}(v_1)$ is minimal, where $t = \frac{\mathrm{lm}(\tilde{\mathbf{u}})}{\mathrm{lm}(\mathbf{u}_1)}$. We assert that $tp_1$ is not regular top-reducible by $G$.

If otherwise, $tp_1$ is regular top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$, then by Lemma 23 $t_1 p_1$ is the J-pair of $p_1$ and $p_2$, and is regular top-reducible by $p_2$, where $t_1 = \frac{\mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}{\mathrm{lm}(v_1)}$ and $t = t_2 t_1$ for some monomial $t_2$. Since every J-pair of $G$ is covered by $G$, there is a pair $p_3 = (\mathbf{u}_3, v_3) \in G$ such that $t_1 p_1$ is covered by $p_3$, i.e., $\mathrm{lm}(\mathbf{u}_3) \mid t_1\mathrm{lm}(\mathbf{u}_1)$ and $t_3\mathrm{lm}(v_3) \prec t_1\mathrm{lm}(v_1)$, where $t_3 = \frac{t_1\mathrm{lm}(\mathbf{u}_1)}{\mathrm{lm}(\mathbf{u}_3)}$. Thus, $\mathrm{lm}(\tilde{\mathbf{u}}) = t_2 t_1 \mathrm{lm}(\mathbf{u}_1) = t_2 t_3 \mathrm{lm}(\mathbf{u}_3)$. This implies that $p_3 \in T_{\tilde{\mathbf{u}}}$. However, $t_2 t_3 \mathrm{lm}(v_3) \prec t_2 t_1 \mathrm{lm}(v_1) = t\mathrm{lm}(v_1)$, which contradicts the choice of $p_1 \in T_{\tilde{\mathbf{u}}}$. Therefore, $tp_1$ is not regular top-reducible by $G$. □

Let $(\tilde{\mathbf{u}}, \tilde{v}) \in M$, then we can reduce the leading term of $\tilde{\mathbf{u}}$ by some special pair $(\mathbf{u}_1, v_1) \in G$, and obtain the following important results.

**Lemma 25.** *Let $G \subset M$ be a finite set, and suppose $(\tilde{\mathbf{u}}, \tilde{v}) \in M$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. Assume that there is a pair $(\mathbf{u}_1, v_1) \in G$ such that $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\tilde{\mathbf{u}})$ and $\frac{\mathrm{lm}(\tilde{\mathbf{u}})}{\mathrm{lm}(\mathbf{u}_1)}(\mathbf{u}_1, v_1)$ is not regular top-reducible by $G$. Let $(\tilde{\mathbf{u}}', \tilde{v}') = (\tilde{\mathbf{u}}, \tilde{v}) - \frac{\mathrm{lt}(\tilde{\mathbf{u}})}{\mathrm{lt}(\mathbf{u}_1)}(\mathbf{u}_1, v_1)$, then*

1. *$\mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$ and $\mathrm{lm}(\tilde{v}') \succeq \mathrm{lm}(\tilde{v})$, and*
2. *$(\tilde{\mathbf{u}}', \tilde{v}')$ cannot be top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$.*

**Proof.** Obviously, $\mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$. Since $(\tilde{\mathbf{u}}, \tilde{v})$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$, we have $\mathrm{lm}(\tilde{v}) \neq t\mathrm{lm}(v_1)$, where $t = \frac{\mathrm{lm}(\tilde{\mathbf{u}})}{\mathrm{lm}(\mathbf{u}_1)}$. It follows from $\tilde{v}' = \tilde{v} - \frac{\mathrm{lt}(\tilde{\mathbf{u}})}{\mathrm{lt}(\mathbf{u}_1)} v_1$ that $\mathrm{lm}(\tilde{v}') = \max\{\mathrm{lm}(\tilde{v}), t\mathrm{lm}(v_1)\}$. Thus, $\mathrm{lm}(\tilde{v}') \succeq \mathrm{lm}(\tilde{v})$.

If $(\tilde{\mathbf{u}}', \tilde{v}')$ is top-reducible by some pair $(\mathbf{u}_0, v_0) \in G$ with $v_0 \neq 0$, then there is some monomial $t_0$ such that $\mathrm{lm}(\tilde{v}') = t_0\mathrm{lm}(v_0)$ and $t_0\mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}')$. We consider the following two cases:

(I) If $\mathrm{lm}(\tilde{v}') = \mathrm{lm}(\tilde{v})$, then $t_0\mathrm{lm}(v_0) = \mathrm{lm}(\tilde{v})$. Moreover, $t_0\mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$. It follows that $(\tilde{\mathbf{u}}, \tilde{v})$ is top-reducible by $(\mathbf{u}_0, v_0) \in G$ with $v_0 \neq 0$, which leads to a contradiction.

(II) If $\mathrm{lm}(\tilde{v}') = t\mathrm{lm}(v_1)$, then $t_0\mathrm{lm}(v_0) = t\mathrm{lm}(v_1)$. Moreover, $t_0\mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}}) = t\mathrm{lm}(\mathbf{u}_1)$. It follows that $t(\mathbf{u}_1, v_1)$ is regular top-reducible by $(\mathbf{u}_0, v_0) \in G$, which leads to a contradiction.

Therefore, $(\tilde{\mathbf{u}}', \tilde{v}')$ cannot be top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. □

**Lemma 26.** *Let $G \subset M$ be a finite set, and suppose $(\tilde{\mathbf{u}}, \tilde{v}) \in M$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. Assume that the set*

$$T_{(\tilde{\mathbf{u}}, \tilde{v})} = \left\{(\boldsymbol{u}, v) \in M \;\middle|\; \mathrm{lm}(\boldsymbol{u}) \succ_m \mathrm{lm}(\tilde{\boldsymbol{u}}) \text{ and } \mathrm{lm}(v) \preceq \mathrm{lm}(\tilde{v})\right\}$$

*is nonempty and there is a pair $(\mathbf{u}_1, v_1) \in T_{(\tilde{\mathbf{u}}, \tilde{v})}$ such that $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\tilde{\mathbf{u}})$. Let $(\tilde{\mathbf{u}}', \tilde{v}') = (\tilde{\mathbf{u}}, \tilde{v}) - \frac{\mathrm{lt}(\tilde{\mathbf{u}})}{\mathrm{lt}(\mathbf{u}_1)}(\mathbf{u}_1, v_1)$, then*

1. *$\mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$ and $\mathrm{lm}(\tilde{v}') = \mathrm{lm}(\tilde{v})$, and*
2. *$(\tilde{\mathbf{u}}', \tilde{v}')$ cannot be top-reduced by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$.*

**Proof.** Obviously, $\mathrm{lm}(\tilde{\mathbf{u}}') \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$. Since $(\mathbf{u}_1, v_1) \in T_{(\tilde{\mathbf{u}}, \tilde{v})}$, we obtain $\mathrm{lm}(\mathbf{u}_1) \succ_m \mathrm{lm}(\tilde{\mathbf{u}})$ and $\mathrm{lm}(v_1) \preceq \mathrm{lm}(\tilde{v})$. Let $t = \frac{\mathrm{lm}(\tilde{\mathbf{u}})}{\mathrm{lm}(\mathbf{u}_1)}$, then $1 \succ t$ and $t\mathrm{lm}(v_1) \prec \mathrm{lm}(\tilde{v})$. It follows from $\tilde{v}' = \tilde{v} - \frac{\mathrm{lt}(\tilde{\mathbf{u}})}{\mathrm{lt}(\mathbf{u}_1)} v_1$ that $\mathrm{lm}(\tilde{v}') = \mathrm{lm}(\tilde{v})$.

If $(\tilde{\mathbf{u}}', \tilde{v}')$ is top-reducible by some pair $(\mathbf{u}_0, v_0) \in G$ with $v_0 \neq 0$, then there is some monomial $t_0$ such that $\mathrm{lm}(\tilde{v}') = t_0\mathrm{lm}(v_0)$ and $t_0\mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}')$. Thus, $\mathrm{lm}(\tilde{v}) = t_0\mathrm{lm}(v_0)$ and $t_0\mathrm{lm}(\mathbf{u}_0) \prec_m \mathrm{lm}(\tilde{\mathbf{u}})$. This implies that $(\tilde{\mathbf{u}}, \tilde{v})$ is top-reducible by $(\mathbf{u}_0, v_0) \in G$ with $v_0 \neq 0$, which leads to a contradiction. □

We now present the main theorem, which serves as the theoretical foundation of the signature-based standard basis algorithm w.r.t. any semigroup order under the framework of the GVW algorithm. Clearly, the subsequent main theorem is more comprehensive than Theorem 3.1 in Lu et al. (2018) since $\succ$ and $\succ_m$ are not restricted to the antigraded order and TOP order, respectively.

**Theorem 27** *(Cover Theorem). Let $G \subset M$ be a finite set such that $\{(\boldsymbol{e}_i, f_i)\}_{i=1}^m \subset G$, then the following are equivalent:*

1. *$G$ is a strong standard basis for $M$;*
2. *every J-pair of $G$ is eventually super top-reducible by $G$;*
3. *every J-pair of $G$ is covered by $G$.*

Before presenting the proof of Theorem 27, we provide further explanations. The proofs of $1 \Rightarrow 2$ and $2 \Rightarrow 3$ are essentially the same as these of Theorem 2.4 in Gao et al. (2016), except that we utilize Algorithm 1 to conduct regular top-reductions on every J-pair of $G$. Thus, they are omitted here. Now, we prove $3 \Rightarrow 1$ by contradiction. The main idea is as follows.

If $G$ is not a strong standard basis for $M$, then there exists a pair $(\tilde{\mathbf{u}}_1, \tilde{v}_1) \in M$ such that it is not top-reducible by $G$. Based on Lemmas 24, 25 and 26, we reduce $\mathrm{lt}(\tilde{\mathbf{u}}_1)$ by repeatedly using pairs in $M$ and obtain a sequence $(\tilde{\mathbf{u}}_1, \tilde{v}_1), (\tilde{\mathbf{u}}_2, \tilde{v}_2), (\tilde{\mathbf{u}}_3, \tilde{v}_3), \ldots$ with special properties. That is, $(\tilde{\mathbf{u}}_i, \tilde{v}_i)$ is not top-reducible by $G$, $\mathrm{lm}(\tilde{\mathbf{u}}_i)$ is strictly decreasing and $\mathrm{lm}(\tilde{v}_i) \neq 0$ for $i \geq 2$. In the above calculation process, we reduce $\mathrm{lt}(\tilde{\mathbf{u}}_i)$ not only by pairs in $G$, but also by pairs in $\{(\tilde{\mathbf{u}}_1, \tilde{v}_1), \ldots, (\tilde{\mathbf{u}}_{i-1}, \tilde{v}_{i-1})\}$. This guarantees that there exists some positive integer $N$ such that $\deg(\tilde{\mathbf{u}}_N) \geq \deg(\tilde{\mathbf{u}}_{N+1}) \geq \ldots$. Since the set of monomials in $k[X]^m$ whose total degrees are limited by $\deg(\tilde{\mathbf{u}}_N)$ is finite, the strictly decreasing sequence $\mathrm{lm}(\tilde{\mathbf{u}}_N) \succ_m \mathrm{lm}(\tilde{\mathbf{u}}_{N+1}) \succ_m \cdots$ will terminate within a finite number of steps, i.e., there is another positive integer $N_1$ with $N_1 > N$ such that $\tilde{\mathbf{u}}_{N_1} = \mathbf{0}$. However, $\mathrm{lm}(\tilde{v}_{N_1}) \neq 0$. This implies that we obtain a pair $(\mathbf{0}, \tilde{v}_{N_1}) \in M$ with $\tilde{v}_{N_1} \neq 0$, which leads to a contradiction.

**Proof.** Let $W = \left\{(\mathbf{u}, v) \in M \;\middle|\; (\mathbf{u}, v) \text{ is not top-reducible by } G\right\}$. If $W \neq \emptyset$, then we can choose a nonzero pair $(\tilde{\mathbf{u}}_1, \tilde{v}_1)$ from $W$. Now, we consider the following two cases depending on whether $\tilde{v}_1$ is equal to zero.

**First case:** $\tilde{v}_1 \neq 0$

Obviously, $\tilde{\mathbf{u}}_1 \neq \mathbf{0}$ and $(\tilde{\mathbf{u}}_1, \tilde{v}_1)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. Since every J-pair of $G$ is covered by $G$, by Lemma 24 there is a pair $p_1 = (\mathbf{u}_1, v_1) \in G$ such that $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\tilde{\mathbf{u}}_1)$ and $\frac{\mathrm{lm}(\tilde{\mathbf{u}}_1)}{\mathrm{lm}(\mathbf{u}_1)} p_1$ is not regular top-reducible by $G$. Let

$$(\tilde{\mathbf{u}}_2, \tilde{v}_2) = (\tilde{\mathbf{u}}_1, \tilde{v}_1) - \frac{\mathrm{lt}(\tilde{\mathbf{u}}_1)}{\mathrm{lt}(\mathbf{u}_1)}(\mathbf{u}_1, v_1), \tag{16}$$

then $\mathrm{lm}(\tilde{\mathbf{u}}_2) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_1)$ and $\mathrm{lm}(\tilde{v}_2) \succeq \mathrm{lm}(\tilde{v}_1)$ by Lemma 25. Moreover, $(\tilde{\mathbf{u}}_2, \tilde{v}_2)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. Setting $T_1 = \{(\tilde{\mathbf{u}}_1, \tilde{v}_1)\}$.

Since $\mathrm{lm}(\tilde{v}_2) \succeq \mathrm{lm}(\tilde{v}_1)$, we have $\tilde{\mathbf{u}}_2 \neq \mathbf{0}$. Using Lemma 24 again, there is a pair $p_2 = (\mathbf{u}_2, v_2) \in G$ such that $\mathrm{lm}(\mathbf{u}_2) \mid \mathrm{lm}(\tilde{\mathbf{u}}_2)$ and $\frac{\mathrm{lm}(\tilde{\mathbf{u}}_2)}{\mathrm{lm}(\mathbf{u}_2)} p_2$ is not regular top-reducible by $G$. Let

$$T_{\tilde{\mathbf{u}}_2} = \left\{(\mathbf{u}, v) \in T_1 \cup \{p_2\} \;\middle|\; \mathrm{lm}(\mathbf{u}) \mid \mathrm{lm}(\tilde{\mathbf{u}}_2)\right\},$$

then $T_{\tilde{\mathbf{u}}_2}$ is nonempty and finite. We select a pair $p_2' = (\mathbf{u}_2', v_2')$ from $T_{\tilde{\mathbf{u}}_2}$ such that écart$(\mathbf{u}_2')$ is minimal. Let

$$(\tilde{\mathbf{u}}_3, \tilde{v}_3) = (\tilde{\mathbf{u}}_2, \tilde{v}_2) - \frac{\mathrm{lt}(\tilde{\mathbf{u}}_2)}{\mathrm{lt}(\mathbf{u}_2')}(\mathbf{u}_2', v_2'), \tag{17}$$

then there are two cases:

(I) If $p_2' = p_2$, then $\mathrm{lm}(\tilde{\mathbf{u}}_3) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_2)$ and $\mathrm{lm}(\tilde{v}_3) \succeq \mathrm{lm}(\tilde{v}_2)$ by Lemma 25. In addition, $(\tilde{\mathbf{u}}_3, \tilde{v}_3)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$.

(II) If $p_2' \in T_1$, then there is a pair $(\tilde{\mathbf{u}}_*, \tilde{v}_*) \in T_1$ such that $p_2' = (\tilde{\mathbf{u}}_*, \tilde{v}_*)$. Let

$$T_{(\tilde{\mathbf{u}}_2, \tilde{v}_2)} = \left\{(\mathbf{u}, v) \in M \;\middle|\; \mathrm{lm}(\mathbf{u}) \succ_m \mathrm{lm}(\tilde{\mathbf{u}}_2) \text{ and } \mathrm{lm}(v) \preceq \mathrm{lm}(\tilde{v}_2)\right\},$$

then $p_2' \in T_{(\tilde{\mathbf{u}}_2, \tilde{v}_2)}$.[1] By Lemma 26, we have $\mathrm{lm}(\tilde{\mathbf{u}}_3) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_2)$ and $\mathrm{lm}(\tilde{v}_3) = \mathrm{lm}(\tilde{v}_2)$. Moreover, $(\tilde{\mathbf{u}}_3, \tilde{v}_3)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$.

The above shows that in either case, we can always conclude that $\mathrm{lm}(\tilde{\mathbf{u}}_3) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_2)$, $\mathrm{lm}(\tilde{v}_3) \succeq \mathrm{lm}(\tilde{v}_2)$, and $(\tilde{\mathbf{u}}_3, \tilde{v}_3)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. Let $L(T_1) = \left\langle x_{n+1}^{\text{écart}(\mathbf{u})}\mathrm{lm}(\mathbf{u}) \;\middle|\; (\mathbf{u}, v) \in T_1 \right\rangle$, where $x_{n+1}$ is a new variable. Then we construct a subset $T_2$ of $M$ based on one of the following two cases:

(a) If $x_{n+1}^{\text{écart}(\tilde{\mathbf{u}}_2)}\mathrm{lm}(\tilde{\mathbf{u}}_2) \notin L(T_1)$, then setting $T_2 = T_1 \cup \{(\tilde{\mathbf{u}}_2, \tilde{v}_2)\}$.

(b) If $x_{n+1}^{\text{écart}(\tilde{\mathbf{u}}_2)}\mathrm{lm}(\tilde{\mathbf{u}}_2) \in L(T_1)$, then setting $T_2 = T_1$. Furthermore, we can assert that $\deg(\tilde{\mathbf{u}}_3) \leq \deg(\tilde{\mathbf{u}}_2)$. The reason is as follows. There is a pair $(\tilde{\mathbf{u}}_\star, \tilde{v}_\star) \in T_1$ such that $x_{n+1}^{\text{écart}(\tilde{\mathbf{u}}_\star)}\mathrm{lm}(\tilde{\mathbf{u}}_\star) \mid x_{n+1}^{\text{écart}(\tilde{\mathbf{u}}_2)}\mathrm{lm}(\tilde{\mathbf{u}}_2)$.[2] Obviously, écart$(\tilde{\mathbf{u}}_\star) \leq$ écart$(\tilde{\mathbf{u}}_2)$. Moreover, $\mathrm{lm}(\tilde{\mathbf{u}}_\star) \mid \mathrm{lm}(\tilde{\mathbf{u}}_2)$ implies that $(\tilde{\mathbf{u}}_\star, \tilde{v}_\star) \in T_{\tilde{\mathbf{u}}_2}$. Depending on the choice of $p_2' = (\mathbf{u}_2', v_2')$ in Equation (17), we have écart$(\mathbf{u}_2') \leq$ écart$(\tilde{\mathbf{u}}_\star) \leq$ écart$(\tilde{\mathbf{u}}_2)$. By Proposition 22, we get $\deg(\tilde{\mathbf{u}}_3) \leq \deg(\tilde{\mathbf{u}}_2)$.

We repeat the above calculation process to obtain the following two sequences

$$(\tilde{\mathbf{u}}_1, \tilde{v}_1), (\tilde{\mathbf{u}}_2, \tilde{v}_2), (\tilde{\mathbf{u}}_3, \tilde{v}_3), \ldots \text{ and } T_1, T_2, T_3, \ldots \tag{18}$$

For the first sequence of (18), we have a strictly decreasing sequence

$$\mathrm{lm}(\tilde{\mathbf{u}}_1) \succ_m \mathrm{lm}(\tilde{\mathbf{u}}_2) \succ_m \mathrm{lm}(\tilde{\mathbf{u}}_3) \succ_m \cdots \tag{19}$$

and a non-decreasing sequence

$$\mathrm{lm}(\tilde{v}_1) \preceq \mathrm{lm}(\tilde{v}_2) \preceq \mathrm{lm}(\tilde{v}_3) \preceq \cdots \tag{20}$$

Moreover, each pair $(\tilde{\mathbf{u}}_i, \tilde{v}_i) \in M$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$. For the second sequence of (18), we have

$$T_1 \subseteq T_2 \subseteq T_3 \subseteq \cdots \text{ and } L(T_1) \subseteq L(T_2) \subseteq L(T_3) \subseteq \cdots$$

Since $k[X, x_{n+1}]^m$ is Noetherian, there exists some positive integer $N$ such that $L(T_i)$ becomes stable for $i \geq N$, i.e., $L(T_i) = L(T_{i+1})$ for $i \geq N$. This implies that $x_{n+1}^{\text{écart}(\tilde{\mathbf{u}}_{i+1})}\mathrm{lm}(\tilde{\mathbf{u}}_{i+1}) \in L(T_i)$ for all $i \geq N$. Using the same argument as in case (b) above, we can obtain a non-increasing sequence

[1] Since $T_1 = \{(\tilde{\mathbf{u}}_1, \tilde{v}_1)\}$, we have $p_2' = (\tilde{\mathbf{u}}_1, \tilde{v}_1)$. When we analyze properties of $(\tilde{\mathbf{u}}_{i+1}, \tilde{v}_{i+1})$ with $i \geq 2$, it can be inferred from multiple recursive formulas similar to Equation (17) that $\mathrm{lm}(\tilde{\mathbf{u}}_1) \succ_m \cdots \succ_m \mathrm{lm}(\tilde{\mathbf{u}}_i)$ and $\mathrm{lm}(\tilde{v}_1) \preceq \cdots \preceq \mathrm{lm}(\tilde{v}_i)$. Therefore, $(\tilde{\mathbf{u}}_j, \tilde{v}_j) \in T_{(\tilde{\mathbf{u}}_i, \tilde{v}_i)}$ for all $1 \leq j < i$. Since $T_{i-1}$ is a nonempty subset of $\{(\tilde{\mathbf{u}}_1, \tilde{v}_1), \ldots, (\tilde{\mathbf{u}}_{i-1}, \tilde{v}_{i-1})\}$ and $p_i' \in T_{i-1}$, we obtain $p_i' \in T_{(\tilde{\mathbf{u}}_i, \tilde{v}_i)}$.

[2] Since $T_1 = \{(\tilde{\mathbf{u}}_1, \tilde{v}_1)\}$, we obtain $(\tilde{\mathbf{u}}_\star, \tilde{v}_\star) = (\tilde{\mathbf{u}}_1, \tilde{v}_1)$.

$$\deg(\tilde{\mathbf{u}}_N) \geq \deg(\tilde{\mathbf{u}}_{N+1}) \geq \deg(\tilde{\mathbf{u}}_{N+2}) \geq \cdots \tag{21}$$

Combining the sequences (19) and (21), there is another positive integer $N_1$ with $N_1 > N$ such that $\tilde{\mathbf{u}}_{N_1} = \mathbf{0}$. However, $\mathrm{lm}(\tilde{v}_{N_1}) \neq 0$ by the sequence (20). Thus, we get a pair $(\mathbf{0}, \tilde{v}_{N_1}) \in M$ with $\tilde{v}_{N_1} \neq 0$, which contradicts the definition of $M$.

**Second case:** $\tilde{v}_1 = 0$

Obviously, $\tilde{\mathbf{u}}_1 \neq \mathbf{0}$ and $(\tilde{\mathbf{u}}_1, 0)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v = 0$. Since every J-pair of $G$ is covered by $G$, by Lemma 24 there is a pair $(\mathbf{u}_1, v_1) \in G$ such that $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\tilde{\mathbf{u}}_1)$ and $\frac{\mathrm{lm}(\tilde{\mathbf{u}}_1)}{\mathrm{lm}(\mathbf{u}_1)}(\mathbf{u}_1, v_1)$ is not regular top-reducible by $G$. In addition, we have $v_1 \neq 0$. Otherwise, $(\tilde{\mathbf{u}}_1, 0)$ is top-reducible by $(\mathbf{u}_1, 0) \in G$, which leads to a contradiction. Let

$$(\tilde{\mathbf{u}}_2, \tilde{v}_2) = (\tilde{\mathbf{u}}_1, 0) - \frac{\mathrm{lt}(\tilde{\mathbf{u}}_1)}{\mathrm{lt}(\mathbf{u}_1)}(\mathbf{u}_1, v_1),$$

then $\mathrm{lm}(\tilde{\mathbf{u}}_2) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_1)$ and $\tilde{v}_2 = -\frac{\mathrm{lt}(\tilde{\mathbf{u}}_1)}{\mathrm{lt}(\mathbf{u}_1)} v_1 \neq 0$. We assert that $(\tilde{\mathbf{u}}_2, \tilde{v}_2)$ is not top-reducible by any pair $(\mathbf{u}, v) \in G$ with $v \neq 0$.

If otherwise, there is some pair $(\mathbf{u}_0, v_0) \in G$ with $v_0 \neq 0$ such that $\mathrm{lm}(\tilde{v}_2) = t_0 \mathrm{lm}(v_0)$ for some monomial $t_0$ and $t_0 \mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}_2)$. It follows from $\tilde{v}_2 = -\frac{\mathrm{lt}(\tilde{\mathbf{u}}_1)}{\mathrm{lt}(\mathbf{u}_1)} v_1$ that $t_0 \mathrm{lm}(v_0) = t \mathrm{lm}(v_1)$, where $t = \frac{\mathrm{lm}(\tilde{\mathbf{u}}_1)}{\mathrm{lm}(\mathbf{u}_1)}$. Since $t_0 \mathrm{lm}(\mathbf{u}_0) \preceq_m \mathrm{lm}(\tilde{\mathbf{u}}_2) \prec_m \mathrm{lm}(\tilde{\mathbf{u}}_1) = t \mathrm{lm}(\mathbf{u}_1)$, we get that $t(\mathbf{u}_1, v_1)$ is regular top-reducible by $(\mathbf{u}_0, v_0) \in G$, which leads to a contradiction.

Therefore, we can use the same argument as in the **First case** to address $(\tilde{\mathbf{u}}_2, \tilde{v}_2)$.

**Conclusion**

According to the analysis of the above two cases, we have $W = \emptyset$. It follows that every pair in $M$ is top-reducible by $G$. Therefore, $G$ is a strong standard basis of $M$. The proof is completed. □

Theorem 27 tells us that any J-pair of $G$ that is covered by $G$ can be discarded without performing any reductions. As special cases of the condition 3 in Theorem 27, we have the following two criteria.

**Syzygy Criterion** Any J-pair of $G$ can be discarded if it is top-reducible by a syzygy.

**Signature Criterion** All J-pairs with the same signature, one just needs to store one of them (the one with the $v$-part minimal).

## 4. Signature-based standard basis algorithm

Based on Theorem 27, we now propose a signature-based standard basis algorithm. Although the proof of $3 \Rightarrow 1$ in Theorem 27 is essentially different from that of Theorem 2.4 in Gao et al. (2016) and Theorem 3.1 in Lu et al. (2018), the framework of the signature-based algorithm remains the same as that proposed by Gao et al. (2016).

Before proceeding further, let us remark on Algorithm 2, and some observations in the following come from Lu et al. (2018).

1. From the perspective of practical calculation, we only store the signature and $v$-component for any pair during the computation.
2. In Step 3, the trivial principle syzygies $f_i \mathbf{e}_j - f_j \mathbf{e}_i$ are used to delete redundant J-pairs.
3. In Steps 4 and 14, we only store the J-pairs whose signatures are not divided by some element in $H$ (syzygy criterion) and one J-pair for each distinct signature with the $v$-part as minimal (signature criterion).
4. In Step 8, $(\mathbf{w}, r)$ is not regular top-reducible by $G$.
5. In Step 13, a principle syzygy is stored only if $\mathrm{lm}(v_j \mathbf{w} - r \mathbf{u}_j) = \max\{\mathrm{lm}(v_j \mathbf{w}), \mathrm{lm}(r \mathbf{u}_j)\}$.

**Theorem 28.** *Algorithm 2 outputs as specified within a finite number of steps.*

**Algorithm 2:** Signature-based standard basis algorithm.

**Input :** $\{f_1, \ldots, f_m\} \subset k[X]$, a semigroup order $\succ$ and a module order $\succ_m$.
**Output:** $V$, a standard basis for $\langle f_1, \ldots, f_m\rangle \subset R$; $H$, a set consisting of the leading monomials of a standard basis for the syzygies of $\{f_1, \ldots, f_m\}$.

1 **begin**
2 $G := \{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\}$;
3 $H := \{\mathrm{lm}(f_i\mathbf{e}_j - f_j\mathbf{e}_i) \mid 1 \le i < j \le m\}$;
4 $JP := \{\text{J-pairs of } G\}$;
5 **while** $JP \neq \emptyset$ **do**
6 choose $(\tilde{\mathbf{u}}, \tilde{v})$ from $JP$ and $JP := JP \setminus \{(\tilde{\mathbf{u}}, \tilde{v})\}$;
7 **if** $(\tilde{\mathbf{u}}, \tilde{v})$ is not covered by $G$ **then**
8 $(\mathbf{w}, r) :=$ result of reducing $(\tilde{\mathbf{u}}, \tilde{v})$ with Algorithm 1;
9 **if** $r = 0$ **then**
10 $H := H \cup \{\mathrm{lm}(\mathbf{w})\}$;
11 $JP := JP \setminus \{(\mathbf{u}', v') \in JP \mid \mathrm{lm}(\mathbf{w}) \mid \mathrm{lm}(\mathbf{u}')\}$;
12 **else**
13 $H := H \cup \{\mathrm{lm}(r\mathbf{u} - v\mathbf{w}) \mid (\mathbf{u}, v) \in G\}$;
14 $JP := JP \cup \{\text{J-pair of } (\mathbf{w}, r) \text{ and } (\mathbf{u}, v) \mid (\mathbf{u}, v) \in G\}$;
15 $G := G \cup \{(\mathbf{w}, r)\}$;
16 **return** $V := \{v \mid (\mathbf{u}, v) \in G\}$ and $H$.

**Proof.** The correctness follows directly from Theorem 27. The termination depends on Algorithm 1 and the Noetherian property of any polynomial ring over a field. Although the proof is essentially the same as that of Theorem 3.1 in Gao et al. (2016), we provide a proof of this fact to keep our presentation self-contained.

For any two pairs $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in M$, we say that $p_1$ divides $p_2$ if $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\mathbf{u}_2)$ and $\mathrm{lm}(v_1) \mid \mathrm{lm}(v_2)$. We list the pairs in $G$ in exactly the same order as they were obtained:

$$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m), (\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2), \ldots, (\mathbf{u}_i, v_i), \ldots \tag{22}$$

Then we claim that $p_j = (\mathbf{u}_j, v_j)$ does not divide $p_i = (\mathbf{u}_i, v_i)$ for all $j < i$. If otherwise, there is some positive integer $j$ with $j < i$ such that $p_j \mid p_i$. Then, there are some monomials $t_1, t_2 \in k[X]$ such that $\mathrm{lm}(\mathbf{u}_i) = t_1\mathrm{lm}(\mathbf{u}_j)$ and $\mathrm{lm}(v_i) = t_2\mathrm{lm}(v_j)$. If $t_1 \succ t_2$, then $t_2\mathrm{lm}(\mathbf{u}_j) \prec_m t_1\mathrm{lm}(\mathbf{u}_j) = \mathrm{lm}(\mathbf{u}_i)$. This implies that $p_i$ is regular top-reducible by $p_j$, contradicting to Step 8 of Algorithm 2 which makes sure that all pairs added to $G$ are not regular top-reducible by $G$. Clearly, it is crucial that Algorithm 1 outputs the related results within a finite number of steps. Therefore, we must have $t_1 \preceq t_2$. Then, $t_1\mathrm{lm}(v_j) \preceq t_2\mathrm{lm}(v_j) = \mathrm{lm}(v_i)$. Let $p = (\tilde{\mathbf{u}}, \tilde{v})$ be the J-pair in Step 8 that was reduced to $p_i$, then $\mathrm{lm}(\tilde{\mathbf{u}}) = \mathrm{lm}(\mathbf{u}_i)$ and $\mathrm{lm}(v_i) \prec \mathrm{lm}(\tilde{v})$ (as a J-pair is always regular top-reducible). Hence, the J-pair $p$ is covered by $p_j$, and should have been discarded before Step 7. Therefore, we have a sequence

$$(\mathrm{lm}(\mathbf{u}_1), \mathrm{lm}(v_1)), (\mathrm{lm}(\mathbf{u}_2), \mathrm{lm}(v_2)), \ldots, (\mathrm{lm}(\mathbf{u}_i), \mathrm{lm}(v_i)), \ldots \tag{23}$$

where none of them is divisible by any previous one.

We introduce new variables $Y_i = (y_{i1}, y_{i2}, \ldots, y_{in})$, where $i = 1, \ldots, m$. Each pair $(X^\alpha\mathbf{e}_i, X^\beta)$ corresponds to a monomial $Y_i^\alpha X^\beta$, which in the variables $y_{ij}$'s and $x_j$'s, where $j = 1, \ldots, n$. Then, the pairs in the sequence (23) give us a list of monomials in the variables $y_{ij}$ and $x_j$ with the property that none is divisible by any previous one. Since every polynomial ring over a field is Noetherian, the ascending chain condition tells us that this list of monomials must be finite. It follows that $G$ is finite. Therefore, Algorithm 2 terminates within a finite number of steps. □

## 5. Illustrative example

The following example is basically the same as Example 4.1 in Lu et al. (2018), except that the orders are different.

**Example 29.** Let $I$ be an ideal in $R=\mathbb{C}[x_1,x_2,x_3]_{\succ}$ generated by $f_1,f_2,f_3$, where $f_1=x_1^2-5x_2x_3-2x_2^2x_3$, $f_2=2x_1x_2+2x_2^3-x_3^3$, $f_3=-x_1x_2+x_2x_3^2$ and $\mathbb{C}$ is the complex field. $\succ$ is a mixed order defined as follows: $x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}\succ x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$ if either $x_1^{\alpha_1}\succ_1 x_1^{\beta_1}$, or $x_1^{\alpha_1}=x_1^{\beta_1}$ and $x_2^{\alpha_2}x_3^{\alpha_3}\succ_2 x_2^{\beta_2}x_3^{\beta_3}$, where $\succ_1$ is the lexicographic order with $x_1$ and $\succ_2$ is the antigraded lexicographic order with $x_2>x_3$. Let $\succ_3$ be the POT order in $R^3$ with $\mathbf{e}_1>\mathbf{e}_2>\mathbf{e}_3$, then we compute a standard basis for $I$ and the leading monomials of a standard basis for the syzygy module of $\{f_1,f_2,f_3\}$.

**Initial:**

$G_0:=\{p_1,p_2,p_3\}=\{(\mathbf{e}_1,f_1),(\mathbf{e}_2,f_2),(\mathbf{e}_3,f_3)\}$;

$H_0:=\{x_1x_2\mathbf{e}_1,x_1x_2\mathbf{e}_2\}$ is the set of the leading monomials of principle syzygies $\{\mathbf{e}_1f_2-\mathbf{e}_2f_1,\mathbf{e}_1f_3-\mathbf{e}_3f_1,\mathbf{e}_2f_3-\mathbf{e}_3f_2\}$;

$JP_0:=\{(T_1,v_1),(T_2,v_2)\}=\{(\mathbf{e}_2,f_2),(x_2\mathbf{e}_1,x_2f_1)\}$ is the J-pairs set of $G_0$.

**First loop:**

We select the J-pair $(T_1,v_1)$ from $JP_0$ and $JP_1:=\{(T_2,v_2)\}$. By checking, $(T_1,v_1)$ is not covered by $G_0$, but it can be regular top-reducible by $G_0$ to $p_4:=(T_1,\tilde{v}_1)=(\mathbf{e}_2,2x_2^3+2x_2x_3^2-x_3^3)$. Since $\tilde{v}_1\neq 0$, we compute the principle syzygies of $p_4$ with $G_0$, and add the leading monomial of these syzygies to $H_0$ (delete any redundant ones), and obtain $H_1:=H_0\cup\{x_2^3\mathbf{e}_1\}$. We compute the J-pairs of $p_4$ with elements in $G_0$ and get $JP_1:=\{(T_3,v_3),(T_2,v_2)\}$, where $(T_3,v_3)=(x_1\mathbf{e}_2,x_1\tilde{v}_1)$. Moreover, $G_1:=G_0\cup\{p_4\}$.

**Second loop:**

We select $(T_3,v_3)$ from $JP_1$ and $JP_2:=\{(T_2,v_2)\}$. $(T_3,v_3)$ can be regular top-reducible by $G_1$ to $p_5:=(T_3,\tilde{v}_3)=(x_1\mathbf{e}_2,2x_2^3x_3^2+2x_2x_3^4-x_1x_3^3)$. According to syzygy criterion and signature criterion, we obtain $H_2:=H_1\cup\{x_1x_3^3\mathbf{e}_1\}$, $JP_2:=\{(T_4,v_4),(T_2,v_2)\}$ and $G_2:=G_1\cup\{p_5\}$, where $(T_4,v_4)=(x_3^3\mathbf{e}_1,x_3^3f_1)$.

**Third loop:**

We select $(T_4,v_4)$ from $JP_2$ and $JP_3:=\{(T_2,v_2)\}$. $(T_4,v_4)$ can be regular top-reducible by $G_2$ to $p_6:=(T_4,\tilde{v}_4)=(x_3^3\mathbf{e}_1,2x_2^3x_3^4+2x_2x_3^6-2x_2^2x_3^4-5x_2x_3^4)$. According to syzygy criterion and signature criterion, we obtain $H_3:=H_2$, $JP_3:=\{(T_5,v_5),(T_2,v_2)\}$ and $G_3:=G_2\cup\{p_6\}$, where $(T_5,v_5)=(x_2^2x_3^3\mathbf{e}_1,x_2^2\tilde{v}_4)$.

**Fourth loop:**

We select $(T_5,v_5)$ from $JP_3$ and $JP_4:=\{(T_2,v_2)\}$. $(T_5,v_5)$ can be regular top-reducible by $G_3$ to $p_7:=(T_5,\tilde{v}_5)=(x_2^2x_3^2\mathbf{e}_1,2x_2^5x_3^4+4x_2^3x_3^6-2x_2^4x_3^4-\frac{5}{2}x_3^7+2x_2x_3^8-2x_2^2x_3^6)$. According to syzygy criterion and signature criterion, we obtain $H_4:=H_3$, $JP_4:=\{(T_2,v_2)\}$ and $G_4:=G_3\cup\{p_7\}$.

**Fifth loop:**

We select $(T_2,v_2)$ from $JP_4$ and $JP_5:=\emptyset$. $(T_2,v_2)$ can be regular top-reducible by $G_4$ to $p_8:=(T_2,\tilde{v}_2)=(x_2\mathbf{e}_1,x_2x_3^4-2x_2^3x_3-5x_2^2x_3)$. According to syzygy criterion and signature criterion, we obtain $H_5:=H_4$, $JP_5:=\{(T_6,v_6)\}$ and $G_5:=G_4\cup\{p_8\}$, where $(T_6,v_6)=(x_2^2\mathbf{e}_1,x_2\tilde{v}_2)$.

**Sixth loop:**

We select $(T_6,v_6)$ from $JP_5$ and $JP_6:=\emptyset$. $(T_6,v_6)$ can be regular top-reducible by $G_5$ to $p_9:=(T_6,\tilde{v}_6)=(x_2^2\mathbf{e}_1,x_2^2x_3^4-2x_2^4x_3+5x_3^3x_2-\frac{5}{2}x_3^4)$. According to syzygy criterion and signature criterion, we obtain $H_6:=H_5$, $JP_6:=\{(T_7,v_7)\}$ and $G_6:=G_5\cup\{p_9\}$, where $(T_7,v_7)=(x_2^2x_3\mathbf{e}_1,x_3\tilde{v}_6)$.

**Seventh loop:**

We select $(T_7,v_7)$ from $JP_6$ and $JP_7:=\emptyset$. $(T_7,v_7)$ can be regular top-reducible by $G_6$ to $p_{10}:=(T_7,\tilde{v}_7)=(x_2^2x_3\mathbf{e}_1,x_2^2x_3^5-2x_2^4x_3^2-\frac{5}{2}x_3^5+2x_2^3x_3^4+2x_2x_3^6-2x_2^2x_3^4)$. According to syzygy criterion and signature criterion, we obtain $H_7:=H_6$, $JP_7:=\emptyset$ and $G_7:=G_6\cup\{p_{10}\}$.

**Output:**

Since $JP_7$ is empty, the algorithm terminates. Therefore, the standard basis of $I$ in $R$ is $\{f_1, f_2, f_3, \tilde{v}_1, \tilde{v}_2, \tilde{v}_3, \tilde{v}_4, \tilde{v}_6, \tilde{v}_7\}$, and the leading monomials of the standard basis for the syzygy module is $\{x_1x_2\mathbf{e}_2, x_1x_2\mathbf{e}_1, x_2^3\mathbf{e}_1, x_1x_3^3\mathbf{e}_1\}$.

It is apparent from the above example that we discard 36 J-pairs by using three criteria, and only perform 7 regular top-reductions.

## 6. Concluding remarks

In previous work, we always need to pick a pair with a minimal signature from some subset to prove the cover theorem. In order to pick a minimal signature successfully, a local order $\succ$ and module order $\succ_m$ in Lu et al. (2018) are restricted to be the antigraded order and TOP order, respectively. In this paper, we relax the restrictions on a local order and module order to allow for any semigroup order and a compatible module order. The key is that using the idea of the Mora normal form algorithm, we can avoid the selection of minimal signatures, and provide a more essential proof for the cover theorem.

## CRediT authorship contribution statement

**Dong Lu:** Investigation, Methodology, Writing – original draft, Writing – review & editing. **Dingkang Wang:** Investigation, Methodology, Writing – original draft, Writing – review & editing. **Fanghui Xiao:** Investigation, Methodology, Writing – original draft, Writing – review & editing. **Xiaopeng Zheng:** Investigation, Methodology, Writing – original draft, Writing – review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

No data was used for the research described in the article.

## Acknowledgements

The authors are grateful to the three anonymous reviewers for their insightful suggestions. This research was supported by the National Natural Science Foundation of China under Grant Nos. 12171469, 12201210 and 12001030, the National Key Research and Development Program under Grant No. 2020YFA0712300, the Sichuan Science and Technology Program under Grant No. 2024NSFSC0418, and the Fundamental Research Funds for the Central Universities under Grant No. 2682024ZTPY052.

## References

Arri, A., Perry, J., 2011. The F5 criterion revised. J. Symb. Comput. 46, 1017–1029.

Ars, G., Hashemi, A., 2010. Extended F5 criteria. J. Symb. Comput. 45, 1330–1340.

Buchberger, B., 1965. Ein algorithmus zum auffinden der basiselemente des restklassenrings nach einem nulldimensionalen polynomideal. Ph.D. thesis.

Buchberger, B., 1979. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In: Ng, E.W. (Ed.), Symbolic and Algebraic Computation, EUROSAM 1979. In: Lecture Notes in Computer Science, vol. 72. Springer, Berlin, Heidelberg, pp. 3–21.

Buchberger, B., 1985. Gröbner bases: an algorithmic method in polynomial ideal theory. In: Bose, N.K. (Ed.), Multidimensional Systems Theory – Progress, Directions and Open Problems in Multidimensional Systems. D. Reidel Publ. Comp., Dordrecht, pp. 184–232.

Caruso, X., Vaccon, T., Verron, T., 2020. Signature-based algorithms for Gröbner bases over tate algebras. In: Proceedings of the 2020 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 70–77.
Cox, D., Little, J., O'shea, D., 2005. Using Algebraic Geometry, second edition. Graduate Texts in Mathematics. Springer, New York.
Cox, D., Little, J., O'shea, D., 2007. Ideals, Varieties, and Algorithms, third edition. Undergraduate Texts in Mathematics. Springer, New York.
Eder, C., Faugère, J.-C., 2017. A survey on signature-based Gröbner basis computations. J. Symb. Comput. 80, 719–784.
Eder, C., Perry, J., 2010. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. J. Symb. Comput. 45, 1442–1458.
Eder, C., Perry, J., 2011. Signature-based algorithms to compute Gröbner bases. In: Proceedings of the 2011 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 99–106.
Eder, C., Pfister, G., Popescu, A., 2017. On signature-based Gröbner bases over Euclidean rings. In: Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 141–148.
Faugère, J.-C., 1999. A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra 139 (1), 61–88.
Faugère, J.-C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 75–83.
Francis, M., Verron, T., 2021. On two signature variants of Buchberger's algorithm over principal ideal domains. In: Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 139–146.
Gao, S., Guan, Y., Volny IV, F., 2010. A new incremental algorithm for computing Gröbner bases. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 13–19.
Gao, S., Volny IV, F., Wang, M., 2016. A new framework for computing Gröbner bases. Math. Comput. 85 (297), 449–465.
Gebauer, R., Möller, H., 1986. Buchberger's algorithm and staggered linear bases. In: Proceedings of the 1986 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 218–221.
Gerdt, V.-P., Hashemi, A., M.-Alizadeh, B., 2013. Involutive bases algorithm incorporating F5 criterion. J. Symb. Comput. 59, 1–20.
Greuel, G., Pfister, G., 2002. A SINGULAR Introduction to Commutative Algebra. Springer-Verlag.
Hironaka, H., 1964. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. Ann. Math. 79 (1), 109–203.
Lazard, D., 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (Ed.), Computer Algebra, EUROCAL 1983. In: Lecture Notes in Computer Science, vol. 162. Springer, Berlin, Heidelberg, pp. 146–156.
Lu, D., Wang, D., Xiao, F., Zhou, J., 2018. Extending the GVW algorithm to local ring. In: Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 271–278.
Möller, H., Mora, T., Traverso, C., 1992. Gröbner bases computation using syzygies. In: Proceedings of the 1992 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 320–328.
Mora, F., 1982. An algorithm to compute the equations of tangent cones. In: Calmet, J. (Ed.), Computer Algebra, EUROCAM 1982. In: Lecture Notes in Computer Science, vol. 144. Springer, Berlin, Heidelberg, pp. 158–165.
Sun, Y., Wang, D., 2011a. The F5 algorithm in Buchberger's style. J. Syst. Sci. Complex. 24 (6), 1218–1231.
Sun, Y., Wang, D., 2011b. A generalized criterion for signature related Gröbner basis algorithms. In: Proceedings of the 2011 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 337–344.