A signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings

Abstract: Signature-based algorithms are efficient algorithms for computing Gröbner-Shirshov bases in commutative polynomial rings, and some noncommutative rings. In this paper, we first define skew solvable polynomial rings, which are generalizations of solvable polynomial algebras and (skew) PBW extensions. Then we present a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings over fields.

Keywords: Gröbner-Shirshov basis, Skew solvable polynomial ring, Signature-based algorithm

MSC: 16S36, 13P10

1 Introduction

Gröbner-Shirshov basis is a powerful tool in mathematics, science, engineering, and computer science. The theory of Gröbner-Shirshov bases was introduced independently by A.I. Shirshov [19] for Lie algebras in 1962, and by B. Buchberger ([3]) for commutative algebras in 1965. Buchberger([3]) gave the first algorithm to compute Gröbner-Shirshov bases in commutative polynomial rings. However, Buchberger’s algorithm is not efficient since it has to reduce the S-polynomial for every pair of elements from the input set. There have been extensive efforts to improve the efficiency of Buchberger’s algorithm in commutative polynomial rings, and several more efficient signature-based algorithms have been proposed, such as F5 by Faugère ([6, 7]), G2V and GVW by Gao et al.([10, 11]). The essential idea in these algorithms is to detect “useless” S-polynomials, i.e., S-polynomials which can be reduced to zero (and thus the computations of these S-polynomials are redundant), in Buchberger’s algorithm.

Noncommutative Gröbner-Shirshov bases and their computations have also been widely investigated (see the survey [2]), especially for various skew polynomial rings, for example, Gröbner-Shirshov basis theory for Weyl algebras [9], solvable polynomial algebras [14], rings of differential operators [13, 16, 22], G-algebras [15], skew polynomial rings [5], differential difference algebras [17, 21], PBW algebras [4, 12] and skew PBW extensions [8]. Owing to the noncommutativity, it is difficult to detect and reject redundant computations effectively. In ISSAC 2012, a signature-based algorithm was presented by Sun et al. [20] to compute Gröbner-Shirshov bases in solvable polynomial algebras.

In this paper, we define skew solvable polynomial rings, which are generalizations of several well-known classes of rings such as solvable polynomial algebras and (skew) Poincaré-Birkhoff-Witt extensions (see Definition 2.1 and Examples 2.2 and 2.3). We extend the signature-based algorithm proposed in [20] to skew solvable polynomial rings.
over fields. The signature-based algorithms for more general skew solvable polynomial rings will be investigated in the near future.

This paper is organized as follows. In Section 2, we introduce basic definitions of skew solvable polynomial rings and Gröbner-Shirshov bases. Then we define and investigate strong Gröbner-Shirshov bases of skew solvable polynomial rings in Section 3. Finally a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings is given in Section 4.

2 Preliminaries

2.1 Skew solvable polynomial rings

In order to define skew solvable polynomial rings, let us recall some basic definitions of orderings first. Let \( \mathbb{N} \) be the set of nonnegative integers. Suppose \(<\) is a monomial ordering on \( \mathbb{N}^n \), \( n \in \mathbb{N} \), i.e., a total ordering on \( \mathbb{N}^n \) such that \( 0 \in \mathbb{N}^n \) is the smallest element in \( \mathbb{N}^n \) and \( \alpha < \beta \) implies \( \alpha + \gamma < \beta + \gamma \) for any \( \alpha, \beta, \gamma \in \mathbb{N}^n \). The set of (standard) monomials in \( n \) indeterminates \( \{ x_1, \ldots, x_n \} \) is defined as \( \{ x_1^{a_1} \cdots x_n^{a_n} : a_i \in \mathbb{N}, 1 \leq i \leq n \} \). We also denote \( x_1^{a_1} \cdots x_n^{a_n} \) by \( x^\alpha \) and call \( \alpha \) the exponent of \( x^\alpha \) (denoted by \( \exp(x^\alpha) = \alpha \)), where \( \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \). We say \( x^\alpha < x^\beta \) if \( \alpha < \beta \). Thus, a monomial ordering on \( \mathbb{N}^n \) is also called a monomial ordering on the set of standard monomials.

The multiple degree and the total degree of a monomial \( x^\alpha \) are defined as \( \text{mdeg}(x^\alpha) = \alpha \) and \( \text{tdeg}(x^\alpha) = |\alpha| = \alpha_1 + \cdots + \alpha_n \), respectively. For any nonzero \( f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \), where only finitely many constants \( c_\alpha \) are nonzero, the multiple degree and the total degree of \( f \) are defined as \( \text{mdeg}(f) = \max\{ \alpha : c_\alpha \neq 0 \} \) and \( \text{tdeg}(f) = \max\{|\alpha| : c_\alpha \neq 0 \} \), respectively. The monomial \( x^\gamma = \max\{ x^\alpha : c_\alpha \neq 0 \} \) is called the leading monomial of \( f \) and \( c_\gamma \) is called the leading coefficient of \( f \), denoted by \( \text{lm}(f) \) and \( \text{lc}(f) \), respectively.

From now on, we fix a monomial ordering \( < \) on \( \mathbb{N}^n \).

Throughout this paper, we suppose all rings considered are unitary and associative. If \( R \) is a ring and \( \sigma \) is a ring endomorphism of \( R \), then a mapping \( \delta : R \rightarrow R \) is called a \( \sigma \)-derivation of \( R \) if for any \( a, b \in R \), \( \delta(a + b) = \delta(a) + \delta(b) \) and \( \delta(ab) = \sigma(a)\delta(b) + \delta(a)b \).

**Definition 2.1.** Let \( R \) and \( A \) be two rings with \( R \subseteq A \). Then \( A \) is called a skew solvable polynomial ring over \( R \) if the following conditions hold:

(i) There exist finitely many elements \( x_1, \ldots, x_n \in A \) such that \( A \) is a free left \( R \)-module with basis

\[
\mathcal{M} = \{ x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \}.
\]

(ii) For \( 1 \leq i \leq n \), there are an injective ring endomorphism \( \sigma_i \) of \( R \) and a \( \sigma_i \)-derivation \( \delta_i \) of \( R \) such that \( x_i r = \sigma_i(r)x_i + \delta_i(r) \) for any \( r \in R \). Furthermore, for any \( 1 \leq i, j \leq n \),

\[
\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i, \quad \delta_i \circ \delta_j = \delta_j \circ \delta_i, \quad \sigma_i \circ \delta_j = \delta_j \circ \sigma_i.
\]

(iii) For \( 1 \leq i < j \leq n \), there exist \( 0 \neq c_{ij} \in R \) and \( p_{ij} \in A \) with \( \text{lm}(p_{ij}) < x_i x_j \) such that \( x_j x_i = c_{ij} x_i x_j + p_{ij} \). Then we write \( A = R\langle X; \sigma, \delta, c, p \rangle \). Clearly every nonzero element in \( A \) can be uniquely represented as \( f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \), where only finitely many \( c_\alpha \in R \) are nonzero.

Skew solvable polynomial rings are generalizations of several well-known kinds of skew polynomial rings.

**Example 2.2.** Let \( A = R\langle X; \sigma, \delta, c, p \rangle \) be a skew solvable polynomial ring.

(i) If \( R \) is a field, \( \sigma_i = \text{id}_R \) and \( \delta_i = 0 \) for all \( 1 \leq i \leq n \), then \( A \) is a solvable polynomial algebra \([14]\). Any solvable polynomial algebra can be viewed as a skew solvable polynomial ring in this way.

(ii) If \( \text{tdeg}(p_{ij}) = 1 \) for all \( 1 \leq i < j \leq n \), then \( A \) is a skew PBW extension of \( R \) \([8]\). Any skew PBW extension can be viewed as a skew solvable polynomial ring in this way.
Therefore, any ring belonging to the above two classes of rings is a skew solvable polynomial ring, for example, a Weyl algebra, the universal enveloping algebra of a finite dimensional Lie algebra, and an Ore extension of automorphism and/or derivation type.

**Example 2.3** ([18]). Let \( 0 \neq q \in k \). The coordinate ring of quantum Euclidean space, denoted by \( \mathcal{O}_q(\text{ok}^{2n+1}) \), is the \( k \)-algebra generated by \( 2n + 1 \) variables \( w, x_1, \ldots, x_n, y_1, \ldots, y_n \) with the following relations:

\[
\begin{align*}
wy_j &= q y_j w, & 1 \leq j \leq n, \\
w x_j &= q^{-1} x_j w, & 1 \leq j \leq n, \\
y j y_i &= q^{-1} y_i y_j, & i < j, \\
y j x_i &= q^{-1} x_i y_j, & i \neq j, \\
x_j x_i &= q x_i x_j, & i < j, \\
y_j x_j &= x_j y_j + f_{jj}, & 1 \leq j \leq n,
\end{align*}
\]

where

\[
f_{jj} = q^{1-j}(q^{1/2} - q^{-1/2})w^2 + (q^2 - 1) \sum_{1 \leq l < j} q^{l-j} y_l x_l.
\]

Let \( R = k[w] \). For \( 1 \leq i \leq n \), let \( x_{n+i} = y_i, \sigma_i \) be the \( k \)-algebra isomorphism over \( R \) determined by \( \sigma_i(w) = qw \), \( \sigma_{n+i} \) be the \( k \)-algebra isomorphism over \( R \) determined by \( \sigma_{n+i}(w) = q^{-1} w \), and \( \delta_j = 0 \) be the zero mapping for any \( 1 \leq j \leq 2n \). Let

\[
c_{ij} = \begin{cases} q, & i < j \leq n, \\
q^{-1}, & n < i < j, \text{ or } i < n < j \text{ and } i \neq j - n, \\
1, & i = j - n, \end{cases}
\]

and

\[
p_{ij} = \begin{cases} 0, & i \neq j, \\
f_{ij}, & i = j. \end{cases}
\]

It is easy to prove by induction that, for any \( 1 \leq j \leq n \), \( f_{jj} \) (and thus \( p_{jj} \)) can be written as

\[
f_{jj} = \sum_{1 \leq l < j} c_{l} x_l y_l + c w^2, \quad c, c \in k.
\]

Let \( > \) be a monomial ordering on \( \{ x^\alpha : \alpha \in \mathbb{N}^{2n} \} \) such that \( x_{2n} > x_{2n-1} > \cdots > x_1 \). With the above notation, it is easy to check that \( \mathcal{O}_q(\text{ok}^{2n+1}) = R[X; \sigma, \delta, c, p] \) is a skew solvable polynomial ring.

In this paper, we consider Gröbner-Shirshov bases in a skew solvable polynomial ring over a field (i.e., \( R \) is a field) and the general case will be studied in the near future.

**From now on, let \( R = k \) be a field and \( A = R[X; \sigma, \delta, c, p] \) be a skew solvable polynomial ring.**

Let us fix more notation. Denote \( \sigma_1 \alpha_1 \cdots \sigma_n \alpha_n = \sigma^\alpha(c) \) and \( \delta_1 \alpha_1 \cdots \delta_n \alpha_n = \delta^\alpha(c) \) for \( \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \) and \( c \in k \). Suppose \( x^\alpha, x^\beta \in M \). Then the least common multiple of \( x^\alpha \) and \( x^\beta \) is defined as \( \text{lcm}(x^\alpha, x^\beta) = x^\gamma \) where \( \gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}) \in \mathbb{N}^n \). We say that \( x^\alpha \) is divisible by \( x^\beta \), or \( x^\beta \) divides \( x^\alpha \), if \( x^\alpha = \text{lcm}(x^\alpha, x^\beta) \) for some \( t \in M \). For convenience, denote \( x^\alpha / x^\beta = x^{\alpha - \beta} \) (but keep in mind that \( x^\alpha - x^\beta \) is \( x^\alpha \) in general in a skew solvable polynomial ring). We make the convention that \( \text{lcm}(0) = 0 < t \) for any \( 0 \neq t \in M \).

With the above notation, the proof of the following lemma is straightforward.

**Lemma 2.4.** Suppose \( x^\alpha, x^\beta, x^\gamma \in M \). We have:

(i) \( \text{lcm}(x^\alpha, x^\beta) = x^{\alpha + \beta} = \text{lcm}(x^\beta, x^\alpha) \).

(ii) \( x^\beta \) divides \( x^\alpha \) if and only if \( \alpha - \beta \in \mathbb{N}^n \).

(iii) If \( x^\alpha < x^\beta \) then \( \text{lcm}(x^\gamma x^\alpha) < \text{lcm}(x^\gamma x^\beta) \).
2.2 Gröbner-Shirshov bases of skew solvable polynomial rings

In this subsection, we briefly introduce concepts related to Gröbner-Shirshov bases and Buchberger’s algorithm for skew solvable polynomial rings.

**Definition 2.5.** Let $I$ be a left ideal of $A$. A (left) Gröbner-Shirshov basis (with respect to $<$) is a finite subset $G \subset I$ with the property that for every nonzero $f \in I$, $\text{lm}(f)$ is divisible by $\text{lm}(g)$ for some $g \in G$.

Let $f, g \in A$ be nonzero. Suppose that

\[
\begin{align*}
t_f &= \frac{\text{lcm}(\text{lm}(f), \text{lm}(g))}{\text{lm}(f)} \\
t_g &= \frac{\text{lcm}(\text{lm}(f), \text{lm}(g))}{\text{lm}(g)}.
\end{align*}
\]

The $S$-polynomial of $f$ and $g$, denoted by \( \text{SPoly}(f, g) \), is defined as

\[
\text{SPoly}(f, g) = t_f f - c t_g g \in I,
\]

where $c = \frac{\text{lcm}(t_f f)}{\text{lcm}(t_g g)} = \frac{\exp(t_f)(\text{lc}(f))}{\exp(t_g)(\text{lc}(g))}$.

Suppose $f, g \in I$. We say $f$ is reducible by $g$ if there exists $t \in M$ such that $\text{lm}(t g) = \text{lm}(f)$. Moreover, if $G \subseteq A$ and $g \in G$, then $f \rightarrow_G f - ct g$ is called one-step-reduction by $G$. If an element $r \in A$ is obtained from $f$ by finitely many one-step-reductions by $G$ and $r$ is not reducible by $G$, then we say that $r$ is a remainder of $f$ modulo $G$.

The following algorithm is an analogue of the Buchberger’s Algorithm for (commutative) polynomial algebras.

**Algorithm 2.6 (Algorithm for (left) Gröbner-Shirshov bases).**

**Input:** $F = \{f_1, \ldots, f_m\} \subseteq A$

**Output:** A Gröbner-Shirshov basis $G$ of the left ideal $I$ of $A$ generated by $F$.

\[
G := F
\]

While Pairs$\neq \emptyset$ Do

Choose $(f, g) \in \text{Pairs}$

Pairs$:=\text{Pairs} \setminus \{(f, g)\}$

$h := \text{a remainder of } \text{SPoly}(f, g) \text{ modulo } G$

If $h \neq 0$ Then

Pairs$:=\text{Pairs} \cup \{(h, h') : h' \in G\} \cup \{(h', h) : h' \in G\}$

$G := G \cup \{h\}$

End If

End Do

Return $G$

The correctness and termination of the above algorithm can be proved in a way similar to the case of commutative polynomial algebras ([3]).

3 Strong Gröbner-Shirshov bases

In this section, we introduce the definition of strong Gröbner-Shirshov bases and investigate their properties which will be used in the next section.

Recall that $A$ is a skew solvable polynomial ring over a field $k$. Let

\[
f = (f_1, \ldots, f_m) \in A^m, m \in \mathbb{N}.
\]

We denote by $I$ the left ideal of $A$ generated by $f_1, \ldots, f_m$. Then an element $f \in I$ can be written as

\[
f = u_1 f_1 + \cdots + u_m f_m = u \cdot f, \text{ where } u = (u_1, \ldots, u_m) \in A^m.
\]
Note that this expression for $f$ is not unique, i.e., there may exist $u' \in A^m$ such that $u' \neq u$ and $f = u' \cdot f$. We write $f[u] \in I \times A^m$ to indicate $f \in I$, $u \in A^m$ and $f = u \cdot f$. That is, $f[u]$ is actually a pair $(f, u) \in I \times A^m$ such that $f = u \cdot f$. With this convention, for $u \in A$, $f[u], g[v], h[w] \in I \times A^m$, by the equation $h[w] = f[u] + ag[v]$ it means $h = f + ag$ and $w = u + av$, particularly, $h[w] = f[u]$ if and only if $h = f$ and $w = u$.

Note that $A^m$ is a left $A$-module with the standard basis $\{e_i : 1 \leq i \leq m\}$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the $i$-component 1 and the other components 0. The set of (standard) monomials in $A^m$ is

$$\mathcal{N} = \{x^\alpha e_i : \alpha \in \mathbb{N}^m, 1 \leq i \leq m\}.$$ 

A (left) monomial ordering on $\mathcal{N}$ is a well-ordering on $\mathcal{N}$ such that

$$\text{if } m > n \text{ then } \text{lm}(tm) > \text{lm}(tn) \text{ for all } m, n \in \mathcal{N} \text{ and } t \in M.$$ 

A monomial ordering on $M$ can be extended to a monomial ordering on $\mathcal{N}$.

**Example 3.1.** Let $<_0$ be a monomial ordering on $M$. Then $<_0$ can be extended to a monomial ordering on $\mathcal{N}$ as follows.

(i) We say $x^\alpha e_i <_1 x^\beta e_j$ if and only if $x^\alpha < x^\beta$, or $x^\alpha = x^\beta$ and $i < j$. It is easy to see that $<_1$ is a monomial ordering on $\mathcal{N}$. We call $<_1$ the TOP extension of $<_0$, where TOP stands for “term over position”, following terminology in [1].

(ii) Similarly, we can introduce the POT (“position over term”) extension [1]: Define $x^\alpha e_i <_2 x^\beta e_j$ if and only if $i < j$ or $i = j$ and $x^\alpha < x^\beta$. It is easy to see that $<_2$ is also a monomial ordering on $\mathcal{N}$.

From now on, we fix a monomial ordering, also denoted by $<$, on $\mathcal{N}$ such that it is compatible with the monomial ordering on $M$, i.e., for any $x^\alpha, x^\beta \in M$ and $1 \leq i \leq m$, if $x^\alpha < x^\beta$ in $M$ then $x^\alpha e_i < x^\beta e_i$ in $\mathcal{N}$.

Every element $u \in A^m$ can be written uniquely as a $k$-linear combination of monomials: $u = \sum_{1 \leq i \leq q} c_i m_i$ where $q \in \mathbb{N}, 0 \neq c_i \in k, m_i \in \mathcal{N}$. Then, as what we did for elements in $A$, we can define the leading monomial $\text{lm}(u)$ and leading coefficient $\text{lc}(u)$ of $u$.

**Definition 3.2.** Given $f[u] \in I \times A^m$, the leading monomial $\text{lm}(u)$ is called the signature of $f[u]$.

**Definition 3.3.** A finite set $G = \{g_1^{[v_1]}, \ldots, g_s^{[v_s]}\} \subseteq I \times A^m$ is called a strong Gröbner-Shirshov basis (cf. [11, 20]) of $I$ if, for any $f[u] \in I \times A^m$, there exist $g_i^{[v_i]} \in G$ and $t \in M$ such that $\text{lm}(tv_i) = \text{lm}(u)$ and $\text{lm}(tg_i) \leq \text{lm}(f)$.

We call $G$ a $t$-strong Gröbner-Shirshov basis for a monomial $t$ in $A^m$ if for any $f[u] \in I \times A^m$ with $\text{lm}(u) < t$, there exist $g_i^{[v_i]} \in G$ and $t \in M$ such that $\text{lm}(tv_i) = \text{lm}(u)$ and $\text{lm}(tg_i) \leq \text{lm}(f)$.

**Lemma 3.4.** Suppose that $G = \{g_1^{[v_1]}, \ldots, g_s^{[v_s]}\}$ is a strong Gröbner-Shirshov basis of $I$. Then $G' = \{g_1, \ldots, g_s\}$ is a Gröbner-Shirshov basis of $I$.

**Proof.** By way of contradiction, we suppose that $G'$ is not a Gröbner-Shirshov basis, i.e., the following set $E$ is not empty:

$$E = \{f[u] \in I \times A^m : f \neq 0, \text{lm}(f) \text{ is not divisible by } \text{lm}(g) \text{ for any } g \in G'\}.$$ 

We choose $f[u] \in E$ such that $f[u]$ has minimal signature among $E$. By the definition of a strong Gröbner-Shirshov basis, there exist $g_i^{[v_i]} \in G$ and $t \in M$ such that $\text{lm}(tv_i) = \text{lm}(u)$ and $\text{lm}(tg_i) \leq \text{lm}(f)$. If $\text{lm}(tg) = \text{lm}(f)$, then $\text{lm}(f)$ is divisible by $\text{lm}(g)$, contradicting our assumption that $f \in E$. Hence $\text{lm}(tg) < \text{lm}(f)$. Let $h[w] = f[u] - ct g[v]$ where $c = \frac{\text{lm}(u)}{\text{lm}(tv)}$. Then $\text{lm}(h) = \text{lm}(f)$ and thus $\text{lm}(h)$ is not divisible by $\text{lm}(g')$ for any $g' \in G'$. Hence $h[w] \in E$. By the choice of $c$, we have that $\text{lm}(u) = \text{lm}(ctv)$ and thus $\text{lm}(u) < \text{lm}(u)$, which contradicts the minimality of $f[u]$ in $E$.

In a similar way, we can prove the following

**Lemma 3.5.** Suppose that $G$ is a $t$-strong Gröbner-Shirshov basis of $I$. Then, for any $f[u] \in I \times A^m$ with $\text{lm}(u) < t$, there exist $g_i^{[v_i]} \in G$ and $t \in M$ such that $\text{lm}(tg) = \text{lm}(f)$ and $\text{lm}(tv) \leq \text{lm}(u)$.
Suppose that \( f^{[u]}, g^{[v]} \in I \times A^m \) are nonzero and \( \text{lm}(tf^{[u]}) \geq \text{lm}(tg^{[v]}) \) where
\[
    t_f = \frac{\text{lcm}(\text{lm}(f), \text{lm}(g))}{\text{lm}(f)}, \quad t_g = \frac{\text{lcm}(\text{lm}(f), \text{lm}(g))}{\text{lm}(g)}.
\]
Then the ordered 4-tuple \((t_f, f^{[u]}, t_g, g^{[v]})\) is called the critical pair of \( f^{[u]} \) and \( g^{[v]} \). Furthermore, the critical pair \((t_f, f^{[u]}, t_g, g^{[v]})\) is said to be regular if \( \text{lm}(tf^{[u]}) > \text{lm}(tg^{[v]}) \). With the above notation, we have the following

**Lemma 3.6.** Suppose that \((t_f, f^{[u]}, t_g, g^{[v]})\) is the critical pair of \( f^{[u]} \) and \( g^{[v]} \). Then \( \text{lm}(\text{SPoly}(f, g)) < \text{lm}(tf f) = \text{lm}(tg g) \).

Recall that a non-strict partial order on a set \( P \) is a binary relation \( \leq_P \) over \( P \) which is reflexive, antisymmetric, and transitive. We call \( <_P \) a (strict) partial order over \( P \).

Now we are in a position to introduce the rewriting criterion.

**Definition 3.7 (Rewriting Criterion).** Let \( S = \{ f^{[u]} : j \in J \} \subseteq I \times A^m \) where \( J \subseteq \mathbb{N} \) is a nonempty index set, and \( < \) be a partial order on \( S \). Suppose that \( f^{[u]} \in S \) and \( t \in M \). Then \( t(f^{[u]}) \) is called rewritable by \( S \) (with respect to \( < \)) if there exist \( g^{[v]} \in S \) and \( t' \in M \) such that \( \text{lm}(t'v) = \text{lm}(tu) \) and \( g^{[v]} <_S f^{[u]} \). In particular, a critical pair \((t_f, f^{[u]}, t_g, g^{[v]})\) of \( S \) is called rewritable by \( S \) if either \( t_f(f^{[u]}) \) or \( t_g(g^{[v]}) \) is rewritable by \( S \).

**Lemma 3.8.** Suppose that \( t(f^{[u]}) \) is rewritable by a finite subset \( S \subseteq I \times A^m \) with respect to a partial order \( <_S \) on \( S \). Then there exist \( g^{[v]} \in S \) such that \( \text{lm}(t'v) = \text{lm}(tu) \), \( g^{[v]} <_S f^{[u]} \) and \( t'g(v) \) is not rewritable by \( S \).

**Proof.** Since \( t(f^{[u]}) \) is rewritable by \( S \), by definition, there exist \( g^{[v_0]} \in S \) such that \( t_0(g^{[v_0]}) \) is not rewritable by \( S \), then \( g^{[v]} := g^{[v_0]} \) is as required. We assume that \( t_0(g^{[v_0]}) \) is rewritable by \( S \). Then there exist \( g^{[v_1]} \in S \) and \( t_1 \in M \) such that \( \text{lm}(t_1v_0) = \text{lm}(t_0u_0) \) and \( g^{[v_1]} <_S g^{[v_0]} \). If \( t_1(g^{[v_1]}) \) is not rewritable by \( S \), then \( g^{[v]} := g^{[v_1]} \) is as required. Otherwise, if \( t_1(g^{[v_1]}) \) is rewritable by \( S \) then we repeat the above process and obtain a chain
\[
    f^{[u]} >_S g^{[v_0]} >_S g^{[v_1]} >_S g^{[v_2]} >_S \cdots
\]
where each \( g_i \) is rewritable by \( g^{[v_i+1]} \in S \). Since \( S \) is finite, the above chain contains only finitely many \( g_i \), say it ends with \( g^{[v_n]} \) for some \( n \in \mathbb{N} \). Then \( g^{[v]} := g^{[v_n]} \) is as required.

The following is a key lemma for deriving the criterion for strong Gröbner-Shirshov bases (Theorem 3.10). Roughly speaking, this lemma tells us that, among elements with the same signature, a nonrewritable one has a minimal leading monomial.

**Lemma 3.9.** Let \( t \) be a monomial in \( A^m \) and let \( G \) be a \( t \)-strong Gröbner-Shirshov basis of \( I \) with a partial order \( <_G \). Suppose that every regular critical pair of \( G \) is rewritable by \( G \). For any \( t_0 \in M \) and \( f_0^{[u_0]} \in G \) with \( \text{lm}(t_0u_0) \leq t \), if \( t_0(f_0^{[u_0]}) \) is not rewritable by \( G \), then \( \text{lm}(t_0f_0) \leq \text{lm}(f) \) for any \( f^{[u]} \in I \times A^m \) with \( \text{lm}(u) = \text{lm}(t_0u_0) \).

**Proof.** By way of contradiction, we assume that \( N \neq \emptyset \), where
\[
    N = \{ (t_0, f_0^{[u_0]}), f_0^{[u_0]} \in M \times G : \text{lm}(t_0u_0) \leq t, \text{lm}(t_0f_0) > \text{lm}(f) \}.
\]
Suppose \( (t_0, f_0^{[u_0]}) \in N \) with minimal \( \text{lm}(t_0u_0) \) among \( N \) and suppose \( t_0 = x^\alpha \). Then there exists \( f^{[u]} \in I \times A^m \) such that \( \text{lm}(u) = \text{lm}(t_0u_0) \) and \( \text{lm}(t_0f_0) > \text{lm}(f) \). Let \( f^{[u]} = t_0(f_0^{[u_0]}) - c f^{[u]} \in I \times A^m \) where \( c = \frac{\alpha^\beta(k(u))}{k(u)} \).

Then
\[
    \text{lm}(f) = \text{lm}(t_0f_0) \quad \text{and} \quad \text{lm}(f) < \text{lm}(t_0u_0) \leq t.
\]
Since $G$ is a $t$-strong Gröbner-Shirshov basis, by Lemma 3.5, there exist $g^{[v]} \in G$ and $t_g \in M$ such that $\text{Im}(t_g g) = \text{Im}(\overline{f})$ and $\text{Im}(t_g v) \leq \text{Im}(\overline{u})$. Let

$$D = \{(t_g, g^{[v]}) \in M \times G : \text{Im}(t_g g) = \text{Im}(\overline{f}), \text{Im}(t_g v) \leq \text{Im}(\overline{u})\}.$$ 

Suppose $(t_g, g^{[v]})$ is a minimal pair in $D$, i.e., there is no pair $(t_g', g^{[v]'}) \in D$ such that either $\text{Im}(t_g g') < \text{Im}(t_g v)$, or $\text{Im}(t_g' v') = \text{Im}(t_g v)$ and $g^{[v']} <_G g^{[v]}$.

We claim that $(\overline{t}_0, f_0^{[u_0]}, \overline{t}_g, g^{[v]})$ is a regular critical pair of $f_0^{[u_0]}$ and $g^{[v]}$, where

$$\overline{t}_0 = \frac{\text{lcm}(\text{Im}(f_0), \text{Im}(g))}{\text{Im}(f_0)}$$

and $\overline{t}_g = \frac{\text{lcm}(\text{Im}(f_0), \text{Im}(g))}{\text{Im}(g)}$.

To obtain a contradiction, we assume that $\text{Im}(\overline{t}_0 u_0) \leq \text{Im}(\overline{t}_g v)$. Note that $\text{Im}(t_0 f_0) = \text{Im}(t_g g)$ is a multiple of $\text{lcm}(\text{Im}(f_0), \text{Im}(g)) = \text{Im}(\overline{t}_0 f_0) = \text{Im}(\overline{t}_g g)$, hence

$$\text{Im}(\overline{t}_0 f_0) = \text{Im}(\overline{t}_g g).$$

i.e., $\text{Im}(t_0 u_0) \leq \text{Im}(t_g v)$, contradicting the fact $\text{Im}(t_g v) \leq \text{Im}(\overline{u}) < \text{Im}(t_0 u_0)$. Hence our claim is true.

By the hypothesis of the lemma, the regular critical pair $(\overline{t}_0, f_0^{[u_0]}, \overline{t}_g, g^{[v]})$ is rewritable by $G$, i.e., either $\overline{t}_0(f_0^{[u_0]})$ or $\overline{t}_g(g^{[v]})$ is rewritable by $G$. Since $\overline{t}_0$ divides $t_0$, if $\overline{t}_0(f_0^{[u_0]})$ is rewritable by $G$ then so is $(f_0^{[u_0]})$, which is a contradiction. Thus $\overline{t}_g(g^{[v]})$ is rewritable by $G$ and hence so is $t_g g^{[v]}$. By Lemma 3.8, there exist $g^{[v_0]} \in G$ and $t_g' \in M$ such that $\text{Im}(t_0' v_0) = \text{Im}(t_g g)$, $g^{[v_0]} <_G g^{[v]}$, and $t_0' v_0$ is not rewritable by $G$. Now we claim that $\text{Im}(t_0' v_0) \leq \text{Im}(t_g g)$. Otherwise, if $\text{Im}(t_0' v_0) > \text{Im}(t_g g)$, then it is easy to see that $(t_0' v_0) \in N$ (note that $t_g g^{[v]} \in I$ and $\text{Im}(t_0' v_0) = \text{Im}(t_g v) \leq \text{Im}(\overline{u}) < t$). But, $\text{Im}(t_0' v_0) = \text{Im}(t_g v) < \text{Im}(t_0 u_0)$, contradicting the fact that $(t_0', f_0^{[u_0]})$ has minimal $\text{Im}(t_0 u_0)$ among $N$. Thus our claim holds true.

Now we have two cases to consider: $\text{Im}(t_0' v_0) = \text{Im}(t_g g)$ and $\text{Im}(t_0' v_0) < \text{Im}(t_g g)$. Our goal is to deduce a contradiction for each case and thus end the proof of the lemma. If $\text{Im}(t_0' v_0) = \text{Im}(t_g g)$, then $\text{Im}(t_g g) \leq \text{Im}(\overline{r}_0)$, we have $(t_0' v_0) \in D$. By the minimality of $(t_0', g^{[v]})$ among $D$, we have $g^{[v]} \geq G \overline{t}_0 g^{[v_0]}$, which contradicts the fact that $g^{[v_0]} <_G g^{[v]}$. Now consider the second case: $\text{Im}(t_0' v_0) < \text{Im}(t_g g)$. Let

$$\overline{g}^{[v]} = t_g g^{[v]} - c_0' g^{[v_0]} \in G, \quad c = \frac{\text{exp}(t_g) \text{lcm}(v)}{\text{exp}(t_g) \text{lcm}(v_0)}.$$ 

Then $\text{Im}(\overline{g}) = \text{Im}(t_g g)$ and $\text{Im}(\overline{f}) < \text{Im}(t_g v) < \text{Im}(t_0 u_0) \leq t$. Since $G$ is a $t$-strong Gröbner-Shirshov basis, by Lemma 3.5, there exist $h^{[w]} \in G$ and $t_h \in M$ such that $\text{Im}(t_h h) = \text{Im}(\overline{g}) = \text{Im}(t_g g) = \text{Im}(t_0 f_0)$ and $\text{Im}(t_h w) \leq \text{Im}(\overline{f}) < \text{Im}(t_g v) \leq \text{Im}(\overline{u})$. Thus, $h^{[w]} \in D$. But then the inequality $\text{Im}(t_h w) < \text{Im}(t_g v)$ implies that $(t_g, g^{[v]})$ is not minimal in $D$, which is a contradiction.

The following theorem gives a criterion for strong Gröbner-Shirshov bases.

**Theorem 3.10.** Let $A$ be a skew solvable polynomial ring and let $I$ be a left ideal of $A$ generated by $m \in \mathbb{N}$ elements. Suppose that $G = \{s^{[u]}_i : 1 \leq i \leq s \} \subseteq I \times A^M$ with a partial order $<_G$, where $s \in \mathbb{N}$. Then $G$ is a strong Gröbner-Shirshov basis of $I$ if the following conditions hold:

(i) For any $1 \leq i \leq m$, there exists $g^{[w]} \in G$ such that $\text{Im}(u) = e_i$.

(ii) Every regular critical pair of elements from $G$ is rewritable by $G$ with respect to $<_G$.

**Proof.** (By contradiction.) Suppose $G$ is not a strong Gröbner-Shirshov basis, i.e., $N \neq \emptyset$ where

$$N = \{f^{[u]} \in I \times A^M : \text{there exists no } (t, g^{[v]}) \in M \times G \text{ such that } \text{Im}(t v) = \text{Im}(u), \text{Im}(g) \leq \text{Im}(f)\}.$$ 

Let $f^{[w]} \in N$ with a minimal signature $\text{Im}(u)$ among $N$. Suppose $\text{Im}(u) = t e_j$ for some $t \in M$ and $1 \leq j \leq m$. Then $G$ is a $t e_j$-strong Gröbner-Shirshov basis. By condition (i) of the theorem, there exists $g^{[v]} \in G$ such that $\text{Im}(v) = e_j$. Then $\text{Im}(t v) = \text{Im}(u)$. If $t(g^{[v]})$ is rewritable by $G$, then there exist $f_1^{[v_1]} \in G$ and $t_1 \in M$ such that $\text{Im}(t_1 v_1) = \text{Im}(t v) = \text{Im}(u)$ and $f_1^{[v_1]} <_G g^{[v]}$. Repeating this process and by a similar argument as in the proof of Lemma 3.8, we can prove that there exist $h^{[w]} \in G$ and $s \in M$ such that $\text{Im}(s w) = \text{Im}(u)$ and $s(h^{[w]})$ is not rewritable by $G$. Applying Lemma 3.9 gives that $\text{Im}(s h) = \text{Im}(f)$. But the facts $\text{Im}(s w) = \text{Im}(u)$ and $f^{[w]} \in N$ imply that $\text{Im}(s h) > \text{Im}(f)$, which is a contradiction.
4 A Signature-based algorithm

In this section, we present a signature-based algorithm for computing a strong Gröbner-Shirshov basis in skew solvable polynomial rings.

As before, let $A = k(x; \sigma, \delta, c, p)$ be a skew solvable polynomial ring over $k$, $f_1, \ldots, f_m \in A$, $m \in \mathbb{N}$, and let $I$ be the left ideal of $A$ generated by $f_1, \ldots, f_m$.

Suppose $f^{[u]}$, $g^{[v]} \in I \times A^m$. We say $f^{[u]}$ is reducible by $g^{[v]}$ if there exists $t \in M$ such that $\text{lm}(tg) = \text{lm}(f)$ and $\text{lm}(tv) < \text{lm}(u)$. Moreover, if $G \subseteq A \times A^m$ and $g^{[v]} \in G$, then $f^{[u]} \rightarrow_G f^{[u]} - ct(g^{[v]})$ is said to be a one-step-reduction by $G$ where $c = \text{lc}(f)/\text{lc}(g)$. If $f^{[u]}$ is obtained from $f^{[u]}$ by finitely many one-step-reductions by $G$ and $f^{[u]}$ is not reducible by $G$, then we say that $f^{[u]}$ is a remainder of $f^{[u]}$ modulo $G$. With the above definitions, we have the following

**Lemma 4.1.** Suppose that $f^{[u]}$ is a remainder of $f^{[u]}$ modulo $G$. Then $\text{lm}(f') < \text{lm}(f)$ and $\text{lm}(u') = \text{lm}(u)$.

**Proof.** Note that in a one-step-reduction $f^{[u]} \rightarrow_G f^{[u]} - ct(g^{[v]}) = (f - ctg)u - ctv$, since $\text{lm}(tg) = \text{lm}(f)$ and $\text{lm}(tv) < \text{lm}(u)$, we have $\text{lm}(g) < \text{lm}(f)$ and $\text{lm}(v) = \text{lm}(u)$. Thus the lemma follows by induction on the number of one-step-reductions to obtain $f^{[u]}$ from $f^{[u]}$. \hfill $\square$

Now we are in a position to state our main algorithm.

**Algorithm 4.2** (Algorithm for strong Gröbner-Shirshov bases).

**Input:** $F = \{ f_1^{[e_1]}, \ldots, f_m^{[e_m]} \} \subseteq A \times A^m$

**Output:** A strong Gröbner-Shirshov basis $G$ of the left ideal $I$ of $A$ generated by $F$.

1. $G := F$
2. $\text{CPairs} := \{ \text{regular critical pair} (t_f, f^{[u]}, t_g, g^{[v]}): f^{[u]}, g^{[v]} \in G \}$
3. **While** $\text{CPairs} \neq \emptyset$ **Do**
4. Choose $(t_f, f^{[u]}, t_g, g^{[v]}) \in \text{CPairs}$
5. $\text{CPairs} := \text{CPairs} \setminus \{ (t_f, f^{[u]}, t_g, g^{[v]} \}$
6. If $(t_f, f^{[u]}, t_g, g^{[v]})$ is not rewritable by $G$ **then**
7. $h^{[w]} := \text{a remainder of SPoly}(f^{[u]}, g^{[v]}$ modulo $G$
8. $\text{CPairs} := \text{CPairs} \cup \{ \text{regular critical pair} (t_h, h^{[w]}, t_h, h^{[w]}): h^{[w]} \in G \}$
9. $G := G \cup \{ h^{[w]} \}$
10. **End If**
11. **End Do**
12. **Return** $G$

Note that in Line 6 of the above algorithm, a partial order on $G$ is needed. The GVW-orders implied by the criterion in [11] will be used in our algorithm, which can be updated automatically when a new element is added to $G$, i.e., when $G := G \cup \{ h^{[w]} \}$ in the algorithm.

**Definition 4.3.** A partial order $<_G$ on $G \subseteq I \times A^m$ is called a GVW-order if, for any $f^{[u]}, g^{[v]} \in G$, we have $f^{[u]} <_G g^{[v]}$ whenever one of the following conditions hold:

(a) $\text{lm}(t'g) < \text{lm}(tf)$ where $t' = \frac{\text{lcm}(\text{lm}(u), \text{lm}(v))}{\text{lm}(f)}$ and $t = \frac{\text{lcm}(\text{lm}(u), \text{lm}(v))}{\text{lm}(u)}$.
(b) $\text{lm}(t'g) = \text{lm}(tf)$ and $g^{[v]}$ is added to $G$ later than $f^{[u]}$.

**Theorem 4.4.** If a GVW-order is used in the Rewriting Criterion of Algorithm 4.2, then the algorithm terminates after finitely many steps and returns a strong Gröbner-Shirshov basis of $I$.

**Proof.** (Correctness.) If the algorithm terminates after finitely many steps, then its correctness follows clearly from Theorem 3.10.
Thus, from Lemma 4.1, \( h \) is denoted as \( \text{S} \) by \( L \). By the Hilbert basis theorem of polynomial algebras, the above chain has a finite length (we may suppose the chain \( \text{S} \) is rewritable by \( h \)). Then \( h \) is divisible by \( h(\mathbf{w}) \) for any \( h(\mathbf{w}) \in G \). Otherwise, we assume that \( h(\mathbf{w}) \) is divided by \( \mathbf{h}^{(\mathbf{w})} \) for some \( \mathbf{h}^{(\mathbf{w})} \in G \). Now we have the following three cases and we deduce a contradiction for each case, which ends the proof of the claim.

Case (1): \( h_0 = 0 \). In this case, it is easy to see from the definition of \( \varphi \) that \( \text{S} \) divides \( \text{S} \). Then \( \text{S} \) is a regular critical pair and not rewritable by \( G \) with respect to a GVW-order \( \prec_G \), and \( h(\mathbf{w}) \) is a remainder of \( h(\mathbf{w}) \) modulo \( G \). Therefore \( h(\mathbf{w}) \) is divisible by \( h(\mathbf{w}) \) and \( h(\mathbf{w}) \) is a contradiction.

Case (2): \( h_0 \neq 0 \) and \( h = 0 \). From the definition of \( \varphi \), it is impossible that \( \varphi(h(\mathbf{w})) \) divides \( \varphi(h(\mathbf{w})) \).

Case (3): \( h_0 \neq 0 \) and \( h \neq 0 \). Let \( s = \text{S} / \text{S} \) and \( t = \text{S} / \text{S} \). If \( s \leq t \), then, by Lemmas 3.6 and 4.1, we have that \( \text{S} \leq \text{S} \) and \( \text{S} \leq \text{S} \). Suppose that

\[
\alpha = \frac{\text{S}}{\text{S}}, \quad \beta = \frac{\text{S}}{\text{S}},
\]

and \( \alpha', \beta' \) divides \( \alpha \). Hence \( \alpha' \) divides \( \alpha' \). Now \( \alpha' \) is a GVW-order, it follows from Definition 4.3 that \( h(\mathbf{w}) \prec_G h(\mathbf{w}) \). Thus \( \text{S} \prec_G \text{S} \). Now suppose \( s > t \). Then \( \text{S} \) is divisible by \( \text{S} \) and \( \text{S} \) is divisible by \( \text{S} \). Hence, \( h(\mathbf{w}) \) is reducible by the set \( \{ h(\mathbf{w}) \} \). Now return to the proof of the termination of the algorithm. The “While Loop” of the algorithm (Lines 3–11), if \( \{ h(\mathbf{w}) \} \) is regular and not rewritable by \( G \) with respect to \( \prec_G \), then \( h(\mathbf{w}) \) is added to \( G \), and the new \( G \) is denoted as \( G_1 = G \cup \{ h(\mathbf{w}) \} \). From the above claim, the ideal of \( k[Y, Z, W] \) generated by \( \varphi(G) \) is strictly contained in the ideal generated by \( \varphi(G) \). Repeating the While Loop gives a chain of ideals of \( k[Y, Z, W] \):

\[
\varphi(G) \subsetneq \varphi(G) \subsetneq \varphi(G) \subsetneq \cdots
\]

By the Hilbert basis theorem of polynomial algebras, the above chain has a finite length (we may suppose the chain ends with \( \varphi(G_L) \), \( L \in \mathbb{N} \)). Hence after finitely many repeats of the While Loop, every regular critical pair in \( \text{CPairs} \) is rewritable by \( G_L \) and thus the algorithm terminates.

In summary, a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings over a field has been presented in this paper. This algorithm can detect redundant S-polynomials (i.e., the S-polynomials corresponding to nonregular critical pairs) and therefore it is more efficient than Buchberger’s algorithm. The implementation of the proposed algorithms in a computer algebra system (e.g., Maple, and Singular) and computing examples will be discussed in the near future.

Acknowledgement: We would like to thank the anonymous referees for their careful reading and valuable comments that have improved the readability of this article. The majority of this work was done during the stay of the first author at the University of Manitoba. This work was supported in part by NSERC and MGS.
References

[1] Adams W. W. and Loustaunau P., An introduction to Gröbner bases, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.
[2] Bokut' L. A., Chen Y., and Shum K. P., Some new results on Gröbner-Shirshov bases, Proceedings of International Conference on Algebra 2010–Advances in Algebraic Structures (W. Hemakul, S. Wahyuni, and P. W. Sy, eds.), 2012, pp. 53–102.
[3] Buchberger B., Ein algorithmus zum auffinden der basislemente des restklassenringes nach einem nulldimensionalen polynomialideal, Ph.D. thesis, University of Innsbruck, 1965.
[4] Bueso J. L., Gómez-Torrecillas J., and Verschoren A., Algorithmic methods in non-commutative algebra: Applications to quantum groups, Mathematical Modelling: Theory and Applications, vol. 17, Springer, 2003.
[5] Chyzak F. and Salvy B., Non-commutative elimination in Ore algebras proves multivariate identities, J. Symbolic Comput. 26 (1998), no. 2, 187–227.
[6] Faugère J. C., A new efficient algorithm for computing Gröbner bases (F4), J. Pure Appl. Algebra 139 (1999), no. 1, 61–88.
[7] 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, ACM, 2002, pp. 75–83.
[8] Gallego C. and Lezama O., Gröbner bases for ideals of a -PBW extensions, Comm. Algebra 39 (2011), no. 1, 50–75.
[9] Galligo A., Some algorithmic questions on ideals of differential operators, EUROCAL 85, Springer, 1985, pp. 413–421.
[10] 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, ACM, 2010, pp. 13–19.
[11] Gao S., Volny IV F., and Wang M., A new algorithm for computing Gröbner bases, Cryptology ePrint Archive (2010).
[12] Giesbrecht M., Reid G., and Zhang Y., Non-commutative Gröbner bases in Poincaré-Birkhoff-Witt extensions, Computer Algebra in Scientific Computing (CASC), 2002.
[13] Insa M. and Pauer F., Gröbner bases in rings of differential operators, London Math. Soc. Lecture Note Ser. (1998), 367–380.
[14] Kandri-Rody A. and Weispfenning V., Non-commutative Gröbner bases in algebras of solvable type, J. Symbolic Comput. 9 (1990), no. 1, 1–26.
[15] Levandovskyy V. and Schönemann H., Plural: a computer algebra system for noncommutative polynomial algebras, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 176–183.
[16] Ma X., Sun Y., and Wang D., On computing Gröbner bases in rings of differential operators, Sci. China Math. 54 (2011), no. 6, 1077–1087.
[17] Mansfield E. L. and Szanto A., Elimination theory for differential difference polynomials, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 191–198.
[18] Oh S.-Q., Catenarity in a class of iterated skew polynomial rings, Comm. Algebra 25 (1997), no. 1, 37–49.
[19] Shirshov A. I., Some algorithmic problems for Lie algebras, Sibirsk. Mat. Zh. 3 (1962), no. 2, 292–296.
[20] Sun Y., Wang D., Ma X., and Zhang Y., A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras, Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation, ACM, 2012, pp. 351–358.
[21] Zhang Y. and Zhao X., Gel’fand-Kirillov dimension of differential difference algebras, LMS J. Comput. Math. 17 (2014), no. 1, 485–495.
[22] Zhou M. and Winkler F., On computing Gröbner bases in rings of differential operators with coefficients in a ring, Math. Comput. Sci. 1 (2007), no. 2, 211–223.