A Signature-Based Algorithm for Computing Gröbner Bases in Solvable Polynomial Algebras *

Yao Sun[1,2], Dingkang Wang[1], Xiaodong Ma[1], Yang Zhang[3]
[1] KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China
[2] SKLOIS, Institute of Information Engineering, CAS, Beijing 100093, China
[3] Dept. of Mathematics, University of Manitoba, Winnipeg, MB R3T 2N2 Canada
sunyao@iie.ac.cn, (dwang, maxiaodong)@mmrc.iss.ac.cn, zhang39@cc.umanitoba.ca

ABSTRACT

Signature-based algorithms, including F5, F5C, G2V and GVW, are efficient algorithms for computing Gröbner bases in commutative polynomial rings. In this paper, we present a signature-based algorithm to compute Gröbner bases in solvable polynomial algebras which include usual commutative polynomial rings and some non-commutative polynomial rings like Weyl algebra. The generalized Rewritten Criterion (discussed in Sun and Wang, ISSAC 2011) is used to reject redundant computations. When this new algorithm uses the partial order implied by GVW, its termination is proved without special assumptions on computing orders of critical pairs. Data structures similar to F5 can be used to speed up this new algorithm, and Gröbner bases of syzygy modules of input polynomials can be obtained from the outputs easily. Experimental data show that most redundant computations can be avoided in this new algorithm.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms

General Terms

Algorithms

Keywords

Gröbner basis, signature-based algorithm, F5, GVW, solvable polynomial algebra.

1. INTRODUCTION

Gröbner bases were developed by Buchberger in 1965 [3]. Since then, many important improvements have been made to speed up the algorithms for computing Gröbner bases in usual commutative polynomial rings [4, 20, 21, 30]. One important improvement is Lazard pointed out the connection between Gröbner bases and linear algebra methods [26]. This idea is also implemented as the F4 algorithm by Faugère [14], and as XL type algorithms by Courtois et al. [7] and Ding et al. [10]. Up to now, Faugère's F5 algorithm [15] is one of the most efficient algorithms for computing Gröbner bases in commutative polynomial rings, and its variants and termination have been studied by Eder and Perry [11, 12, 13], Hashemi and Ars [22], Zobnin [37], Arri and Perry [2], and the authors [32, 33, 34]. Gao et al. proposed another signature-based algorithms G2V and GVW in [17, 18].

Computing Gröbner bases in non-commutative rings have also been widely investigated, for example, Weyl algebra [16], solvable polynomial algebras [25], free algebras [29, 31], rings of differential operators [24, 36, 28], G-algebra [27], PBW algebras [5, 19] and skew polynomial rings [6].

Due to the non-commutativity, it is difficult to reject redundant computations effectively, as well as to compute Gröbner bases for syzygy modules of input polynomials. In this paper, a signature-based algorithm is presented to compute Gröbner bases in solvable polynomial algebras. The generalized criterion proposed in [34] is extended to reject redundant computations in this non-commutative algebra, and its correctness is proved in a much simpler way. In this generalized criterion, the partial order implied by GVW is used, and the termination is proved without special assumptions on computing orders of critical pairs, while the termination of the original GVW is proved by assuming that the critical pair with minimal signature is always computed first [23]. During practical implementations, in order to improve the efficiency, this new algorithm can use a similar data structure to F5, and by using similar methods introduced in [35], we can also obtain Gröbner bases for syzygy modules of input polynomials from the outputs of this new algorithm easily. Experimental data show this new algorithm can reject most redundant critical pairs appearing in the computation.

This paper is organized as follows. Preliminaries about signature-based algorithms are given in Section 2. Algorithms are described in Section 3, and the related proofs come in Section 4. A simple example is presented in Section 5 to illustrate this new algorithm, and some experimental data are listed in Section 6. Conclusions follow in Section 7.

2. PRELIMINARIES

2.1 Notations

We first recall the definition of solvable polynomial alge-

*The first three authors are supported by NKBRPC 2011CB302400, NSFC 10971217, 60970152 and 61121062, and the last author is supported by Canadian NSERC.

ISSAC 2012, July 22–25, 2012, Grenoble, France.

bras. Let $\mathbb{N}$ be the set of non-negative integers, and $\prec$ be an admissible order on $\mathbb{N}^n$, i.e., a total order on $\mathbb{N}^n$ such that $0 \in \mathbb{N}^n$ is the smallest element and $\alpha \prec \beta$ implies $\alpha+\gamma \prec \beta+\gamma$ for all $\alpha, \beta, \gamma \in \mathbb{N}^n$. For n indeterminates $\{x_1, \ldots, x_n\}$, the standard power product set is defined as $\mathbb{M} = \{x^\alpha = x_1^{a_1} \cdots x_n^{a_n} \mid \alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n\}$. We say $x^\alpha \prec x^\beta$ if $\alpha \prec \beta$. Let k be a field. For any finite sum $0 \neq f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, where $c_\alpha \in k$, the multi-degree of f is defined as $\mathrm{mdeg}(f) := \max_\prec\{\alpha \mid c_\alpha \neq 0\} \in \mathbb{N}^n$.

Let R be a finitely generated k-algebra with n generators $\{x_1, \ldots, x_n\}$. R is called a **solvable polynomial algebra** if R satisfies (i) $\mathbb{M}$ is a k-basis of R, (ii) for any $0 \leq i \leq j \leq n$, there exist $0 \neq c_{ij} \in k$ and $p_{ij} \in R$ such that $x_j x_i = c_{ij} x_i x_j + p_{ij}$ and $x^{\mathrm{mdeg}(p_{ij})} \prec x_i x_j$. Clearly, every element in R has a unique form $\sum c_\alpha x^\alpha$, and moreover, for any $f, g \in R$, we have $\mathrm{mdeg}(fg) = \mathrm{mdeg}(gf)$. If $f = c_\alpha x^\alpha + f' \in R$, where $\mathrm{mdeg}(f') \prec \mathrm{mdeg}(f) = \alpha$, we define $\mathrm{lpp}(f) := x^\alpha$ and $\mathrm{lc}(f) := c_\alpha$.

It is well-known that solvable polynomial algebras include many important non-commutative algebras like the Weyl algebra $\mathbb{A}_n(k)$, the enveloping algebra of any finite dimensional Lie algebra and a fairly large class of quantum groups.

A **left ideal** $\mathcal{I}$ generated by $F \subset R$ in R is defined as: $\mathcal{I} := \langle F \rangle = \{\sum_{f \in F} p_f f \mid p_f \in R\}$. Only *left ideals* are considered in current paper, so we usually say "ideal" instead of "left ideal" for short.

For any $x^\alpha, x^\beta \in R$, we say that x^α **divides** x^β if $\beta - \alpha \in \mathbb{N}^n$. If x^α divides x^β, $x^{\beta-\alpha}$ is called a **quotient** of x^β and x^α, denoted by $x^{\beta-\alpha} := x^\beta / x^\alpha$. Note that, in solvable polynomial algebra R, the relation $x^{\beta-\alpha}x^\alpha = x^\beta$ usually does *not* hold, but we always have $\mathrm{lpp}(x^{\beta-\alpha}x^\alpha) = x^\beta$. Given a left ideal $\mathcal{I}$ in R, its Gröbner basis is defined as following:

Definition 2.1 *Let $\mathcal{I}$ be a left ideal in R and G be a finite subset of $\mathcal{I} \setminus \{0\}$. Then G is a Gröbner basis of $\mathcal{I}$ w.r.t. $\prec$ iff for all $f \in \mathcal{I}$, there exists $g \in G$ such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$.*

Note that when R is a usual commutative polynomial ring, the above definition is consistent with the usual definition of a Gröbner basis.

2.2 Signature

Let $\mathbf{f} := (f_1, \cdots, f_m) \in R^m$. We want to compute a Gröbner basis for the following left ideal

$$\mathcal{I} := \langle f_1, \ldots, f_m \rangle$$

$$= \{\mathbf{u} \cdot \mathbf{f} = p_1 f_1 + \cdots + p_m f_m \mid \mathbf{u} = (p_1, \ldots, p_m) \in R^m\}$$

with respect to some term order on R.

Given $f \in \mathcal{I}$ and $\mathbf{u} \in R^m$ such that $f = \mathbf{u} \cdot \mathbf{f}$, we use the notation $f^{[\mathbf{u}]}$ to express this relation between f and $\mathbf{u}$. Computations on $f^{[\mathbf{u}]}$ can be defined naturally. Let $f, g \in \mathcal{I}$ and $\mathbf{u}, \mathbf{v} \in R^m$ such that $f = \mathbf{u} \cdot \mathbf{f}$ and $g = \mathbf{v} \cdot \mathbf{f}$, c be a constant in k and t be a power product in R. Then $f^{[\mathbf{u}]} + g^{[\mathbf{v}]} = (f+g)^{[\mathbf{u}+\mathbf{v}]}$, and $ct(f^{[\mathbf{u}]}) = (ctf)^{[ct\mathbf{u}]}$. These operations are well defined, i.e., $f + g = (\mathbf{u} + \mathbf{v}) \cdot \mathbf{f}$ and $ctf = (ct\mathbf{u}) \cdot \mathbf{f}$ due to the distributivity of R. In fact, any $f^{[\mathbf{u}]}$ such that $f = \mathbf{u} \cdot \mathbf{f}$ is an element of the R-module: $\{f^{[\mathbf{u}]} \mid f = \mathbf{u} \cdot \mathbf{f} \text{ and } \mathbf{u} \in R^m\} = \{p_1 f_1^{[\mathbf{e}_1]} + \cdots + p_m f_m^{[\mathbf{e}_m]} \mid p_1, \cdots, p_m \in R\}$, where $\mathbf{e}_i$ is the i-th unit vector of R^m, i.e., $(\mathbf{e}_i)_j = \delta_{ij}$ where δ_{ij} is the Kronecker delta.

In order to make the notation $f^{[\mathbf{u}]}$ easier to be understood, we also call $f^{[\mathbf{u}]}$ **an element in $\mathcal{I}$ and write $f^{[\mathbf{u}]} \in \mathcal{I}$**. Besides, **the notation $f^{[\mathbf{u}]}$ always means $f \in \mathcal{I}$ and $f = \mathbf{u} \cdot \mathbf{f}$ in this paper**. For any $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ in $\mathcal{I}$, we say $f^{[\mathbf{u}]} = g^{[\mathbf{v}]}$ only if $f = g$ and $\mathbf{u} = \mathbf{v}$ hold at the same time.

Fix *any* term order $\prec_1$ on R and *any* term order $\prec_2$ on R^m. We must emphasize that the order $\prec_2$ may or may not be related to $\prec_1$ in general, although $\prec_2$ is usually an extension of $\prec_1$ to R^m in implementation. For example, the term order $\prec_2$ on R^m can be a POT (position over term) extension of $\prec_1$, i.e., $x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_j$, if either $i > j$, or $i = j$ and $x^\alpha \prec_1 x^\beta$.

With order $\prec_2$, we can define the leading power product (lpp), leading coefficient (lc), "divide", and "quotient" in R^m similarly. For more terminologies on "module", we refer the readers to Chapter 5 of [8].

For sake of convenience, we use $\prec$ to represent $\prec_1$ on R and $\prec_2$ on R^m if no confusion occurs. In current paper, elements in R are expressed by letters f, g, h; while elements in R^m are denoted by boldface letters such as $\mathbf{u}, \mathbf{v}, \mathbf{w}$. We make the convention that if $f = 0$ then $\mathrm{lpp}(f) = 0$ and $0 \prec t$ for any non-zero power product t in R.

For any $f^{[\mathbf{u}]} \in \mathcal{I}$, we define $\mathrm{lpp}(\mathbf{u})$ as the **signature** of $f^{[\mathbf{u}]}$. The original definition of signature is introduced by Faugère in [15], and recently, Gao et al. give a generalized definition of signature in [18]. In current paper, we use the definition given by Gao et al.

2.3 Strong Gröbner Bases

Let $G := \{g_1^{[\mathbf{v}_1]}, \ldots, g_s^{[\mathbf{v}_s]}\}$ be a finite subset of $\mathcal{I}$. We call G a **strong Gröbner basis** of $\mathcal{I}$, if for any $f^{[\mathbf{u}]} \in \mathcal{I}$, there exists $g^{[\mathbf{v}]} \in G$ such that

1. $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$, and
2. $\mathrm{lpp}(tg) \preceq \mathrm{lpp}(f)$, where $t = \mathrm{lpp}(\mathbf{u})/\mathrm{lpp}(\mathbf{v})$.

A finite strong Gröbner basis exists for any left ideal $\mathcal{I}$ by Theorem 3.5. The above definition of a strong Gröbner basis is simpler than the definition of a strong Gröbner basis in [18], and it is easy to show both definitions are equivalent. A strong Gröbner basis of $\mathcal{I}$ has the following property.

Proposition 2.2 *If G is a strong Gröbner basis of $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$, then (1) the set $\{g \mid g^{[\mathbf{v}]} \in G\}$ is a Gröbner basis of $\mathcal{I}$ w.r.t. $\prec_1$; and (2) the set $\{\mathbf{v} \mid g^{[\mathbf{v}]} \in G \text{ and } g = 0\}$ is a Gröbner basis of the syzygy module $\{(p_1, \ldots, p_m) \in R^m \mid p_1 f_1 + \cdots + p_m f_m = 0\}$ w.r.t. $\prec_2$.*

Proof. We prove (1) by contradiction. Let $E := \{0 \neq f \in \mathcal{I} \mid \text{there does not exist } g^{[\mathbf{v}]} \in G \text{ such that } \mathrm{lpp}(g) \text{ divides } \mathrm{lpp}(f)\}$, $N := \{f^{[\mathbf{u}]} \in \mathcal{I} \mid \mathbf{u} \cdot (f_1, \cdots, f_m) = f, f \in E\}$, and $f^{[\mathbf{u}]} \in N$ be an element with the *minimal signature* in N w.r.t. $\prec_2$. Then by the definition of strong Gröbner basis, there exists $g^{[\mathbf{v}]} \in G$ such that $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$, and $\mathrm{lpp}(tg) \preceq \mathrm{lpp}(f)$, where $t = \mathrm{lpp}(\mathbf{u})/\mathrm{lpp}(\mathbf{v})$. If $\mathrm{lpp}(tg) = \mathrm{lpp}(f)$, then this contradicts the fact that f is in E. Otherwise, we get $\mathrm{lpp}(tg) \prec \mathrm{lpp}(f)$. For $\bar{f}^{[\bar{\mathbf{u}}]} := f^{[\mathbf{u}]} - ct(g^{[\mathbf{v}]}) \in \mathcal{I}$ where $c = \mathrm{lc}(\mathbf{u})/\mathrm{lc}(t\mathbf{v})$, since $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(f)$, we will have $\bar{f} \in E$ and $\bar{f}^{[\bar{\mathbf{u}}]} \in N$. However, as $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(\mathbf{u})$, this is a contradiction that $f^{[\mathbf{u}]}$ has the minimal signature in N.

Next we prove (2). For any nonzero $\mathbf{u} = (p_1, \ldots, p_m) \in R^m$ such that $p_1 f_1 + \cdots + p_m f_m = 0$, we have $0^{[\mathbf{u}]} \in \mathcal{I}$. Then by the definition of strong Gröbner basis, there exists $g^{[\mathbf{v}]} \in G$ such that $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$, and $\mathrm{lpp}(tg) \preceq 0$, where $t = \mathrm{lpp}(\mathbf{u})/\mathrm{lpp}(\mathbf{v})$. So we have $g = 0$, and $0^{[\mathbf{v}]} \in G$. □

The following deduced definition and proposition will be used in the proofs in Section 4.

Let $\mathcal{I} := \langle f_1, \ldots, f_m \rangle$, and $\mathbf{t} := x^\alpha \mathbf{e}_i$ be a term in R^m. We say $G \subset \mathcal{I}$ is a **strong Gröbner basis**$_{\prec \mathbf{t}}$ of $\mathcal{I}$, if for any $f^{[\mathbf{u}]} \in \mathcal{I}$ with $\mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$, there exists $g^{[\mathbf{v}]} \in G$ such that (1) $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$, and (2) $\mathrm{lpp}(tg) \preceq \mathrm{lpp}(f)$, where $t = \mathrm{lpp}(\mathbf{u})/\mathrm{lpp}(\mathbf{v})$.

Proposition 2.3 *Let $\mathcal{I} := \langle f_1, \cdots, f_m \rangle$ and $\mathbf{t} := x^\alpha \mathbf{e}_i$ be a term in R^m. If G is a strong Gröbner basis$_{\prec \mathbf{t}}$ of $\mathcal{I}$, then for any $f^{[\mathbf{u}]} \in \mathcal{I}$ with $\mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$ and $f \neq 0$, there exists $g^{[\mathbf{v}]} \in G$, such that*

1. *$\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$, and*
2. *$\mathrm{lpp}(t\mathbf{v}) \preceq \mathrm{lpp}(\mathbf{u})$, where $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$.*

Note that in the definition of a strong Gröbner basis, the first condition is "$\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$"; while in the above proposition, it is "$\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$".

Proof. We prove this proposition by contradiction. Let $N := \{f^{[\mathbf{u}]} \in \mathcal{I} \mid f \neq 0, \mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$, and there do not exist $g^{[\mathbf{v}]} \in G$ and power product t_g such that $\mathrm{lpp}(t_g g) = \mathrm{lpp}(f)$ and $\mathrm{lpp}(t_g \mathbf{v}) \preceq \mathrm{lpp}(\mathbf{u})\}$, and let $f^{[\mathbf{u}]} \in N$ be an element with the *minimal signature* in N. Since G is a strong Gröbner basis$_{\prec \mathbf{t}}$ of $\mathcal{I}$ and $\mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$, there exists $g^{[\mathbf{v}]} \in G$ such that $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{u})$, and $\mathrm{lpp}(tg) \preceq \mathrm{lpp}(f)$ where $t = \mathrm{lpp}(\mathbf{u})/\mathrm{lpp}(\mathbf{v})$. Note that $\mathrm{lpp}(t\mathbf{v}) = \mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$. If $\mathrm{lpp}(tg) = \mathrm{lpp}(f)$, then it implies $f^{[\mathbf{u}]} \notin N$, which is a contradiction. Otherwise, we get $\mathrm{lpp}(tg) \prec \mathrm{lpp}(f)$. For $\bar{f}^{[\bar{\mathbf{u}}]} := f^{[\mathbf{u}]} - ct(g^{[\mathbf{v}]}) \in \mathcal{I}$ where $c = \mathrm{lc}(\mathbf{u})/\mathrm{lc}(t\mathbf{v})$, then $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(f)$ and $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(\mathbf{u}) \prec \mathbf{t}$. Since $f^{[\mathbf{u}]}$ has the minimal signature in N, we have $\bar{f}^{[\bar{\mathbf{u}}]} \notin N$. So for this $\bar{f}^{[\bar{\mathbf{u}}]} \in \mathcal{I}$, there exists $h^{[\mathbf{w}]} \in G$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(f)$, and $\mathrm{lpp}(t_h \mathbf{w}) \preceq \mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(\mathbf{u})$, where $t_h = \mathrm{lpp}(\bar{f})/\mathrm{lpp}(h)$. This contradicts $f^{[\mathbf{u}]} \in N$. □

3. ALGORITHM

3.1 Criterion

Now, it is the time to define the *critical pair* of two elements. Suppose $f^{[\mathbf{u}]}, g^{[\mathbf{v}]}$ are two elements such that both f and g are *nonzero*. Assume $\mathrm{lpp}(f) = x^\alpha = x_1^{a_1} \cdots x_n^{a_n}$ and $\mathrm{lpp}(g) = x^\beta = x_1^{b_1} \cdots x_n^{b_n}$. The **least common multiple of** $\mathrm{lpp}(f)$ **and** $\mathrm{lpp}(g)$ is defined as $\mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g)) := x^{(\max\{a_1,b_1\},\cdots,\max\{a_n,b_n\})}$. We can also define least common multiples for terms in R^m in a similar way. Let $t := \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$, $t_f := t/\mathrm{lpp}(f)$ and $t_g := t/\mathrm{lpp}(g)$, if $\mathrm{lpp}(t_f \mathbf{u}) \succeq \mathrm{lpp}(t_g \mathbf{v})$, then the *ordered* 4-tuple vector $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is called the **critical pair** of $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$, and its corresponding **S-polynomial** is $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$ where $c = \mathrm{lc}(t_f f)/\mathrm{lc}(t_g g)$. Please keep in mind that, for any critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$, we always have $\mathrm{lpp}(t_f \mathbf{u}) \succeq \mathrm{lpp}(t_g \mathbf{v})$. Particularly, a critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is said to be **regular** if $\mathrm{lpp}(t_f \mathbf{u}) \succ \mathrm{lpp}(t_g \mathbf{v})$.

For convenience, the critical pair of $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ is sometimes denoted by $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ or $[g^{[\mathbf{v}]}, f^{[\mathbf{u}]}]$ for short. Please note that, we *only* care about the order of $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ in the form $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$, but we *do not* care about this order in the simple form $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$. We also say that $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is a critical pair of B if both $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ are in B.

For a finite set $B \subset \mathcal{I}$, "$<_B$" is a **partial order** defined on B in general sense, i.e. " $<_B$ " has non-reflexivity, antisymmetry, and transitivity. The subscript B of "$<_B$" means the partial order $<_B$ is defined on the set B. For more details about the partial order, we refer to [34].

Definition 3.1 (Rewritten Criterion) *Let B be a subset of $\mathcal{I}$, $<_B$ be a partial order on B, $f^{[\mathbf{u}]}$ be an element in B, and t be a power product in R. $t(f^{[\mathbf{u}]})$ is called* **rewritable** *by B if there exists $g^{[\mathbf{v}]} \in B$ such that*

1. *$\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(t\mathbf{u})$, and*
2. *$g^{[\mathbf{v}]} <_B f^{[\mathbf{u}]}$.*

In particular, a **critical pair** $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ **of** B is called **rewritable** by B if *either* $t_f(f^{[\mathbf{u}]})$ *or* $t_g(g^{[\mathbf{v}]})$ is rewritable by B. The critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of B is said to be rejected by Rewritten Criterion w.r.t. B if $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is rewritable by B.

$f^{[\mathbf{u}]} \in \mathcal{I}$ is said to be a **syzygy element** in $\mathcal{I}$ if $f = 0$. Similar to F5 and GVW, in order to enhance Rewritten Criterion, we can add known syzygy elements to B, and assume that syzygy elements are *smaller* than non-syzygy elements in B under the partial order $<_B$ such that more redundant computations can be avoided. Please notice that, for any two elements f and g in the solvable polynomial algebra R, the relation $gf - fg = 0$ does not always hold. That is, if $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in \mathcal{I}$, the element $g(f^{[\mathbf{u}]}) - f(g^{[\mathbf{v}]}) = (gf - fg)^{[g\mathbf{u} - f\mathbf{v}]}$ may not be a syzygy element in $\mathcal{I}$.

The following theorem is the main result of this paper, and it is an extended version of the main result in [34]. The detailed proof will be given in Subsection 4.1.

Theorem 3.2 (Correctness) *Let G be a* finite *subset of the ideal $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$, and $<_G$ be* any *partial order on G. Then G is a strong Gröbner basis of $\mathcal{I}$ if both the following two conditions hold:*

1. *For any $1 \leq i \leq m$, there exists $f^{[\mathbf{u}]} \in G$ such that $\mathrm{lpp}(\mathbf{u}) = \mathbf{e}_i$, and*
2. *Every* regular critical pair *of G is rewritable by G.*

In Theorem 3.2, the order $<_G$ can be **any** partial order.

3.2 Algorithm

Theorem 3.2 induces an algorithm to compute a strong Gröbner basis for $\mathcal{I}$ directly. We start with the set $G_0 := \{f_1^{[\mathbf{e}_1]}, \ldots, f_m^{[\mathbf{e}_m]}\}$. If every regular critical pair of G_0 is rewrit- able by G_0, then G_0 is a strong Gröbner basis. Otherwise, if there exists a *regular* critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G_0 such that it is *not* rewritable by G_0, then we *create* an $h^{[\mathbf{w}]}$ from $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ such that $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is rewritable by $\{h^{[\mathbf{w}]}\}$. Next, we expand G_0 to $G_1 := G_0 \cup \{h^{[\mathbf{w}]}\}$ and repeat the above discussions on *regular* critical pairs of G_1. The set G_i can be expanded repeatedly in this way until all regular critical pairs of some G_s are rewritable by G_s.

There is only one question left: *how to create an $h^{[\mathbf{w}]}$ from a regular critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G_i such that $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is rewritable by $\{h^{[\mathbf{w}]}\}$?*

All existing signature-based algorithms for computing Gröbner bases in polynomial rings solve the above problem by using a special reduction and an *admissible* partial order on G ("admissible" will be defined later).

Now, let us consider the special reduction.

Definition 3.3 *$f^{[\mathbf{u}]}$ is said to be **reducible** by $h^{[\mathbf{w}]} \in G$ if*

1. $\mathrm{lpp}(h)$ *divides* $\mathrm{lpp}(f)$, *and*
2. $\mathrm{lpp}(t\mathbf{w}) \prec \mathrm{lpp}(\mathbf{u})$ *where* $t = \mathrm{lpp}(f)/\mathrm{lpp}(h)$.

*If $f^{[\mathbf{u}]}$ is reducible by $h^{[\mathbf{w}]} \in G$, then $f^{[\mathbf{u}]} \longmapsto_G f^{[\mathbf{u}]} - ct(h^{[\mathbf{w}]})$ is said to be a **one-step-reduction** by G where $c = \mathrm{lc}(f)/\mathrm{lc}(th)$ and $t = \mathrm{lpp}(f)/\mathrm{lpp}(h)$.*

$f^{[\mathbf{u}]}$ is said to be **reduced to** *$f'^{[\mathbf{u}']}$* **by** *G if $f'^{[\mathbf{u}']}$ is obtained by several one-step-reductions from $f^{[\mathbf{u}]}$, and $f'^{[\mathbf{u}']}$ is not reducible by G.*

The following result follows directly from above definition.

Proposition 3.4 *Let $f^{[\mathbf{u}]}$ be an element in $\mathcal{I} = \langle f_1, \ldots, f_m\rangle$, and G be a subset of $\mathcal{I}$. If $f^{[\mathbf{u}]}$ is reduced to $f'^{[\mathbf{u}']}$ by G, then $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(\mathbf{u}')$ and $\mathbf{u}' \cdot (f_1, \ldots, f_m) = f'$.*

If the S-polynomial of a regular critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G is reduced to $h^{[\mathbf{w}]}$ by G, then we have $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(\mathbf{w})$ by above proposition. To make $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ rewritable by $h^{[\mathbf{w}]}$, by the definition of rewritable, we only need $h^{[\mathbf{w}]}$ is *smaller* than $f^{[\mathbf{u}]}$ under the partial order on $G \cup \{h^{[\mathbf{w}]}\}$.

A partial order "$<_G$" on G is **admissible** if for any *regular* critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G, *whenever* we need to reduce the S-polynomial of $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ to $h^{[\mathbf{w}]}$ by G, we always have $h^{[\mathbf{w}]} <_{G\cup\{h^{[\mathbf{w}]}\}} f^{[\mathbf{u}]}$ after expanding "$<_G$" to $G \cup \{h^{[\mathbf{w}]}\}$. We have shown in [34] that the partial orders implied by criteria of F5 and GVW are both admissible. In particular, the new algorithm in this paper will use the following GVW-order.

GVW-order: For any $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G$, we define $g^{[\mathbf{v}]} <_G f^{[\mathbf{u}]}$ if one of the following two conditions holds:
(a) $\mathrm{lpp}(t'g) \prec \mathrm{lpp}(tf)$, where $t' = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{v})}$ and $t = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{u})}$ such that $\mathrm{lpp}(t\mathbf{u}) = \mathrm{lpp}(t'\mathbf{v})$.
(b) $\mathrm{lpp}(t'g) = \mathrm{lpp}(tf)$ and $g^{[\mathbf{v}]}$ is added to G later than $f^{[\mathbf{u}]}$.

The algorithm SGB deduced from Theorem 3.2 computes a strong Gröbner basis for the ideal $\mathcal{I} = \langle f_1, \ldots, f_m\rangle$ in the solvable polynomial algebra R.

In the algorithm SGB, $\mathrm{SPoly}([f^{[\mathbf{u}]}, g^{[\mathbf{v}]}])$ refers to the S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$. There are several useful facts:

(A). Since only signatures of elements in $\mathcal{I}$ are used in the definitions of regular critical pairs, rewritable and reducible, similar to F5, for sake of efficiency, for all elements in $\mathcal{I}$ appearing in the algorithm SGB, such as $f^{[\mathbf{u}]}, g^{[\mathbf{v}]}$ and $h^{[\mathbf{w}]}$, **it suffices to use the data structure** $(\mathrm{lpp}(\mathbf{u}), f)$**,** $(\mathrm{lpp}(\mathbf{v}), g)$ **and** $(\mathrm{lpp}(\mathbf{w}), h)$ **to express them in practical implementations**.

(B). Using algorithms in Subsection 3.3, elements, such as $f^{[\mathbf{u}]}$, can be recovered from the data structure $(\mathrm{lpp}(\mathbf{u}), f)$. By Proposition 2.2, a Gröbner basis of $\mathcal{I}$ and a Gröbner basis of the syzygy module $\{(p_1, \ldots, p_m) \in R^m \mid p_1f_1 + \cdots + p_mf_m = 0\}$ can be obtained directly.

(C). Rewritten Criterion uses a partial order defined on G. While new elements are added to G (line ended with (3)), the partial order on G needs to be updated simultaneously. Fortunately, most partial orders, such as GVW-order, can be updated automatically.

(D). For the line ended with (1), we emphasize that **any** critical pair can be selected.

(E). In line marked with (2), we can append the codes

$$G \longleftarrow G \setminus \{f^{[\mathbf{u}]} \in G \mid f^{[\mathbf{u}]} \text{ is } \mathbf{rewritable} \text{ by } h^{[\mathbf{w}]}\}$$

to remove redundant elements from G. This step will not affect the correctness of the algorithm. An element $f^{[\mathbf{u}]}$ is removed from G only if there is an $h^{[\mathbf{w}]}$ such that $f^{[\mathbf{u}]}$ is rewritable by $h^{[\mathbf{w}]}$. In this case, any regular critical pair involving $f^{[\mathbf{u}]}$ is rewritable by $h^{[\mathbf{w}]}$, and any regular critical pair that is rewritable by $f^{[\mathbf{u}]}$ is also rewritable by $h^{[\mathbf{w}]}$.

Algorithm 1: Algorithm for computing Strong Gröbner bases in solvable polynomial algebras (SGB)

Input : $f_1^{[\mathbf{e}_1]}, \ldots, f_m^{[\mathbf{e}_m]}$.
Output: A strong Gröbner basis G of $\langle f_1, \ldots, f_m\rangle$.
begin
  $G \longleftarrow \{f_i^{[\mathbf{e}_i]} \mid i = 1, \ldots, m\}$
  $CPairs \longleftarrow \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] \text{ is } \mathbf{regular} \mid \forall\, f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G\}$
  while $CPairs \neq \emptyset$ **do**
    $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]}) \longleftarrow$ **any** critical pair in $CPairs$ (1)
    $CPairs \longleftarrow CPairs \setminus \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]\}$
    if $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ *is* **not rewritable** *by* G **then**
      $h^{[\mathbf{w}]} \longleftarrow$ reduce $\mathrm{SPoly}([f^{[\mathbf{u}]}, g^{[\mathbf{v}]}])$ by G (2)
      $CPairs \longleftarrow CPairs \cup \{[h^{[\mathbf{w}]}, h'^{[\mathbf{w}']}] \text{ is } \mathbf{regular} \mid h'^{[\mathbf{w}']} \in G\}$
      $G \longleftarrow G \cup \{h^{[\mathbf{w}]}\}$ (3)
  return G

Theorem 3.5 (Termination) *The algorithm SGB terminates after a finite number of steps if GVW-order is used in Rewritten Criterion, and the term orders $\prec_1$ on R and $\prec_2$ on R^m are compatible, which means that $x^\alpha \prec_1 x^\beta$ if and only if $x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_i$ for all $1 \le i \le m$.*

Theorem 3.5 shows the termination of the algorithm SGB does not depend on computing orders of critical pairs. The proof for the above theorem is given in Subsection 4.2.

3.3 Recover $f^{[\mathbf{u}]}$ from $(\mathrm{lpp}(\mathbf{u}), f)$

If we use the data structure $(\mathrm{lpp}(\mathbf{u}), f)$ instead of $f^{[\mathbf{u}]}$ to express elements in G, the algorithm SGB will be more efficient, and we can also derive a Gröbner basis for $\mathcal{I}$ from the data structure $(\mathrm{lpp}(\mathbf{u}), f)$ according to Proposition 2.2. However, we cannot get a Gröbner basis for the syzygy module $\{(p_1, \ldots, p_m) \in R^m \mid p_1f_1 + \cdots + p_mf_m = 0\}$ from the data structure $(\mathrm{lpp}(\mathbf{u}), f)$ directly. So we need methods of recovering $f^{[\mathbf{u}]}$ from $(\mathrm{lpp}(\mathbf{u}), f)$. The methods in this subsection are slight revisions of methods in [35].

Proposition 3.6 *Let $S = \{(\mathbf{t}_1, g_1), \ldots, (\mathbf{t}_s, g_s)\}$ be the set returned by Algorithm SGB through using the data structure $(\mathrm{lpp}(\mathbf{u}), f)$ instead of $f^{[\mathbf{u}]}$. Then the algorithm RecoverSGB constitutes a strong Gröbner basis $\{g_1^{[\mathbf{v}_1]}, \ldots, g_s^{[\mathbf{v}_s]}\}$ for $\langle f_1, \ldots, f_m\rangle$ such that $\mathrm{lpp}(\mathbf{v}_i) = \mathbf{t}_i$, where $i = 1, \ldots, s$.*

The above proposition can be proved by Corollary 3.2 and Theorem 3.5 of [35] after a slight modification. Due to the page limit, we omit the proof.

Algorithm 2: RecoverSGB

Input : $S = \{(\mathbf{t}_1, g_1), \ldots, (\mathbf{t}_s, g_s)\}$ returned by the algorithm SGB.

Output: $G = \{g_1^{[\mathbf{v}_1]}, \ldots, g_s^{[\mathbf{v}_s]}\}$ a strong Gröbner basis of $\mathcal{I} = \langle f_1, \ldots, f_m\rangle$ s.t. $\mathrm{lpp}(\mathbf{v}_i) = \mathbf{t}_i$.

begin
  $G \longleftarrow \emptyset$;
  while $S \neq \emptyset$ **do**
    $(x^\alpha \mathbf{e}_j, f) \longleftarrow$ $x^\alpha \mathbf{e}_j$ is minimal in S, i.e., $x^\alpha \mathbf{e}_j \preceq \mathbf{t}_i$, for $\forall (\mathbf{t}_i, g_i) \in S$;
    $S \longleftarrow S \setminus \{(x^\alpha \mathbf{e}_j, f)\}$;
    $g \longleftarrow \mathrm{IncSF}(x^\alpha \mathbf{e}_j, f, S)$;
    $g_0 \longleftarrow \mathrm{IncSF}(x^\alpha \mathbf{e}_j, x^\alpha f_j, S)$;
    if $g \neq 0$ **then** $c \longleftarrow \mathrm{lc}(g)/\mathrm{lc}(g_0)$; **else** $c \longleftarrow 1$; **end if**
    $(p_1, \ldots, p_t) \longleftarrow \mathrm{Rep}(cx^\alpha \mathbf{e}_j, f, G)$(where $t = \#G$);
    $\mathbf{u} \longleftarrow cx^\alpha \mathbf{e}_j + \sum p_i \mathbf{v}_i$ where $g_i^{[\mathbf{v}_i]} \in G$;
    $G \longleftarrow G \cup \{f^{[\mathbf{u}]}\}$;
  return G.

In the above algorithm, we need two functions Rep$(\cdot)$ and IncSF$(\cdot)$.

The function $\mathrm{Rep}(cx^\alpha \mathbf{e}_j, f, G = \{g_1^{[\mathbf{v}_1]}, \ldots, g_t^{[\mathbf{v}_t]}\})$ computes a set $\{p_1, \ldots, p_t\} \subset R$ such that $f = cx^\alpha f_j + p_1 g_1 + \cdots + p_t g_t$ where $x^\alpha \mathbf{e}_j \succ \mathrm{lpp}(p_i \mathbf{v}_i)$ and $g_i^{[\mathbf{v}_i]} \in G$ for $i = 1, \ldots, t$. Corollary 3.2 of [35] assures that the p_i's always exist in the algorithm RecoverSGB .

Function Rep$(\cdot)$.

Step 1: Let $p_i := 0$ for $i = 1, \ldots, t$, and $h := f - cx^\alpha f_j$.

Step 2: If there exists $g_i^{[\mathbf{v}_i]} \in G$ s.t. $\mathrm{lpp}(g_i)$ divides $\mathrm{lpp}(h)$ and $\mathrm{lpp}(t\mathbf{v}_i) \prec x^\alpha \mathbf{e}_j$, where $t = \mathrm{lpp}(h)/\mathrm{lpp}(g_i)$, then set $p_i := p_i + (\mathrm{lc}(h)/\mathrm{lc}(tg_i))t$, and $h := h - (\mathrm{lc}(h)/\mathrm{lc}(tg_i))tg_i$.

Step 3: If $h \neq 0$, then goto step 2.

Step 4: Return $\{p_1, \ldots, p_t\}$.

The function $\mathrm{IncSF}(x^\alpha \mathbf{e}_j, f, S = \{(\mathbf{t}_1, g_1), \ldots, (\mathbf{t}_s, g_s)\})$ computes an *incomplete standard form* (see [35] for definition) g for $x^\alpha \mathbf{e}_j$ such that $g = f + p_1 g_1 + \cdots + p_t g_t$ where $p_1, \ldots, p_t \in R$, $x^\alpha \mathbf{e}_j \succ \mathrm{lpp}(p_i \mathbf{t}_i)$ and $(\mathbf{t}_i, g_i) \in S$ for $i = 1, \ldots, t$, and there do not exist $(\mathbf{t}_i, g_i) \in S$ and power product t, s.t. $\mathrm{lpp}(tg_i) = \mathrm{lpp}(g)$ and $\mathrm{lpp}(t\mathbf{t}_i) \prec x^\alpha \mathbf{e}_j$.

Function IncSF$(\cdot)$.

Step 1: Let $g := f$.

Step 2: If there exists $(\mathbf{t}_i, g_i) \in S$ s.t. $\mathrm{lpp}(g_i)$ divides $\mathrm{lpp}(g)$ and $\mathrm{lpp}(t\mathbf{t}_i) \prec x^\alpha \mathbf{e}_j$, where $t = \mathrm{lpp}(g)/\mathrm{lpp}(g_i)$, then set $g := g - (\mathrm{lc}(g)/\mathrm{lc}(tg_i))tg_i$; Otherwise, return g.

Step 3: If $g \neq 0$, then goto step 2; otherwise, return 0.

For more details about algorithms above, we refer to [35].

4. THEORY

In this section, we give detailed proofs for Theorem 3.2 and Theorem 3.5.

4.1 Correctness

The following proof is more general and is also much simpler than the proofs given in [34].

PROOF OF THEOREM 3.2. We prove this theorem by contradiction. Assume G is not a strong Gröbner basis of $\mathcal{I}$, then the set $N := \{f^{[\mathbf{u}]} \in \mathcal{I} \mid$ there do not exist $g^{[\mathbf{v}]} \in G$ and power product t such that $\mathrm{lpp}(t\mathbf{v}) = \mathrm{lpp}(\mathbf{u})$ and $\mathrm{lpp}(tg) \preceq \mathrm{lpp}(f)\}$ is not empty. Let $f^{[\mathbf{u}]} \in N$ be an element with the *minimal non-zero signature* in N. In this case, let $\mathbf{t} := \mathrm{lpp}(\mathbf{u})$. Then G is a strong Gröbner basis$_{\prec \mathbf{t}}$.

Next, we will find some $f_0^{[\mathbf{u}_0]} \in G$ such that $\mathrm{lpp}(\mathbf{u}_0)$ divides $\mathbf{t}$ and $t_0(f_0^{[\mathbf{u}_0]})$ is *not rewritable* by G, where $t_0 = \mathbf{t}/\mathrm{lpp}(\mathbf{u}_0)$. Suppose $\mathbf{t} = x^\alpha \mathbf{e}_i$, then there exists $g_1^{[\mathbf{v}_1]} \in G$ such that $\mathrm{lpp}(\mathbf{v}_1) = \mathbf{e}_i$ by hypothesis. Let $t_1 := x^\alpha$. Then we have $\mathbf{t} = \mathrm{lpp}(t_1 \mathbf{v}_1)$. If $t_1(g_1^{[\mathbf{v}_1]})$ is not rewritable by G, then $g_1^{[\mathbf{v}_1]}$ is what we are looking for. Otherwise, there exists $g_2^{[\mathbf{v}_2]} \in G$ such that $t_1(g_1^{[\mathbf{v}_1]})$ is rewritable by $g_2^{[\mathbf{v}_2]}$. Let $t_2 := \mathrm{lpp}(t_1 \mathbf{v}_1)/\mathrm{lpp}(\mathbf{v}_2)$. Then we have $\mathbf{t} = \mathrm{lpp}(t_2 \mathbf{v}_2)$. Next we discuss whether $t_2(g_2^{[\mathbf{v}_2]})$ is rewritable by G or not. If $t_2(g_2^{[\mathbf{v}_2]})$ is not rewritable by G, then $g_2^{[\mathbf{v}_2]}$ is the desired $f_0^{[\mathbf{u}_0]}$; Otherwise, $t_2(g_2^{[\mathbf{v}_2]})$ is rewritable by some $g_3^{[\mathbf{v}_3]} \in G$. We can repeat the above discussions. Finally, by the definition of rewritable, we get a chain $g_1^{[\mathbf{v}_1]} >_G g_2^{[\mathbf{v}_2]} >_G g_3^{[\mathbf{v}_3]} >_G \cdots$. This chain must terminate, since G is finite. Let $g_s^{[\mathbf{v}_s]}$ be the last element in this chain. Then $g_s^{[\mathbf{v}_s]}$ is the desired $f_0^{[\mathbf{u}_0]}$, since $\mathbf{t} = \mathrm{lpp}(t_s \mathbf{v}_s)$ and $t_s(g_s^{[\mathbf{v}_s]})$ is *not rewritable* by G, where $t_s = \mathbf{t}/\mathrm{lpp}(\mathbf{v}_s)$.

Let $f_0^{[\mathbf{u}_0]} \in G$ be the element found in the last paragraph. Then $\mathrm{lpp}(t_0 \mathbf{u}_0) = \mathbf{t}$ and $t_0(f_0^{[\mathbf{u}_0]})$ is *not rewritable* by G, where $t_0 = \mathbf{t}/\mathrm{lpp}(\mathbf{u}_0)$. Since $\mathrm{lpp}(t_0 \mathbf{u}_0) = \mathbf{t} = \mathrm{lpp}(\mathbf{u})$ and $f^{[\mathbf{u}]} \in N$, we must have $\mathrm{lpp}(f) \prec \mathrm{lpp}(t_0 f_0)$ by the definition of N. However, this contradicts the result of Lemma 4.1, and the theorem is proved. □

Lemma 4.1 *Let G be a finite subset of $\mathcal{I} = \langle f_1, \ldots, f_m\rangle$, $<_G$ be any partial order on G, and $\mathbf{t}$ be a term in R^m such that G is a strong Gröbner basis$_{\prec \mathbf{t}}$ of $\mathcal{I}$ and every* regular critical pair *of G is rewritable by G. For any $f_0^{[\mathbf{u}_0]} \in G$ and any power product t_0 in R with $\mathrm{lpp}(t_0 \mathbf{u}_0) \preceq \mathbf{t}$, if $t_0(f_0^{[\mathbf{u}_0]})$ is* not *rewritable by G, then for any $f^{[\mathbf{u}]} \in \mathcal{I}$ with $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(t_0 \mathbf{u}_0)$, we have $\mathrm{lpp}(f) \succeq \mathrm{lpp}(t_0 f_0)$.*

PROOF. We prove the lemma by contradiction. Let $N := \{(t_0, f_0^{[\mathbf{u}_0]}) \mid f_0^{[\mathbf{u}_0]} \in G$, t_0 is a power product, $\mathrm{lpp}(t_0 \mathbf{u}_0) \preceq \mathbf{t}$, $t_0(f_0^{[\mathbf{u}_0]})$ is not rewritable by G and there exists $f^{[\mathbf{u}]} \in \mathcal{I}$ with $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(t_0 \mathbf{u}_0)$ s.t. $\mathrm{lpp}(f) \prec \mathrm{lpp}(t_0 f_0)\}$. Assume N is not empty. Let $(t_0, f_0^{[\mathbf{u}_0]})$ be *minimal* in N, i.e., there is no $(t_h, h^{[\mathbf{w}]}) \in N$ such that $\mathrm{lpp}(t_h \mathbf{w}) \prec \mathrm{lpp}(t_0 \mathbf{u}_0)$. Clearly, $f_0 \neq 0$ and $\mathbf{u}_0 \neq 0$.

For such $(t_0, f_0^{[\mathbf{u}_0]}) \in N$, let $f^{[\mathbf{u}]}$ be in $\mathcal{I}$ such that $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(t_0 \mathbf{u}_0)$ and $\mathrm{lpp}(f) \prec \mathrm{lpp}(t_0 f_0)$. Denote $\bar{f}^{[\bar{\mathbf{u}}]} := t_0(f_0^{[\mathbf{u}_0]}) - c(f^{[\mathbf{u}]}) \in \mathcal{I}$ where $c = \mathrm{lc}(t_0 \mathbf{u}_0)/\mathrm{lc}(\mathbf{u})$. Then $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(t_0 f_0)$ and $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_0 \mathbf{u}_0) \preceq \mathbf{t}$. For $\bar{f}^{[\bar{\mathbf{u}}]} \in \mathcal{I}$, since G is a strong Gröbner basis$_{\prec \mathbf{t}}$, by Proposition 2.3, the set $D := \{(t_g, g^{[\mathbf{v}]}) \mid g^{[\mathbf{v}]} \in G$, t_g is a power product, $\mathrm{lpp}(t_g g) = \mathrm{lpp}(\bar{f}) = \mathrm{lpp}(t_0 f_0)$ and $\mathrm{lpp}(t_g \mathbf{v}) \preceq \mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_0 \mathbf{u}_0)\}$ is not empty.

Let $(t_g, g^{[\mathbf{v}]}) \in D$ be *minimal* in D, i.e., there is no $(t_h, h^{[\mathbf{w}]}) \in D$ such that either $\mathrm{lpp}(t_h \mathbf{w}) \prec \mathrm{lpp}(t_g \mathbf{v})$, or $\mathrm{lpp}(t_h \mathbf{w}) = \mathrm{lpp}(t_g \mathbf{v})$ and $h^{[\mathbf{w}]} <_G g^{[\mathbf{v}]}$.

For such $(t_g, g^{[\mathbf{v}]}) \in D$, let $(\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_g, g^{[\mathbf{v}]})$ be the critical pair of $f_0^{[\mathbf{u}_0]}$ and $g^{[\mathbf{v}]}$. Since $\mathrm{lpp}(t_g g) = \mathrm{lpp}(t_0 f_0)$ and $\mathrm{lpp}(t_g \mathbf{v}) \preceq \mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_0 \mathbf{u}_0)$, we have $\bar{t}_0$ divides t_0, $\bar{t}_g$ divides t_g and $t_0/\bar{t}_0 = t_g/\bar{t}_g$, and moreover, this critical pair $(\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_g, g^{[\mathbf{v}]})$ is regular. By hypothesis, $(\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_g, g^{[\mathbf{v}]})$ is rewritable by G. If $\bar{t}_0(f_0^{[\mathbf{u}_0]})$ is rewritable by G, so does

$t_0(f_0^{[\mathbf{u}_0]})$, which contradicts that $(t_0, f_0^{[\mathbf{u}_0]}) \in N$ and $t_0(f_0^{[\mathbf{u}_0]})$ is *not* rewritable by G. So $\bar{t}_g(g^{[\mathbf{v}]})$ must be rewritable by G.

Since $\bar{t}_g(g^{[\mathbf{v}]})$ is rewritable by G, so does $t_g(g^{[\mathbf{v}]})$. Similar to the second paragraph in the proof of Theorem 3.2, for $t_g(g^{[\mathbf{v}]})$, we can also find some $g_0^{[\mathbf{v}_0]} \in G$ such that $t_g(g^{[\mathbf{v}]})$ is rewritable by $g_0^{[\mathbf{v}_0]}$ where $g_0^{[\mathbf{v}_0]} <_G g^{[\mathbf{v}]}$, and $t_0'(g_0^{[\mathbf{v}_0]})$ is *not rewritable* by G, where $t_0' = \mathrm{lpp}(t_g\mathbf{v})/\mathrm{lpp}(\mathbf{v}_0)$. Note that $\mathrm{lpp}(t_0'\mathbf{v}_0) = \mathrm{lpp}(t_g\mathbf{v}) \preceq \mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_0\mathbf{u}_0) \preceq \mathbf{t}$, so $(t_0', g_0^{[\mathbf{v}_0]}) \notin N$, because $(t_0, f_0^{[\mathbf{u}_0]})$ is minimal in N. Thus, we have $\mathrm{lpp}(t_g g) \succeq \mathrm{lpp}(t_0' g_0)$. Since $(t_g, g^{[\mathbf{v}]})$ is minimal in D, the relation $\mathrm{lpp}(t_g g) = \mathrm{lpp}(t_0' g_0)$ does not hold (otherwise we would have $(t_0', g_0^{[\mathbf{v}_0]}) \in D$, $\mathrm{lpp}(t_0'\mathbf{v}_0) = \mathrm{lpp}(t_g\mathbf{v})$ and $g_0^{[\mathbf{v}_0]} <_G g^{[\mathbf{v}]}$ such that $(t_g, g^{[\mathbf{v}]})$ is not minimal in D). So we must have $\mathrm{lpp}(t_g g) \succ \mathrm{lpp}(t_0' g_0)$.

Denote $\bar{g}^{[\bar{\mathbf{v}}]} := t_g(g^{[\mathbf{v}]}) - ct_0'(g_0^{[\mathbf{v}_0]})$ where $c = \mathrm{lc}(t_g\mathbf{v})/\mathrm{lc}(t_0'\mathbf{v}_0)$. Then $\mathrm{lpp}(\bar{g}) = \mathrm{lpp}(t_g g)$ and $\mathrm{lpp}(\bar{\mathbf{v}}) \prec \mathrm{lpp}(t_g\mathbf{v}) \prec \mathrm{lpp}(t_0\mathbf{u}_0) \preceq \mathbf{t}$. Since G is a strong Gröbner basis$_{\prec\mathbf{t}}$, by Proposition 2.3, there exists $h^{[\mathbf{w}]} \in G$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(\bar{g}) = \mathrm{lpp}(t_g g) = \mathrm{lpp}(t_0 f_0)$ and $\mathrm{lpp}(t_h\mathbf{w}) \preceq \mathrm{lpp}(\bar{\mathbf{v}}) \prec \mathrm{lpp}(t_g\mathbf{v}) \prec \mathrm{lpp}(t_0\mathbf{u}_0)$, where $t_h = \mathrm{lpp}(\bar{g})/\mathrm{lpp}(h)$. So we have $(t_h, h^{[\mathbf{w}]}) \in D$ and $\mathrm{lpp}(t_h\mathbf{w}) \prec \mathrm{lpp}(t_g\mathbf{v})$. This contradicts that $(t_g, g^{[\mathbf{v}]})$ is minimal in D.

Hence N must be empty, and the lemma is proved. □

4.2 Termination

Consider a map $\sigma : R \times R^m \to k[Y, Z, W]$, where $Y = \{y_1, \ldots, y_n\}$, $Z = \{z_1, \ldots, z_m\}$, and $W = \{w_0, w_1, \ldots, w_n\}$ are new variables that commute with each other, i.e., $k[Y, Z, W]$ is a polynomial ring. For any $f^{[\mathbf{u}]} \in \mathcal{I}$ with $\mathrm{lpp}(\mathbf{u}) = x_1^{a_1} \cdots x_n^{a_n}\mathbf{e}_i \neq 0$, if $f = 0$, then we define

$$\sigma(0^{[\mathbf{u}]}) = y_1^{a_1} \cdots y_n^{a_n} z_i \in k[Y, Z, W].$$

Otherwise, assuming $\mathrm{lpp}(f) = x_1^{b_1} \cdots x_n^{b_n}$, then we define

$$\sigma(f^{[\mathbf{u}]}) = y_1^{a_1} \cdots y_n^{a_n} z_i w_0 w_1^{b_1} \cdots w_n^{b_n} \in k[Y, Z, W].$$

The variable w_0 is introduced to define σ when $f \neq 0$. In [13], Eder and Perry introduced a similar map to study the termination of some signature-based algorithms.

Proof of Theorem 3.5. We first claim that, in any loop of the algorithm SGB, if the regular critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is *not* rewritable by G and its S-polynomial is *reduced* to $h^{[\mathbf{w}]}$ by G, then $\sigma(h^{[\mathbf{w}]})$ is *not* divisible by any $\sigma(h_0^{[\mathbf{w}_0]})$ where $h_0^{[\mathbf{w}_0]} \in G$.

We prove the claim by contradiction. Assume there exists some $h_0^{[\mathbf{w}_0]} \in G$ such that $\sigma(h_0^{[\mathbf{w}_0]})$ divides $\sigma(h^{[\mathbf{w}]})$. When both h_0 and h are nonzero, we have that $\mathrm{lpp}(\mathbf{w}_0)$ divides $\mathrm{lpp}(\mathbf{w})$ and $\mathrm{lpp}(h_0)$ divides $\mathrm{lpp}(h)$. Let $s := \mathrm{lpp}(\mathbf{w})/\mathrm{lpp}(\mathbf{w}_0)$ and $t := \mathrm{lpp}(h)/\ \mathrm{lpp}(h_0)$. There are two cases:

(1) $s \preceq_1 t$. Now, we have $\mathrm{lpp}(sh_0) \preceq_1 \mathrm{lpp}(th_0) = \mathrm{lpp}(h) \prec \mathrm{lpp}(t_f f)$ and $\mathrm{lpp}(s\mathbf{w}_0) = \mathrm{lpp}(\mathbf{w}) = \mathrm{lpp}(t_f\mathbf{u})$. Since GVW-order is used in Rewritten Criterion, we get $h_0^{[\mathbf{w}_0]} <_G f^{[\mathbf{u}]}$, and $t_f(f^{[\mathbf{u}]})$ is rewritable by $h_0^{[\mathbf{w}_0]} \in G$. This contradicts the fact that $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is not rewritable by G.

(2) $s \succ_1 t$. Since the orders $\prec_1$ and $\prec_2$ are compatible, we have $\mathrm{lpp}(th_0) = \mathrm{lpp}(h)$ and $\mathrm{lpp}(t\mathbf{w}_0) \prec \mathrm{lpp}(s\mathbf{w}_0) = \mathrm{lpp}(\mathbf{w})$. So $h_0^{[\mathbf{w}_0]} \in G$ can be used to reduce $h^{[\mathbf{w}]}$ further, which contradicts the fact that the S-polynomial of $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is reduced to $h^{[\mathbf{w}]}$ by G.

Note that if $\sigma(h_0^{[\mathbf{w}_0]})$ divides $\sigma(h^{[\mathbf{w}]})$, then $h = 0$ implies $h_0 = 0$ by the definition of σ. When $h_0 = 0$, a contradiction can be constructed similar to case (1).

After all, the claim is proved by contradiction.

Using above claim, in each loop of the algorithm SGB, the regular critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is either rejected by Rewritten Criterion or its S-polynomial is reduced to $h^{[\mathbf{w}]}$ such that $\sigma(h^{[\mathbf{w}]})$ is not divisible by any $\sigma(h_0^{[\mathbf{w}_0]})$ where $h_0^{[\mathbf{w}_0]} \in G$. In the former case, the number of critical pairs in $CPairs$ decreases. In the latter case, the ideal generated by $\{\sigma(h^{[\mathbf{w}]})\} \cup \{\sigma(h_0^{[\mathbf{w}_0]}) \mid h_0^{[\mathbf{w}_0]} \in G\}$ over $k[Z, Y, W]$ strictly contains the ideal generated by $\{\sigma(h_0^{[\mathbf{w}_0]}) \mid h_0^{[\mathbf{w}_0]} \in G\}$. According to Hilbert's theorem on ascending chains, the algorithm SGB must terminate in finite steps. □

5. EXAMPLE

In this section, we use a simple example to illustrate how to compute a strong Gröbner basis by Algorithm SGB. In this example, we first use the data structure $(\mathrm{lpp}(\mathbf{u}), f)$ to express elements in G, and then recover a strong Gröbner basis by algorithms in Subsection 3.3.

Example 5.1 *Let R be the Weyl algebra $\mathbb{A}_2 = k[x_1, x_2, D_1, D_2]$, and $\mathcal{I} := \langle f_1, f_2, f_3\rangle \subset R$, where $f_1 = x_1D_1 + 1$, $f_2 = x_2D_2$, $f_3 = x_1D_2 + D_2$ and $D_i = \frac{\partial}{\partial x_i}$. The term order $\prec_1$ is a block order such that $\{D_1 > D_2\} \gg \{x_1 > x_2\}$, and within each block, term orders are graded reverse lex orders. The term order on R^3 is a POT extension of $\prec_1$, i.e., $x^\alpha\mathbf{e}_i \prec_2 x^\beta\mathbf{e}_j$, if either $i > j$, or $i = j$ and $x^\alpha \prec_1 x^\beta$.*

(1) Compute a Gröbner basis for $\mathcal{I}$ by Algorithm SGB. The critical pair with *minimal degree* in *CPairs* is selected in the algorithm SGB, and GVW-order is used in Rewritten Criterion.

Initially, $S_0 := \{r_1 = (\mathbf{e}_1, f_1), r_2 = (\mathbf{e}_2, f_2), r_3 = (\mathbf{e}_3, f_3)\}$, and $CPairs_0 := \{[r_1, r_2], [r_1, r_3], [r_2, r_3]\}$.

LOOP 1: $[r_2, r_3] = (x_1, r_2, x_2, r_3)$ is selected.
Its S-polynomial is $(x_1\mathbf{e}_2, -x_2D_2)$, which can be reduced to $r_4 := (x_1\mathbf{e}_2, 0)$ by r_2. Now $S_1 := S_0 \cup \{r_4\}$ and $CPairs_1 := CPairs_0 \setminus \{[r_2, r_3]\}$.

LOOP 2: $[r_1, r_3] = (D_2, r_1, D_1, r_3)$ is selected.
Its S-polynomial is $(D_2\mathbf{e}_1, -D_1D_2)$. No polynomial in S_1 can be used for reduction. So we get $r_5 := (D_2\mathbf{e}_1, -D_1D_2)$. Now $S_2 := S_1 \cup \{r_5\}$ and $CPairs_2 := CPairs_1 \cup \{[r_5, r_1], [r_5, r_2], [r_5, r_3]\} \setminus \{[r_1, r_3]\}$.

LOOP 3: $[r_5, r_2] = (x_2, r_5, D_1, r_2)$ is selected.
Its S-polynomial is $r_6 := (x_2D_2\mathbf{e}_1, 0)$. Now $S_3 := S_2 \cup \{r_6\}$ and $CPairs_3 := CPairs_2 \setminus \{[r_5, r_2]\}$.

LOOP 4: $[r_5, r_3] = (x_1, r_5, D_1, r_3)$ is selected.
Its S-polynomial is $(x_1D_2\mathbf{e}_1, D_1D_2 + D_2)$, which can be reduced to $r_7 := (x_1D_2\mathbf{e}_1, D_2)$ by r_5. Now $S_4 := S_3 \cup \{r_7\}$ and $CPairs_4 := CPairs_3 \cup \{[r_7, r_1], [r_7, r_2], [r_7, r_3], [r_7, r_5]\} \setminus \{[r_5, r_3]\} = \{[r_1, r_2], [r_5, r_1], [r_7, r_1], [r_7, r_2], [r_7, r_3], [r_7, r_5]\}$.

LOOP 5: $[r_7, r_2] = (x_2, r_7, 1, r_2)$ is selected. However, it is rejected by Rewritten Criterion, since $x_2(r_7)$ is rewritable by r_6. Now $S_5 := S_4$ and $CPairs_5 := \{[r_1, r_2], [r_5, r_1], [r_7, r_1], [r_7, r_3], [r_7, r_5]\}$.

LOOP 6: $[r_7, r_3] = (x_1, r_7, 1, r_3)$ is selected.
Its S-polynomial is $(x_1^2D_2\mathbf{e}_1, -D_2)$, which can be reduced to $r_8 := (x_1^2D_2\mathbf{e}_1, 0)$ by r_7. Now $S_6 := S_5 \cup \{r_8\}$ and $CPairs_6 := \{[r_1, r_2], [r_5, r_1], [r_7, r_1], [r_7, r_5]\}$.

LOOP 7: $[r_7, r_5] = (D_1, r_7, 1, r_5)$ is selected.
Its S-polynomial is $r_9 := (x_1D_1D_2\mathbf{e}_1, 0)$. Now $S_7 := S_6 \cup \{r_9\}$ and $CPairs_7 := \{[r_1, r_2], [r_5, r_1], [r_7, r_1]\}$.

LOOP 8: $[r_5, r_1] = (x_1, r_5, D_2, r_1)$ is selected. However, it

is rejected by Rewritten Criterion, since $x_1(r_5)$ is rewritable by r_7. Now $S_8 := S_7$ and $CPairs_8 := \{[r_1, r_2], [r_7, r_1]\}$.
LOOP 9: $[r_7, r_1] = (x_1D_1, r_7, D_2, r_1)$ is selected. However, it is rejected by Rewritten Criterion, since $x_1D_1(r_7)$ is rewritable by r_9. Now $S_9 := S_8$ and $CPairs_9 := \{[r_1, r_2]\}$.
LOOP 10: $[r_1, r_2] = (x_2D_2, r_1, x_1D_1, r_2)$ is selected. However, it is rejected by Rewritten Criterion, since $x_2D_2(r_1)$ is rewritable by r_6. Now $S_{10} := S_9$ and $CPairs_{10} := \emptyset$.

Finally, we get a simpler version of strong Gröbner basis $S_{10} = \{r_1, r_2, \ldots, r_9\}$ of $\mathcal{I}$. By Proposition 2.2, the set

$$\{f_1, f_2, f_3, -D_1D_2, D_2\}$$

is a Gröbner basis of $\mathcal{I}$.

(2) Recover a strong Gröbner basis from S_{10} for $\mathcal{I}$ by Algorithm RecoverSGB. First, we sort r_i's in an ascending order on signature, and get

$$S := \{r_3, r_2, r_4, r_1, r_5, r_6, r_7, r_8, r_9\}.$$

Initially, $G_0 := \emptyset$. Loop 1 and 2 are trivial, and we can easily get $\mathbf{u}_3 := \mathbf{e}_3$ and $\mathbf{u}_2 := \mathbf{e}_2$ from r_3 and r_2. Now $G_2 := \{f_3^{[\mathbf{e}_3]}, f_2^{[\mathbf{e}_2]}\}$.
LOOP 3: $r_4 = (x_1\mathbf{e}_2, 0)$. Then $g := \mathrm{IncSF}(x_1\mathbf{e}_2, 0, S) = 0$, and hence $c_4 := 1$. Next, $(p_3, p_2) := \mathrm{Rep}(c_4x_1\mathbf{e}_2, 0, G_2) = (-x_2, 1)$. Here p_i corresponds to r_i. Then $\mathbf{u}_4 := c_4x_1\mathbf{e}_2 + p_3\mathbf{e}_3 + p_2\mathbf{e}_2 = (x_1 + 1)\mathbf{e}_2 - x_2\mathbf{e}_3$. Now $G_3 := G_2 \cup \{0^{[\mathbf{u}_4]}\}$.
LOOP 4: $r_1 = (\mathbf{e}_1, f_1)$. The procedure is trivial, and $\mathbf{u}_1 := \mathbf{e}_1$. Now $G_4 := G_3 \cup \{f_1^{[\mathbf{e}_1]}\}$.
LOOP 5: $r_5 = (D_2\mathbf{e}_1, -D_1D_2)$. Then $g := \mathrm{IncSF}(D_2\mathbf{e}_1, -D_1D_2, S) = -D_1D_2$ and $g_0 := \mathrm{IncSF}(D_2\mathbf{e}_1, D_2f_1, S) = -D_1D_2$, and hence, $c_5 := (-1)/(-1) = 1$. Next, $(p_3, p_2, p_1) := \mathrm{Rep}(c_5D_2\mathbf{e}_1, -D_1D_2, G_4) = (-D_1, 0, 0)$. Then $\mathbf{u}_5 := c_5D_2\mathbf{e}_1 + p_3\mathbf{e}_3 = D_2\mathbf{e}_1 - D_1\mathbf{e}_3$. Now $G_5 := G_4 \cup \{(-D_1D_2)^{[\mathbf{u}_5]}\}$.

LOOP 6: $r_6 = (x_2D_2\mathbf{e}_1, 0)$. Then $g := \mathrm{IncSF}(x_2D_2\mathbf{e}_1, 0, S) = 0$, and hence, $c_6 := 1$. Next, $(p_3, p_2, p_1, p_5) := \mathrm{Rep}(c_6x_2D_2\mathbf{e}_1, 0, G_5) = (0, -x_1D_1 - 1, 0, 0)$. Then $\mathbf{u}_6 := c_6x_2D_2\mathbf{e}_1 + p_2\mathbf{e}_2 = x_2D_2\mathbf{e}_1 - (x_1D_1 + 1)\mathbf{e}_2$. Now $G_6 := G_5 \cup \{0^{[\mathbf{u}_6]}\}$.
LOOP 7: $r_7 = (x_1D_2\mathbf{e}_1, D_2)$. Then $g := \mathrm{IncSF}(x_1D_2\mathbf{e}_1, D_2, S) = D_2$ and $g_0 := \mathrm{IncSF}(x_1D_2\mathbf{e}_1, x_1D_2f_1, S) = D_2$, and hence, $c_7 := 1/1 = 1$. Next, $(p_3, p_2, p_1, p_5) := \mathrm{Rep}(c_7x_1D_2\mathbf{e}_1, D_2, G_6) = (-x_1D_1 + D_1, 0, 0, 1)$. Then $\mathbf{u}_7 := c_7x_1D_2\mathbf{e}_1 + p_3\mathbf{e}_3 + p_5(D_2\mathbf{e}_1 - D_1\mathbf{e}_3) = (x_1D_2 + D_2)\mathbf{e}_1 - x_1D_1\mathbf{e}_3$. Now $G_7 := G_6 \cup \{(D_2)^{[\mathbf{u}_7]}\}$.
LOOP 8: $r_8 = (x_1^2D_2\mathbf{e}_1, 0)$. Then $g := \mathrm{IncSF}(x_1^2D_2\mathbf{e}_1, 0, S) = 0$, and hence, $c_8 := 1$. Next, $(p_3, p_2, p_1, p_5, p_7) := \mathrm{Rep}(c_8x_1^2D_2\mathbf{e}_1, 0, G_7) = (-x_1^2D_1 + x_1D_1 - 1, 0, 0, x_1, 1)$. Then $\mathbf{u}_8 := c_8x_1^2D_2\mathbf{e}_1 + p_3\mathbf{e}_3 + p_5(D_2\mathbf{e}_1 - D_1\mathbf{e}_3) + p_7((x_1D_2 + D_2)\mathbf{e}_1 - x_1D_1\mathbf{e}_3) = (x_1^2D_2 + 2x_1D_2 + D_2)\mathbf{e}_1 - (x_1^2D_1 + x_1D_1 + 1)\mathbf{e}_3$. Now $G_8 := G_7 \cup \{0^{[\mathbf{u}_8]}\}$.
LOOP 9: $r_9 = (x_1D_1D_2\mathbf{e}_1, 0)$. Then $g := \mathrm{IncSF}(x_1D_1D_2\mathbf{e}_1, 0, S) = 0$, and hence, $c_9 := 1$. Next, $(p_3, p_2, p_1, p_5, p_7) := \mathrm{Rep}(c_9x_1D_1D_2\mathbf{e}_1, 0, G_8) = (-x_1D_1^2 + D_1^2, 0, 0, D_1 + 2, 0)$. Then $\mathbf{u}_9 := c_9x_1D_1D_2\mathbf{e}_1 + p_3\mathbf{e}_3 + p_5(D_2\mathbf{e}_1 - D_1\mathbf{e}_3) = (x_1D_1D_2 + D_1D_2 + 2D_2)\mathbf{e}_1 - (x_1D_1^2 + 2D_1)\mathbf{e}_3$. Now $G_9 := G_8 \cup \{0^{[\mathbf{u}_9]}\}$.

From S_{10}, we know the set $\{f_1, f_2, f_3, -D_1D_2, D_2\}$ is a Gröbner basis of $\mathcal{I}$. Using G_9, we can express elements in this Gröbner basis as an R-representation w.r.t. f_1, f_2, f_3, i.e., $-D_1D_2 = D_2f_1 - D_1f_3$ and $D_2 = (x_1D_2 + D_2)f_1 - x_1D_1f_3$. Besides, from G_9, the set $\{(0, x_1 + 1, -x_2), (x_2D_2, -x_1D_1 - 1, 0), (x_1^2D_2 + 2x_1D_2 + D_2, 0, -x_1^2D_1 - x_1D_1 - 1), (x_1D_1D_2 + D_1D_2 + 2D_2, 0, -x_1D_1^2 - 2D_1)\}$ is a Gröbner basis of the syzygy module $\{(p_1, p_2, p_3) \in R^3 \mid p_1f_1 + p_2f_2 + p_3f_3 = 0\}$ w.r.t. $\prec_2$ by Proposition 2.2.

6. EXPERIMENTAL DATA

The algorithm SGB with GVW-order has been implemented on Singular (ver 3-1-4 [9]). We generated some random examples in the Weyl Algebra $R = k[x_1, \ldots, x_6, D_1, \ldots, D_6]$, where $D_i = \frac{\partial}{\partial x_i}$ is the partial derivative by x_i for $i = 1, \ldots, 6$. The term order $\prec_1$ is a block order such that $\{D_1 > \cdots > D_6\} \gg \{x_1 > \cdots > x_6\}$, and within each block, term orders are graded reverse lex orders. The term order on R^m is an extension of $\prec_1$ in the following way: $x^\alpha\mathbf{e}_i \prec_2 x^\beta\mathbf{e}_j$, if either $\mathrm{lpp}(x^\alpha f_i) \prec_1 \mathrm{lpp}(x^\beta f_j)$, or $\mathrm{lpp}(x^\alpha f_i) = \mathrm{lpp}(x^\beta f_j)$ and $i > j$. The critical pair with *minimal signature* in *CPairs* is selected in the algorithm SGB.

(E1): $\{D_1D_6 + x_1D_1, D_1D_3 + x_3D_4 + x_2, x_3D_3 + x_3D_5, x_4D_4D_5 + x_2^2\}$.
(E2): $\{x_3D_4 + x_1D_6 + x_1^2, x_3D_2 - x_2D_4 + x_3D_5, D_2D_3 + x_4D_3 + x_1^2 - x_1x_5\}$.
(E3): $\{x_6D_6 + x_1^2 - x_5, D_4D_6 + x_1D_1 + x_4^2, D_3D_4 + D_6^2 - x_1D_5\}$.
(E4): $\{D_1D_4 - D_2D_6 - x_1D_3 - x_4D_4 + x_2, D_3D_5 + x_3D_5 + x_2x_3 - x_1x_4 + x_5\}$.
(E5): $\{x_3D_4 + x_5D_6 + x_2^2 + x_4x_6, D_1^2 - D_1D_4 - x_2D_6, x_4D_2 - x_5D_2 + x_2^2\}$.
(E6): $\{D_2D_6 + x_4D_2 + x_6D_5 + x_1x_6, D_1D_3 + D_4^2 - D_6^2 + x_1D_2 + x_3x_5\}$.
(E7): $\{D_2^2 + D_2D_3, D_1D_4 + D_3D_6 - D_4D_6, D_1D_2 - x_2D_3 + x_2D_5, x_6D_3 + x_1x_3\}$.

The following table shows the performance of Rewritten Criterion.

Table 1: Total, Reject, $\to 0$, and $\to \neq 0$ refer to the number of total critical pairs, critical pairs rejected by Rewritten Criterion, critical pairs (not rejected) reduced to 0, and critical pairs (not rejected) reduced to nonzero elements respectively.

Exam.	Total	Reject	$\to 0$	$\to \neq 0$	Reject(%)
E1	465	402	36	27	86%
E2	2628	2452	106	70	93%
E3	3321	3158	84	79	95%
E4	3403	3242	80	81	95%
E5	8001	7731	146	124	97%
E6	15400	15089	137	174	98%
E7	34980	34459	260	261	99%

From Table 1, we can see that about 95% critical pairs are redundant and rejected by Rewritten Criterion, and Rewritten Criterion performs even better for complicated examples. However, some critical pairs, which are not rejected by Rewritten Criterion, are reduced to 0. This is because the vector $(-g, f)$ is usually not a principle syzygy for (f, g) in the Weyl Algebra, so fewer known syzygies can be used to reject redundant computations. Using algorithms in Subsection 3.3, we can also obtain Gröbner bases for syzygy modules of input polynomials easily.

7. CONCLUSIONS

A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras is developed. Generalized criterion is used to reject redundant computations in non-commutative cases. Experimental data show that Rewritten Criterion can also reject most redundant computations in solvable polynomial algebras. The termination is proved if GVW-order is used in Rewritten Criterion. An important application of the algorithm is to compute Gröbner bases for syzygy modules in solvable polynomial algebras. Other admissible partial orders, such as the partial order implied by F5, can also be used to construct this new algorithm, but the corresponding proofs for terminations need to be studied further.

Acknowledgements We would like to thank Professor Ziming Li for advising us to extend Rewritten Criterion to non-commutative cases, and also thank Professor Shuhong Gao and Mingsheng Wang for helpful suggestions.

8. REFERENCES

[1] W. Adams and P. Loustaunau. An Introduction to Gröbner Bases. American Mathematical Society, Providence, 1994.

[2] A. Arri and J. Perry. The F5 criterion revised. J. Symb. Comp., vol. 46(9), 1017-1029, 2011.

[3] B. Buchberger. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, 1965.

[4] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner basis. In Proc. of EUROSAM'79, Lect. Notes in Comp. Sci., vol. 72, 3-21, 1979.

[5] J.L. Bueso, J. Gómez Torrecillas, and A. Verschoren. Algorithmic Methods in Non-commutative Algebra: Applications to Quantum Groups. Kluwer, 2003.

[6] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities, J. Symb. Comp., vol. 26, 187-227, 1998.

[7] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Proc. of EUROCRYPT'00, Lect. Notes in Comp. Sci., vol. 1807, 392-407, 2000.

[8] D. Cox, J. Little, and D. O'Shea. Using algebraic geometry. Springer, second edition, 2005.

[9] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann. SINGULAR 3-1-4 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de, 2012.

[10] J. Ding, J. Buchmann, M.S.E. Mohamed, W.S.A.E. Mohamed, and R.-P. Weinmann. MutantXL. In Proc. SCC'08, 16-22, 2008.

[11] C. Eder and J. Perry. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. J. Symb. Comp., vol. 45(12), 1442-1458, 2010.

[12] C. Eder, J. Gash, and J. Perry. Modifying Faugere's F5 algorithm to ensure termination. ACM SIGSAM Communi. in Comp. Alg., vol. 45(2), 70-89, 2011.

[13] C. Eder and J. Perry. Signature-based algorithms to compute Gröbner bases. In Proc. ISSAC'11, ACM Press, 99-106, 2011.

[14] J.-C. Faugère. A new effcient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra, vol. 139(1-3), 61-88, 1999.

[15] J.-C. Faugère. A new effcient algorithm for computing Gröbner bases without reduction to zero (F_5). In Proc. ISSAC'02, ACM Press, 75-82, 2002.

[16] A. Galligo. Some algorithmic questions on ideals of differential operators. Lect. Notes in Comp. Sci., vol. 204, 413-421, 1985.

[17] S.H. Gao, Y.H. Guan, and F. Volny. A new incremental algorithm for computing Gröbner bases. In Proc. ISSAC'10, ACM Press, 13-19, 2010.

[18] S.H. Gao, F. Volny, and M.S. Wang. A new algorithm for computing Gröbner bases. Cryptology ePrint Archive, Report 2010/641, 2010.

[19] M. Giesbrecht, G. Reid and Yang Zhang. Non-commutative Gröbner bases in Poincar-Birkhoff -Witt extensions. In Proc. CASC'02, 97-106, 2002.

[20] R. Gebauer and H.M. Moller. Buchberger's algorithm and staggered linear bases. In Proc. SYMSAC'86, ACM press, 218-221, 1986.

[21] A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso. "One sugar cube, please" or selection strategies in the Buchberger algorithm. In Proc. ISSAC'91, ACM Press, 49-54, 1991.

[22] A. Hashemi and G. Ars. Extended F5 criteria. J. Symb. Comp., vol. 45(12), 1330-1340, 2010.

[23] L. Huang. A new conception for computing Gröbner basis and its applications. ArXiv:1012.5425, 2010.

[24] M. Insa and F. Pauer. Gröbner bases in rings of differential operators. In: Buchberger, B.,Winkler, F. (Eds.), Gröbner Bases and Applications, 1998.

[25] A. Kandri-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. J. Symb. Comp., vol. 9, 1-26, 1990.

[26] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In Proc. EUROCAL'83, Lect. Notes in Comp. Sci., vol. 162, 146-156, 1983.

[27] V. Levandovskyy and H. Schönemann. Plural-a computer algebra system for noncommutative polynomial algebras. In Proc. ISSAC'03, ACM Press, 176-183, 2003.

[28] X.D. Ma, Y. Sun, and D.K. Wang. On Computing Gröbner Bases in the Rings of Differential Operators. Sci. China Math., vol. 54(6), 1077-1087, 2011.

[29] F. Mora. Gröbner bases for non-commutative polynomial rings. In Proc. AAECC-3, Lect. Notes in Comp. Sci., vol. 229, 353-362, 1986.

[30] H.M. Möller, T. Mora, and C. Traverso. Gröbner bases computation using syzygies. In Proc. ISSAC'92, ACM Press, 320-328, 1992.

[31] T. Mora. An introduction to commutative and noncommutative Gröbner bases. Theoret. Comp. Sci., vol. 134(1), 131-173, 1994.

[32] Y. Sun and D.K. Wang. The F5 algorithm in Buchberger's style. J. Syst. Sci. Complex., vol. 24(6), 1218-1231, 2011.

[33] Y. Sun and D.K. Wang. A proof for the correctness of the F5 algorithm. To appear in Sci. China Math., 2010.

[34] Y. Sun and D.K. Wang. A generalized criterion for signature related Gröbner basis algorithms. In Proc. ISSAC'11, ACM Press, 337-344, 2011.

[35] Y. Sun and D.K. Wang. Solving detachability problem for the polynomial ring by signature-based Gröbner basis algorithms. ArXiv:1108.1301, 2011.

[36] M. Zhou, and F. Winkler. On computing Gröbner bases in rings of differential operators with coefficients in a ring. Math. in Comp. Sci., vol. 1, 211-223, 2007.

[37] A. Zobnin. Generalization of the F5 algorithm for calculating Gröbner bases for polynomial ideals. Programming and Comp. Software, vol. 36(2), 75-82, 2010.