Doctoral Dissertation

Efficient signature-based algorithms for computing Gröbner bases

Signatureを用いたGröbner基底を求める効率的なアルゴリズムについて

Kosuke Sakata

Graduate School of Environmental and Information Science,

Yokohama National University

Supervisor: Associate professor Shushi Harashita

March 2021

Abstract

Gröbner bases is a field of algebra, and Buchberger proposed a Gröbner basis and an algorithm to find it in 1964 [3]. When there is an ideal on a polynomial ring, the Gröbner basis is always found and has special characteristics. Due to its characteristics, Gröbner bases have a wide range of applications and is used in many topics of mathematics and engineering. After Buchberger proposed the algorithm, many improvements and speed-up methods were proposed. F4 algorithm proposed by Faugère in 1999 [15] is known to be fast and is implemented in many algebraic computing software. In calculating a Gröbner basis, unnecessary calculations called zero reductions occur. Zero reductions are not only calculations for which information about a Gröbner basis cannot be obtained, but also calculations that generally require a large amount of calculations. Several methods have been proposed to reduce the number of zero reductions by detecting zero reductions that appear in the middle of the calculations and omitting them. The major improvement of algorithms for finding Gröbner basis is F5 algorithm proposed by Faugère in 2001 [16]. While the improvements and speed-up methods proposed so far have been based on the Buchberger algorithm, F5 has different processes and we require additional (or different) arguments to prove the termination and the correctness of F5 algorithm. It is known that the theory is difficult and implementations for efficient calculations are difficult. However, when the set of input polynomials is a regular sequence, F5 can be calculated without zero reductions. If we have less zero reductions that occur during the calculations, the amount of calculations is small, so efficient and fast calculations are possible. After that, F5 was generalized as a signature-based algorithm, and efficient calculation methods, and the proofs of the termination and the correctness were modified. One of them is rewrite basis algorithm, which is a generalization of the previous signature-based algorithm by Eder and Roune [12]. The algorithm is a compilation of many signature-based algorithms proposed so far. This paper introduces an improved version of Rewrite basis algorithm, which we call alternative rewrite basis algorithm. Unlike Buchberger algorithm, signature-based algorithms require a module order to be

selected in addition to a monomial order, and when an arbitrary module order is chosen, alternative rewrite basis algorithm detects and omits extra zero reductions that occur in rewrite basis algorithm. Alternative rewrite basis algorithm is concretely designed and is provided in a form that is easy to be implemented. Thanks to that, the proofs of the termination and the correctness are simpler, and written in more detail. In addition, this paper proposes a method for efficient calculations for signature-based algorithms. Gröbner bases algorithms have procedures for reducing polynomials, and this procedures occupy most of the computational complexity of the algorithm. There are two conventional strategies to reduce polynomials for signature-based algorithms. One is the only-top reduction strategy that reduces only the leading terms. The other is the full reduction strategy that reduces every term which can be reduced. In this paper, we propose a strategy for reducing polynomials, called the selective-full reduction strategy. In the proposed strategy, we reduce the leading terms and then, when the condition is satisfied, we reduce the terms of entire polynomial. When the condition is not satisfied, we stop reducing terms. The conventional two strategies and the proposed strategy were evaluated using Gröbner bases benchmark problem. As a result, it was found that the selective-full reduction strategy can be calculated more efficiently than the conventional two strategies for finding the reduced Gröbner basis. In addition, the selective-full reduction strategy is a valid strategy because it does not give the worst result among the three strategies when finding the Gröbner basis.

Acknowledgments

This dissertation is 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. A part of this work has been supported by Joint research promotion program of Graduate School of Environment and Information Sciences, Yokohama National University.

Contents

List of Tables

Chapter 1

Introduction

1.1 Background and Motivation

Gröbner bases is one of important research topics in algebra. In 1964, Buchberger [3] introduced Gröbner basis and proposed a basic algorithm for finding a Gröbner basis. The algorithm is called Buchberger algorithm. If an ideal on a polynomial ring and an monomial order is given, a Gröbner basis for the the ideal is found. The Gröbner basis shows the characteristics of the ideal, and is a useful set. Therefore, there are many propositions and it is widely used for applications. One of well-known applications is the elimination theory [6]. When we solve a multivariate polynomial equation, finding a Gröbner basis for the lexicographical order is helpful, because we obtain a Gröbner basis of the ideal generated by polynomials with some variables restricted. As other applications of Gröbner bases, we have cryptography, 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 require to deal with polynomial systems including parameters. In that case, a comprehensive Gröbner system, which treats parametrized polynomial systems, is possible to solve the problem. A comprehensive Gröbner system is obtained by computing Gröbner bases multiple time. Thus, Gröbner bases has a wide range of applications, and a lot of research related to the applications would progress by improving algorithms computing a Gröbner basis. Avoiding zero reduction operations leads to more efficient algorithms because the number of reductions related to reducing polynomials to zero is tend to be

larger than that of reductions of polynomials which are not reduced to zero. Moreover, the calculations of zero reduction operations do not give any information of a Gröbner basis. Therefore, in order to decrease amount of calculations, it is important to study algorithms detecting polynomials which are reduced to zero.

1.2 Earlier research

A first signature-based algorithm, called F5, was proposed by Faugère in 2002 [16]. By using F5, we can detect and discard many polynomials which will be reduced to zero. Moreover, a zero reduction does not happen when the input polynomials are regular sequence. Therefore, F5 is recognized as an efficient algorithm for computing Gröbner bases. The proofs of the termination and the correctness of F5 are in the paper [16]. However, the descriptions of F5 and the proofs are complicated, and the proof of the termination is not sufficient.

After F5 was proposed, many propositions related to F5 were submitted. In the Stegers's dissertation [26], an efficient computation method for F5 was proposed. The method used the characteristic that the calculation of F5 proceeds incrementally. Let $F = \{f_1, f_2, \ldots, f_m\} \subset R$ be a polynomial system. At first, we compute a Gröbner basis of the ideal $\langle f_1 \rangle$. Second, we compute a Gröbner basis of the ideal $\langle f_1, f_2 \rangle$. Next, we compute a Gröbner basis of $\langle f_1, f_2, f_3 \rangle$. After a series of computations in order, we finish to compute a Gröbner basis of $\langle F \rangle$. That is the process of F5. Stegers proposed the process to find reduced Gröbner basis $\langle f_1, \ldots, f_l \rangle$ for $l < m$ after the computation of a Gröbner basis of $\langle f_1, \ldots, f_l \rangle$. In the next phase about $\langle f_1, \ldots, f_l, f_{l+1} \rangle$, we use the reduced Gröbner basis of $\langle f_1, \ldots, f_l \rangle$ for reducing polynomials. By this method, the number of reductions are suppressed in the calculation. In 2010, Eder and Perry proposed further improvement from the above method, named F5C [8]. In Steger's method, the reduced Gröbner basis is used for only reductions. In F5C, the reduced Gröbner basis is used for reductions and generating S-pairs. F5C can decrease the more number of reductions. Ars and Hashemi proposed the selectivity of a module order in F5 [14]. Original F5 and the algorithms related F5 use the same module order called POT order. In the paper [14], F5 with a module order other than POT was described, and the result

of the computations by several module orders are shown. In original F5, zero reductions which can be detected are only syzygies generated by trivial syzigies $f_i f_j - f_j f_i$. By Arri and Perry [1] as well as Gao, Guan and Volny [21], the method to detect zero reductions by zero reductions calculated before was proposed. The method is useful even when a module order other than POT is chosen. The paper [13] 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**) [12]. The algorithm in [1] called Arri and the algorithm in [22] 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 become the most efficient. The proofs of correctness and termination in [13] 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.

1.3 Structure of this thesis

In Chapter 2, we review notations and basic notions of a polynomial rings, Gröbner bases and modules. In Chapter 3, we introduce alternative rewrite basis algorithm (**altRB**). The algorithm is efficient for an arbitrary module order other than POT, and moreover it is concrete to be implemented. We prove the correctness (Theorem 56) and the termination (Theorem 57) 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. We take up some signature-based (semi-)algorithms for computing Gröbner bases: **fundSB**, **simpleSB**, **syzSB** and **altRB**. In each step, we discuss the correctness and the termination of an algorithm. 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**. In Chapter 4, we introduce an efficient strategy for signature-based algorithms. The idea of the strategy we proposed is following: when we have computed a signature Gröbner basis, there are unnecessary

elements for a minimal Gröbner basis, so candidates of elements needed for a minimal Gröbner basis should be sufficiently reduced, that means full $\mathfrak{s}$-reduced. Overview of the strategy is following: after generating an S-pair, we operate only-top reduction. If the S-pair meets a certain condition (**SF** in §4), we operate full reduction. We name the strategy *selective-full reduction strategy* (**Algorithm 5**). The efficiency of the strategy was evaluated by some Gröbner basis benchmarks which is commonly used. The selective-full strategy operates fewer times of reduction for computing the reduced Gröbner basis.

Chapter 2

Notations and algorithms of Gröbner bases

2.1 Fields and Rings

Gröbner bases is one of topics of algebra. In this paper, we consider a commutative polynomial ring.

Definition 1. A *commutative ring* consists of a set R and two binary operations "+" and "$\cdot$" defined on R that satisfy the following conditions: for all $a, b, c \in R$

(i) $(a + b) + c = a + (b + c)$.

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) $a + b = b + a$.

(iv) $a \cdot b = b \cdot a$.

(v) $a \cdot (b + c) = a \cdot b + a \cdot c$.

(vi) There exists $0, 1 \in R$ such that $a + 0 = a \cdot 1 = a$.

(vii) Given $a \in R$, there exists $b \in R$ such that $a + b = 0$.

A commutative ring is defined over a certain field.

Definition 2. A *field* consists of a set K and two binary operations "$+$" and "$\cdot$" defined on K and following conditions are satisfied: for all $a, b, c \in K$

(i) $(a + b) + c = a + (b + c)$.

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) $a + b = b + a$.

(iv) $a \cdot b = b \cdot a$.

(v) $a \cdot (b + c) = a \cdot b + a \cdot c$.

(vi) There exists $0, 1 \in K$ such that $a + 0 = a \cdot 1 = a$.

(vii) Given $a \in K$, there exists $b \in K$ such that $a + b = 0$.

(viii) Given $a \in K$, $a \neq 0$, there exists $c \in K$ such that $a \cdot c = 1$.

Note that any field is clearly a commutative ring. An ideal is a subset of a ring. A Gröbner basis, a theme of this thesis, is defined for an ideal.

Definition 3. Let R be a commutative ring. A subset $I \subset R$ is an *ideal* if the following conditions satisfies:

(i) $0 \in I$.

(ii) If $a, b \in I$, then $a + b \in I$.

(iii) If $a \in I$ and $b \in R$, then $b \cdot a \in I$.

We now define polynomials. We start by defining monomials. We consider polynomials with n variables and coefficients over K.

Definition 4. A *monomial* of $x_1, x_2, \ldots, x_n$ is the product of the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ in which all exponents $a_1, a_2, \ldots, a_n$ are non-negative integers. The total degree of this monomial is $|a| = a_1 + \cdots + a_n$ in total.

A polynomial is consisted by sum of monomials.

Definition 5. A *polynomial* f in $x_1, \ldots, x_n$ with coefficients in a field K is a finite linear combination of monomials. We write a polynomial f of the form $f = \sum_a c_a x^a$ which is a finite sum with $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ for $a = (a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^n$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in K is denoted by $K[x_1, \ldots, x_n]$.

Let K be a field. The set $K[x_1, \ldots, x_n]$ satisfies the conditions of Definition 2. Therefore, $K[x_1, \ldots, x_n]$ is a commutative ring. Consider $a, b \in K[x_1, \ldots, x_n]$. If a is divisible by b, we write $a \mid b$.

We use the following notations for dealing with polynomials.

Definition 6. Let $f = \sum_a c_a x^a$ be a polynomial in $K[x_1, \ldots, x_n]$.

(i) We call c_a the *coefficient* of the monomial x^a.

(ii) We call $c_a x^a$ a *term* of f.

(iii) The *total degree* of f, denoted $deg(f)$, is the maximum $|a| = a_1 + a_2 + \cdots + a_n$ such that the coefficient of $c_a x^a$ is nonzero. The total degree of the zero polynomial is not defined.

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring. Let $f_1, \ldots, f_m$ be elements of R. The elements $f_1, \ldots, f_m$ generate an ideal.

Lemma 7. *Let $f_1, \ldots, f_m$ be polynomials in R. Then, the following set*

$$\langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} h_i f_i \mid h_1, \ldots, h_m \in R \right\}$$

is an ideal.

2.2 Monomial Order

Let f be a certain polynomial over a polynomial ring R which includes more than two variables. There are many ways to write f, namely there are many ways to arrange the monomials of f. Certainly, the monomial which is written at the first is not canonically determined. Hence, we need to consider a monomial ordering, for Gröbner basis computation. Especially, the first term written in f, called the leading term, is determined after we fix a monomial ordering, and it plays an important role for the definitions and calculations of Gröbner bases.

Definition 8. A *monomial ordering* $>$ on $K[x_1, \ldots, x_n]$ is a relation on $\mathbb{Z}^n_{\geq 0}$ on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

(i) $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.

(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

Here is an example of an important monomial order for a Gröbner basis. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{Z}^n_{\geq 0}$. We say $x^\alpha >_{lex} x^\beta$ is *lexicographic ordering* if the leftmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive. We say $x^\alpha >_{grevlex} x^\beta$ is *graded reverse lexicographic ordering* if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}_n$ is negative. Generally, it is known that a Gröbner basis can be obtained at fast using graded reverse lexicographic ordering. For some applications, a Gröbner basis of lexicographic ordering has a useful characteristic. Since it has polynomials with variables eliminated, it is easy to find the solutions of the simultaneous equations.

Example 9. Consider $R = \mathbb{Q}[x, y, z]$ with $x > y > z$. Consider monomials $x^2y, y^2z^2, x^3 \in R$. On lexicographic ordering, $x^3 > x^2y > y^2z^2$. On graded reverse lexicographic ordering, $y^2z^2 > x^3 > x^2y$.

Fix a monomial ordering. Representations of any polynomial f over R is determined. Especially, the largest term of f is unique. Such a term is important for the definitions and calculations of Gröbner bases, so it is given a special notation.

Definition 10. Let f be a nonzero polynomial in $K[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

(i) the *leading term* of f is the term which is the largest monomial for the chosen monomial ordering. We write $\mathrm{LT}(f)$.

(ii) the *leading coefficient* of f is the coefficient of the leading term of f. We write $\mathrm{LC}(f)$.

(iii) the *leading monomial* of f is the monomial of the leading term of f. We write $\mathrm{LM}(f)$.

Clearly, $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$.

Example 11. Consider a polynomial $f = 2x^2y + 3y^2z^2 + 7x^3$. On lexicographic ordering, $\mathrm{LT}(f) = 7x^3, \mathrm{LC}(f) = 7, \mathrm{LM}(f) = x^3$. On graded reverse lexicographic ordering, $\mathrm{LT}(f) = 3y^2z^2, \mathrm{LC}(f) = 3, \mathrm{LM}(f) = y^2z^2$.

2.3 Gröbner bases

When we see an ideal generated by polynomials, the ideal generated by the leading terms of polynomials plays an important role. Since the monomial ordering is fixed, the leading terms of polynomials in I can be considered.

Definition 12. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal other than 0, and fix a monomial ordering. Then:

(i) We denote by $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I.

(ii) We denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

Consider an ideal I of a polynomial ring. Theorem 13 says, there exists a set of finite elements which generate I.

Theorem 13. *(Hilbert basis theorem) Every ideal $I \subset R$ has a finite generating set. In other words, $I = \langle g_1, \ldots, g_s \rangle$ for some $g_1, \ldots, g_s \in I$.*

Proof. The proof is found in many algebraic books. For example, see [6]. □

There are many sets which generate an ideal. When a monomial ordering is fixed, there exists a special set which generate I.

Definition 14. Fix a monomial order on the polynomial ring R. A finite subset $G = \{g_1, \ldots, g_s\}$ of an ideal $I \subset R$ is said to be a Gröbner basis if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle$.

From Hilbert basis theorem, every ideal of R has a Gröbner basis. A special property of a Gröbner basis is described in next section.

Algorithm 1 Buchberger algorithm

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

Output : a Gröbner basis G of F

Step 0 $G \leftarrow \emptyset, P \leftarrow \{S(f_i, f_j) \mid 1 \leq i < j \leq m\}$

Step 1 If $P = \emptyset$, return G

$p \leftarrow$ an element in P

$P \leftarrow P \backslash \{p\}$

Step 2 $p' \leftarrow$ result of reduced p by G

Step 3 (i) If $p' = 0$

Go to Step 1

(ii) If $p' \neq 0$

$P \leftarrow P \cup \{S(g, p') \mid g \in G\}$

$G \leftarrow G \cup \{p'\}$

Go to Step 1

2.4 Buchberger algorithm

Gröbner bases and an algorithm which calculates it are introduced by B. Buchberger [3]. The algorithm, called Buchberger algorithm, is a basic Gröbner bases algorithm. We review a special polynomial, called S-polynomial, and a special operation, called a reduction. They are indispensable for Buchberger algorithm.

Definition 15. (i) Let $x^\alpha, x^\beta, x^\gamma$ be monomials in R, and let α, β, γ be in $\mathbb{Z}^n_{\geq 0}$. Let $\gamma = (\gamma_1, \ldots, \gamma_n)$ satisfy $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call x^γ the *least common multiple* of x^α and x^β, written $x^\gamma = \mathrm{LCM}(x^\alpha, x^\beta)$.

(ii) Let $f, g \in R$ be polynomials. The *S-polynomial* of f and g is defined as follows.

$$\mathrm{S}(f, g) = \frac{\mathrm{LCM}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{LCM}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(g)} g \tag{2.1}$$

Definition 16. Let $f, f' \in R$ be polynomials. We say that f is reduced to f' if there exist a polynomial $g \in R$ and a monomial $r \in R$ satisfying the conditions:

(a) $\mathrm{LT}(rf) = t$ for a (certain) monomial t in f

(b) $f' = f - rg$

Corollary 17 says a Gröbner basis of an ideal I has a special property for I.

Corollary 17. Let G be a Gröbner basis for an ideal $I \subset R$ and let $f \in R$. Then $f \in I$ if and only if f is reduced to zero by G.

Proof. The proof is found in many algebraic books. For example, see [6]. □

Algorithm 1 is the pseudocode of Buchberger algorithm. The termination of the algorithm follows from Theorem 13, but here we do not explain the proof, see [6] for the proof. The details of the proofs are in [6]. The correctness of the algorithm follows from the next theorem.

Theorem 18. *Let $I \subset R$ be an ideal. $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of I if and only if S-polynomials $S(g_i, g_j)$ for all pairs $i \neq j$ are reduced to zero by G.*

Proof. The proof is found in many algebraic books. For example, see [6]. □

A Gröbner basis is not uniquely determined for a given ideal. A minimal Gröbner basis is not unique, but the number of elements in the basis is unique.

Definition 19. Let $G \subset R$ be a Gröbner basis for an certain ideal. G is called a *minimal Gröbner basis* if G satisfy the following condition.

- There do not exist $g, g' \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(g')$ and $g \neq g'$.

The reduced Gröbner basis is determined uniquely for an ideal. For applications, the reduced Gröbner basis play important roles.

Definition 20. Let $G \subset R$ be a Gröbner basis for an certain ideal. G is called a *reduced Gröbner basis* if G satisfy the following condition.

- There do not exist $g, g' \in G$ such that $\mathrm{LT}(g) \mid t$ (t is a term in g') and $g \neq g'$.

Now consider a problems of Buchberger algorithm. In the algorithm, S-polynomials which are selected at Step 1 may be reduced to zero (Step 3 (ii)). If an S-polynomial is reduced to zero, no information about the Gröbner basis is available. Therefore, these calculations are useless. Also, in general, the number of reductions of polynomials that become zero tends to increase. Thus, if it is known in advance that the polynomial is

reduced to zero before the S-polynomial is reduced, it is possible to perform an efficient computation by discarding it without reductions. Signature-based algorithms, which are the theme of this paper, can detect many polynomials which are reduced to zero and can omit unnecessary calculations.

2.5 Modules over Rings

For descriptions of signature-based algorithms, we review the definition of modules over rings. Let R be a commutative ring. An R-module is defined as follows.

Definition 21. A module over R is a set M with two operations (addition $+$ and scalar multiple by elements of R) such that the following conditions: for $a, b \in R$ and $f, g \in M$

(i) M is an abelian group under the addition. There is an additive identity element $0 \in M$, and each element has an additive inverse element.

(ii) $a(f+g) = af + ag$.

(iii) $(a+b)f = af + bf$.

(iv) $(ab)f = a(bf)$.

(v) If 1 is multiplicative identity in R, $1f = f$.

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 $\alpha = a\mathbf{e}_i, \beta = b\mathbf{e}_j$ be terms in R-module. If $a \mid b$ and $i = j$, we write $\alpha \mid \beta$.

Definition 22. Let M be a module over a ring R. We say that M is free if M has a basis, namely there exist $f_1, \ldots, f_m \in M$ such that each $m \in M$ is uniquely written of the form $\sum a_i f_i$ with $a_i \in R$. .

The R-module R^m is a free module. The standard basis elements

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \mathbf{e}_m = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{2.2}$$

form a basis for R^m.

Definition 23. Let M be an R-module. Let $f_1, \ldots, f_m$ be elements of M. The set of all $(h_1, \ldots, h_m) \in R^m$ such that $h_1 f_1 + \cdots + h_m f_m = 0$ is called the (first) syzygy module of $(f_1, \ldots, f_m)$, and denoted $Syz(f_1, \ldots, f_m)$.

Like monomial ordering, we consider ordering for modules. For signature-based algorithms, it is required to fix a module order in addition to a monomial order. Original F5 algorithm [16] uses POT order for a module order. Let a, b be monomials in R. We say $a\mathbf{e}_i \succ_{POT} b\mathbf{e}_j$ is POT (Position over Term) order if $i > j$ or $i = j$ and $a > b$.

Chapter 3

Signature-based algorithms for computing Gröbner bases

In this section, the proofs of the termination and the correctness of signature-based algorithms are given. Four signature-based algorithms are presented. They are named as fundamental signature-based semi-algorithm (**fundSB**), simple signature-based algorithm (**simpleSB**), syzygy simple signature-based algorithm (**syzSB**) and alternative rewrite basis algorithm (**altRB**). By discussing the correctness and the termination of these algorithms step by step, we obtain the correctness and the termination of **altRB**. The proofs are self-contained and clear by discussing as the above. **altRB** is presented to be efficient when a arbitrary module order other than POT is chosen.

3.1 Notation

Let R be a polynomial ring over a field K. Let us denote $K\backslash\{0\}$ by $K^{\times}$. 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.

Definition 24. Consider the homomorphism

$$^{-}\colon \quad R^m \quad \longrightarrow \quad R$$

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.

Example 25. Consider $R = \mathbb{Q}[x, y, z]$ with $x > y > z$ and graded reverse lexicographical ordering, and consider $f_1 = x^2 + y, f_2 = xy + z$. Let $\alpha = x^3\mathbf{e}_1 + z\mathbf{e}_2$ be an element of R^m. Then, we have $\overline{\alpha} = x^3\overline{\mathbf{e}_1} + z\overline{\mathbf{e}_2} = x^5 + x^3y + xyz + z^2$.

We fix a monomial order $\leq$ on R, and fix a module order $\preceq$. In the classical Gröbner bases algorithm like Buchberger algorithm, we fix a monomial order. In signature-based algorithm, we fix a module order as well as a monomial order. The calculations in the algorithms vary by the module order we choose. 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 $a \leq b$.

Definition 26. 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*.

Signature is just defined as the leading term of the element of R^m, but it has an important role in signature-based algorithms.

Definition 27. 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.

Example 28. Consider POT order with $\mathbf{e}_1 \prec \mathbf{e}_2$. Let $\alpha = (x^3 + z)\mathbf{e}_1 + (z^2 + y)\mathbf{e}_2$ be an element of R^m. The signature of α is $\mathfrak{s}(\alpha) = z^2\mathbf{e}_2$.

In the classical Gröbner bases algorithm, we reduce polynomials. In signature-based algorithms, we operate different reductions named $\mathfrak{s}$-reductions.

Definition 29. 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.

A difference between $\mathfrak{s}$-reductions and reductions operated in the classical Gröbner bases algorithm is (b).

Definition 30. 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'.

Example 31. Consider $f_1 = x^2 + y, f_2 = xy + z$. Let $\alpha = y\mathbf{e}_1 + \mathbf{e}_2$, $\beta = \mathbf{e}_2$ be elements of R^m. This implies that $\overline{\alpha} = y\overline{\mathbf{e}_1} + \overline{\mathbf{e}_2} = x^2y + y^2 + xy + z$ and $\overline{\beta} = \overline{\mathbf{e}_2} = xy + z$. We have $\mathfrak{s}(\alpha) \succ \mathfrak{s}(y\beta)$ and $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(y\overline{\beta})$. Then, α is regularly $\mathfrak{s}$-reduced to $\alpha - y\beta$ by a reducer β.

Definition 32. Let α be an element in R^m.

(i) Let β be a reducer of α. If there exists $c \in K$ such that $\mathrm{LT}(b\overline{\beta}) = c\,\mathrm{LT}(\overline{\alpha})$, the $\mathfrak{s}$-reduction is called *top* $\mathfrak{s}$*-reduction* and otherwise called *tail* $\mathfrak{s}$*-reduction*.

(ii) If α cannot be $\mathfrak{s}$-reduced, we say that α is *completely* $\mathfrak{s}$*-reduced*.

(iii) If α cannot be regularly top $\mathfrak{s}$-reduced, we say that α is *completely regularly top* $\mathfrak{s}$*-reduced*.

(iv) If α 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*.

When α is $\mathfrak{s}$-reduced, $\overline{\alpha} = 0$ or $\alpha = 0$ happens. These are confusing, so we introduce the following notation. 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 $0 \in R$.

Definition 33. The *S-pair* of $\alpha, \beta \in R^m$ is defined as following

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

where λ is the least common multiple of $\mathrm{LT}(\overline{\alpha})$ and $\mathrm{LT}(\overline{\beta})$. 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 call the S-pair is *singular*, otherwise, the S-pair *regular*.

S-pairs are substitutions of S-polynomials.

In signature-based algorithms, we compute a signature Gröbner basis. In the middle of the algorithms, we compute a signature Gröbner basis up to or in T.

Definition 34. Let T be a term in R^m.

(i) A subset $G \subseteq R^m$ is a *signature Gröbner basis up to* 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.

(ii) A subset $G \subseteq R^m$ is a *a signature Gröbner basis in* 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.

(iii) 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.

Next proposition proves that 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 35. *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. □

Definition 36. 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.

3.2 Fundamental signature-based semi-algorithm

In this section, fundamental signature-based semi-algorithm (**fundSB**) is considered. **fundSB** does not terminate, so we call **fundSB** a "semi"-algorithm. This means that

Algorithm 2 Fundamental signature-based semi-algorithm (**fundSB**)

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

Step 0 $G \leftarrow \emptyset$

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 is not appropriate for implementation and computation. However, **fundSB** helps us to comprehend how signature-based algorithms work. Specifically, it shows that why signature-based algorithms proceed in the ascending order of signatures. **Algorithm 2** is the pseudocode of **fundSB**. **fundSB** does not terminate, since **fundSB** will compute all terms in R^m and the number of elements of R^m are infinite. However, we can prove the following properties of **fundSB**.

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

(B) At the end of Step 1 in **fundSB**, G is a signature Gröbner basis up to α.

For **(A)**, note that α is a term chosen in Step 1 of the same loop. If **(A)** is true, **(B)** is true since **fundSB** computes in the ascending order of terms in R^m step by step. We prove **(A)** in Proposition 40.

Lemma 37 is called singular criterion [25]. Let α, β be elements in R^m whose signature is equivalent to that of the other. The criterion means that the results of regular $\mathfrak{s}$-reduction are the same. This property is the most significant in the signature-based algorithm.

Lemma 37. *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. First, we prove the former. For the sake of contradiction, assume that $\mathrm{LT}(\overline{\alpha}) \neq \mathrm{LT}(\overline{\beta})$. Then, either $\mathrm{LT}(\overline{\alpha - \beta}) = \mathrm{LT}(\overline{\alpha})$ or $\mathrm{LT}(\overline{\alpha - \beta}) = \mathrm{LT}(\beta)$ holds. From the condition, $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$, then we have $\mathfrak{s}(\alpha - \beta) \prec \mathfrak{s}(\alpha) \preceq T$. Therefore, $\alpha - \beta$ is top $\mathfrak{s}$-reducible by G, 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.

Next, we prove the latter. For the sake of contradiction, 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 α be an element after Step 2 in **fundSB**. If α is singularly top $\mathfrak{s}$-reducible by G, then the signature of α is the same as the signature of the reducer.

Lemma 38. *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. For the sake of contradiction, 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. □

Let α be an element after Step 2 in **fundSB**. By Lemma 39, If α is singularly top $\mathfrak{s}$-reducible by G, α is $\mathfrak{s}$-reduced to $0 \in R$ by G.

Lemma 39. *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 38, 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. □

By Lemmas 37, 38 and 39, we prove **(A)** at the end of Step 3 in **fundSB**, G is a signature Gröbner basis in α.

Proposition 40. *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 37 and 38, 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 37.

(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 39, 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 39, 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. □

Actually, **fundSB** computes a minimal signature Gröbner basis. Similarly, signature-based algorithms presented after this compute a minimal signature Gröbner basis.

Lemma 41. *Let $T \in R^m$ be a term chosen at Step 1 in* **fundSB**. *Let G in* **fundSB** *be the set after Step 3 of T. Then, G is a minimal signature Gröbner basis in T.*

Proof. From Proposition 40, G is a signature Gröbner basis in T. Let α be an element in G. We prove that there does not exist $\beta \in G \setminus \{\alpha\}$ such that $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$ and $\mathrm{LT}(\alpha) = \mathrm{LT}(\beta)$. 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. □

Algorithm 3 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

3.3 Simple signature-based algorithm

In this section, we consider simple signature-based algorithm (**simpleSB**). **simpleSB** terminates in finite steps and outputs a signature Gröbner basis. We use a conception of S-pair in **simpleSB**. An S-pair is generated by two elements of R^m, and we focus on the signatures of S-pairs. In **fundSB**, all terms in R^m are intended to be computed, and it is not impossible. Therefore, **simpleSB** does not terminate. In **simpleSB**, the terms which appear as the signatures of the S-pairs are computed. We prove that such terms are finite in Proposition 48, that means **simpleSB** terminates. However, some terms which appear as the signatures of the S-pairs are not computed. We prove that such terms do not need to be computed in Propositions 47 and 49.

Algorithm 3 is the pseudocode of **simpleSB**. Note that **simpleSB** outputs a minimal signature Gröbner basis by Lemma 41.

The proof of the termination of **simpleSB** is proved by Proposition 48. The proof of

the correctness is proved by Proposition 49. For proving the two Propositions, we prove several Lemmas below.

Let T be a term in R^m. Let G be a signature Gröbner basis up to T. Let $a\alpha$ with $a \in R$ and $\alpha \in G$ be an regularly top $\mathfrak{s}$-reducible by G. This means that an element whose signature is $\mathfrak{s}(a\alpha)$ may be an element of a signature Gröbner basis. Lemma 42 says that the signature of such an element appear as the signature of a certain S-pair.

Lemma 42. *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). □

Let $\alpha \in R^m$ be completely regularly top $\mathfrak{s}$-reduced. Consider $\alpha' \in R^m$ with $\mathfrak{s}(\alpha') = \mathfrak{s}(\alpha)$. Lemma 43 says that there does not exist an element α' whose leading term $\mathrm{LT}(\overline{\alpha'})$ is smaller than the leading term $\mathrm{LT}(\overline{\alpha})$.

Lemma 43. *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 37. □

Let $\alpha \in R^m$ be completely regularly top $\mathfrak{s}$-reduced by G. Of course, α is not regularly top $\mathfrak{s}$-reducible by G. The signatures of the terms computed after this are larger than $\mathfrak{s}(\alpha)$ because signature-based algorithms compute in ascending order of terms in R^m. Therefore, α is not regular top $\mathfrak{s}$-reducible even if G is a signature Gröbner basis. Thus, there does not exist a regular S-pair $\alpha - b\beta$ with $\beta \in G, b \in R$.

Lemma 44. *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 45 is clear because of Lemma 37.

Lemma 45. *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 37, we have $\mathrm{LT}(\overline{\beta}) = \mathrm{LT}(\overline{\alpha})$. This contradicts $\mathrm{LT}(\overline{\beta}) > \mathrm{LT}(\overline{\alpha})$. □

Unlike **fundSB**, **simpleSB** computes the terms which appear as the signatures of the regular S-pairs. Therefore, some terms in R^m are not computed. We prove that such terms do not need to be computed by Lemma 46. When such terms are completely regularly top $\mathfrak{s}$-reduced, they are singularly top $\mathfrak{s}$-reducible. Singularly top $\mathfrak{s}$-reducible elements are discarded in **simpleSB**, that is, they do not need to be computed.

Lemma 46. *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 43, 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 45, $a\beta$ 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 38, 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 42 and 44, 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 39 that α' is $\mathfrak{s}$-reduced to $0 \in R$ by G. Thus, G is a signature Gröbner basis in T. □

simpleSB so not compute some terms in R^m. However, when a term $\alpha \in R^m$ is chosen in Step 1, G is a signature Gröbner basis in α after Step 3 like **fundSB**.

Proposition 47. *Let T' in R^m be a term chosen at Step 1 in* **simpleSB**, *and let T be the term chosen just before T'. Assume that G in* **simpleSB** *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 46, 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 **simpleSB** is exactly same as that in **fundSB**.

By Proposition 40, G is a signature Gröbner basis in T' after Step 3 of the loop starting with $\alpha = T'$. □

Our proof of termination is almost the same as Eder and Perry [9], Roune and Stillman [25] and Eder and Roune [12].

Proposition 48. 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 **simpleSB**) 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 **simpleSB**. 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 **simpleSB** 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}. But, in Step 1, the number of elements in P decreases by one in each step. Thus, **simpleSB** terminates in finite steps. □

Proposition 47 says that G is a signature Gröbner basis in α for every loops like

fundSB. When **simpleSB** terminates, G is a signature Gröbner basis by Proposition 49.

Proposition 49 (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 47, 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 46, 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. □

3.4 Simple syzygy signature-based algorithm

In this section, a method to detect zero reductions is described. The method is used in most signature-based algorithms, and is characteristic in signature-based algorithms. The method can be used thanks to the use of signature, and also thanks to regular $\mathfrak{s}$-reductions instead of reductions which is used in Buchberger algorithm. There are two criteria, Propositions 50 and 51 for detecting zero reductions. By Lemma 37, 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 $0 \in R$, because of a following equation $\overline{f_i\mathbf{e}_j - f_j\mathbf{e}_i} = 0$. Moreover, 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 $0 \in R$ because of a following equation $\overline{r(f_i\mathbf{e}_j - f_j\mathbf{e}_i)} = 0$ for all $r \in R\backslash\{0\}$. By this, we have Proposition 50.

Proposition 50. *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 37, 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. □

Signature-based algorithms can detect zero reductions using zero reductions which happens before. In detail, let $\alpha \in R^m$ be completely regularly $\mathfrak{s}$-reduced to $0 \in R$. Consider $\beta \in R^m$ with $\mathfrak{s}(\beta) = \mathfrak{s}(\alpha)$. By similar discussion on Proposition 50, β is completely regularly $\mathfrak{s}$-reduced to $0 \in R$.

Proposition 51. *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 37, β is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. □

Algorithm 4 is simple syzygy signature-based algorithm (**syzSB**). **syzSB** is modified **simpleSB** as to Propositions 50 and 51.

The proofs of the correctness and the termination are described briefly because **syzSB** computes terms which is also computed in **simpleSB**, but do not compute terms which will be regularly $\mathfrak{s}$-reduced to $0 \in R$.

Proposition 52 (Termination)**. syzSB** *terminates in finite loops.*

Proof. By Propositions 50 and 51, 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. □

Proposition 53 (Correctness)**. syzSB** *outputs a signature Gröbner basis.*

Algorithm 4 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

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 50 and 51, **syzSB** computes the set $A \setminus B$. Then, the output G of **syzSB** is the same as that of **simpleSB**. □

3.5 Alternative rewrite basis algorithm

In this section, alternative rewrite basis algorithm (**altRB**) is introduced. So far, many signature-based algorithms are introduced. In 2013, The paper [12] introduced rewrite basis algorithm **RB** as a generalized signature-based algorithm. **altRB** is introduced easily to understand operations of the algorithm and easily to implement comparing to **RB**. In this paper, **altRB** is the most useful signature-based algorithm for implementa-

Algorithm 5 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

tion. 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. By discarding these elements without reducing them, we can expect improvements of **syzSB**. In other words, it is enough to regularly $\mathfrak{s}$-reduce the elements which is expected to be the element of minimal signature Gröbner basis. We can also expect to improve efficiency by replacing elements which have the same signature and are not needed to reduce the number of times. Among the algorithms proposed in [1], [22] and etc., the method is used implicitly. The paper [13] introduced such algorithms as **RB** with RAT selected for rewrite order. When we choose RAT for a rewrite order, rewrite basis algorithm become the most efficient. **altRB** is simply introduced and as efficient as **RB** with RAT. **Algorithm 5** is the pseudocode of **altRB**.

Lemma 54. *Let α' and α'' be obtained at Step 3 and at Step 4 in* **altRB** *respectively. Let G be a signature Gröbner basis up to $\mathfrak{s}(\alpha'')$. The condition at Step 5 (ii) in* **altRB** *is equivalent to the condition that α'' is not singularly top $\mathfrak{s}$-reducible by G.*

Lemma 55. *Let α' and α'' be obtained at Step 3 and at Step 4 in* **altRB** *respectively. Let G be a signature Gröbner basis up to $\mathfrak{s}(\alpha'')$. The condition at Step 5 (ii) in* **altRB** *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 43, 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 56 (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 37, 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 55, they are equivalent. □

Theorem 57 (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. □

3.6 Module orders and zero reductions

In the paper [13], **RB** does not have a $(*)$ line which is in **altRB**. That is because **RB** is introduced as a generalized signature-based algorithm. When implemented **RB**, we have to be careful about the number of zero reductions in the calculation. If we select POT as the module order and calculate incrementally like **Algorithm 6**, we can calculate with fewer zero reductions. Especially if the polynomial system is a regular sequence, the number of zero reductions is zero. If we select a module order other than POT or a module order that is not suitable for incremental calculation, the number of zero reductions will increase during the calculation. If we choose POT as the module order and calculate it incrementally, we can prove that it is sufficient to update H at first, as in **Algorithm 6**.

Lemma 58. *Let α'' be a new element at Step 5 (ii) in* **Algorithm 6** *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 $\overline{\alpha''} = \sum_{i=1}^m r_i f_i \equiv h_m f_m \pmod{F}$.

$$\begin{aligned}\overline{\alpha''}\beta - \overline{\beta}\alpha'' &= (\sum_{i=1}^m r_i f_i)\cdot(\sum_{j=1}^m r'_j\mathbf{e}_j) - (\sum_{j=1}^m r'_j f_j)\cdot(\sum_{i=1}^m r_i\mathbf{e}_i) \\ &= \{(\sum_{i=1}^m r_i f_i)\cdot r'_m - (\sum_{j=1}^m r'_j f_j)\cdot r_m\}\mathbf{e}_m + \cdots \end{aligned} \tag{3.1}$$

Algorithm 6 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

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

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

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

Chapter 4

An efficient strategy for signature-based algorithms

In order for efficient Gr öbner basis computation, it is one of the important problems to decrease the number of reduction that occupy a large proportion in the calculation. In this chapter, a new strategy for regular $\mathfrak{s}$-reduction aiming to decrease the number of regular $\mathfrak{s}$-reductions and usual reductions is introduced. The idea of the strategy is that when a signature Gröbner basis is calculated, there are unnecessary elements for a minimal Gröbner basis. If candidates of elements which will be included in a minimal Gröbner basis should be sufficiently reduced, we can compute the minimal signature Gröbner basis from a signature Gröbner basis by low calculations. Overview of the strategy is following: after generating an S-pair, we fulfill only-top reduction. If the S-pair meets a certain condition (**SF** in §4), we execute full reduction. We name the strategy *selective-full reduction strategy* (**Algorithm 11**). Efficiency of the strategy was evaluated by several Gröbner basis benchmarks. The selective-full reduction strategy reduces the number of reductions to calculate the reduced Gröbner basis. To calculate the signature Gr öbner basis, the selective-full reduction strategy is the most efficient or not the worst.

Note that reductions handled in Buchberger algorithm is called normal reductions to distinguish $\mathfrak{s}$-reduction.

Algorithm 7 TOP_REDUCE

input : a finite subset G of R^m, $\alpha \in R^m$

output : $\gamma \in R^m$

for $\beta \in G$ **do**

  if $\mathrm{LT}(\overline{\beta}) \mid \mathrm{LT}(\overline{\alpha})$ and $\mathfrak{s}(\alpha) \succ \frac{\mathrm{LT}(\overline{\alpha})}{\mathrm{LT}(\overline{\beta}))} \cdot \mathfrak{s}(\beta)$ **then**

    $\gamma \leftarrow \alpha - \frac{\mathrm{LT}(\overline{\alpha})}{\mathrm{LT}(\overline{\beta}))} \cdot \beta$

    return γ

  end if

end for

$\gamma \leftarrow \alpha$

return γ

4.1 Conventional $\mathfrak{s}$-reduction strategies

In this section, we review two strategies of regular $\mathfrak{s}$-reducing S-pairs mentioned in the paper [13]. One is only-top reduction strategy. How to calculate by the only-top reduction strategy is following. After generating an S-pair, regularly $\mathfrak{s}$-reduce leading monomials until the leading monomial cannot be regularly $\mathfrak{s}$-reduced. The algorithm of the only-top reduction strategy is **Algorithm 9**. By this procedure, the S-pair is completely regularly top $\mathfrak{s}$-reduced. The other is full reduction strategy. How to calculate by the full reduction strategy is following. After generating S-pairs, regularly $\mathfrak{s}$-reduce the monomials included in the S-pairs. The algorithm of the full reduction strategy is **Algorithm 10**. First, run regular top $\mathfrak{s}$-reduction, and if the S-pair is completely regular top $\mathfrak{s}$-reduction, then execute regular tail $\mathfrak{s}$-reduction. By this procedure, the S-pair is completely regularly full $\mathfrak{s}$-reduced.

Each strategy has advantages and disadvantages. If we choose the only-top reduction strategy, it is expected that the number of times of regular $\mathfrak{s}$-reduction is fewer because we regularly $\mathfrak{s}$-reduce the only leading terms. However, the number of times of top $\mathfrak{s}$-reduction may increase. Because, the polynomials used to regularly $\mathfrak{s}$-reduce the S-pairs are not reduced many with respect to the fixed monomial order. On the other

Algorithm 8 TAIL_REDUCE

input : a finite subset G of R^m, $\alpha \in R^m$

output : $\gamma \in R^m$

for $t \in \mathrm{T}(\overline{\alpha} - \mathrm{LT}(\overline{\alpha}))$ **do** (t is a monomial in $\overline{\alpha} - \mathrm{LT}(\overline{\alpha})$)
  for $\beta \in G$ **do**
    if $\mathrm{LT}(\overline{\beta}) \mid t$ and $\mathfrak{s}(\alpha) \succ \frac{t}{\mathrm{LT}(\overline{\beta}))} \cdot \mathfrak{s}(\beta)$ **then**
      $\gamma \leftarrow \alpha - \frac{t}{\mathrm{LT}(\overline{\beta}))} \cdot \beta$
      return γ
    end if
  end for
end for
$\gamma \leftarrow \alpha$
return γ

hand, consider the case of the full reduction strategy. We regularly $\mathfrak{s}$-reduce all terms included in S-pairs. The terms included in regularly $\mathfrak{s}$ -reduced S-pairs is relatively small in terms of the fixed monomial order. Also, the number of times of interreductions for computing the reduced Gröbner basis becomes few because regular tail $\mathfrak{s}$-reductions has been operated in advance. However, regular tail $\mathfrak{s}$-reductions are restricted reductions comparing to usual reductions, so we cannot reduce terms enough in comparison with usual reductions. In addition, the number of signature Gröbner basis elements is greater than the number of the minimal Gröbner basis elements. Therefore, the number of S-pairs that we need to completely regularly full $\mathfrak{s}$-reduce is also much greater.

Whether the good strategy is the only-top reduction strategy or the full reduction strategy depends on the polynomial system we solve. Tables 1 and 3 show the benchmark results. When computing a signature Gröbner basis or a reduced Gröbner basis, it is not sure which strategy is better for the actual problem.

Algorithm 9 ONLY-TOP_REDUCE

input : a finite subset G of R^m, $\alpha \in R^m$

output : $\beta \in R^m$ which is completely regular top $\mathfrak{s}$-reduced by G

repeat

$\beta \leftarrow \alpha$

$\alpha \leftarrow \mathrm{TOP\_REDUCE}(G, \beta)$

until $\alpha = \beta$

return β

4.2 Our $\mathfrak{s}$-reduction strategy

Consider that we calculate the reduced Gröbner basis after a signature Gröbner basis has been calculated. The number of elements of a signature Gröbner basis which signature-based algorithms output is greater than the minimal Gröbner basis. Therefore, we first calculate the minimal Gröbner basis from a signature Gröbner basis we has computed. How to calculate it is to remove $\alpha \in G$ satisfying the following condition from the found signature Gröbner basis: There exists $\alpha' \in G, \mathrm{LT}(\overline{\alpha}) \mid \mathrm{LT}(\overline{\alpha'})$. Then, we obtain a minimal Gröbner basis. By interreducing the found minimal Gröbner basis, the reduced Gröbner basis is obtained.

Here we consider the relation between the full reduction strategy and the reduced Gröbner basis. The full reduction strategy can be thought of as a strategy that decreases the number of interreductions. In that sense, the $\mathfrak{s}$-reductions of S-pairs removed in the step of calculating the minimal Gröbner basis do not need. An algorithm based on this idea to $\mathfrak{s}$-reduce an S-pair is **Algorithm 11**. First, we regularly top $\mathfrak{s}$-reduce an S-pairs until the S-pair is completely regularly top $\mathfrak{s}$-reduced. Then, perform regularly tail $\mathfrak{s}$-reduction only if the following conditions are satisfied:

$$\text{for all } \alpha' \in G, \mathrm{LT}(\overline{\alpha'}) \nmid \mathrm{LT}(\overline{\alpha}) \qquad \boxed{\textbf{SF}}$$

We call this strategy *selective-full reduction*. The output of the **Algorithm 11** denotes a *completely regular selective-full reduced* S-pair.

Following shows that selective-full strategy is reasonable.

Algorithm 10 FULL_REDUCE

input : a finite subset $G \in R^m$, $\alpha \in R^m$

output : $\beta \in R^m$ which is completely regular full $\mathfrak{s}$-reduced by G

repeat

$\beta \leftarrow \alpha$

$\alpha \leftarrow \mathrm{TOP\_REDUCE}(G, \beta)$

until $\alpha = \beta$

repeat

$\beta \leftarrow \alpha$

$\alpha \leftarrow \mathrm{TAIL\_REDUCE}(G, \beta)$

until $\alpha = \beta$

return β

(1) Let α be an S-pair which does not satisfy **SF**. We can predict that α will be removed when calculating the minimal Gröbner basis. If we choose the selective-full reduction strategy, we will not regularly tail $\mathfrak{s}$-reduce α that will eventually be discarded. Therefore, the number of times of regularly $\mathfrak{s}$-reductions by selective-full reduction strategy is expected to be less than the number of times of regularly $\mathfrak{s}$-reductions by a full reduction strategy.

(2) Consider the case where a signature Gröbner basis has been calculated. Then, we compute the minimal Gröbner basis. If we choose selective-full strategy, all elements of the minimal Gröbner basis are completely regularly full $\mathfrak{s}$-reduced. Therefore, the number of interreductions with the selective-full reduction strategy is expected to be much less than the number of interductions with the only-top reduction strategy.

(3) Let $\alpha \in G$ be a possible reducer for a certain S-pair, and α was not completely regularly full $\mathfrak{s}$-reduced, that is, α did not satisfy **SF**. Then there exists α' that satisfies the following (i) and (ii): (i) $\mathrm{LT}(\overline{\alpha'}) \mid \mathrm{LT}(\overline{\alpha})$, (ii) α' is completely regularly full $\mathfrak{s}$-reduced or an input module of the algorithm. Especially with regard to

Algorithm 11 SELECTIVE-FULL_REDUCE

input : a finite subset $G \in R^m$, $\alpha \in R^m$

output : $\beta \in R^m$ which is completely regular selective-full $\mathfrak{s}$-reduced by G

repeat

  $\beta \leftarrow \alpha$

  $\alpha \leftarrow \mathrm{TOP\_REDUCE}(G, \beta)$

until $\alpha = \beta$

for $\gamma \in G$ **do**

  if $\mathrm{LT}(\overline{\gamma}) \mid \mathrm{LT}(\overline{\alpha})$ **then**

    return β (if α does not satisfy **SF**, return α)

  end if

end for

repeat

  $\beta \leftarrow \alpha$

  $\alpha \leftarrow \mathrm{TAIL\_REDUCE}(G, \beta)$

until $\alpha = \beta$

return β

(ii), there exists $\alpha' \in G$ such that $\mathrm{LT}(\overline{\alpha'}) \mid \mathrm{LT}(\overline{\alpha})$ and $\mathrm{LT}(\overline{\beta}) \nmid \mathrm{LT}(\overline{\alpha'})$ for all $\beta \in G \backslash \{\alpha'\}$. Then α' was generated from a certain S-pair that satisfies **SF** or an input module of the algorithm. Therefore, if we can regularly $\mathfrak{s}$-reduce the S-pair, we can choose a reducer that is regularly full $\mathfrak{s}$-reduced. Therefore, to some extent, the number of regular $\mathfrak{s}$-reductions is expected to be low compared to the only top reduction strategy.

4.3 Results

In this section, we evaluate the proposed $\mathfrak{s}$-reduction strategy, selective-full reduction strategy, using well-known Gröbner basis benchmarks. Implementation is done by C, and we count the times of $\mathfrak{s}$-reductions, normal reductions and multiplications. Benchmarks

were computed on both homogeneous and inhomogeneous ideals. We compared three strategies, only-top reduce, full reduce, and selective-full reduce. We refer to [13] for recording the number of multiplications and reductions. All systems are computed over a field of characteristic 32003, with graded reverse lexicographical monomial order. For a module order, we used the POT order which is used in the original F5. For finding the syzygy modules, we used signatures which are zero reduced. Therefore, like F5, all algorithms proceeds incrementally. Like F5C [8], the reduced Gröbner basis was found at each incremental steps.

The results are shown in table 4.1, 4.2, 4.3, 4.4, 4.5, 4.6. In table 4.1, 4.3, the numbers of sum of one-time $\mathfrak{s}$-reductions and usual reductions to compute a signature Gröbner basis(SGB:ALL), among them the numbers of one-time $\mathfrak{s}$-reductions(SGB:S-RED) and the numbers of sum of one-time $\mathfrak{s}$-reductions and usual reductions to compute the reduced Gröbner basis(RGB:ALL) are shown. In table 4.2, 4.4, the numbers of times of multiplications processed in above computation are shown. In table 4.5, 4.6, the numbers of generated S-pairs which satisfy $\boxed{\textbf{SF}}$ and does not satisfy $\boxed{\textbf{SF}}$ are shown.

There are benchmarks with many elements which satisfy $\boxed{\textbf{SF}}$ during the computations, for example noon-8,9 and HRandom(10,2,2) and HRandom(11,2,2). The elements which satisfy $\boxed{\textbf{SF}}$ have a high probability of being included in a minimal Gröbner basis. If the elements are regularly full $\mathfrak{s}$-reduced, they need to be reduced fewer times in computing the reduced Gröbner basis step. Actually, the number of times of reductions by the full reduction strategy is smaller than that of reductions by the only-top reduction strategy at benchmarks with many elements which satisfy $\boxed{\textbf{SF}}$. The number of times of reductions by the selective-full strategy is the almost same as that of reductions by the full reduction strategy. In case of benchmarks with few elements which satisfy $\boxed{\textbf{SF}}$ during the computations, for example cyclic-8 and eco-11. The number of times of reductions by the full reduction strategy is bigger than that of reductions by the only-top reduction strategy. The number of times of reductions by the selective-full strategy is smaller than that of reductions by the only-top reduction strategy.

To calculate the reduced Gröbner basis, the selective-full reduction strategy calculates the least number of times of $\mathfrak{s}$-reductions and normal reductions of the three strategies. The number of multiplications is also small on the selective-full strategy, except

for little disadvantage to full reduction strategy at the two benchmarks Random(10,2,2) and Random(11,2,2). Therefore, the selective-full reduction strategy is efficient strategy for the reduced Gröbner basis.

To calculate a signature-Gröbner basis, the selective-full strategy is superior to the only-top reduction strategy on most benchmarks except for two benchmarks, noon-8 and noon-9. When comparing the full reduction strategy to the selective-full strategy, the selective-full reduction strategy is better or equivalent. From table 5 and 6, the more effective the selective-full reduction strategy is, the more number the difference between the reduced Gröbner basis and a signature Gröbner basis is. Only-top reduction strategy is ineffective against Random(10,2,2) and Random(11,2,2)(both homogeneous and inhomogeneous) and full reduction strategy is ineffective against katstura-11(both homogeneous and inhomogeneous). However, the selective-full reduction strategy is not bad against Random(10,2,2) Random(11,2,2) and katstura-11. Moreover, for all the benchmarks in this paper, the selective-full strategy is not the worst of the three strategies. Therefore, the selective-full reduction strategy is a rational strategy for signature-based algorithms.

Table 4.1: The numbers of times of reductions (homogeneous)

benchmark		ADD			RAT		
		SGB		RGB	SGB		RGB
		ALL	$\mathfrak{s}$-RED	ALL	ALL	$\mathfrak{s}$-RED	ALL
cyclic-7	only-top	$2^{17.380}$	$2^{17.118}$	$2^{17.528}$	$2^{17.099}$	$2^{16.740}$	$2^{17.284}$
	full	$2^{16.954}$	$2^{16.936}$	$2^{17.035}$	$2^{16.442}$	$2^{16.416}$	$2^{16.557}$
	selective	$2^{16.699}$	$2^{16.677}$	$2^{16.795}$	$2^{16.344}$	$2^{16.316}$	$2^{16.466}$
cyclic-8	only-top	$2^{22.788}$	$2^{22.484}$	$2^{22.837}$	$2^{21.983}$	$2^{21.382}$	$2^{22.075}$
	full	$2^{23.319}$	$2^{23.298}$	$2^{23.333}$	$2^{22.041}$	$2^{21.990}$	$2^{22.076}$
	selective	$2^{22.336}$	$2^{22.295}$	$2^{22.365}$	$2^{21.280}$	$2^{21.192}$	$2^{21.339}$
eco-10	only-top	$2^{19.026}$	$2^{18.902}$	$2^{19.435}$	$2^{18.781}$	$2^{18.632}$	$2^{19.255}$
	full	$2^{20.314}$	$2^{20.302}$	$2^{20.350}$	$2^{19.013}$	$2^{18.983}$	$2^{19.101}$
	selective	$2^{18.852}$	$2^{18.819}$	$2^{18.950}$	$2^{18.741}$	$2^{18.704}$	$2^{18.846}$
eco-11	only-top	$2^{21.541}$	$2^{21.421}$	$2^{21.950}$	$2^{21.166}$	$2^{21.008}$	$2^{21.679}$
	full	$2^{23.739}$	$2^{23.734}$	$2^{23.755}$	$2^{21.486}$	$2^{21.465}$	$2^{21.563}$
	selective	$2^{21.401}$	$2^{21.378}$	$2^{21.482}$	$2^{21.166}$	$2^{21.139}$	$2^{21.261}$
f-633	only-top	$2^{9.852}$	$2^{9.718}$	$2^{10.723}$	$2^{9.647}$	$2^{9.492}$	$2^{10.530}$
	full	$2^{9.990}$	$2^{9.956}$	$2^{10.007}$	$2^{9.533}$	$2^{9.486}$	$2^{9.557}$
	selective	$2^{9.635}$	$2^{9.591}$	$2^{9.656}$	$2^{9.496}$	$2^{9.447}$	$2^{9.520}$
f-744	only-top	$2^{16.942}$	$2^{16.752}$	$2^{17.074}$	$2^{16.598}$	$2^{16.348}$	$2^{16.757}$
	full	$2^{17.398}$	$2^{17.393}$	$2^{17.414}$	$2^{16.435}$	$2^{16.426}$	$2^{16.465}$
	selective	$2^{16.801}$	$2^{16.795}$	$2^{16.825}$	$2^{16.340}$	$2^{16.331}$	$2^{16.373}$
katsura-11	only-top	$2^{21.797}$	$2^{18.644}$	$2^{22.331}$	$2^{21.747}$	$2^{18.356}$	$2^{22.257}$
	full	$2^{23.709}$	$2^{23.700}$	$2^{23.713}$	$2^{23.515}$	$2^{23.504}$	$2^{23.520}$
	selective	$2^{21.600}$	$2^{21.560}$	$2^{21.618}$	$2^{21.594}$	$2^{21.553}$	$2^{21.612}$
noon-8	only-top	$2^{15.849}$	$2^{15.847}$	$2^{20.145}$	$2^{14.541}$	$2^{14.537}$	$2^{19.993}$
	full	$2^{18.103}$	$2^{18.103}$	$2^{18.109}$	$2^{17.940}$	$2^{17.940}$	$2^{17.948}$
	selective	$2^{18.024}$	$2^{18.024}$	$2^{18.031}$	$2^{17.865}$	$2^{17.865}$	$2^{17.873}$
noon-9	only-top	$2^{18.401}$	$2^{18.400}$	$2^{23.045}$	$2^{16.756}$	$2^{16.755}$	$2^{22.881}$
	full	$2^{20.685}$	$2^{20.685}$	$2^{20.690}$	$2^{20.515}$	$2^{20.515}$	$2^{20.521}$
	selective	$2^{20.603}$	$2^{20.603}$	$2^{20.608}$	$2^{20.445}$	$2^{20.445}$	$2^{20.451}$
HRandom(10,2,2)	only-top	$2^{19.452}$	$2^{18.004}$	$2^{19.575}$	$2^{19.454}$	$2^{18.009}$	$2^{19.577}$
	full	$2^{17.659}$	$2^{17.616}$	$2^{17.761}$	$2^{17.660}$	$2^{17.617}$	$2^{17.762}$
	selective	$2^{17.655}$	$2^{17.611}$	$2^{17.757}$	$2^{17.656}$	$2^{17.613}$	$2^{17.758}$
HRandom(11,2,2)	only-top	$2^{21.620}$	$2^{20.097}$	$2^{21.727}$	$2^{21.621}$	$2^{20.101}$	$2^{21.729}$
	full	$2^{19.612}$	$2^{19.571}$	$2^{19.690}$	$2^{19.612}$	$2^{19.571}$	$2^{19.691}$
	selective	$2^{19.596}$	$2^{19.555}$	$2^{19.676}$	$2^{19.598}$	$2^{19.556}$	$2^{19.677}$

Table 4.2: The numbers of times of multiplications (homogeneous)

benchmark		ADD			RAT		
		SGB		RGB	SGB		RGB
		ALL	$\mathfrak{s}$-RED	ALL	ALL	$\mathfrak{s}$-RED	ALL
cyclic-7	only-top	$2^{24.401}$	$2^{24.275}$	$2^{24.523}$	$2^{23.994}$	$2^{23.820}$	$2^{24.155}$
	full	$2^{24.305}$	$2^{24.286}$	$2^{24.400}$	$2^{23.758}$	$2^{23.730}$	$2^{23.895}$
	selective	$2^{24.057}$	$2^{24.034}$	$2^{24.169}$	$2^{23.616}$	$2^{23.584}$	$2^{23.766}$
cyclic-8	only-top	$2^{31.140}$	$2^{30.971}$	$2^{31.181}$	$2^{30.132}$	$2^{29.769}$	$2^{30.214}$
	full	$2^{31.978}$	$2^{31.959}$	$2^{31.995}$	$2^{30.698}$	$2^{30.650}$	$2^{30.739}$
	selective	$2^{30.861}$	$2^{30.818}$	$2^{30.898}$	$2^{29.789}$	$2^{29.696}$	$2^{29.865}$
eco-10	only-top	$2^{24.460}$	$2^{24.340}$	$2^{24.839}$	$2^{24.291}$	$2^{24.155}$	$2^{24.713}$
	full	$2^{26.007}$	$2^{25.996}$	$2^{26.043}$	$2^{24.708}$	$2^{24.681}$	$2^{24.795}$
	selective	$2^{24.513}$	$2^{24.481}$	$2^{24.612}$	$2^{24.409}$	$2^{24.375}$	$2^{24.515}$
eco-11	only-top	$2^{27.628}$	$2^{27.505}$	$2^{27.992}$	$2^{27.339}$	$2^{27.187}$	$2^{27.775}$
	full	$2^{29.978}$	$2^{29.974}$	$2^{29.996}$	$2^{27.812}$	$2^{27.791}$	$2^{27.889}$
	selective	$2^{27.711}$	$2^{27.689}$	$2^{27.793}$	$2^{27.484}$	$2^{27.458}$	$2^{27.580}$
f-633	only-top	$2^{12.429}$	$2^{12.302}$	$2^{13.305}$	$2^{12.232}$	$2^{12.086}$	$2^{13.105}$
	full	$2^{12.687}$	$2^{12.649}$	$2^{12.702}$	$2^{12.300}$	$2^{12.251}$	$2^{12.321}$
	selective	$2^{12.356}$	$2^{12.309}$	$2^{12.376}$	$2^{12.258}$	$2^{12.207}$	$2^{12.279}$
f-744	only-top	$2^{21.553}$	$2^{21.438}$	$2^{21.701}$	$2^{21.258}$	$2^{21.111}$	$2^{21.433}$
	full	$2^{22.201}$	$2^{22.198}$	$2^{22.223}$	$2^{21.274}$	$2^{21.267}$	$2^{21.315}$
	selective	$2^{21.554}$	$2^{21.549}$	$2^{21.588}$	$2^{21.152}$	$2^{21.145}$	$2^{21.196}$
katsura-11	only-top	$2^{29.633}$	$2^{27.907}$	$2^{30.009}$	$2^{29.548}$	$2^{27.635}$	$2^{29.926}$
	full	$2^{32.170}$	$2^{32.162}$	$2^{32.175}$	$2^{31.969}$	$2^{31.961}$	$2^{31.976}$
	selective	$2^{29.932}$	$2^{29.897}$	$2^{29.958}$	$2^{29.907}$	$2^{29.871}$	$2^{29.934}$
noon-8	only-top	$2^{20.402}$	$2^{20.401}$	$2^{23.998}$	$2^{19.802}$	$2^{19.801}$	$2^{23.906}$
	full	$2^{22.249}$	$2^{22.249}$	$2^{22.388}$	$2^{22.128}$	$2^{22.128}$	$2^{22.279}$
	selective	$2^{22.169}$	$2^{22.169}$	$2^{22.316}$	$2^{22.059}$	$2^{22.059}$	$2^{22.218}$
noon-9	only-top	$2^{23.198}$	$2^{23.198}$	$2^{27.216}$	$2^{22.394}$	$2^{22.393}$	$2^{27.110}$
	full	$2^{25.156}$	$2^{25.156}$	$2^{25.332}$	$2^{25.029}$	$2^{25.029}$	$2^{25.220}$
	selective	$2^{25.076}$	$2^{25.076}$	$2^{25.261}$	$2^{24.969}$	$2^{24.969}$	$2^{25.167}$
Random(10,2,2)	only-top	$2^{27.035}$	$2^{26.085}$	$2^{27.103}$	$2^{27.036}$	$2^{26.087}$	$2^{27.105}$
	full	$2^{25.936}$	$2^{25.872}$	$2^{25.984}$	$2^{25.937}$	$2^{25.874}$	$2^{25.985}$
	selective	$2^{26.038}$	$2^{25.979}$	$2^{26.083}$	$2^{26.039}$	$2^{25.980}$	$2^{26.084}$
Random(11,2,2)	only-top	$2^{29.967}$	$2^{29.024}$	$2^{30.022}$	$2^{29.968}$	$2^{29.025}$	$2^{30.023}$
	full	$2^{28.831}$	$2^{28.770}$	$2^{28.867}$	$2^{28.831}$	$2^{28.770}$	$2^{28.867}$
	selective	$2^{28.937}$	$2^{28.880}$	$2^{28.970}$	$2^{28.938}$	$2^{28.882}$	$2^{28.972}$

Table 4.3: The numbers of times of reductions (inhomogeneous)

benchmark		ADD			RAT		
		SGB		RGB	SGB		RGB
		ALL	$\mathfrak{s}$-RED	ALL	ALL	$\mathfrak{s}$-RED	ALL
cyclic-7	only-top	$2^{17.380}$	$2^{17.118}$	$2^{17.433}$	$2^{17.099}$	$2^{16.740}$	$2^{17.163}$
	full	$2^{16.954}$	$2^{16.936}$	$2^{16.979}$	$2^{16.442}$	$2^{16.416}$	$2^{16.478}$
	selective	$2^{16.699}$	$2^{16.677}$	$2^{16.729}$	$2^{16.344}$	$2^{16.316}$	$2^{16.382}$
cyclic-8	only-top	$2^{22.788}$	$2^{22.484}$	$2^{22.793}$	$2^{21.983}$	$2^{21.382}$	$2^{21.994}$
	full	$2^{23.319}$	$2^{23.298}$	$2^{23.320}$	$2^{22.041}$	$2^{21.990}$	$2^{22.046}$
	selective	$2^{22.355}$	$2^{22.314}$	$2^{22.358}$	$2^{21.288}$	$2^{21.200}$	$2^{21.295}$
eco-10	only-top	$2^{17.942}$	$2^{17.650}$	$2^{18.422}$	$2^{16.892}$	$2^{16.252}$	$2^{17.741}$
	full	$2^{20.878}$	$2^{20.868}$	$2^{20.888}$	$2^{18.283}$	$2^{18.223}$	$2^{18.346}$
	selective	$2^{18.031}$	$2^{17.960}$	$2^{18.106}$	$2^{17.528}$	$2^{17.427}$	$2^{17.634}$
eco-11	only-top	$2^{20.637}$	$2^{20.369}$	$2^{21.048}$	$2^{19.125}$	$2^{18.247}$	$2^{20.064}$
	full	$2^{24.492}$	$2^{24.489}$	$2^{24.495}$	$2^{20.790}$	$2^{20.742}$	$2^{20.825}$
	selective	$2^{20.710}$	$2^{20.659}$	$2^{20.747}$	$2^{19.890}$	$2^{19.797}$	$2^{19.954}$
f-633	only-top	$2^{9.716}$	$2^{9.568}$	$2^{10.654}$	$2^{9.502}$	$2^{9.329}$	$2^{10.460}$
	full	$2^{9.950}$	$2^{9.914}$	$2^{9.979}$	$2^{9.474}$	$2^{9.424}$	$2^{9.514}$
	selective	$2^{9.583}$	$2^{9.537}$	$2^{9.620}$	$2^{9.435}$	$2^{9.384}$	$2^{9.476}$
f-744	only-top	$2^{16.039}$	$2^{15.449}$	$2^{16.148}$	$2^{15.398}$	$2^{14.364}$	$2^{15.561}$
	full	$2^{16.286}$	$2^{16.278}$	$2^{16.313}$	$2^{15.424}$	$2^{15.409}$	$2^{15.472}$
	selective	$2^{15.560}$	$2^{15.546}$	$2^{15.604}$	$2^{14.458}$	$2^{14.427}$	$2^{14.550}$
katsura-11	only-top	$2^{21.797}$	$2^{18.644}$	$2^{22.331}$	$2^{21.747}$	$2^{18.356}$	$2^{22.257}$
	full	$2^{23.709}$	$2^{23.700}$	$2^{23.713}$	$2^{23.515}$	$2^{23.504}$	$2^{23.520}$
	selective	$2^{21.600}$	$2^{21.560}$	$2^{21.618}$	$2^{21.594}$	$2^{21.553}$	$2^{21.612}$
noon-8	only-top	$2^{15.849}$	$2^{15.847}$	$2^{20.145}$	$2^{14.541}$	$2^{14.537}$	$2^{19.993}$
	full	$2^{17.940}$	$2^{17.940}$	$2^{17.948}$	$2^{18.011}$	$2^{18.011}$	$2^{18.018}$
	selective	$2^{18.024}$	$2^{18.024}$	$2^{18.031}$	$2^{17.865}$	$2^{17.865}$	$2^{17.873}$
noon-9	only-top	$2^{18.401}$	$2^{18.400}$	$2^{23.045}$	$2^{16.756}$	$2^{16.755}$	$2^{22.881}$
	full	$2^{20.515}$	$2^{20.515}$	$2^{20.521}$	$2^{20.584}$	$2^{20.584}$	$2^{20.589}$
	selective	$2^{20.603}$	$2^{20.603}$	$2^{20.608}$	$2^{20.445}$	$2^{20.445}$	$2^{20.451}$
Random(10,2,2)	only-top	$2^{19.452}$	$2^{18.004}$	$2^{19.575}$	$2^{19.454}$	$2^{18.009}$	$2^{19.577}$
	full	$2^{17.659}$	$2^{17.616}$	$2^{17.761}$	$2^{17.660}$	$2^{17.617}$	$2^{17.762}$
	selective	$2^{17.655}$	$2^{17.611}$	$2^{17.757}$	$2^{17.656}$	$2^{17.613}$	$2^{17.758}$
Random(11,2,2)	only-top	$2^{21.620}$	$2^{20.097}$	$2^{21.727}$	$2^{21.621}$	$2^{20.101}$	$2^{21.729}$
	full	$2^{19.612}$	$2^{19.571}$	$2^{19.690}$	$2^{19.612}$	$2^{19.571}$	$2^{19.691}$
	selective	$2^{19.596}$	$2^{19.555}$	$2^{19.676}$	$2^{19.598}$	$2^{19.556}$	$2^{19.677}$

Table 4.4: The numbers of times of multiplications (inhomogeneous)

benchmark		ADD			RAT		
		SGB		RGB	SGB		RGB
		ALL	$\mathfrak{s}$-RED	ALL	ALL	$\mathfrak{s}$-RED	ALL
cyclic-7	only-top	$2^{24.401}$	$2^{24.275}$	$2^{24.438}$	$2^{23.994}$	$2^{23.820}$	$2^{24.042}$
	full	$2^{24.305}$	$2^{24.286}$	$2^{24.326}$	$2^{23.758}$	$2^{23.730}$	$2^{23.788}$
	selective	$2^{24.057}$	$2^{24.034}$	$2^{24.081}$	$2^{23.616}$	$2^{23.584}$	$2^{23.649}$
cyclic-8	only-top	$2^{31.140}$	$2^{30.971}$	$2^{31.143}$	$2^{30.132}$	$2^{29.769}$	$2^{30.138}$
	full	$2^{31.978}$	$2^{31.959}$	$2^{31.979}$	$2^{30.698}$	$2^{30.650}$	$2^{30.701}$
	selective	$2^{30.864}$	$2^{30.821}$	$2^{30.866}$	$2^{29.788}$	$2^{29.695}$	$2^{29.793}$
eco-10	only-top	$2^{23.162}$	$2^{22.849}$	$2^{23.661}$	$2^{22.403}$	$2^{21.843}$	$2^{23.161}$
	full	$2^{26.466}$	$2^{26.457}$	$2^{26.480}$	$2^{23.914}$	$2^{23.860}$	$2^{23.993}$
	selective	$2^{23.504}$	$2^{23.431}$	$2^{23.607}$	$2^{23.017}$	$2^{22.914}$	$2^{23.160}$
eco-11	only-top	$2^{26.551}$	$2^{26.256}$	$2^{26.932}$	$2^{25.409}$	$2^{24.679}$	$2^{26.136}$
	full	$2^{30.544}$	$2^{30.540}$	$2^{30.549}$	$2^{27.051}$	$2^{27.002}$	$2^{27.100}$
	selective	$2^{26.844}$	$2^{26.787}$	$2^{26.900}$	$2^{26.044}$	$2^{25.944}$	$2^{26.141}$
f-633	only-top	$2^{12.207}$	$2^{12.058}$	$2^{13.219}$	$2^{11.987}$	$2^{11.812}$	$2^{13.022}$
	full	$2^{12.554}$	$2^{12.513}$	$2^{12.608}$	$2^{12.112}$	$2^{12.057}$	$2^{12.186}$
	selective	$2^{12.187}$	$2^{12.134}$	$2^{12.257}$	$2^{12.064}$	$2^{12.006}$	$2^{12.140}$
f-744	only-top	$2^{20.627}$	$2^{20.098}$	$2^{20.762}$	$2^{19.945}$	$2^{19.005}$	$2^{20.153}$
	full	$2^{21.094}$	$2^{21.084}$	$2^{21.128}$	$2^{20.284}$	$2^{20.267}$	$2^{20.344}$
	selective	$2^{20.275}$	$2^{20.258}$	$2^{20.336}$	$2^{19.192}$	$2^{19.156}$	$2^{19.318}$
katsura-11	only-top	$2^{29.633}$	$2^{27.907}$	$2^{30.009}$	$2^{29.548}$	$2^{27.635}$	$2^{29.926}$
	full	$2^{32.170}$	$2^{32.162}$	$2^{32.175}$	$2^{31.969}$	$2^{31.961}$	$2^{31.976}$
	selective	$2^{29.932}$	$2^{29.897}$	$2^{29.958}$	$2^{29.907}$	$2^{29.871}$	$2^{29.934}$
noon-8	only-top	$2^{20.402}$	$2^{20.401}$	$2^{23.998}$	$2^{19.802}$	$2^{19.801}$	$2^{19.801}$
	full	$2^{22.128}$	$2^{22.128}$	$2^{22.279}$	$2^{22.231}$	$2^{22.231}$	$2^{22.373}$
	selective	$2^{22.169}$	$2^{22.169}$	$2^{22.316}$	$2^{22.059}$	$2^{22.059}$	$2^{22.218}$
noon-9	only-top	$2^{23.198}$	$2^{23.198}$	$2^{27.216}$	$2^{22.394}$	$2^{22.393}$	$2^{27.110}$
	full	$2^{25.029}$	$2^{25.029}$	$2^{25.220}$	$2^{25.140}$	$2^{25.140}$	$2^{25.317}$
	selective	$2^{25.076}$	$2^{25.076}$	$2^{25.261}$	$2^{24.969}$	$2^{24.969}$	$2^{25.167}$
Random(10,2,2)	only-top	$2^{27.035}$	$2^{26.085}$	$2^{27.103}$	$2^{27.036}$	$2^{26.087}$	$2^{27.104}$
	full	$2^{25.936}$	$2^{25.872}$	$2^{25.984}$	$2^{25.937}$	$2^{25.874}$	$2^{25.985}$
	selective	$2^{26.038}$	$2^{25.979}$	$2^{26.083}$	$2^{26.039}$	$2^{25.980}$	$2^{26.084}$
Random(11,2,2)	only-top	$2^{29.967}$	$2^{29.024}$	$2^{30.022}$	$2^{29.968}$	$2^{29.025}$	$2^{30.023}$
	full	$2^{28.831}$	$2^{28.770}$	$2^{28.867}$	$2^{28.831}$	$2^{28.770}$	$2^{28.867}$
	selective	$2^{28.937}$	$2^{28.880}$	$2^{28.970}$	$2^{28.938}$	$2^{28.882}$	$2^{28.972}$

Table 4.5: The numbers of generated S-pairs which satisfy **SF** compared to the numbers which do not satisfy **SF** (homogeneous)

	ADD		RAT	
benchmark	**SF**	not **SF**	**SF**	not **SF**
cyclic-7	477	465	477	265
cyclic-8	1515	4011	1515	2342
eco-10	417	507	417	135
eco-11	844	1517	844	303
f-633	46	7	46	2
f-744	380	354	380	158
katsura-11	884	1293	884	1245
noon-8	1336	40	1336	40
noon-9	3680	54	3680	54
HRandom(10,2,2)	778	144	778	144
HRandom(11,2,2)	1479	342	1479	342

Table 4.6: The numbers of generated S-pairs which satisfy **SF** compared to the numbers which do not satisfy **SF** (inhomogeneous)

	ADD		RAT	
benchmark	**SF**	not **SF**	**SF**	not **SF**
cyclic-7	475	467	475	267
cyclic-8	1504	4022	1504	2353
eco-10	315	629	315	130
eco-11	634	1849	634	283
f-633	46	7	46	2
f-744	333	229	333	160
katsura-11	884	1293	884	1245
noon-8	1336	40	1336	40
noon-9	3680	54	3680	54
Random(10,2,2)	778	144	778	144
Random(11,2,2)	1479	342	1479	342

Chapter 5

Conclusions

5.1 Contributions

This thesis is devoted to the followings:

- 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**. 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.

- We have introduced a new strategy for $\mathfrak{s}$-reduction, named the selective-full strategy, aiming to decrease the number of sum of $\mathfrak{s}$-reductions and usual reductions. Efficiency of the strategy has been evaluated by some Gröbner basis benchmarks. For computing the reduced Gröbner basis, the selective-full reduction strategy is more efficient comparing with conventional $\mathfrak{s}$-reduction strategies. For computing a signature Gröbner basis, the selective-full reduction strategy is better or equivalent to the full reduction strategy. Although, the selective-full strategy is not the

worst strategy in the three strategies in the case of all benchmarks in this paper.

5.2 Future works

We will aim to clarify the folowings:

- It is known that if an input system is regular sequence, singature-based algorithms with POT moudule order do not calculate zero reduction. When a module order other than POT is chosen, zero reductions happen even if an input system is regular. The calculations with POT has inefficiency for some input systems because the calculations proceed incrementally. Therefore, methods to detect zero reductions for regular input systems with a module order other than POT is required. We aim to establish the method.

- In cryptgraphy, Gröbner bases is used for attacking some cryptography. That means the security of cryptography is evaluated by algorithms of Gröbner bases. The input systems appeared in cryptography has characteristics, so we aim to establish methods to compute these problems efficiently.

Publications

Refereed papers

- Sakata, K.: An efficient reduction strategy for signature-based algorithms to compute Gröbner basis.: ACM Comunications in Computer Algebra, Vol.53, No.3, 2019.
- Sakata, K.: Simple signature-based algorithms with correctness and termination: Communications of Japan Society for Symbolic and Algebraic Computation, Vol.4, 1–31, 2020.

References

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

[2] Bardet, M., Faugère, J.-C., and Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations.: `http://www-salsa.lip6.fr/jcf/Papers/43BF.pdf`, November 2004.

[3] Buchberger, B.: Bruno Buchberger's PhD 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`

[4] Buchberger, B.: A criterion for detecting unnecessary reductions in the construction of Gröbner bases.: In *EUROSAM '79, An International Symposium on Symbolic and Algebraic Manipulation*, **72**, 3–21. Springer, 1979.

[5] Buchberger, B.: Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.: pages 184–232, 1985.

[6] Cox, D. A., Little, J., and O'Shea, D.: Using Algebraic Geometry, 2nd ed.: Graduate Texts in Mathematics, Springer Verlag, 2008.

[7] Cox, D. A., Little, J., and O'Shea, D.: Ideals, Varieties, and Algorithms, 3rd ed.: Undergraduate Texts in Mathematics, Springer, 2007.

[8] Eder, C., Perry, J.: F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases.: *Journal of Symbolic Computation*, **45**, 1442–1458, 2010.

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

[10] Eder, C. and Perry, J.: Signature-based Algorithms to Compute Gröbner Bases.: In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, 99–106, 2011.

[11] Eder, C.: Improving incremental signature-based Groebner bases algorithms.: *ACM SIGSAM Communications in Computer Algebra*, 47(1):1–13, 2013.

[12] 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.

[13] 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.

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

[15] Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4).: Journal of Pure and Applied Algebra 139, 61-88, June 1999.

[16] 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.

[17] 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.

[18] Faugère, J.-C. and Lachartre, S.: Parallel Gaussian Elimination for Gröbner bases computations in finite fields.: Proceedings of the 4th International Workshop on Parallel and Symbolic Computation, PASCO '10, pages 89–97, New York, NY, USA, July 2010.

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

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

[21] Gao, S., Guan, Y., and Volny IV, F.: A new incremental algorithm for computing Gröbner bases.: Proceedings of the 2010 international symposium on Symbolic and algebraic computation, pages 13–19. ACM, 2010.

[22] 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

[23] Gebauer, R. and Möller, H. M.: On an installation of Buchberger's algorithm.: Journal of Symbolic Computation, **6**, 275–286, October/December 1988.

[24] Mora, T. : An introduction to commutative and noncommutative Gröbner bases. : Journal of Symbolic Computation, **134**, 131–173, Novenmber 1994.

[25] 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)

[26] Stegers, T. : Faugère's F5 algorithm revisited. : Master's thesis, Technische Universtat Darmstadt, revised version 2007.

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

[28] 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.