Communications of JSSAC (2020)
Vol. 4, pp. 33 – 49

Simple Signature-Based Algorithms with Correctness and Termination

Kosuke Sakata*

Graduate School of Environment and Information Sciences, Yokohama National University

(Received 3/Jun/2020 Accepted 12/Nov/2020)

Abstract

We show correctness and termination of signature-based algorithms for computing Gröbner bases, together with some remarks on those algorithms. Compared to rewrite basis algorithm introduced by Eder and Roune in 2012, we describe an equivalent algorithm called "alternative rewrite basis algorithm" more concretely, with giving self-contained proofs of the correctness and the termination of the algorithm more clearly and transparently. The original rewrite basis algorithm seems to be designed so that it is efficient when POT is chosen as a module order and it proceeds incrementally like: computing Gröbner bases of $\langle f_1 \rangle$, $\langle f_1, f_2 \rangle$, $\langle f_1, f_2, f_3 \rangle, \ldots, \langle f_1, f_2, \ldots, f_m \rangle$ in order for polynomials $\{f_i\}_{i=1,2,3,\ldots,m}$. We clarify the reason of the efficiency in that case. If we use the original rewrite basis algorithm with a module order other than POT, we compute extra zero reductions. The algorithm presented in this paper is modified to keep the efficiency as much as possible when we choose a module order other than POT.

Keywords: Gröbner Basis, rewrite basis algorithm, signature-based algorithm

1 Introduction

Gröbner bases are one of important research topics in algebra and is widely used in applications. It is well-known that Gröbner bases are utilized for solving systems of polynomial equations. In cryptography, Gröbner basis method was utilized for breaking a challenge of the first hidden field equations (HFE) crypto system [10]. For other applications like coding theory, statistics and integer programming problem etc., it is possible to obtain a solution by converting a problem into a polynomial system and computing its Gröbner basis. Some engineering problems are necessary to be dealt with problems of polynomial systems including parameters. For these problems, there exits algorithms for computing comprehensive Gröbner bases. In the algorithms, Gröbner bases are computed multiple times. In summary, Gröbner bases have a wide range of applications. It can be expected that many works for such applications would progress by improving Gröbner basis algorithms, as it accelerates computation of Gröbner bases.

*sakata-kosuke-rb@g.ecc.u-tokyo.ac.jp

In 1964, Buchberger [2] introduced the notion of Gröbner bases and proposed an algorithm for computing Gröbner bases. Since then, various improvements about the algorithm have been proposed. As for computing a Gröbner basis, it is required to simplify polynomials, called a reduction. Elements of a Gröbner basis are generated by reducing polynomials, and some polynomials are reduced to zero. The computations of zero reductions do not give any information of the Gröbner basis. Moreover the number of zero reductions is tend to be larger than that of nonzero reductions. Therefore, in order to decrease amount of calculations, methods for detecting polynomials which are reduced to zero have been studied by many researchers.

One important improvement of Gröbner basis algorithms is F5 algorithm proposed by Faugère in 2002 [9]. F5 algorithm discards many polynomials that are reduced to zero, comparing to conventional algorithms.

When first proposed, the algorithm was complicated and the proof was incomplete. Since then, F5 has been deeply studied and accurate proofs of correctness and termination have been submitted (main references are [5, 11, 12, 14, 15]). Several algorithms and methods for improving F5 have been proposed (main references are [1, 3, 4, 6, 8, 13]). F5 is now recognized as one of signature-based algorithms. The paper [7] compiled studies of signature-based algorithms, so that we can overview research of signature-based algorithms. In the paper, signature-based algorithms are generalized as rewrite basis algorithm (**RB**) [6]. The algorithm in [1] called Arri and the algorithm in [13] called GVW are introduced as **RB** with RAT selected for a rewrite order. The explanations and the definitions of rewrite basis algorithm, a rewrite order and RAT are not given in this paper because they are too long. When we choose RAT for a rewrite order, rewrite basis algorithm becomes the most efficient. The proofs of correctness and termination in [7] are not self-contained unfortunately. Additionally, **RB** is not provided as an efficient algorithm in case we choose module orders other than POT (position over term) because **RB** is introduced as a generalized signature-based algorithm.

In this paper, we introduce alternative rewrite basis algorithm (**altRB**) (see **Algorithm 4** in Section 6). This algorithm is efficient for an arbitrary module order other than POT, and moreover it is concrete enough to be implemented. As the main results of this paper, we prove the correctness (Theorem 20) and the termination (Theorem 21) of **altRB**. By designing the algorithm concretely, the proofs of the correctness and the termination are clearer and more transparent. The proofs are done by several steps. In each step, we discuss the correctness and the termination of an algorithm. The algorithms are fundamental signature-based semi-algorithm[1)] (**fundSB**), simple signature-based algorithm (**simpleSB**), simple syzygy signature-based algorithm (**syzSB**), alternative rewrite basis algorithm (**altRB**). The algorithms in earlier steps are less complex. We believe that the proofs of Theorem 20 and Theorem 21 are easy for the reader to understand, as so are the proofs of each step. In Section 7, we prove that RB has an exceptional advantage when POT is chosen for a module order and RB proceeds incrementally. On the other hand, **altRB** is designed to be suitable for an arbitrary module order.

This paper is organized as follows. In Section 2, we recall notations and definitions in [7] of signature-based algorithms. In Section 3, we focus on that signature-based algorithms compute a Gröbner basis in the ascending order of signature. In order to look at the behavior of the algorithms, we study fundamental signature-based semi-algorithm (**fundSB**), which is simpler than subsequent algorithms. Although this semi-algorithm does not terminate, it helps us grasp the idea and how signature-based algorithms work, and also make clear the proofs of the correctness and the termination of the subsequent algorithms. In Section 4, we study a basic signature-based algorithm, which terminates in finite steps. The algorithm is called "simple signature-based algorithm (**simpleSB**)".

[1)] When the word semi-algorithm is used, it is intended that the process may not terminate. The word semi-algorithm is used only for fundamental signature-based semi-algorithm (**fundSB**).

It is essentially equivalent to the algorithm genSB [7]. However, the proofs of the correctness and the termination are partially different to those of [7] and are described in detail. In Section 5, we focus on methods for detecting polynomials which are reduced to zero. The methods are specific to signature-based algorithms. Simple syzygy signature-based algorithm (**syzSB**) is considered to illustrate the method. In Section 6, alternative rewrite basis algorithm (**altRB**) is introduced. We show the termination and the correctness of **altRB**. In Section 7, we discuss the number of zero reductions and module orders as in one previous paragraph.

It is known that signature-based algorithms compute not only a signature Gröbner basis but also a Gröbner basis of the syzygy module for a given input system. **syzSB** and **altRB** outputs the leading terms of Gröbner basis of the syzygy module. If you give small modification, they can output a Gröbner basis itself. But we do not refer to the fact and its proofs, see [13] and [7].

2 Notation

Let R be a polynomial ring over a field K. Let us denote $K \setminus \{0\}$ by $K^\times$. For $a, b \in R$, we write $a \mid b$ if b is divisible by a.

Let $f_1, f_2, \ldots, f_m$ be elements of R. Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m$ be the standard basis of a free module R^m. Consider the homomorphism

$$\overline{\ }: \quad R^m \quad \longrightarrow \quad R$$

defined by

$$\alpha = \sum_{i=1}^{m} a_i \mathbf{e}_i \quad \longmapsto \quad \overline{\alpha} = \sum_{i=1}^{m} a_i f_i,$$

where $a_1, \ldots, a_m \in R$, especially $\overline{\mathbf{e}_i} = f_i$ holds.

We choose a monomial order $\leq$ on R, and choose a module order $\preceq$. The module order is required to be compatible with the monomial order, that means: $a\mathbf{e}_i \preceq b\mathbf{e}_i$ for $i = 1, \ldots, m$ for all monomials $a, b \in R$ in case $a \leq b$. An element of R^m of the form $a\mathbf{e}_i$ for a monomial a of R is called a *term* of R^m. Let $\alpha = a\mathbf{e}_i$ and $\beta = b\mathbf{e}_j$ be terms, if there exists $c \in K^\times$ such that $a = cb$ and $i = j$, we write $\alpha \simeq \beta$ and we say that α and β are *equivalent*. If $a \mid b$ and $i = j$, we write $\alpha \mid \beta$. For $f \in R$, $\mathrm{LT}(f)$ denotes the leading term of f with respect to the monomial order. For $\alpha \in R^m$, the *signature* $\mathfrak{s}(\alpha)$ of α is defined to be the leading term of α with respect to the module order.

Let G be a subset of R^m. For $\alpha, \alpha' \in R^m$, we say that α is $\mathfrak{s}$-*reduced* to α' if there exist $\beta \in G$ and $b \in R$ satisfying the three conditions:

(a) $\mathrm{LT}(\overline{b\beta}) = t$ for a (certain) monomial t in $\overline{\alpha}$

(b) $\mathfrak{s}(b\beta) \preceq \mathfrak{s}(\alpha)$

(c) $\alpha' = \alpha - b\beta$.

At this time, we call β a reducer. We say that α is *singularly* $\mathfrak{s}$-*reduced* to α' if the condition **(b)** above is replaced by $\mathfrak{s}(b\beta) \simeq \mathfrak{s}(\alpha)$, and otherwise that α is *regularly* $\mathfrak{s}$-*reduced* to α'. If there exists $c \in K$ such that $\mathrm{LT}(\overline{b\beta}) = c\,\mathrm{LT}(\overline{\alpha})$, the $\mathfrak{s}$-reduction is called *top* $\mathfrak{s}$-*reduction* and otherwise called *tail* $\mathfrak{s}$-*reduction*. If the $\alpha \in R^m$ cannot be $\mathfrak{s}$-reduced, we say that α is *completely* $\mathfrak{s}$-*reduced*. If the $\alpha \in R^m$ cannot be regularly top $\mathfrak{s}$-reduced, we say that α is *completely regularly top* $\mathfrak{s}$-*reduced*. If the $\alpha \in R^m$ can be both neither regularly top $\mathfrak{s}$-reduced nor regularly tail $\mathfrak{s}$-reduced, we say that α is *completely regularly full* $\mathfrak{s}$-*reduced*. If $\alpha \in R^m$ is completely $\mathfrak{s}$-reduced and $\overline{\alpha}$ is $0 \in R$, then we say

that α is completely $\mathfrak{s}$-reduced to $0 \in R$ (Remark: it does not mean that α is completely $\mathfrak{s}$-reduced to $0 \in R^m$).

A subset $G \subseteq R^m$ is *a signature Gröbner basis up to signature T* if all $\alpha \in R^m$ with $\mathfrak{s}(\alpha) \prec T$ are completely $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. A subset $G \subseteq R^m$ is *a signature Gröbner basis in signature T* if all $\alpha \in R^m$ with $\mathfrak{s}(\alpha) \prec T$ are completely $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. A subset $G \subseteq R^m$ is *a signature Gröbner basis* if all $\alpha \in R^m$ are $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. The signature-based algorithms compute a signature Gröbner basis. If G is a signature Gröbner basis, then $\{\overline{g} \mid g \in G\}$ is a Gröbner basis of the ideal generated by $\{\overline{g} \mid g \in G\}$.

Proposition 1
Let I be the ideal generated by $\{f_1, \ldots, f_m\}$, let G be a signature Gröbner basis. Then, $\{\overline{g} \mid g \in G\}$ is a Gröbner basis of the ideal $\langle \overline{g} \mid g \in G \rangle$.

Proof First, we show $\overline{\alpha} \in I$ for any $\alpha \in G$. Let $\alpha \in G$, which is written as $\sum_{i=1}^{m} r_i \mathbf{e}_i$, for $r_i \in R$. Then $\overline{\alpha} = \sum_{i=1}^{m} r_i \overline{\mathbf{e}_i} = \sum_{i=1}^{m} r_i f_i$.

Assume that $\{\overline{g} \mid g \in G\}$ is not a Gröbner basis of I. Then, there exists $h \in I$ such that h is not top reducible by $\{\overline{g} \mid g \in G\}$. As $h \in I$, one can write h as $\sum_{i=1}^{m} a_i f_i$ for $a_i \in R$. Put $\beta = \sum_{i=1}^{m} a_i \mathbf{e}_i \in R^m$. Then, we have $\overline{\beta} = h$. Since G is a signature Gröbner basis, β is top $\mathfrak{s}$-reducible. This means that h is top reducible. This is a contradiction. ∎

A signature Gröbner basis G is *minimal* if there does not exist an element α in G which top $\mathfrak{s}$-reduces any other elements in $G \setminus \{\alpha\}$. We also use the word "minimal" for a signature Gröbner basis in G and up to G.

3 Fundamental signature-based semi-algorithm

In this section, fundamental signature-based semi-algorithm (**fundSB**) is considered. It helps us to comprehend how signature-based algorithms work. Specifically almost all signature-based algorithms proceed in the ascending order of signatures. **fundSB** is a prototype of them. **Algorithm 1** is the pseudocode of **fundSB**.

Algorithm 1 Fundamental signature-based semi-algorithm (**fundSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.

Step 1 $\alpha \leftarrow$ the minimal term in R^m which is bigger than the terms computed before
Step 2 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 3 (i) If $\overline{\alpha'} = 0$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

fundSB does not terminate, because it will compute all terms in R^m and the number of elements of R^m are infinite. However, we can prove the following properties:

(A) at the end of Step 3, G is a signature Gröbner basis in α,

(B) at the end of Step 1, G is a signature Gröbner basis up to α.

If **(A)** is satisfied, **(B)** is true because **fundSB** computes in the ascending order of terms in R^m step by step. We shall prove **(A)** in Proposition 5. For this, we need Lemmas 2, 3 and 4 below.

Remark : fundSB could terminate, if we modify **fundSB** as following:

(1) Select a term $\beta \in R^m$, a monomial order and a module order such that the number of terms up to β is finite.

(2) Terminate **fundSB** when the calculation progresses to β.

In this case, **fundSB** outputs a signature Gröbner basis up to β.

Lemma 2 is called singular criterion [3].

Lemma 2
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \preceq T$,

(2) α *and* β *are completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{\beta})$. *Moreover, if* α *and* β *are completely regularly* $\mathfrak{s}$*-reduced, then* $\overline{\alpha} = \overline{\beta}$.

Proof (The former) Assume that $\mathrm{LT}(\overline{\alpha}) \neq \mathrm{LT}(\overline{\beta})$. Then, either $\mathrm{LT}(\overline{\alpha-\beta}) = \mathrm{LT}(\overline{\alpha})$ or $\mathrm{LT}(\overline{\alpha-\beta}) = \mathrm{LT}(\beta)$ is satisfied. Since $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$, we have $\mathfrak{s}(\alpha-\beta) \prec \mathfrak{s}(\alpha) \preceq T$. Therefore, $\alpha-\beta$ is top $\mathfrak{s}$-reducible by G, that is, there exists a pair $(\gamma, a) \in G \times R$ such that $\mathfrak{s}(a\gamma) \preceq \mathfrak{s}(\alpha-\beta)$ and $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha-\beta})$. This $a\gamma$ satisfies that $\mathfrak{s}(a\gamma) \prec \mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$ and either $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha})$ or $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\beta})$. Then, $a\gamma$ regularly top $\mathfrak{s}$-reduce α or β. This contradicts that α and β are completely regularly top $\mathfrak{s}$-reduced.

(The latter) Assume that $\overline{\alpha-\beta} \neq 0$. The leading term of $\overline{\alpha-\beta}$ is the term included in either $\overline{\alpha}$ or $\overline{\beta}$. Since $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$, we have $\mathfrak{s}(\alpha-\beta) \prec \mathfrak{s}(\alpha) \preceq T$. Therefore, $\alpha-\beta$ is top $\mathfrak{s}$-reducible by G, that is, there exists a pair$(\gamma, a) \in (G, R)$ such that $\mathfrak{s}(a\gamma) \preceq \mathfrak{s}(\alpha-\beta)$ and $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha-\beta})$. This $a\gamma$ satisfies that $\mathfrak{s}(a\gamma) \prec \mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$ and there exists a term in $\overline{\alpha}$ or $\overline{\beta}$ such that the term is the same as $\mathrm{LT}(\overline{a\gamma})$. Then, $a\gamma$ regularly $\mathfrak{s}$-reduce α or β. This contradicts that α and β are completely regularly $\mathfrak{s}$-reduced. ∎

Let T be a term in R^m. When we have a signature Gröbner basis up to $T \in R^m$, and let $\alpha \in R^m$ satisfy $\mathfrak{s}(\alpha) \preceq T$ and α is completely regularly top $\mathfrak{s}$-reduced and singularly top $\mathfrak{s}$-reducible, then we can discard α thanks to Lemmas 3 and 4 below.

Lemma 3
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ and $\beta \in G$ satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regularly top* $\mathfrak{s}$*-reduced by* G,

(3) there exists $a \in R$ *which satisfies* $\mathfrak{s}(\alpha) \simeq \mathfrak{s}(a\beta)$ *and* $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{a\beta})$.

Then, $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$.

Proof Assume that $\mathfrak{s}(\alpha) \neq \mathfrak{s}(a\beta)$. Then, there exists $c \in K$ that satisfies $c \neq 1$ and $\mathfrak{s}(\alpha) = c\mathfrak{s}(a\beta)$. Since $\mathfrak{s}(\alpha - ca\beta) \prec \mathfrak{s}(\alpha) \preceq T$, we have that $\alpha - ca\beta$ is top $\mathfrak{s}$-reducible by G. Therefore, there exists a pair $(\gamma, b) \in G \times R$ that satisfies $\mathfrak{s}(b\gamma) \preceq \mathfrak{s}(\alpha - ca\beta)$ and $\mathrm{LT}(\overline{b\gamma}) = \mathrm{LT}(\overline{\alpha - ca\beta})$. Since $\mathrm{LT}(\overline{\alpha - ca\beta}) \simeq \mathrm{LT}(\overline{\alpha})$, we have that γ regularly top $\mathfrak{s}$-reduce α. This contradicts that α is completely regularly top $\mathfrak{s}$-reduced. ∎

Lemma 4
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfies

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α is completely regularly top $\mathfrak{s}$-reduced by G,

(3) α is singular top $\mathfrak{s}$-reducible by G.

Then, α is $\mathfrak{s}$-reduced to $0 \in R$ by G.

Proof Let $\beta \in G$ be a reducer which singularly top $\mathfrak{s}$-reduces α. From Lemma 3, there exists $a \in R$ that satisfies $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{a\beta})$ and $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$. Then, we have that $\mathfrak{s}(\alpha - a\beta) \prec \mathfrak{s}(\alpha)$, so $\alpha - a\beta$ is $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

Let us prove **(A)** mentioned in the second paragraph of this section.

Proposition 5
At the end of Step 3 in **fundSB**, *G is a signature Gröbner basis in α at the every loop.*

Proof Let α be the term chosen in the latest Step 1. Let α' be the result of completely regularly top $\mathfrak{s}$-reducing α. Let G be a signature Gröbner basis up to α. We prove that G is a signature Gröbner basis in α after the end of Step 3, that is, all $\beta \in R^m$ with $\mathfrak{s}(\beta) \preceq \alpha$ are $\mathfrak{s}$-reduced to $0 \in R$ by G.

Since G is a signature Gröbner basis up to α, then $\beta \in R^m$ with $\mathfrak{s}(\beta) \prec \alpha$ is $\mathfrak{s}$-reduced to $0 \in R$ by G. Then, let β satisfy $\mathfrak{s}(\beta) \simeq \alpha$. As we $\mathfrak{s}$-reduce β by G step by step, suppose β would be changed as follows: $\beta \to \beta^{(1)} \to \beta^{(2)} \to \cdots \to \beta^{(i)} \to \cdots$. Assume an $\mathfrak{s}$-reduction such that $\mathfrak{s}(\beta^{(i)}) = \mathfrak{s}(a\gamma)$ $(a \in R, \gamma \in G)$ occurs for a certain i. Since $\mathfrak{s}(\beta^{(i+1)}) \prec \alpha$ for the i, in this case, β is $\mathfrak{s}$-reduced to $0 \in R$. Suppose that such an $\mathfrak{s}$-reduction does not occur. Let β' be the result of completely $\mathfrak{s}$-reducing β. Note that $\mathfrak{s}(\beta') \simeq \alpha$ and β' is completely regularly top $\mathfrak{s}$-reduced. From Lemmas 2 and 3, there exists $c \in K$ such that $\mathfrak{s}(\alpha') = c\mathfrak{s}(\beta')$ and $\mathrm{LT}(\overline{\alpha'}) = c\,\mathrm{LT}(\overline{\beta'})$.

We consider the result of $\mathfrak{s}$-reducing β in the following three cases according to how α' was handled in Step 3.

(i) If $\overline{\alpha'} = 0$, then β' as well as α' is $\mathfrak{s}$-reduced to $0 \in R$ by Lemma 2.

(ii) If $\overline{\alpha'} \neq 0$ and α' is singularly top $\mathfrak{s}$-reducible, then β' as well as α' is singularly top $\mathfrak{s}$-reducible. By Lemma 4, we have that β' is $\mathfrak{s}$-reduced to $0 \in R$.

(iii) If $\overline{\alpha'} \neq 0$ and α' is not singularly top $\mathfrak{s}$-reducible, then β' is singularly top $\mathfrak{s}$-reducible by α' since $\mathfrak{s}(\alpha') = c\mathfrak{s}(\beta')$ and $\mathrm{LT}(\overline{\alpha'}) = c\,\mathrm{LT}(\overline{\beta'})$, and α' is included in G. By Lemma 4, β' is $\mathfrak{s}$-reduced to $0 \in R$.

From the above, we have proved that all $\beta \in R^m$ with $\mathfrak{s}(\beta) \preceq \alpha$ are $\mathfrak{s}$-reduced to $0 \in R$ by G. Thus, G is a signature Gröbner basis in α at the end of Step 3. ∎

The set G computed in **fundSB** is minimal.

Lemma 6
Let $T \in R^m$ be a term chosen at Step 1 in **fundSB**. *Let G in* **fundSB** *be the set after Step3 of T. Then, G is a minimal signature Gröbner basis in T.*

Proof By Proposition 5, G is a signature Gröbner basis in T. Let α be an element in G. For $\beta \in G$ with $\mathfrak{s}(\beta) \prec \mathfrak{s}(\alpha)$, clearly β is not top $\mathfrak{s}$-reducible by α. For $\beta \in G$ with $\mathfrak{s}(\beta) \succeq \mathfrak{s}(\alpha)$, β is not regularly top $\mathfrak{s}$-reducible by α because of Step 2. Moreover, β is not singularly top $\mathfrak{s}$-reducible by α because of Step 3 (ii) (b). Then, β is not top $\mathfrak{s}$-reducible by α. Thus, there is no element in G which top $\mathfrak{s}$-reduces any other elements in G. Therefore, G is a minimal signature Gröbner basis in T. ∎

4 Simple signature-based algorithm

In this section, we introduce simple signature-based algorithm (**simpleSB**), and show that it terminates and outputs a signature Gröbner basis. Before introducing the algorithm, we define an S-pair, which is an analogy of S-polynomial. The *S-pair* of $\alpha, \beta \in R^m$ is defined to be

$$\mathrm{spair}(\alpha,\beta) = \frac{\lambda}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{\lambda}{\mathrm{LT}(\overline{\beta})}\beta,$$

where λ is the least common multiple (of monomials) as $\lambda = \mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))$. If

$$\mathfrak{s}\left(\frac{\lambda}{\mathrm{LT}(\overline{\alpha})}\alpha\right) \simeq \mathfrak{s}\left(\frac{\lambda}{\mathrm{LT}(\overline{\beta})}\beta\right),$$

we say that the S-pair is *singular*, otherwise, we say that the S-pair *regular*. **Algorithm 2** is the pseudocode of **simpleSB**. Note that **simpleSB** outputs a minimal signature Gröbner basis by Lemma 6.

Algorithm 2 Simple signature-based algorithm (**simpleSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 3 (i) If $\overline{\alpha'} = 0$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha', \beta) \text{ is regular}\}$ (#)
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

Remark : In Step 2 of Algorithm 2, we execute only regularly "top" $\mathfrak{s}$-reduction depending on the description of the algorithm. However, we can execute regularly "tail" $\mathfrak{s}$-reduction, and the correctness and the termination of the algorithm are not affected by the modification. In terms of (#) in **simpleSB**, it is sufficient to leave only one term α among terms which are equivalent to α in P. Even if more than two equivalent terms are left in P, **simpleSB** terminates and outputs a signature Gröbner basis.

Let us give an outline of the proofs of the correctness and the termination. The difference between **fundSB** and **simpleSB** is that **simpleSB** computes terms in R^m that appear in Step 3 (ii) (b). In Proposition 12, we prove that G is a signature Gröbner basis in α when Step 3 for α is finished. It follows from Lemma 11 that it is not necessary to compute terms $\preceq \alpha$ that do not appear at (#). The termination of **simpleSB** is proved by Proposition 13. When the algorithm terminates, G is a signature Gröbner basis, by Lemma 11 and Propositions 14 and 12.

Lemmas 7, 8, 9 and 10 are used for proving Lemma 11.

Lemma 7
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in G$ and let a be a monomial in R satisfy

(1) $\mathfrak{s}(a\alpha) \preceq T$,

(2) $a\alpha$ *is regularly top* $\mathfrak{s}$*-reducible by* G.

Then, there exists an S-pair $a'\alpha - b\beta$ (a' and b are monomials in R, β is in G) such that

(3) $\mathfrak{s}(a'\alpha - b\beta) = \mathfrak{s}(a'\alpha)$,

(4) $a' \mid a$.

Proof Let a' be the minimal monomial in the set consisting of the monomials $r \in R$ satisfying that $r \mid a$ and $r\alpha$ is regularly top $\mathfrak{s}$-reducible. Since $a'\alpha$ is regularly top $\mathfrak{s}$-reducible, there exists a pair $(\beta, b) \in G \times R$ such that $\mathfrak{s}(a'\alpha) \succ \mathfrak{s}(b\beta)$ and $\mathrm{LT}(\overline{a'\alpha}) = \mathrm{LT}(\overline{b\beta})$. Let $d = a' \mathrm{LT}(\overline{\alpha}) = b \mathrm{LT}(\overline{\beta})$. Assume that $\mathrm{GCD}(a', b) = m$ with $m \neq 1$. Then, a' and b are written as $a' = ma''$ and $b = mb'$ such that $\mathrm{GCD}(a'', b') = 1$. For $a''\alpha$ and $b'\beta$, note that $\mathfrak{s}(a'\alpha) \succ \mathfrak{s}(b\beta)$ leads to $\mathfrak{s}(a''\alpha) \succ \mathfrak{s}(b'\beta)$ and $a' \mathrm{LT}(\overline{\alpha}) = b \mathrm{LT}(\overline{\beta})$ leads to $a'' \mathrm{LT}(\overline{\alpha}) = b' \mathrm{LT}(\overline{\beta})$. This means that $a''\alpha$ is regularly top $\mathfrak{s}$-reducible and $a'' < a'$. This contradicts the minimality of a'. Therefore, $m = 1$ and $\mathrm{GCD}(a', b) = 1$. There exists $e \in K^\times$ such that $d = e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))$. Then, we have

$$a'\alpha - b\beta = \frac{d}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{d}{\mathrm{LT}(\overline{\beta})}\beta = \frac{e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))}{\mathrm{LT}(\overline{\beta})}\beta.$$

This is an S-pair satisfying (3) and (4). ∎

Lemma 8
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, any pair $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$ satisfies $\mathrm{LT}(\overline{\alpha}) \leq \mathrm{LT}(\overline{a\beta})$.

Proof Assume that there exists a pair $(\beta, a) \in G \times R$ such that $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$ and $\mathrm{LT}(\overline{\alpha}) > \mathrm{LT}(\overline{a\beta})$. Let γ be the result of completely regularly top $\mathfrak{s}$-reducing $a\beta$. Then, we have $\mathrm{LT}(\overline{\alpha}) > \mathrm{LT}(\overline{a\beta}) \geq \mathrm{LT}(\overline{\gamma})$ and $\mathfrak{s}(\alpha) = \mathfrak{s}(\gamma)$. This contradicts Lemma 2. ∎

Lemma 9
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in G$ and let a be a monomial in R satisfy

(1) $\mathfrak{s}(a\alpha) \preceq T$,

(2) $a\alpha$ *is completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, there do not exists a pair $(\beta, b) \in G \times R$ such that

(3) $\mathfrak{s}(a\alpha - b\beta) = \mathfrak{s}(a\alpha)$,

(4) $a\alpha - b\beta$ *is a regular S-pair.*

Proof We prove the contraposition. Assume that there exists a pair $(\beta, b) \in G \times R$ satisfying (3) and (4). This means that $\mathfrak{s}(a\alpha) \succ \mathfrak{s}(b\beta)$ and $\mathrm{LT}(\overline{a\alpha}) = \mathrm{LT}(\overline{b\beta})$. Then, $a\alpha$ is regularly top $\mathfrak{s}$-reducible by $b\beta$. ∎

Lemma 10
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regular top* $\mathfrak{s}$*-reduced,*

(3) $\mathfrak{s}(\beta) \simeq \mathfrak{s}(\alpha)$,

(4) $\mathrm{LT}(\overline{\beta}) > \mathrm{LT}(\overline{\alpha})$.

Then, β is regularly top $\mathfrak{s}$-reducible.

Proof Assume that β is not regularly top $\mathfrak{s}$-reducible, that is, β is completely regularly top $\mathfrak{s}$-reduced by G. From Lemma 2, we have $\mathrm{LT}(\overline{\beta}) = \mathrm{LT}(\overline{\alpha})$. This contradicts $\mathrm{LT}(\overline{\beta}) > \mathrm{LT}(\overline{\alpha})$. ∎

Lemma 11 means that we do not need to compute terms that do not appear as signatures of regular S-pairs.

Lemma 11
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfies

(1) $\mathfrak{s}(\alpha) \simeq T$,

(2) $\mathfrak{s}(\alpha)$ *is equivalent to a signature of a regular S-pair that does not appear in Step 3 (ii) (b).*

Let α' be the result of completely regularly top $\mathfrak{s}$-reducing α by G. Then, α' is singularly top $\mathfrak{s}$-reducible by G. In particular, G is a signature Gröbner basis in T.

Proof Let $\beta \in G$ and let a be a monomial in R satisfying $\mathfrak{s}(a\beta) = \mathfrak{s}(\alpha')$ such that $\mathrm{LT}(\overline{a\beta})$ is minimal. We prove that $\mathrm{LT}(\overline{a\beta}) \simeq \mathrm{LT}(\overline{\alpha'})$. By Lemma 8, we have $\mathrm{LT}(\overline{\alpha'}) \leq \mathrm{LT}(\overline{a\beta})$.

Assume that $\mathrm{LT}(\overline{\alpha'}) < \mathrm{LT}(\overline{a\beta})$. By Lemma 10, $a\beta$ is regularly top $\mathfrak{s}$-reducible. Consider $a'\beta$ such that a' is a monomial in R and the monomial $a/a' \in R \setminus K$. Assume that $a'\beta$ is regularly top $\mathfrak{s}$-reducible by G. And let γ be the result of regularly top $\mathfrak{s}$-reducing $a'\beta$. Then, we have $\mathrm{LT}(\overline{a'\beta}) > \mathrm{LT}(\overline{\gamma})$. As $a' < a$, we have $\mathfrak{s}(\gamma) = \mathfrak{s}(a'\beta) \prec \mathfrak{s}(a\beta) \simeq T$. This means that γ is top $\mathfrak{s}$-reducible. However, γ is completely regularly $\mathfrak{s}$-reduced, then γ is singularly top $\mathfrak{s}$-reducible. By Lemma 3, there exists a pair $(\omega, r) \in G \times R$ such that $\mathfrak{s}(\gamma) = \mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{\gamma}) = \mathrm{LT}(\overline{r\omega})$. Note that $\mathfrak{s}(a'\beta) = \mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{a'\beta}) > \mathrm{LT}(\overline{r\omega})$. By multiplying the both sides of the two equations by a/a', we have $\mathfrak{s}(a\beta) = a/a'\mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{a\beta}) > a/a'\,\mathrm{LT}(\overline{r\omega})$ and note that $\frac{a}{a'}$ is a term of R. This means that there exists a pair $(\omega, ar/a') \in G \times R$ such that $\mathfrak{s}((ar/a')\omega) = \mathfrak{s}(a\beta)$ and $\mathrm{LT}(\overline{(ar/a')\omega}) < \mathrm{LT}(\overline{a\beta})$. This contradicts the minimality of $\mathrm{LT}(\overline{a\beta})$.

Therefore, $a'\beta$ with $a/a' \in R \setminus K$ is not regularly top $\mathfrak{s}$-reducible. From Lemmas 7 and 9, there exists an S-pair $a\beta - b\omega'$ such that $\mathfrak{s}(a\beta - b\omega') = \mathfrak{s}(a\beta)$ for $b \in R$ and $\omega' \in G$. This means that a regular S-pair whose signature is $\mathfrak{s}(a\beta) = \alpha$ appears in Step 3 (ii) (b) (#). This is a contradiction. Thus, we have $\mathrm{LT}(\overline{\alpha'}) \simeq \mathrm{LT}(\overline{a\beta})$. Then, α' is singularly top $\mathfrak{s}$-reducible by G.

It follows from Lemma 4 that α' is $\mathfrak{s}$-reduced to $0 \in R$ by G. Thus, G is a signature Gröbner basis in T. ∎

Proposition 12
Let T' in R^m be a term chosen at Step 1 in **Algorithm 2**, *and let T be the term chosen just before T'. Assume that G in* **Algorithm 2** *is a signature Gröbner basis in T after Step 3 of the loop starting with $\alpha = T$. Then, G is a signature Gröbner basis in T' after Step 3 of the loop starting with $\alpha = T'$.*

Proof First, we prove that G is a signature Gröbner basis up to T' when T' is chosen in Step 1. Suppose G is not a signature Gröbner basis up to T'. Consider the set of terms $\alpha \in R^m$ with $T \prec \alpha \prec T'$ satisfying that G is not a signature Gröbner basis in α. Let α_0 be the minimal element of the set. Note that any set of terms in R^m has a minimal element. Then, G is a signature Gröbner basis up to α_0. Because α_0 is not selected before T' is selected, an S-pair whose signature is equivalent to α_0 does not appear in the algorithm. By Lemma 11, G is a signature Gröbner basis in α_0. This contradicts that G is not a signature Gröbner basis in α_0. Therefore, G is a signature Gröbner basis up to T'. The operation on G for T' in **Algorithm 2** is exactly same as that in **Algorithm 1**. By Proposition 5, G is a signature Gröbner basis in T' after Step 3 of the loop starting with $\alpha = T'$. ∎

Our proof of termination is similar to the papers Eder-Perry [5], Roune-Stillman [3] and Eder-Roune [6].

Proposition 13 (Termination)
simpleSB *terminates in finite steps.*

Proof We write $R = K[x_1, \ldots, x_k]$. Set

$$R' = K[x_1, \ldots, x_k, y_{11}, \ldots, y_{mk}, z_1, \ldots, z_m].$$

For $\beta \in R^m$, we write $(\mathfrak{s}(\beta), \mathrm{LT}(\overline{\beta})) = (cx_1^{v_1}x_2^{v_2}\cdots x_k^{v_k}\mathbf{e}_i, r)$, where $c \in K$, $v = (v_1, \ldots, v_k) \in \mathbb{Z}_{\geq 0}^k$ and r is a term of R. Let $f : R^m \to R'$ be the map defined by $\beta \mapsto r y_{i1}^{v_1} \cdots y_{ik}^{v_k} z_i$. Let $G(\alpha)$ be the G (in Algorithm 2) obtained when Step 3 is finished for α, where α was chosen in Step 1. Consider the following monomial ideal $I(\alpha) = \langle f(\beta) \mid \beta \in G(\alpha) \rangle$.

Let $\alpha_1, \alpha_2, \ldots$ be the elements chosen in this order in Step 1 of Algorithm 2. Then we have the sequence $G(\alpha_1) \subset G(\alpha_2) \subset \cdots$ and also $I(\alpha_1) \subset I(\alpha_2) \subset \cdots$. Any ascending sequence of ideals in R' is stable since R' is a Noetherian ring. There exists i_0 such that for $i > i_0$ we have $I(\alpha_i) = I(\alpha_{i_0})$.

For $i < j$, we claim that $G(\alpha_i) \subsetneq G(\alpha_j)$ if and only if $I(\alpha_i) \subsetneq I(\alpha_j)$. The "if"-part is obvious. We prove the "only if"-part in the following way. Suppose that $G(\alpha_i) \subsetneq G(\alpha_j)$ and $I(\alpha_i) = I(\alpha_j)$. Let $\beta \in G(\alpha_j) \setminus G(\alpha_i)$. By $f(\beta) \in I(\alpha_j) = I(\alpha_i)$, there exists $\beta' \in G(\alpha_i)$ such that $f(\beta') | f(\beta)$, since $I(\alpha_i)$ is the ideal generated by the monomials $f(\beta'')$ for $\beta'' \in G(\alpha_i)$. If $f(\beta') \mid f(\beta)$, we have $\mathrm{LT}(\overline{\beta'}) \mid \mathrm{LT}(\overline{\beta})$ and $\mathfrak{s}(\beta') \mid \mathfrak{s}(\beta)$, by the definition of f. Hence, there exist elements β and β' of $G(\alpha_j)$ with $\beta \neq \beta'$ such that $\mathrm{LT}(\overline{\beta'}) \mid \mathrm{LT}(\overline{\beta})$ and $\mathfrak{s}(\beta') \mid \mathfrak{s}(\beta)$. This contradicts that **simpleSB** computes a minimal signature Gröbner basis in $\mathfrak{s}(\alpha_j)$.

Thus we have shown that $G(\alpha_i) = G(\alpha_{i_0})$ for $i > i_0$. Hence G in Algorithm 2 does not grow after α_{i_0}, which means that Step 3 (ii) (b) does not occur after α_{i_0} and therefore P does not grow after α_{i_0}. However, in Step 1, the number of elements in P decreases by one in each step. Thus, Algorithm 2 terminates in finite steps. ∎

Proposition 14 (Correctness)
simpleSB *outputs a signature Gröbner basis when* **simpleSB** *terminates.*

Proof Let T be the term in R^m chosen in Step 1, and finally computed before **simpleSB** terminates. By Proposition 12, G is a signature Gröbner basis in T. Suppose G is not a signature Gröbner basis. Consider the set of terms $\alpha \in R^m$ with $T \prec \alpha$ satisfying that G is not a signature Gröbner basis in α. Let α_0 be the minimal element of the set. Then, G is a signature Gröbner basis up to α_0. However, an S-pair whose signature is equivalent to α_0 does not appear in the algorithm because the algorithm terminates at T. By Lemma 11, G is a signature Gröbner basis in α_0. This contradicts that G is not a signature Gröbner basis in α_0. Therefore, G is a signature Gröbner basis. ∎

5 Simple syzygy signature-based algorithm

In this section, one of the methods to detect zero reductions like F5 and GVW is described. By Lemma 2, because of $\overline{f_i \mathbf{e}_j - f_j \mathbf{e}_i} = 0$, elements in R^m whose signatures are $\mathfrak{s}(f_i \mathbf{e}_j - f_j \mathbf{e}_i)$ are completely regularly $\mathfrak{s}$-reduced to $0 \in R$. Moreover, because of $\overline{r(f_i \mathbf{e}_j - f_j \mathbf{e}_i)} = 0$ for all $r \in R \setminus \{0\}$, elements in R^m whose signatures are $\mathfrak{s}(r(f_i \mathbf{e}_j - f_j \mathbf{e}_i))$ are completely regularly $\mathfrak{s}$-reduced to $0 \in R$. In summary, we have :

Proposition 15
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha, \beta, \gamma \in R^m$ satisfy $\mathfrak{s}(\alpha) \preceq T$ and $\mathfrak{s}(\overline{\beta}\gamma - \overline{\gamma}\beta) \mid \mathfrak{s}(\alpha)$. Then, α is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G.

Proof Let r be a monomial in R such that $\mathfrak{s}(\alpha) = \mathfrak{s}(r(\overline{\beta}\gamma - \overline{\gamma}\beta))$. Let α' be the element obtained by completely regularly $\mathfrak{s}$-reducing α. Note that $r(\overline{\beta}\gamma - \overline{\gamma}\beta)$ is the completely regularly $\mathfrak{s}$-reduced element by G because $\overline{r(\overline{\beta}\gamma - \overline{\gamma}\beta)} = 0$. By Lemma 2, we have $\mathrm{LT}(\overline{\alpha'}) = \mathrm{LT}(\overline{r(\overline{\beta}\gamma - \overline{\gamma}\beta)}) = 0$. Then, α is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

The next proposition gives a method to detect zero reductions, namely it gives a sufficient condition for $\beta \in R$ to be completely regularly s-reduced to $0 \in R$ by G, by means of the term α which has been completely regularly $\mathfrak{s}$-reduced to $0 \in R$.

Proposition 16
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) α *is completely regularly* $\mathfrak{s}$*-reduced to* $0 \in R$ *by* G *and*

(2) $\mathfrak{s}(\alpha) \mid \mathfrak{s}(\beta)$.

Then, β *is completely regularly* $\mathfrak{s}$*-reduced to* $0 \in R$ *by* G.

Proof From the assumption, there exists $\gamma \in R^m$ such that $\mathfrak{s}(\alpha - \gamma) = \mathfrak{s}(\alpha)$ and $\overline{\alpha - \gamma} = 0$. Let $r \in R$ satisfy $\mathfrak{s}(\beta) = r\mathfrak{s}(\alpha)$. Then, $\mathfrak{s}(r(\alpha - \gamma)) = \mathfrak{s}(r\alpha) = \mathfrak{s}(\beta)$ and $\overline{r(\alpha - \gamma)} = 0$. By Lemma 2, β is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

Algorithm 3 is simple syzygy signature-based algorithm (**syzSB**). **syzSB** is modified **simpleSB** as to Propositions 15 and 16.

Algorithm 3 Simple syzygy signature-based algorithm (**syzSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}, H \leftarrow \emptyset$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 4 (i) If $\overline{\alpha'} = 0$
$H \leftarrow H \cup \{\alpha\}$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha', \beta) \text{ is regular}\}$ (#)
$H \leftarrow H \cup \{\mathfrak{s}(\overline{\beta}\alpha' - \overline{\alpha'}\beta) \mid \beta \in G\}$
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

Proposition 17 (Correctness)
syzSB *outputs a signature Gröbner basis.*

Proof Let A be the set of the terms which **simpleSB** computes, and let B the set of the terms which are completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. By Propositions 15 and 16, **syzSB** computes the set $A \setminus B$. Then, the output G of **syzSB** is the same as that of **simpleSB**. ∎

Proposition 18 (Termination)
syzSB *terminates in finite loops.*

Proof By Propositions 15 and 16, the set P at each step 1 in **syzSB** is exactly same as that at the corresponding Step 1 in **simpleSB**. Further, **simpleSB** computes finite number of the terms. ∎

6 Alternative rewrite basis algorithm

In this section, alternative rewrite basis algorithm (**altRB**) is introduced. In the paper [6], rewrite basis algorithm (**RB**) is introduced as a generalized signature-based algorithm. **altRB** is represented easily to understand operations of the algorithm and easily to implement it. It is the most useful signature-based algorithm for implementation in this paper. From the discussion so far, singularly top $\mathfrak{s}$-reducible elements which are completely regularly top $\mathfrak{s}$-reduced need not be included in G. We can expect to improve the algorithm by discarding such elements without reduction. In other words, it is enough to regularly $\mathfrak{s}$-reduce the elements which will be an elements of a minimal signature Gröbner basis. Moreover, we can expect to improve the efficiency by replacing the element α for the element whose signature is the same and which is not needed to reduce more times . Among the algorithms proposed so far, the algorithm in paper [1], GVW [13], etc. have used the method. The paper [7] introduced such algorithms as **RB** with RAT selected for rewrite order. When we choose RAT for a rewrite order, rewrite basis algorithm becomes the most efficient. **altRB** is simply introduced and as efficient as **RB** with RAT. **Algorithm 4** is the pseudocode of **altRB**.

Algorithm 4 Alternative rewrite basis algorithm (**altRB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}, H \leftarrow \emptyset$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow \omega \in \{\alpha\} \cup \{r\beta \mid r \in R, \beta \in G, \mathfrak{s}(r\beta) = \alpha\}$ such that $\mathrm{LT}(\overline{\omega})$ is minimal
Step 4 $\alpha'' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α' by G
Step 5 (i) If $\overline{\alpha''} = 0$
Append α to H
(ii) If $\overline{\alpha''} \neq 0$ and (α' is regularly top $\mathfrak{s}$-reduced at least one time or $\mathfrak{s}(\alpha'')$ is a standard basis)
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha'', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha'', \beta) \text{ is regular}\}$ (#)
$H \leftarrow H \cup \{\mathfrak{s}(\overline{\beta}\alpha'' - \overline{\alpha''}\beta) \mid \beta \in G\}$ $(*)$
$G \leftarrow G \cup \{\alpha''\}$
Go to Step 1

Remark : In Step 4, we execute only regularly "top" $\mathfrak{s}$-reduction according to the description of the algorithm. However, we can execute regularly "tail" $\mathfrak{s}$-reduction, and correctness and termination of the algorithm are not affected. For (#), it is sufficient to leave only one term α in P as for the terms $\alpha \simeq \beta$. Although it is not efficient, if more than two terms are left, correctness and termination of the algorithm are not affected.

Lemma 19
Let α' and α'' be obtained at Step 3 and at Step 4 in **Algorithm 4** *respectively. Let G be a signature Gröbner basis up to $\mathfrak{s}(\alpha'')$. The condition at Step 5 (ii) in* **Algorithm 4** *is equivalent to the condition that α'' is not singularly top $\mathfrak{s}$-reducible by G.*

Proof If $\mathfrak{s}(\alpha'')$ is a standard basis of R^m, say $\mathbf{e}_i$, there is no element in G whose signature belongs to $R\mathbf{e}_i$. Thus, α'' is not singularly top $\mathfrak{s}$-reducible by G. If α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{\alpha'})$. For all $b \in R$ and $\beta \in G$ such that $\mathfrak{s}(\alpha'') = \mathfrak{s}(b\beta)$, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{\alpha'}) \leq \mathrm{LT}(\overline{b\beta})$ by the minimality of $\mathrm{LT}(\overline{\alpha'})$ at Step 3. Then, α'' is not singularly top $\mathfrak{s}$-reducible by G.

Conversely, if α'' is not singularly top $\mathfrak{s}$-reducible, we consider the following two cases : **(a)** $\mathfrak{s}(\alpha'')$ is not a standard basis of R^m and **(b)** otherwise. In case **(a)**, we claim that there exists a pair $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha'') = \mathfrak{s}(a\beta)$. Let the signature of α'' be $r\mathbf{e}_i$ ($r \in R \setminus K^\times$). The standard basis of R^m $\mathbf{e}_i$ is chosen at Step 1 before $r\mathbf{e}_i$ is chosen because $\mathbf{e}_i$ is smaller than $r\mathbf{e}_i$. Assume that there does not exist an element of G whose signature is $\mathbf{e}_i$. The element whose signature is $\mathbf{e}_i$ is regularly $\mathfrak{s}$-reduced to $0 \in R$, then we proceed Step 5 (i). In this case, elements whose signatures are $r\mathbf{e}_i$ do not appear in P. This means that we do not compute such an element $r\mathbf{e}_i$. It contradicts that the signature of α'' is $r\mathbf{e}_i$ ($r \in R \setminus K^\times$). Then, there is an element of G whose signature is $\mathbf{e}_i$. Thus, $(r, \mathbf{e}_i)$ is a pair that we claimed. Consider the set of pairs $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha'') = \mathfrak{s}(a\beta)$. Let (β', a') be a pair such that $\mathrm{LT}(\overline{a'\beta'})$ is minimal in the set. Note that $\mathrm{LT}(\overline{a\beta}) = \mathrm{LT}(\overline{\alpha'})$ because of the process at Step 3. By Lemma 8, we have $\mathrm{LT}(\overline{\alpha''}) \leq \mathrm{LT}(\overline{a\beta})$. If $\mathrm{LT}(\overline{\alpha''}) = \mathrm{LT}(\overline{a\beta})$, α'' is singularly top $\mathfrak{s}$-reducible. This contradicts that α'' is not singularly top $\mathfrak{s}$-reducible. Then, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{a\beta}) = \mathrm{LT}(\overline{\alpha'})$. This means that α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4. In case **(b)**, there is nothing to prove. ∎

Theorem 20 (Correctness)
altRB *outputs a signature Gröbner basis.*

Proof We prove by confirming the difference between the algorithm and the **syzSB**. At Step 3, by Lemma 2, as long as the signature is the same, we can choose any elements in R^m. Thus, we can choose the element with the smaller leading term.

At Step 5, **altRB** does not have branch whether α'' is singularly top $\mathfrak{s}$-reducible or not. Instead of the above, **altRB** check whether α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4 and check whether $\mathfrak{s}(\alpha'')$ is a standard basis of R^m. By Lemma 19, they are equivalent. ∎

Theorem 21 (Termination)
altRB *terminates in finite steps.*

Proof The set P at every step 1 in **altRB** is exactly same as that at the corresponding Step 1 in **syzSB**. Further, **syzSB** computes finite number of the terms. ∎

7 Module orders and zero reductions

In the paper [7], **RB** does not contain the line $(*)$ of **Algorithm 4**. This is because **RB** is introduced as a generalized signature-based algorithm. If we implement as so, we have to be careful for the number of zero reductions during the calculation. In case we choose POT as a module order and compute incrementally, like **Algorithm 4**, the number of zero reductions becomes small. Especially, if the polynomial systems are regular sequences, the number of zero reductions is zero. In case we choose a module order other than POT or a module order not to be suitable for incremental computation, the number of zero reductions increases during calculation.

It can be proved that the update of H is sufficient to be done first as in **Algorithm 5** in case POT is chosen as the module order and it is calculated incrementally,

Algorithm 5 Alternative rewrite basis algorithm (incremental)

Input : a Gröbner basis $F = \{f_1, \ldots, f_{m-1}\} \subset R$, a polynomial $f_m \in R$.
Output: a minimal signature Gröbner basis G of $F \cup \{f_m\}$.

Step 0 $G \leftarrow \{f_1, \ldots, f_{m-1}\}, P \leftarrow \{\mathbf{e}_m\}, H \leftarrow \{\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m - \overline{\mathbf{e}_m}\mathbf{e}_i) \mid 1 \leq i \leq m-1\}$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow \omega \in \{\alpha\} \cup \{r\beta \mid r \in R, \beta \in G, \mathfrak{s}(r\beta) = \alpha\}$ such that $\mathrm{LT}(\overline{\omega})$ is minimal
Step 4 $\alpha'' \leftarrow$result of completely regularly top $\mathfrak{s}$-reducing α' by G
Step 5 (i) If $\overline{\alpha''} = 0$
Append α to H
(ii) If $\overline{\alpha''} \neq 0$ and (α' is regularly top $\mathfrak{s}$-reduced at least one time or $\mathfrak{s}(\alpha'')$ is a standard basis)
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha'', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha'', \beta) \text{ is regular}\}$ (#)
$G \leftarrow G \cup \{\alpha''\}$
Go to Step 1

Lemma 22
Let α'' be a new element at Step 5 (ii) in **Algorithm 5** *with POT such that $\mathbf{e}_1 \prec \mathbf{e}_2 \prec \cdots \prec \mathbf{e}_m$. For all $\beta \in G$, there exists $\gamma \in H$ such that $\gamma \mid \mathfrak{s}(\overline{\alpha''}\beta - \overline{\beta}\alpha'')$.*

Proof First, we prove $H = \{r\mathbf{e}_m \mid r \in \mathrm{HT}(F)\}$. We have $\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m - \overline{\mathbf{e}_m}\mathbf{e}_i) = \mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m)$ because the module order is POT. Then, we have $\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m) = \mathfrak{s}(f_i\mathbf{e}_m) = \mathfrak{s}(\mathrm{HT}(f_i)\mathbf{e}_m) = \mathrm{HT}(f_i)\mathbf{e}_m$.

Let α'' and $\beta \in G$ be written as $\alpha'' = \sum_{i=1}^{m} r_i\mathbf{e}_i$ and $\beta = \sum_{j=1}^{m} r'_j\mathbf{e}_j$, for $r_i, r'_i \in R$. Then, we have $\overline{\alpha''} = \sum_{i=1}^{m} r_i f_i \equiv h_m f_m \pmod{F}$.

$$\begin{aligned}\overline{\alpha''}\beta - \overline{\beta}\alpha'' &= \left(\sum_{i=1}^{m} r_i f_i\right) \cdot \left(\sum_{j=1}^{m} r'_j\mathbf{e}_j\right) - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot \left(\sum_{i=1}^{m} r_i\mathbf{e}_i\right) \\ &= \left\{\left(\sum_{i=1}^{m} r_i f_i\right) \cdot r'_m - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot r_m\right\}\mathbf{e}_m + \cdots\end{aligned}$$

We focus on polynomial part of $\mathbf{e}_m$.

$$\begin{aligned}\left(\sum_{i=1}^{m} r_i f_i\right) \cdot r'_m - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot r_m &\equiv r_m f_m r'_m - r'_m f_m r_m \pmod{F} \\ &\equiv 0 \pmod{F}\end{aligned}$$

Therefore, there exists an element in H which divides $\mathfrak{s}(\overline{\alpha''}\beta - \overline{\beta}\alpha'')$. ∎

8 Conclusion

We have presented some signature-based (semi-)algorithms for computing Gröbner bases: **fundSB**, **simpleSB**, **syzSB** and **altRB**. Among them, **altRB** is a practical signature-based algorithm and can

be implemented easily in any computer algebra system, as **altRB** is described concretely. The other (semi-)algorithms are used auxiliarily to prove the correctness and the termination of **altRB**. The characteristics of the (semi-)algorithms are as follows:

1. **fundSB** is a prototype of signature-based algorithms, and helps us grasp the idea and how signature-based algorithms work. However, it does not terminate.
2. **simpleSB** is obtained by modifying **fundSB** with the concept of S-pairs so that it terminates. It outputs a signature Gröbner basis with a finite number of operations.
3. **syzSB** is obtained by including a step detecting zero reductions into **simpleSB**. The step is assured by Propositions 15 and 16.
4. **altRB** is obtained by inserting in **syzSB** a step replacing the term by an element which has a smaller leading term. This enables us to reduce the number of regular $\mathfrak{s}$-reductions significantly.

By discussing the correctness and the termination of these (semi-)algorithms step by step, we have finally obtained the correctness and the termination of **altRB**. The proofs are self-contained and very clear. **altRB** is efficient for an arbitrary module order. In the last section, we have discussed how signature-based algorithms work when POT is chosen as a module order and when it proceeds incrementally.

As a future work, it would be meaningful to study the relation between input systems and module orders we choose, toward finding an efficient module order for a given input system.

Acknowledgement

This paper is a part of the dissertation written by the author under the supervision by Prof. Shushi Harashita. The author thanks him for his constant supports. The author thanks Prof. Kazuhiro Yokoyama and Prof. Masayuki Noro for discussions on the topic of this manuscript. The author is grateful to the anonymous referees for their helpful and kind comments. A part of this work has been supported by Joint research promotion program of Graduate School of Environment and Information Sciences, Yokohama National University.

References

[1] Arri, A., Perry, J.: The F5 criterion revised.: *Journal of Symbolic Computation*, **46**, 1017–1029, 2011.

[2] Buchberger, B.: Bruno Buchberger's Ph.D. thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal.: *Journal of Symbolic Computation*, **41**, 475–511, 2006. https://doi.org/10.1016/j.jsc.2005.09.007

[3] Roune, B.H., Stillman, M.: Practical Gröbner basis computation.: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation , 203–210, ACM, New York, 2012. https://arxiv.org/abs/1206.6940 (extended version)

[4] Eder, C., Perry, J.: F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases.: *Journal of Symbolic Computation*, **45**, no. 12, 1442–1458, 2010.

[5] Eder, C., Perry, J.: Modifying Faugère's F5 algorithm to ensure termination.: *ACM SIGSAM Commun. Comput. Algebra*, **45**, 70–89, 2011.

[6] Eder, C., Roune, B.H.: Signature rewriting in Gröbner basis computation.: Proceedings of the 2013 International Symposium on Symbolic and Algebraic Computation, 331–338, 2013.

[7] Eder, C., Faugère, J.-C.: A survey on signature-based algorithms for computing Gröbner bases.: *Journal of Symbolic Computation*, **80**, part 3, 719–784, 2017.

[8] Ars, G., Hashemi, A.: Extended F5 criteria.: *Journal of Symbolic Computation*, **45** (12) , 1330–1340, 2010.

[9] Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 75–83, ACM, New York, 2002.

[10] Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases.: CRYPTO 2003, Advances in Cryptology, vol. 2729, 44–60, 2003.

[11] Pan, S., Hu, Y., Wang, B.: The termination of algorithms for computing Gröbner bases.: 2010. http://arxiv.org/abs/1202.3524

[12] Galkin, V.: Termination of original F5.: 2012. http://arxiv.org/abs/1203.2402

[13] Gao, S., Volny, F. IV, Wang, M.: A new framework for computing Gröbner bases.: *Mathematics of Computation*, **85**, 449–465, 2016. https://doi.org/10.1090/mcom/2969

[14] Vaccon, T., Yokoyama, K.: A tropical F5 algorithm.: Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation, 429–436, ACM, 2017.

[15] Vaccon, T., Verron, T., Yokoyama, K.: On Affine Tropical F5 Algorithms.: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 383–390, ACM, 2018.