Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 31(7): 3999–4010.
DOI: 10.3934/era.2023203
Received: 20 January 2023
Revised: 28 April 2023
Accepted: 08 May 2023
Published: 22 May 2023

Research article

Some improvements for the algorithm of Gröbner bases over dual valuation domain

Licui Zheng, Dongmei Li*and Jinwang Liu

Department of Mathematics and Computing Sciences, Hunan University of Science and Technology, Xiangtan 411201, China

* **Correspondence:** Email: dmli@hnust.edu.cn.

Abstract: As a special ring with zero divisors, the dual noetherian valuation domain has attracted much attention from scholars. This article aims at to improve the Buchberger's algorithm over the dual noetherian valuation domain. We present some criterions that can be applied in the algorithm for computing Gröbner bases, and the criterions may drastically reduce the number of S-polynomials in the course of the algorithm. In addition, we clearly demonstrate the improvement with an example.

Keywords: Gröbner bases; dual noetherian valuation domain; S-polynomials

1. Introduction

The notion of Gröbner bases in polynomials ring over a field was first introduced by Buchberger in [1, 2]. Since then, the works on Gröbner bases have attracted much attention from scholars [3–7]. As the research progressed , the theory was extended to different fields, such as the commutative ring, noncommutative ring, and even the rings with zero divisors [8–13]. We are particularly interested in the approach by [14], which proposed the Buchbergers algorithm over dual noetherian valuation domain $V[\varepsilon]$. $V[\varepsilon]$ is neither a valuation ring nor a Dedekind ring, which satisfies $\varepsilon^2 = 0$, and V is a valuation domain.

The main contribution of this paper is to present a more efficient algorithm for computing Gröbner bases. In the algorithm proposed in [14], we not only need to compute all S-polynomials which are generated by the original polynomials, but also need to calculate the S-polynomials of the new polynomials (produced by each step) and original polynomials. It means that a large number of S-polynomials need to be calculated each time. Therefore, we try to give some criterions to reduce the calculation of S-polynomials. Besides, based on the study of relations between S-polynomial, a criterion is given in Section 3, by using which we can filter the useless S-polynomial in a rather convenient way. Moreover, the other criterion is given by using which we may easily determine which two pairs' S-polynomial

need not to be computed. Finanlly, an improvement algorithm is notably improved, in which we not only obtain a decreased memory requirement, but also improve the efficiency.

Our paper is structured in the following way. We start by giving the mathematical background used in the subsequent sections in Section 2. In Section 3, we introduce some concepts and theories which are needed in our algorithm. In particular, we prove the correctness of our algorithm. In Section 4, we present our algorithm and clearly demonstrate the improvement with an example.

2. Preliminaries

We start with some basic facts from the algebra theory; for the detailed exposition of the subject we refer the reader to [1]. Throughout the paper, $V[\varepsilon]$ is the ring of the dual valuation domain satisfying to $\varepsilon^2 = 0$, whose elements are of the form $a + b\varepsilon$ with $a, b \in V$; here and below, V denotes the valuation domain. The set of all zero divisors corresponding to $V[\varepsilon]$ is denoted by J_ε, and $J_\varepsilon = \varepsilon V[\varepsilon] = \{\varepsilon a / a \in V\}$.

We denote the ring of polynomials in $x_1, x_2, ..., x_n$ over $V[\varepsilon]$ with $V[\varepsilon][x_1, x_2, ..., x_n]$. Given $\alpha = (\alpha_1, ..., \alpha_n) \in Z^n$, we denote by x^α the monomial $x_1^{\alpha_1}...x_n^{\alpha_n}$ in $V[\varepsilon][x_1, x_2, ..., x_n]$.For $f_1, ..., f_n$ in $V[\varepsilon][x_1, x_2, ..., x_n]$, we denote $\langle f_1, ..., f_k\rangle$ a so-called ideal in $V[\varepsilon][x_1, x_2, ..., x_n]$ which refers to a subset of polynomials which is closed under addition and multiplication with elements in $V[\varepsilon][x_1, x_2, ..., x_n]$ and is generated by these polynomials. An element of the form px^α is called a term of $V[\varepsilon][x_1, x_2, ..., x_n]$, where $p \in V[\varepsilon]$.

Now, having set the element's form, the next step is to introduce the concept of reduction. When speaking about the division of the terms of $V[\varepsilon][x_1, x_2, ..., x_n]$, we need to take into account that the division in $V[\varepsilon]$.

Definition 1. Let $p_1 = a_1 + b_1\varepsilon, p_2 = a_2 + b_2\varepsilon$ be two elements in $V[\varepsilon]$, we say p_1 divides p_2 when $a_1|a_2$ and $a_1|(b_2 - b_1\frac{a_1}{a_2})$ in V.

We can extend the division to the terms in R, where $R = V[\varepsilon][x_1, x_2, ..., x_n]$ is the free associative algebra with commuting variables $x_1, ..., x_m$, defined over the ring $V[\varepsilon]$. A term p_1x^α divides p_2x^β in R when p_1 divides p_2 in $V[\varepsilon]$ and x^α divides x^β in R. We shall emphasise here that the monomial order $\prec$ we used refers to a well order and if $x^\alpha \prec x^\beta$ then $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$ for all $\alpha, \beta, \gamma \in N^n$. For example, for lexicographic order, we say $x^\alpha \prec_{lex} x^\beta$ if the first left nonzero component of $\alpha - \beta < 0$.

For any polynomial $g = p_1x^{\alpha_1} + p_2x^{\alpha_2} + ... + p_nx^{\alpha_n}$ in R, and monomial ordering $\prec$, we denote the multidegree of g by $mdeg(g)$, that is, the maximum mutidegree appearing in p with respect to $\prec$, and lc(g), lm(g) and lt(g) stand for the leading coefficient,the leading monomial and the leading term of g respectively. It is obvious that lt(g) = lc(g)lm(g).

Definition 2. Let $f \in R$ and I is a subset of R, then f can be reduced by I if there exist at least one polynomial say g, such that lt(g)|lt(f).

Definition 3. Let $\prec$ be any monomial ordering. For an ideal $I \subset R$, we define its leading terms ideal as the ideal

$$\langle \mathrm{lt}(I)\rangle := \langle \mathrm{lt}(g) | g \in I \setminus \{0\}\rangle.$$

A finite subset $G \subset I$ is a Gröbner basis for I with respect to $\prec$, if $I = \langle G\rangle$ and $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(G)\rangle$.

Definition 4. Let$\prec$ be any monomial ordering, and $f_1, f_2 \in R$. For $i, j \in \{1, 2\}$, set $\mathrm{lt}(f_i) = (a_i+b_i\varepsilon)\mathrm{lm}(f_i)$ and $t = \mathrm{lcm}(\mathrm{lm}(f_1), \mathrm{lm}(f_2)) = t_1\mathrm{lm}(f_1) = t_2\mathrm{lm}(f_2)$, where $a_i, b_i \in V[\varepsilon]$, then the S-polynomial of f_1 and f_2 is given by:
1). Suppose that $\mathrm{lc}(f_1), \mathrm{lc}(f_2) \in J_\varepsilon$, then:

$$S(f_1, f_2) = \begin{cases} \frac{b_2}{b_1}t_1f_1 - t_2f_2, & b_1|b_2 \\ t_1f_1 - \frac{b_1}{b_2}t_2f_2, & b_2|b_1 \end{cases}$$

2). If $\mathrm{lc}(f_1) \in J_\varepsilon, \mathrm{lc}(f_2) \notin J_\varepsilon$, then:

$$S(f_1, f_2) = \begin{cases} \frac{a_2}{b_1}t_1f_1 - t_2\varepsilon f_2, & b_1|a_2 \\ t_1f_1 - \frac{b_1}{a_2}t_2\varepsilon f_2, & a_2|b_1 \end{cases}$$

If $\mathrm{lc}(f_2) \in J_\varepsilon, \mathrm{lc}(f_1) \notin J_\varepsilon$, just replace f_1 by f_2 and vice versa.
3). In the case when $\mathrm{lc}(f_1) \notin J_\varepsilon, \mathrm{lc}(f_2) \notin J_\varepsilon$, then:

$$S(f_1, f_2) = \begin{cases} \frac{a_2}{a_1}t_1(\varepsilon f_1) - t_2(\varepsilon f_2), & a_1|a_2 \\ t_1(\varepsilon f_1) - \frac{a_1}{a_2}t_2(\varepsilon f_2), & a_2|a_1 \end{cases}$$

To note that, compared with the definition of S-polynomial in Buchbergers algorithm, we also consider the S-polynomial of $S(f_1, f_1)$ when $\mathrm{lc}(f_1) \in J[\varepsilon]$ and in addition to the above definition. Set $S(f_1, f_1) = \varepsilon f_1$.

The following lemma is from [14]. We record it here for further use.

Lemma 5. *Let $\prec$ be a monomial order, and $f_1, ..., f_n \in R$, Suppose that the multidegree of $\sum_{i=1}^n v_if_i \prec \gamma$ for some $v_1, ..., v_n \in V[\varepsilon]$ and γ refers to the multidegree of f_i where $1 \le i \le n$:*

1) If for any $i, 1 \le i \le n, lc(f_i) \in J_\varepsilon$, then $\sum_{i=1}^n v_if_i$ is a linear combination with coefficients in $V[\varepsilon]$ of $S-$polynomials $S(f_i, f_j)$ for $1 \le i \le j \le s$;

2) If there exists i_0 such that $lc(f_{i_0}) \notin J_\varepsilon$, then $\varepsilon\sum_{i=1}^n v_if_i$ is a linear combination with coefficients in $V[\varepsilon]$ of $S(f_i, f_j)$, where $1 \le i \le j \le s$.

Furthermore, each $S-$polynomial has multidegree $\prec \gamma$.

3. Main results

This section is devoted to proving the main results in the present paper. Our main technique depends on some new properties of $S-$polynomial. Let us begin with the definition of standard representation.

Definition 6. Let G be a finite subset of $R, 0 \neq f \in R$, then f has a standard representation for G, if

$$f = \sum_{i=1}^{k} m_ip_i,$$

where m_i is a monomial, $p_i \in G, 1 \le i \le k$, and

$$max\{\mathrm{lm}(m_i p_i)|1 \le i \le k\} \le \mathrm{lm}(f).$$

Obviously, if f can be reduced to 0 by G, then f has a standard representation for G. However, the opposition is not necessarily the case, for example, $G = \{g_1, g_2\} = \{x_1x_2 + \varepsilon, x_2x_3 + \varepsilon\} \in V[\varepsilon][x_1, x_2, x_3]$, and $f = x_1x_2^2 + \varepsilon x_1 + \varepsilon x_2 - \varepsilon x_3$, then f has a standard representation for G with respect to the lexicographic oredr as

$$f = x_2(x_1x_2 + \varepsilon) + x_1(x_2x_3 + \varepsilon) - x_3(x_1x_2 + \varepsilon) = x_2g_1 + x_1g_2 - x_3g_1$$

but obviously f can not be reduced to zreo by G as G is not a Gröbner basis for $\{g_1, g_2\}$.

Lemma 7. *Let $\prec$ be a monomial order, $G = \{f_1, ..., f_s\}$ is a finite subset of $V[\varepsilon][x_1, ..., x_n]$ and $0 \notin G$, $I = \langle G\rangle$ is an ideal of R, then G is a Gröbner basis for I if and only if all the S-polynomials by G have a standard representation for G.*

The proof of this lemma we referes to [15].

Theorem 8. *Let I be an ideal of R and $f, g \in I$, then the $S-$polynomial has standard representation for G,in other words, is "useless" if $lm(f), lm(g)$ are coprime.*

Proof. Without loss of generality, let $f = \mathrm{lt}(f) + p, g = \mathrm{lt}(g) + q$, where $\mathrm{lt}(f) = \mathrm{lm}(f)(a_1 + b_1\varepsilon), \mathrm{lt}(g) = \mathrm{lm}(g)(a_2 + b_2\varepsilon)$, $a_1|a_2$ and $b_1|b_2$, (the proof is same when $a_2|a_1$ or $b_1|b_2$). Then, this theorem will be proved by classification as follows:

(i). Suppose that $\mathrm{lc}(f) \in J_\varepsilon, \mathrm{lc}(g) \in J_\varepsilon$, then:

$$\begin{aligned} S(f,g) &= \frac{b_2}{b_1}\mathrm{lm}(g)f - \mathrm{lm}(f)g \\ &= \frac{1}{b_1\varepsilon}[\mathrm{lt}(g)f - \mathrm{lt}(f)g] \\ &= \frac{1}{b_1\varepsilon}[(g-q)f - (f-p)g] \\ &= \frac{1}{b_1\varepsilon}(pg - qf). \end{aligned}$$

Then, $\mathrm{lm}(S(f,g)) = max\{\mathrm{lm}(pg), \mathrm{lm}(qf)\}$ if $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \mathrm{lm}(f)\mathrm{lm}(g)$, then $\mathrm{lm}(pg) \neq \mathrm{lm}(qf)$, or will contradict with the definition of leading term. Furthermore, $\mathrm{lt}(S(f,g)) \in \langle \mathrm{lt}(I)\rangle$, which means $S(f,g)$ has a standard representation for G.

(ii). In the case when $\mathrm{lc}(f) \in J_\varepsilon, \mathrm{lc}(g) \notin J_\varepsilon$. then:

$$\begin{aligned}
S(f,g) &= \frac{a_2}{b_1}\mathrm{lm}(g)f - \mathrm{lm}(f)(\varepsilon g)\\
&= \frac{1}{b_1}\{[\mathrm{lt}(g) - b_2\varepsilon\mathrm{lm}(g)]f - \mathrm{lt}(f)g\}\\
&= \frac{1}{b_1}(\mathrm{lt}(g)f - \mathrm{lt}(f)g) - \frac{1}{b_1}(b_2\varepsilon\mathrm{lm}(g))f\\
&= \frac{1}{b_1}[(g-q)f - (f-p)g] - \frac{1}{b_1}[b_2\varepsilon(b_1\varepsilon\mathrm{lm}(f) + p)]\mathrm{lm}(g)\\
&= \frac{1}{b_1}(pg - qf) - \frac{1}{b_1}(b_2\varepsilon p\mathrm{lm}(g))\\
&= \frac{1}{b_1}[p(g - b_2\varepsilon\mathrm{lm}(g)) - qf].
\end{aligned}$$

Furthermore, $\mathrm{lm}(g-b_2\varepsilon\mathrm{lm}(g)) = \mathrm{lm}(g)$ as $\mathrm{lc}(g) \notin J_\varepsilon$ and $\mathrm{lm}[p(g-b_2\varepsilon\mathrm{lm}(g))] = \mathrm{lm}(pg)$, so $\mathrm{lm}(S(f,g)) = max\{\mathrm{lm}(pg), \mathrm{lm}(qf)\}$, which is the same as above.

(iii). If $\mathrm{lc}(f) \notin J_\varepsilon, \mathrm{lc}(g) \notin J_\varepsilon$, then:

$$\begin{aligned}
S(f,g) &= \frac{a_2}{a_1}\mathrm{lm}(g)(\varepsilon f) - \mathrm{lm}(f)(\varepsilon g)\\
&= \frac{1}{a_1}\{[\mathrm{lt}(g) - b_2\varepsilon\mathrm{lm}(g)]\varepsilon f - [\mathrm{lt}(f) - b_1\varepsilon\mathrm{lm}(f)](\varepsilon g)\}\\
&= \frac{1}{a_1}[\mathrm{lt}(g)\varepsilon f - \mathrm{lt}(f)\varepsilon g]\\
&= \frac{1}{a_1}\varepsilon[\mathrm{lt}(g)f - \mathrm{lt}(f)g]\\
&= \frac{\varepsilon}{a_1}[(g-q)f - (f-p)g]\\
&= \frac{\varepsilon}{a_1}(pg - qf),
\end{aligned}$$

which is the same as case (i).

We complete the proof.

The crucial method for our main results heavily depends on this theorem. From this theorem, we just need to compute the $S-$polynomials of the elements whose leading terms are not coprime instead of computing all $S-$polynomials as in [14], thus finally simplifying the algorithm. We call this criterion the "Product Criterion".

Next, we give another method to reduce the computation of $S-$polynomials.

Definition 9. Let$\prec$ be any monomial ordering and $f_1, f_2 \in R$. For $i, j \in \{1, 2\}$, set $\mathrm{lt}(f_i) = (a_i+b_i\varepsilon)\mathrm{lm}(f_i)$, where $a_i, b_i \in V$, then the least common multiple of $\mathrm{lt}(f_1)$ and $\mathrm{lt}(f_2)$ is given by:

1). Suppose that $\mathrm{lc}(f_1), \mathrm{lc}(f_2) \in J_\varepsilon$, then:

$$\mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2)) = \mathrm{lcm}(\mathrm{lm}(f_1), \mathrm{lm}(f_2)) \cdot \mathrm{lcm}(\mathrm{lc}(f_1), \mathrm{lc}(f_2)).$$

2). If $\mathrm{lc}(f_1) \in J_\varepsilon, \mathrm{lc}(f_2) \notin J_\varepsilon$, then:

$$\mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2)) = \mathrm{lcm}(\mathrm{lm}(f_1), \mathrm{lm}(f_2)) \cdot \mathrm{lcm}(\mathrm{lc}(f_1), \varepsilon\mathrm{lc}(f_2)).$$

If $\mathrm{lc}(f_2) \in J_\varepsilon, \mathrm{lc}(f_1) \notin J_\varepsilon$, just replace f_1 by f_2 and vice versa.

3). In the case when $\mathrm{lc}(f_1) \notin J_\varepsilon, \mathrm{lc}(f_2) \notin J_\varepsilon$, then:

$$\mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2)) = \mathrm{lcm}(\mathrm{lm}(f_1), \mathrm{lm}(f_2)) \cdot \mathrm{lcm}(\varepsilon \mathrm{lc}(f_1), \varepsilon \mathrm{lc}(f_2)).$$

Theorem 10. *Let I be an ideal of R and $p, g_1, g_2 \in I$, then $S(g_1, g_2)$ can be reduced to zero by I if $lt(p)|lcm(lt(g_1), lt(g_2))$ and $S(g_1, p), S(g_2, p)$ can be reduced to zero.*

Proof. In order to prove the theorem, in the following situation, we have to start splitting according to whether $\mathrm{lc}(p), \mathrm{lc}(g_1)$ and $\mathrm{lc}(g_2)$ belong to J_ε.

Without loss of generality, let $\mathrm{lc}(p) = a + b\varepsilon, \mathrm{lc}(g_1) = a_1 + b_1\varepsilon, \mathrm{lc}(g_2) = a_2 + b_2\varepsilon$, and further assume that $u_1\mathrm{lm}(g_1) = v_1\mathrm{lm}(p) = \mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))$ and $v_2\mathrm{lm}(p) = u_2\mathrm{lm}(g_2) = \mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))$, then $\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))|\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))$ as $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$. Say $s_1\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p)) = \mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))$.

For the same reason $\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))|\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))$. Let $s_2\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p)) = \mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))$, then $s_1v_1 = s_2v_2$,

1). In the case when $\mathrm{lc}(p) \in J_\varepsilon$ but $\mathrm{lc}(g_1), \mathrm{lc}(g_2) \notin J_\varepsilon$. Say $\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) = a_1\varepsilon$ and $a_2|b$ (the proof is same when $\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) = a_2\varepsilon$ and $b|a_2$).

It is easy to get $b|a_1$ as $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$. We will then consider the $S-$polynomials of g_1, g_2 and p.

$$\begin{aligned} S(g_1, p) &= \varepsilon\frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_1))}{\mathrm{lm}(g_1)}g_1 - \frac{a_1}{b}\frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_1))}{\mathrm{lm}(p)}p \\ &= \varepsilon u_1 g_1 - \frac{a_1}{b}v_1 p, \end{aligned}$$

$$\begin{aligned} S(g_2, p) &= \varepsilon\frac{b}{a_2}\frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}g_2 - \frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_2))}{\mathrm{lm}(p)}p \\ &= \varepsilon\frac{b}{a_2}u_2 g_2 - v_2 p, \end{aligned}$$

$$\begin{aligned} S(g_1, g_2) &= \varepsilon\frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_1)}g_1 - \frac{a_1}{a_2}\varepsilon\frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}g_2 \\ &= \varepsilon s_1 u_1 g_1 - \varepsilon\frac{a_1}{a_2}s_2 u_2 g_2. \end{aligned}$$

it follows that:

$$s_1 S(g_1, p) - \frac{a_1}{b}s_2 S(g_2, p) = S(g_1, g_2).$$

2). Suppose $\mathrm{lc}(p), \mathrm{lc}(g_1), \mathrm{lc}(g_2) \in J_\varepsilon$, it follows that a, a_1, a_2 all equal to 0, without loss of generality, let $b_1|b$, then $b|b_2$ as $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$ (the proof is same when $b|b_1$ or $b_2|b$).

$$S(g_1, p) = \frac{\mathrm{lc}(p)}{\mathrm{lc}(g_1)}\frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_1))}{\mathrm{lm}(g_1)}g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g_1))}{\mathrm{lm}(p)}p$$

$$= \frac{b}{b_1}u_1g_1 - v_1p,$$

$$\begin{aligned} S(g_2,p) &= \frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}g_2 - \frac{\mathrm{lc}(g_2)}{\mathrm{lc}(p)}\frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_2))}{\mathrm{lm}(p)}p \\ &= u_2g_2 - \frac{b_2}{b}v_2p, \end{aligned}$$

it follows that:

$$\begin{aligned} b_1b_2s_1S(g_1,p) - b_1bs_2S(g_2,p) &= b_2s_1b_1(\frac{b}{b_1}u_1g_1 - v_1p) - bb_1s_2(u_2g_2 - \frac{b_2}{b}v_2p) \\ &= bb_2s_1u_1g_1 - b_1bs_2u_2g_2 \\ &= b(b_2s_1u_1g_1 - b_1s_2u_2g_2). \end{aligned}$$

We will then consider the $S-$polynomial of g_1, g_2.

$$\begin{aligned} S(g_1,g_2) &= \frac{\mathrm{lc}(g_2)}{\mathrm{lc}(g_1)}\frac{\mathrm{lcm}(\mathrm{lm}(g_1),\mathrm{lm}(g_2))}{\mathrm{lm}(g_1)}g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1),\mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}g_2 \\ &= \frac{b_2}{b_1}\frac{s_1\mathrm{lcm}(\mathrm{lm}(g_1),\mathrm{lm}(p))}{\mathrm{lm}(g_1)}g_1 - s_2\frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}g_2 \\ &= \frac{b_2}{b_1}s_1u_1g_1 - s_2u_2g_2. \end{aligned}$$

that means $S(g_1,g_2) = \frac{1}{b}[b_2s_1S(g_1,p) - bs_2S(g_2,p)]$,

3). If $\mathrm{lc}(p), \mathrm{lc}(g_1), \mathrm{lc}(g_2) \notin J_\varepsilon$, and assume that $a_2|a$, and say $\mathrm{lcm}(\mathrm{lc}(g_1),\mathrm{lc}(g_2)) = a_1\varepsilon$, that means $a_2|a_1$, (the proof of the other condition such as $a|a_2$ and $a_1|a_2$ is the same as this one). Then, $a|a_1$ as $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(g_1),\mathrm{lt}(g_2))$.

$$\begin{aligned} S(g_1,p) &= \varepsilon\frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_1))}{\mathrm{lm}(g_1)}g_1 - \frac{a_1}{a}\frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_1))}{\mathrm{lm}(p)}\varepsilon p \\ &= u_1\varepsilon g_1 - \frac{a_1}{a}v_1\varepsilon p, \end{aligned}$$

$$\begin{aligned} S(g_2,p) &= \frac{a}{a_2}\frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}\varepsilon g_2 - \frac{\mathrm{lcm}(\mathrm{lm}(p),\mathrm{lm}(g_2))}{\mathrm{lm}(p)}\varepsilon p \\ &= \frac{a}{a_2}u_2\varepsilon g_2 - v_2\varepsilon p, \end{aligned}$$

$$\begin{aligned} S(g_1,g_2) &= \frac{\mathrm{lcm}(\mathrm{lm}(g_1),\mathrm{lm}(g_2))}{\mathrm{lm}(g_1)}\varepsilon g_1 - \frac{a_1}{a_2}\frac{\mathrm{lcm}(\mathrm{lm}(g_1),\mathrm{lm}(g_2))}{\mathrm{lm}(g_2)}\varepsilon g_2 \\ &= s_1u_1\varepsilon g_1 - \frac{a_1}{a_2}s_2u_2\varepsilon g_2, \end{aligned}$$

and,

$$s_1 S(g_1, p) - \frac{a_1}{a} s_2 S(g_2, p) = S(g_1, g_2).$$

4). Assume that $\mathrm{lc}(p) \notin J_\varepsilon$, but $\mathrm{lc}(g_1), \mathrm{lc}(g_2) \in J_\varepsilon$, that refers to $a \neq 0, a_1 = 0, a_2 = 0$.

Without a loss of generality, let $b_1|b_2$ and $b_1|a$ (vice versa), then $\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) = b_2\varepsilon$.

There exists $c + d\varepsilon \in V[\varepsilon]$ such that $(a + b\varepsilon)(c + d\varepsilon) = b_2\varepsilon$ based on the fact that $\mathrm{lc}(p)|\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2))$, then we can get $c = 0, ad = b_2$, it follows $a|b_2$.

$$\begin{aligned} S(g_1, p) &= \frac{a}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(p)} \varepsilon p \\ &= \frac{a}{b_1} u_1 g_1 - v_1 p\varepsilon, \end{aligned}$$

$$\begin{aligned} S(g_2, p) &= \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(g_2)} g_2 - \frac{b_2}{a} \frac{\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))}{\mathrm{lm}(p)} \varepsilon p \\ &= u_2 g_2 - \frac{b_2}{a} v_2 p\varepsilon, \end{aligned}$$

$$\begin{aligned} S(g_1, g_2) &= \frac{b_2}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_2)} g_2 \\ &= \frac{b_2}{b_1} s_1 u_1 g_1 - s_2 u_2 g_2, \end{aligned}$$

and

$$\begin{aligned} s_1 \frac{b_2}{a} S(g_1, p) - s_2 S(g_2, p) &= s_1 \frac{b_2}{a} \frac{a}{b_1} (\frac{a}{b_1} u_1 g_1 - v_1 p\varepsilon) - s_2 (u_2 g_2 - \frac{b_2}{a} v_2 p\varepsilon) \\ &= S(g_1, g_2), \end{aligned}$$

5). If $\mathrm{lc}(p), \mathrm{lc}(g_1) \notin J_\varepsilon$, but $\mathrm{lc}(g_2) \in J_\varepsilon$, it means that $a, a_1 \neq 0, a_2 = 0$, let us assume $b_1|a$ and $a_1|b_2$ (vice versa), then $\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) = b_2\varepsilon$, and $a|b_2$ as $\mathrm{lc}(p)|\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2))$.

$$\begin{aligned} S(g_1, p) &= \frac{a}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(g_1)} \varepsilon g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(p)} \varepsilon p \\ &= \frac{a}{b_1} u_1 \varepsilon g_1 - v_1 p\varepsilon, \end{aligned}$$

$$\begin{aligned} S(g_2, p) &= \frac{\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))}{\mathrm{lm}(g_2)} g_2 - \frac{b_2}{a} \frac{\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))}{\mathrm{lm}(p)} \varepsilon p \\ &= u_2 g_2 - \frac{b_2}{a} v_2 p\varepsilon, \end{aligned}$$

$$S(g_1, g_2) = \frac{b_2}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_1)} \varepsilon g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_2)} g_2$$

$$= \frac{b_2}{b_1} s_1 u_1 \varepsilon g_1 - s_2 u_2 g_2,$$

$$\begin{aligned}\frac{b_2}{a} s_1 S(g_1, p) - s_2 S(g_2, p) &= \frac{b_2}{a} s_1 (\frac{a}{b_1} u_1 \varepsilon g_1 - v_1 p\varepsilon) - s_2 (u_2 g_2 - \frac{a_2}{a} v_2 p\varepsilon) \\ &= \frac{b_2}{b_1} s_1 u_1 \varepsilon g_1 - s_2 u_2 g_2 \\ &= S(g_1, g_2).\end{aligned}$$

6). The proof is the same as case 5) when $\mathrm{lc}(p), \mathrm{lc}(g_2) \notin J_\varepsilon$, but $\mathrm{lc}(g_1) \in J_\varepsilon$.

7). Suppose $\mathrm{lc}(p), \mathrm{lc}(g_1) \in J_\varepsilon$, but $\mathrm{lc}(g_2) \notin J_\varepsilon$, it follows that a and $a_1 = 0$, but $a_2 \neq 0$. Now further assume that $b_1|b$ and $b_1|a_2$((vice versa), then $b|a_2$ as $\mathrm{lc}(p)|\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2))$. Next, we'll consider the S-polynomials in detail.

$$\begin{aligned}S(g_1, p) &= \frac{b}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(p))}{\mathrm{lm}(p)} p \\ &= \frac{b}{b_1} u_1 g_1 - v_1 p,\end{aligned}$$

$$\begin{aligned}S(g_2, p) &= \frac{\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))}{\mathrm{lm}(g_2)} \varepsilon g_2 - \frac{a_2}{b} \frac{\mathrm{lcm}(\mathrm{lm}(g_2), \mathrm{lm}(p))}{\mathrm{lm}(p)} p \\ &= u_2 \varepsilon g_2 - \frac{a_2}{b} v_2 p,\end{aligned}$$

$$\begin{aligned}S(g_1, g_2) &= \frac{a_2}{b_1} \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2))}{\mathrm{lm}(g_2)} \varepsilon g_2 \\ &= \frac{a_2}{b_1} s_1 u_1 g_1 - s_2 u_2 g_2 \varepsilon,\end{aligned}$$

$$\begin{aligned}\frac{a_2}{b} s_1 S(g_1, p) - s_2 S(g_2, p) &= \frac{a_2}{b} s_1 (\frac{b}{b_1} u_1 g_1 - v_1 p) - s_2 (\varepsilon u_2 g_2 - \frac{a_2}{b} v_2 p) \\ &= \frac{a_2}{b} \frac{b}{b_1} s_1 u_1 g_1 - s_2 u_2 g_2 \varepsilon \\ &= S(g_1, g_2).\end{aligned}$$

8) The proof is the same as case 7) when $\mathrm{lc}(p), \mathrm{lc}(g_2) \in J_\varepsilon$, but $\mathrm{lc}(g_1) \notin J_\varepsilon$.

In all the above situations, $S(g_1, g_2)$ can always be expressed as a linear expression of $S(g_1, p)$ and $S(g_2, p)$, which follows that $S(g_1, g_2)$ can be reduced to zreo when $S(g_1, p), S(g_2, p)$ can be reduced to zero, and we deduce that $S(g_1, g_2)$ is finally "useless". This completes the proof.

Remark 11. In fact, $S(g_1, p)$ and $S(g_2, p)$ can be reduced to zero in the calculation process, as a consequence, $S(g_1, g_2)$ doesn't need to compute any more when $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$. This can finally reduce the amount of computation.

This theorem plays an important role in removing "useless" S-polynomial, and we call this the "Chain Criterion".

4. Algorithm

To further improve the efficiency of the algorithm given in [14], we propose some criterions to detect the useless S-polynomials. First, we propose the conception of standard representation, and prove that the S-polynomial is useless if it can be a standard representation. Furthermore, we only need to check whether it can be a standard representation but not to reduce to zero as in [14]. Second, we propose the leading term coprime to detect not only useless S-polynomial, but also the S-polynomials which need not be generated. We make this by investigating the leading terms of the S-polynomial and detecting useless S-polynomial with Theorem 8, rather than all the S-polynomials in the original algorithm. Hence, the proposed algorithm can greatly improve the efficiency of the original algorithm. We refer to the improved algorithm in Figure 1.

	An improvement algorithm for Gröbner bases of VDR
Input:	$F = \{f_1, ..., f_s\}$,
	a monomial order of $V[\varepsilon]$,
Output:	Gröbner bases of F
	$G := F$
	$B := \{(i, j)\|1 \le i < j \le s\}$
	$t := s$
	while $B \neq \emptyset$ do
	choose$(i, j) \in B$
	if lcm(lt(f_i), lt(f_j)) $\neq$ lt(f_i)lt(f_j) and
	Crit(f_i, f_j, B) =false then
	$h_0 := S(f_i, f_j)_G$
	if $h_0 \neq 0$ then
	$t := t + 1; f_t := h_0$
	$G := G \bigcup \{f_t\}$
	$B := B \bigcup \{(i, t)\|1 \le i \le t - 1\}$
	$B := B - \{(i, j)\}$
end	

Figure 1. An improvement algorithm for Gröbner bases of VDR.

Remark 12. $Crit(f_i, f_j, B) = ture$ if and only if there exists $k \notin \{i, j\}$ such that $(i, k), (j, k) \notin B$ and lt(f_k)|lcm(lt(f_i), lt(f_j)) in the above algorithm. Actually, this is done to verify whether the current polynomials satisfies the "Chain Criterion".

Remark 13. $S(f_i, f_j)_G$ refers to a sequence of reductions for $S(f_i, f_j)$ by polynomials in G that reduce $S(f_i, f_j)$ to h_0, and h_0 is not divisible by any polynomials of G.

5. Example

In this section, an example is given to clearly demonstrate the improvement.

Let $R = Z_{3Z}[\varepsilon][x, y]$, where$Z_{3Z}$ refers to $Z_{3Z} = \{\frac{a}{b}|a \in Z, b \notin 3Z\}$, and $I = \langle p, f_1, f_2\rangle$, where

$p = (5 + 3\varepsilon)x + 1, f_1 = (3 + 5\varepsilon)xy^2 + 3\varepsilon y, f_2 = 5\varepsilon x - (1 + \varepsilon)y^2$. We want to construct a Gröbner basis for I with respect to the given monomial order $y <_{lex} x$.

It is straightforward to check that $\mathrm{lt}(p)|\mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2))$, so $S(f_1, f_2)$ is "useless" according to the Theorem 10.

Additionally, we need to compute $S(f_2, f_2)$ as $\mathrm{lc}(f_2) \in V[\varepsilon]$, $S(f_2, f_2) = -\varepsilon y^2$ which can not be reduced by I, recorded as f_3.

$S(p, f_2) = \varepsilon p - f_2 = (1 + \varepsilon)y^2 + \varepsilon$,which can not be reduced by I anymore, denoted as f_4.

$S(p, f_1) = \frac{3}{5}y^2\varepsilon p - \varepsilon f_1$, which can be reduced to 0.

Add f_3, f_4 to I and compute the $S-$polynomials again. Note that $\mathrm{lt}(p)$ is prime to $\mathrm{lt}(f_3)$, so the $S-$polynomial of them does not need to compute according to the Theorem 8.

For the same reason, $S(p, f_4), S(f_2, f_3), S(f_2, f_4)$ also need not to compute. Notice that:

$S(f_3, f_3) = 0, S(f_1, f_3) = \varepsilon f_1 + 3x f_3 = 0, S(f_1, f_4) = \varepsilon f_1 - 3x\varepsilon f_4 = 0, S(f_3, f_4) = f_3 + \varepsilon f_4 = 0.$

Thus $\{p, f_1, f_2, f_3, f_4\}$ is a Gröbner basis for I.

Remark 14. Theorems 7, 8, and 10 play an important role; by using them we can ignore some $S-$polynomials directly without any computations, such as in the above example, we reduced five $S-$polynomials totally by the theorems above. However, in algorithm in [14] we not only need to compute them but also need to perform a series reduction, so it can save a lot of time by using the improvement algorithm.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grant NO.12201204, 11971161 and 12271154,and the Natural Science Foundation of Hunan Provincial under Grant No.2022JJ30234, 2023JJ40275, Scientific Research Fund of Hunan Province Education Department under Grant No.21A0299 and No.22A0334.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. B. Buchberger, *An Algorithmic Method in Polynomial Ideal Theory*, Reidel Publishing Company, Dodrecht Boston Lancaster, 1985.
2. B. Buchberger, A criterion for detecting unnecessary reductions in the construction of Gröbner bases, in *Symbolic and Algebraic Computation: EUROSM'79, An International Symposium on Symbolic and Algebraic Manipulation*, Springer, Berlin Heidelberg, (1979), 3–21.
3. L. Zheng, D. Li, J. Liu, An improvement for GVW, *J. Syst. Sci. Complexity*, **35** (2022), 427–436. https://doi.org/10.1007/s11424-021-9051-5
4. L. Zheng, J. Liu, W. Liu, D. Li, A new signature-based algorithms for computing Gröbner bases, *J. Syst. Sci. Complexity*, **28** (2015), 210–221. https://doi.org/10.1007/s11424-015-2260-z
5. D. Li, J. Liu, L. Zheng, A zero-dimensional valuation ring is 1-Gröbner , *J. Algebra*, **484** (2017), 334–343. https://doi.org/10.1016/j.jalgebra.2017.04.015

6. S. Monceur, I. Yengui, On the leading terms ideal of polynomial ideal over a valuation ring, *J. Algebra*, **351** (2012), 382–389. https://doi.org/10.1016/j.jalgebra.2011.11.015
7. F. Xiao, D. Lu, D. Wang, Solving multivariate polynomial matrix Diophantine equations with Gröbner basis method, *J. Syst. Sci. Complexity*, **35** (2022), 413–426. https://doi.org/10.1007/s11424-021-0072-x
8. K. Deepak, Y. Cai, An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors, *Math. Comput. Sci.*, **2** (2009), 601–634. https://doi.org/10.1007/s11786-009-0072-z
9. E. Golod, On noncommutative Groöbner bases over rings, *Math. Sci.*, **173** (1999), 29–60. https://doi/10.1007/s10958-007-0420-y
10. I. Yengui, Dynamical Gröbner bases, *J. Algebra*, **301** (2006), 447–458. https://doi/10.1016/j.jalgebra.2006.01.051
11. I. Yengui, Corrigendum to "Dynamical Gröbner bases" [J. Algebra 301 (2) (2006) 447–458] and to "Dynamical Gröbner bases over Dedekind rings" [J. Algebra 324 (1) (2010) 12–24], *J. Algebra*, **339** (2011), 370–375. https://doi/10.1016/j.jalgebra.2011.05.004
12. D. M. Li, J. W. Liu, A Gröbner basis algorithm for ideals over zero-dimensional valuation rings, *J. Syst. Sci. Complexity*, **34** (2021), 2470–2483. https://doi/10.1007/s11424-020-0010-3
13. O. Wienand, Algorithms for symbolic computation and their applications-standard bases over rings and rank tests in statistics, 2011.
14. A. Bouesso, Gröbner bases over a dual valuation domain, *Int. J. Algebra*, **7** (2013), 539–548.
15. T. Markwig, Y. Ren, O. Wienand, Standard bases in mixed power series and polynomial rings over rings, *J. Symb. Comput.*, **79** (2017), 119–139. https://doi/10.1016/j.jsc.2016.08.009

AIMS Press