The Extension of the GVW Algorithm to Valuation Domains

Dongmei Li and Licui Zheng

School of Mathematics and Computations, Hunan University of Science and Technology, Xiangtan 411201, Hunan, China
Correspondence should be addressed to Licui Zheng; zhenglicui@126.com

Received 6 April 2021; Accepted 24 May 2021; Published 7 June 2021

Academic Editor: Hou-Sheng Su

Copyright © 2021 Dongmei Li and Licui Zheng. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The GVW algorithm is an effective algorithm to compute Gröbner bases for polynomial ideals over a field. Combined with properties of valuation domains and the idea of the GVW algorithm, we propose a new algorithm to compute Gröbner bases for polynomial ideals over valuation domains in this study. Furthermore, we use an example to demonstrate the improvement of our algorithm.

1. Introduction

The notion of Gröbner basis was first put forward by Buchberger [1]. The theory of Gröbner has been widely applied in numerous fields such as engineering, signal processing, neuroscience, coding theory, complexity, and control of networked dynamical systems and so on. For example, in the theory of symbolic dynamic systems, the problems of determining whether there is a shift equivalence of lag from one nonnegative matrix to another can be transferred into solving large-scale equations, while the latter can be solved by the Gröbner basis theory [2–13].

Seeking more efficient algorithms for the computation of Gröbner bases is a problem in which many researchers cared about extremely [14–19]. Faugère [19] proposed a fast algorithm called F5 for computing Gröbner bases. In this algorithm, he introduced two notions of rewriting and signatures, which allow them to filter the useless S-polynomials in a rather convenient way. A new algorithm named G2V [20] for computing Gröbner bases is presented by Gao et al., which is an algorithm of incremental signature and based on a simple theory. A few months later, they gave an extend version named the GVW algorithm [21]. We are particularly interested in the GVW algorithm which not only matches the original algorithm given by Buchberger in simplicity but also more effective than F5 under some term orders. The algorithms mentioned above are applied to polynomial ideals over fields.

Several algorithms have been widely investigated for Gröbner bases to rings, such as Euclidean domain, principle ideal domain, and valuation rings that may contain zero divisors [22–24].

In this study, we aim to extend the GVW algorithm to valuation domains and present a signature-based algorithm to compute Gröbner bases for ideals in \( R = V[x_1, \ldots, x_n] \), where \( V \) is a valuation domain. In this algorithm, we study relations between \( J \) pairs and propose a new concept named factor, which allows us to filter the useless \( J \) pairs in a rather convenient way.

The structure of the study is arranged as follows: some basic concepts of the Gröbner basis theory is given in Section 2. In Section 3, we propose theory for the GVW algorithm over valuation domains and obtain main results of this study. Then, we present the new algorithm and demonstrate the improvement clearly by an example in Section 4.

2. Preliminaries

Let \( V \) be a valuation ring. For any two nonzero elements \( a, b \in V \), there always exists \( a|b \) or \( b|a \). The term order for monomials in \( R = V[x_1, \ldots, x_n] \) is arbitrary throughout this section. The form of the monomial in \( R \) is...
where \( \alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n \). The definition of the leading monomial (abbreviated as \( \text{lm} \)), the leading term (abbreviated as \( \text{lt} \)), and the leading coefficient (abbreviated as \( \text{lc} \)) of a given polynomial is as usual.

A nonzero polynomial set \( G_w \) in an ideal \( I \) is named as (weak) Gröbner basis for \( I \) if

\[
\langle \text{lt}(G_w) \rangle = \langle \text{lt}(I) \rangle.
\]

(2)

This does not imply that, for each \( f \in I \), there exists some polynomial \( g \in G_w \) so that \( \text{lt}(g) \mid \text{lt}(f) \). For example, \( I = \langle 2x, 3y \rangle \subset \mathbb{Z}[x, y] \) has a Gröbner basis \( G = \langle 2x, 3y \rangle \), and \( xy = -y(2x) + x(3y) \in I \), but \( xy \) is not divisible by \( 2x \) nor \( 3y \) in \( \mathbb{Z}[x, y] \).

**Definition 1.** A set \( G_s \) is called a strong Gröbner basis for \( I \) if \( \forall f \in I \), there is a polynomial \( g \in G_s \), so that \( \text{lt}(g) \mid \text{lt}(f) \), where \( G_s \) is formed by the nonzero polynomials from \( I \).

For the above example, \( \{2x, 3y, xy\} \) is a strong Gröbner basis for the ideal \( I \), but the set \( \{2x, 3y\} \) is not. This shows already some difference when dealing with polynomials over rings from those over fields.

**Proposition 1.** Suppose \( V \) is a valuation domain. Then, every ideal in \( V[x_1, \ldots, x_n] \) has a strong Gröbner basis.

**Proof.** It can be easily obtained by properties of valuation ring.

We now follow the notations in [21]. Let \( R = V[x_1, \ldots, x_n] \), where \( V \) denotes a valuation domain, and \( h_1, \ldots, h_m \in R \) are the polynomials. Let

\[
I = \langle h_1, \ldots, h_m \rangle = \{ p_1h_1 + \cdots + p_mh_m : (p_1, \ldots, p_m) \in R^m \} \subseteq R
\]

be an ideal, and its Gröbner basis is what we want to obtain. Vectors in \( R^m \) are denoted by bold letters, for example, \( p = (p_1, \ldots, p_m) \). Let \( e_j \) be the \( j \)-th unit vector in \( R^m \) for \( 1 \leq j \leq m \). Define an \( R \) submodule of \( R^m \times R \):

\[
M = \{ (p, f) \in R^m \times R : \text{ph}^t = f, \text{that is, } p_1h_1 + \cdots + p_mh_m = v \}.
\]

Note that, as an \( R \) module, \( M \) is generated by

\[
(e_1, h_1), (e_2, h_2), \ldots, (e_m, h_m).
\]

(5)

\[
H = \{ (p_1, \ldots, p_m) \in R^m : p_1h_1 + \cdots + p_mh_m = 0 \}
\]

is defined to be the syzygy module of \( h = (h_1, \ldots, h_m) \). We shall see that the big module \( M \) allows us to get the Gröbner bases for \( I \) and \( H \) in the same time and allows us to develop a criterion to detect useless \( S \) polynomials.

We define quasiordering in \( V \): for arbitrary \( a, b \in V \), we say \( a < b \) if \( ab \). Following this definition, then a term order (throughout this study, by a monomial order, we mean a global ordering [21]) \( \leq \) on \( R \) is defined by \( a_1t_1 \leq a_2t_2 \) iff

\[
a_1t_1 = a_2t_2,
\]

or \( a_1 = a_2 \), \( t_1 = t_2 \).

We assume \( R^m \) has a term order that is compatible with that of \( R \). We refer the readers to [21] for several examples on how term order of \( R \) can be extended to \( R^m \). Note that a term in \( R^m \) is the form as

\[
x^\alpha e_i,
\]

for some \( \alpha \in \mathbb{N}^m \) and \( 1 \leq i \leq m \). For any nonzero \( p \in R^m \),

\[
\text{lt}(p) = \text{lc}(p) \cdot \text{lm}(p),
\]

where \( \text{lm}(p) \) is the leading monomial of \( p \), and \( \text{lc}(p) \in V \) is the leading coefficient of \( p \).

**3. Theory of the Algorithm**

In this section, we present the theory of our algorithm. First, some basic definitions are needed.

**Definition 2.** \( \text{lt}(p) \) is said to be the signature of \( (p, f) \), where \( (p, f) \in R^m \times R \).

**Definition 3.** We say \( (p_1, f_1) \in R^m \times R \) can be top-reduced by \( (p_2, f_2) \in R^m \times R \) \( \langle \text{lt}(f_2) \rangle \neq 0 \) when they meet the following two conditions:

(i) \( \text{lt}(f_2) \) divides \( \text{lt}(f_1) \) (i.e., \( f_2 \) is top-divisible by \( f_1 \)) and

(ii) \( \text{lt}(t \cdot p_2) < \text{lt}(p_1) \), where \( t = \text{lt}(f_1) / \text{lt}(f_2) \)

Then, the relevant top-reduction is

\[
(p_1, f_1) - t(p_2, f_2) = (p_1 - t p_2, f_1 - t f_2).
\]

(9)

Hence, we can divide this reduction into two types: one is called regular when

\[
\text{lm}(p_2) < \text{lm}(p_1),
\]

and the other is called super if

\[
\frac{\text{lt}(p_1)}{\text{lt}(p_2)} = \frac{\text{lt}(f_1)}{\text{lt}(f_2)}.
\]

(11)

Besides, there is another super top-reduction, that is, when \( f_2 = 0 \), we say that \( (p_1, f_1) \) is super top-reduced by \( (p_2, 0) \) if \( p_1 \) and \( p_2 \) are both nonzero and \( \text{lt}(p_1) \) divides \( \text{lt}(p_2) \). So when a pair \( (p_1, f_1) \) can be reduced by \( (p_2, 0) \), we just reduce the signature of \( (p_1, f_1) \) but without increasing \( \text{lt}(f_1) \) (even if \( f_1 = 0 \)). What attracts more of our attention is that \( (p_2, 0) \) is never top-reduced by \( (p_2, f_2) \) when \( f_2 \neq 0 \).

Similar to Definition 1, we give the definition of strong Gröbner basis for \( M \) in the following.

**Definition 4.** Suppose \( G_s \) is a subset of \( M \), \( G_s \) is said to be a strong Gröbner basis of \( M \), if every pair \( (p, f) \in M \) can be top-reduced by at least one pair in \( G_s \).
It is easy to draw a conclusion from this definition, that is, every pair in \( M \) can be top-reduced to 0 by its strong \( \text{Gröbner basis}. \)

Lemma 1. If \( G_s \) is a strong \( \text{Gröbner basis} \) of \( M \), where \( G_s = \{(p_1, f_1), \ldots, (p_k, f_k)\} \), then

1. A strong \( \text{Gröbner basis} \) for the syzygy module of \( h = (h_1, \ldots, h_m) \) exists, which is \( G_0 = \{p_i \mid f_i = 0, 1 \leq i \leq k\} \).

2. The strong \( \text{Gröbner basis} \) for \( I = \langle h_1, \ldots, h_m \rangle \) also exists, which is \( G_1 = \{f_i \mid 1 \leq i \leq k\} \).

Proof. Assume \( p = (p_1, \ldots, p_m) \) is an element from the syzygy module of \( h \), then \( (p, 0) \in M \), and there must exist some pair \( (p_i, f_i) \) in \( G_s \) that can top-reduce \( (p, 0) \) with \( f_i = 0 \). Thus, \( p_i \in G_0 \) and \( \text{lt}(p) \) can be reduced by \( \text{lt}(p_i) \). This tells us that \( G_0 \) is the set we need, which is a \( \text{Gröbner basis} \) for the syzygy module of \( h \).

For an arbitrary nonzero polynomial \( v \in I \), there is \( p = (p_1, \ldots, p_m) \in R^m \), such that \( ph = f \) according to the definition of \( R^m \) and then \( (p, f) \in M \). Among all such \( p \), we choose the minimum \( \text{lt}(p) \). By our assumption, there exists at least one pair in \( G \) which can top-reduce \( (p, f) \).

If \( f = 0 \), then \( (p, f) \) can be reduced by \( (p_i, 0) \) and get \( (p', f) \), but \( p' h = f \), which contradicts the minimality of \( \text{lt}(p) \) as \( \text{lt}(p') < \text{lt}(p) \). So there exists \( (p_i, f_i) \in G_1 \) with \( f_i \neq 0 \) and \( \text{lt}(f_i) \| \text{lt}(f) \). Hence, \( G_1 \) is a \( \text{Gröbner basis} \) of \( I \). \( \square \)

Definition 5. For any pair, \( P_1 = (p_1, f_1), P_2 = (p_2, f_2) \in R \times R \), and \( f_1 \neq 0, f_2 \neq 0 \). Let \( t_1 = \text{lcm}(\text{lt}(f_1), \text{lt}(f_2)) \)

\[ t_2 = \frac{t}{\text{lt}(f_2)} \]  

(i) If \( \text{max}(\text{lt}(t_1 P_1), \text{lt}(t_2 P_2)) = t_1 \text{lt}(p_1) \), define

\[ J(P_1, P_2) = \begin{cases} t_1 P_1, & \text{if } \text{lcm}(f_2) \| \text{lcm}(f_1) \, \text{lc}(f_1), \\ \text{lcm}(f_2) t_1 P_1, & \text{if } \text{lcm}(f_1) \| \text{lcm}(f_2). \end{cases} \]  

(ii) If \( \text{max}(\text{lt}(t_1 P_1), \text{lt}(t_2 P_2)) = t_2 \text{lt}(p_2) \), define

\[ J(P_1, P_2) = \begin{cases} \text{lcm}(f_2) t_2 P_2, & \text{if } \text{lcm}(f_2) \| \text{lcm}(f_1), \\ t_2 P_2, & \text{if } \text{lcm}(f_1) \| \text{lcm}(f_2). \end{cases} \]

Remark 1. With notations as above, we do not define \( J \) pair for \( P_1 = (p_1, f_1) \) and \( P_2 = (p_2, f_2) \) when one of \( f_1 \) and \( f_2 \) is zero nor when \( \text{lt}(t_1 p_1) = \text{lt}(t_2 p_2) \).

In order to study the relation between \( J \) pairs, we propose the following conception:

Definition 6. Suppose \( t_1 (p_1, f_1), t_2 (p_2, f_2) \) are the \( J \) pairs formed from \( G \) which is a (finite) subset of \( M \), and \( t_1 (p_1, f_1) \) is called a factor of \( t_2 (p_2, f_2) \) if

\[ a t_1 \text{lt}(p_1) w = t_2 \text{lt}(p_2), \]

\[ a t_1 \text{lt}(f_1) w < t_2 \text{lt}(f_2), \]

for some monomial \( aw, a \in V \).

The next result is very useful for reduction.

Lemma 2. Assume at \( (p_1, f_1), (p_2, f_2) \) can be regular top-reduced by \( (p_1, f_1) \) with neither of \( f_1, f_2 \) is zero, where \( a \) is an element from \( V \) and \( t \) is a monomial from \( R \); then, \( c_1 t_1 (p_1, f_1) \) is the \( J \) pair of \( (p_1, f_1) \) and \( (p_2, f_2) \), where

\[ c_1 = \frac{\text{lcm}(\text{lcm}(f_1), \text{lc}(f_1))}{\text{lc}(f_1)}. \]

\[ c_2 = \frac{\text{lcm}(\text{lcm}(f_1), \text{lc}(f_1))}{\text{lc}(f_2)}. \]

where \( c_1 \) is a divisor of \( a \), \( t_1 \text{lt} \), and \( (p_1, f_1) \) can regular topreduce \( c_1 t_1 (p_1, f_1). \)

Proof. By our assumption, there exist \( a_1 \in V \) and a monomial \( w_1 \in R \), so that

\[ a t_1 \text{lt}(f_1) = a_1 w_1 \text{lt}(f_1). \]

Set

\[ c_2 = \frac{\text{lcm}(\text{lcm}(f_1), \text{lc}(f_1))}{\text{lcm}(f_2)} \]

we have that

\[ c_2 t_2 = \frac{\text{lcm}(\text{lcm}(f_1), \text{lc}(f_1))}{\text{lc}(f_2)} \cdot \frac{\text{lcm}(\text{lcm}(f_1), \text{lc}(f_1))}{\text{lcm}(f_2)} \]

\[ = \frac{\text{lt}(f_1)}{\text{lt}(f_1)} \]

Then, some \( a_2 \in V \) and monomial \( w_2 \in R \) exist, such that
\[ a_{1 \omega_1 \text{lcm}(\text{lt}(f_j), \text{lt}(f_i))} = \text{alt}(f_j) = a_{1 \omega_1 \text{lt}(f_i)}. \]

\[ c_{1 t_1} = \frac{\text{lcm}(\text{lcm}(f_j), \text{lcm}(f_i))}{\text{lcm}(\text{lm}(f_j), \text{lm}(f_i))} \cdot \frac{\text{lcm}(\text{lm}(f_j), \text{lm}(f_i))}{\text{lm}(f_j)} \]

Thus,

\[ a_{1 \omega_1 \text{lt}(f_i)} = a_{2 \omega_2 c_1 t_2 \text{lt}(f_i),} \]

\[ \text{alt}(f_j) = a_{2 \omega_2 c_1 t_1 \text{lt}(f_j),} \]

\[ a_{1 c_1 \text{lt}(f_j)} = a_{2 c_1 \text{lt}(f_j)}, \]

\[ a_{1 \text{lc}(f_i)} = a_{2 c_2 \text{lt}(f_i)}, \]

\[ t \text{lm}(f_j) = t \omega_1 \text{lm}(f_j), \]

\[ w_1 \text{lm}(f_i) = t \omega_2 \text{lm}(f_i). \]

Then, we have that

\[ a = a_{2 c_1}, \]

\[ a_1 = a_{2 c_2}, \]

\[ c_{1|a}, \]

\[ t = t_1 \omega_2, \]

\[ w_1 = t_2 \omega_2. \]

Hence, \( c_{1 t_2 \text{lt}(p_i)} < c_{1 t_1 \text{lt}(p_i)} \) as \( \text{slm}(p_i) < t \text{lm}(p_i) \). Thus, \( \max(t_2 \text{lm}(p_i), t_1 \text{lm}(p_i)) = t_1 \text{lm}(p_i) \). And the \( J \) pair of \((p_j, f_j)\) and \((p_i, f_i)\) is \( c_{1 t_1} (p_i, f_i) \) by Definition 5. Note that

\[ \text{alt}(f_i) = a_1 \omega_1 \text{lt}(f_2), \]

and then,

\[ a_{2 c_1 t_1 \omega_2 \text{lt}(f_j)} = a_{2 c_2 t_2 \omega_2 \text{lt}(f_i)}. \]

Then, we have

\[ \text{lt}(f_i)|c_{1 t_1 \text{lt}(f_j)}. \]

We see that \((p_j, f_j)\) can regular top-reduce \( c_{1 t_1} (p_j, f_j) \).

Suppose \( S \) is a set formed by the pairs in \( R^m \times R \), we say \( S \) can regular (super) top-reduce the pair \((p, f) \in R^m \times R\), if there is at least one pair in \( S \) which can regular (super) top-reduce the pair \((p, f)\). Furthermore, we implement a series of such reductions to \((p, f)\) until it cannot be regular top-reduced by this set anymore, but \((p, f)\) can be super top-reduced by \( S \), and this reduction defined as \((p, f)\) is eventually super top-reduced by \( S \).

**Theorem 1.** Suppose \( T \) is any term in \( R^m \), and there always exists a pair \((p, f)\) in \( G_r \), a monomial \( t \in R \) and \( a \in V \), such that \( T = \text{alt}(p_i) \), where \( G_r \) is a subset of \( M \). Then, \( G_r \) is a strong Gröbner basis for \( M \) if and only if, for the \( J \) pairs formed from \( G_r \), such as \((p_i, f_i)\), there always exists a pair \((p_j, f_j) \in G_r \) so that \( \text{lt}(p_j)|t \text{lm}(p) \) and \( t \text{lm}(f_j) < t \text{lm}(f) \), where \( t = \text{lm}(p)/\text{lm}(p_i) \).

Proof. Necessity: let \((p, f)\) be an arbitrary \( J \) pair formed from \( G_r \); then, \((p, f)\) is in \( M \), and it is top-reduced by \( G_r \) as the set \( G_r \) is a strong Gröbner basis for the module \( M \). We can do the regular top-reductions to \((p, f)\) as much as possible until \((p, f)\) cannot be regular top-reduced anymore, say to get \((p_0, f_0)\). And \((p_0, f_0)\) can be top-reduced by \( G_r \) as it is still in \( M_r \); but now, the reduction can only be super reduction, say \((p_0, f_0)\) can be super reduced by \((p_1, f_1) \in G_r \).

1. If \( f_1 = 0 \), then \( \text{lt}(p_1)|t \text{lm}(p_0) = \text{lt}(p) \), and \( t f_1 = 0 \) is smaller than \( \text{lm}(f) \), and the conclusion is true.
2. If \( f_1 \neq 0 \),

\[ t = \frac{\text{lm}(f_0)}{\text{lm}(f_1)}, \]

\[ \frac{\text{lc}(f_0)}{\text{lc}(f_1)} \cdot \text{lc}(p_1) < \text{lc}(p_0). \]

Combined with the definition of quasiordering given, we have that

\[ \frac{\text{lc}(f_0)}{\text{lc}(f_1)} \cdot \text{lc}(p_1) < \text{lc}(p_0). \]

and then, \( \text{lc}(p_1) | \text{lc}(p_0). \)

Since \((p_0, f_0)\) is obtained by performed regular top-reduction to \((p, f)\), then \( \text{lm}(f_0) < \text{lm}(f) \) and \( \text{lt}(p_0) = \text{lt}(p) \); the latter shows that

\[ t \text{lm}(f_1) = \text{lm}(f_0) < \text{lm}(f). \]

So, \( \text{lt}(p_1)|t \text{lm}(p_0) = \text{lt}(p) \) and \( t \text{lm}(f_1) < \text{lt}(f) \).

Sufficiency: suppose there are some pairs in \( M \) which cannot be top-reduced the set \( G_r \), say \((p, f) \in M \) is such a pair. We prove that such a pair does not exist. Select the minimal signature \( T = \text{lt}(p) \) from all such pairs with \( \text{lt}(p) \neq 0 \), and we choose a \( (p_j, f_j) \) from \( G_r \), so that

(i) \( T = a \text{lt}(p_j) \) with \( a \in V \) and \( t = 1 \) is a monomial in \( R \),

(ii) \( \text{tlm}(f_j) \) is the smallest one among all \( 1 \leq j \leq k \) satisfying (i)

In the following, we prove that \( a_t \text{lt}(p_j) \neq 0 \). Suppose that \( a_t \text{lt}(p_j) \) could be regular top-reduced by a pair \((p_j, f_j), i \neq j \), then \( f_j \neq 0, f_j \neq 0 \). What we expect is to get a conclusion that contradicts condition (ii). From Lemma 2, we have that

\[ c_{1 t_1} (p_j, f_j) \]
\[ c_1 = \frac{\text{lcm}(\text{lcf}(f_j), \text{lcf}(f_j))}{\text{lcf}(f_j)} \]
\[ t_1 = \frac{\text{lcm}(\text{lmt}(f_j), \text{lmt}(f_j))}{\text{lmt}(f_j)} \]  \hspace{1cm} (29)
\[ t = t_1 w, c_1 a, \]
\[ a \cdot a_t w \text{lwt}(p_2) = a \cdot t_1 w \text{lc}(p_j) \cdot \text{lmt}(p_j) = a t_1 w \text{lc}(p_j) = a \text{lwt}(p_j) = T, \]
\[ t_1 w \text{lm}(f_j) < w t_1 \text{lm}(f_j) = t \text{lm}(f_j). \]  \hspace{1cm} (30)

This contradicts the condition (ii) for the selection of \((p_j, f_j)\) in \(G_s\).

**Case 2.** If \(\text{lcf}(f_j) || \text{lc}(f_j)\), then \(c_1 = (\text{lcf}(f_j) || \text{lc}(f_j))\), and the \(J\) pair of \((p_j, f_j)\) and \((p_k, f_k)\) is \((\text{lcf}(f_j) || \text{lc}(f_j)) t_1 (p_j, f_j)\). Note that \((\text{lc}(f_j)/\text{lc}(f_j)) t_1 (p_j, f_j)\) is a \(J\) pair formed from \(G_s\), and there must exist some pair \((p_k, f_k) \in G_s\), such that \(\text{lmt}(p_j) || \text{lmt}(p_k)\) and \(t_1 \text{lm}(f_j) < t_1 \text{lm}(f_j)\) with \(t_1 = t_1 \text{lm}(p_j)\). Since \(\text{lc}(p_j)/\text{lc}(p_j)\), we set \(a_j = (\text{lc}(p_j)/\text{lc}(p_j))\) and then,
\[ a \cdot a \cdot \text{lmt}(p_j) = a \cdot a \cdot \text{lc}(p_j) \cdot \text{lm}(p_j) = a t_1 \text{lc}(p_j) = a \text{lc}(p_j) = T, \]
\[ t_1 \text{lm}(f_j) < w t_1 \text{lm}(f_j) = t \text{lm}(f_j). \]  \hspace{1cm} (31)

This contradicts the condition (ii) for the selection of \((p_j, f_j)\) in \(G_s\).

Let \((\tilde{p}, \tilde{f}) = (p, f) - \text{at}(p, f)\),
\[ (\tilde{p}, \tilde{f}) = (p, f) \]  \hspace{1cm} (32)
and then, \(\text{lm}(\tilde{p})/\text{lm}(p)\) and \(\text{lt}(f) \neq \text{at}(f)\). Otherwise, \((p, f)\) would be top-reduced by \((p, f)\) which contradicts with the selection of \((p, f)\). So, \(\tilde{f} \neq 0\) and \((\tilde{p}, \tilde{f})\) can be top-reduced by \(G_s\), as \((\tilde{p}, \tilde{f}) \in M\) and \(\text{lm}(\tilde{p})/\text{lm}(p)\), \(\text{lt}(\tilde{f})/\text{lt}(p)\), say it is top-reduced by \((p_k, f_k)\). If \(f_k = 0\), we use this type of pairs to reduce \((p, f)\) as much as possible and obtain a new pair \((p', f)\) finally, which cannot be top-reduced by the same type of pairs (here, it refers the pairs whose \(f\)-part is zero) in \(G_s\). Since \((p', f) \in M\) and \(\text{lm}(p')/\text{lm}(p)\), \(\text{lt}(p')/\text{lt}(p)\), and then \((p', f)\) can be top-reduced by \(G_s\), say by \((p_k, f_k)\), \(f_k \neq 0\). For \(\text{lt}(f) \neq \text{at}(f)\), there are the following three cases that need to be considered:

(i) If \(\text{lm}(f) < t \text{lm}(f)\), then \(\text{lt}(\tilde{f}) = \text{at}(f)\); but \(\text{lm}(p') < t \text{lm}(p)\), so there must exist some pairs in \(G_s\) that can regular top-reduce at \((p, f)\); assume the pair in \(G_s\) is \((p_k, f_k)\). This is impossible as \(\text{at}(p, f)\) cannot be regular top-reduced by any pair in \(G_s\).

(ii) If \(\text{lm}(f) > t \text{lm}(f)\), then \(\text{lm}(\tilde{f}) = \text{lm}(f)\), and \((p, f)\) can be regular top-reduced by \((p_k, f_k)\); this contradicts the choice of \((p, f)\).

(iii) If \(\text{lm}(f) = t \text{lm}(f)\) and \(\text{lc}(f) \neq \text{alc}(f)\), \((\tilde{p}, \tilde{f})\) is top-reduced by \((p_k, f_k)\), and then \(\text{lt}(\tilde{f})\); this means that \(\text{lm}(f)/\text{lm}(\tilde{f})\) and \(\text{lc}(f)/\text{lc}(\tilde{f})\).

From the property of valuation ring, we consider the relation between \(\text{alc}(f)\) and \(\text{lc}(f)\) in the following three cases:

(a) If \(\text{alc}(f) = \text{bc}(f)\) and \(b\) is not a nonzero unit, note that a valuation ring is a local ring, and \(b\) is in the unique maximal ideal. Since \(\text{lc}(f)/\text{lc}(f) - \text{alc}(f) = (1 - b)\text{lc}(f)\) and \(1 - b\) is invertible, then \(\text{lc}(f)/\text{lc}(f)\). Note that \((\text{lm}(f)/\text{lm}(f)) \text{lm}(p_k) < \text{lm}(p')/\text{lm}(p)\) and \((p, f)\) are regular top-reduced by \((p_k, f_k)\); this contradicts the choice of \((p, f)\).

(b) If \(\text{alc}(f) \cdot b = \text{lc}(f)\) and \(b\) is not a nonzero unit, note that a valuation ring is a local ring, and \(b\) is in the unique maximal ideal. Since \(\text{lc}(f)/\text{lc}(f) - \text{alc}(f) = (1 - b)\text{alc}(f)\) and \(1 - b\) is invertible, then \(\text{lc}(f)/\text{lc}(f)\). Note that \((\text{lm}(f)/\text{lm}(f)) \text{lm}(p_k) < \text{lm}(p')/\text{lm}(p) = \text{lm}(p)\), then \(\text{at}(p_k, f_k)\) is regular top-reduced by \((p_k, f_k)\), and this case is impossible.

(c) If \(\text{alc}(f) = \text{bc}(f)\) and \(b\) is a nonzero unit, then \(\text{alc}(f)/\text{lc}(f)\) and \(\text{lc}(f)/\text{alc}(f) = b^{-1}\). Note that \(\text{lt}(p) = \text{at}(p)\); combining the definition of the
order, we have $b^{-1} \cdot \text{alt}(p_f) < \text{lt}(p)$. Therefore, $(p, f)$ can be top-reduced by $\text{at}(p_f, f_1)$, and this contradicts the choice of $(p, f)$.

Thus, such pairs like $(p, f)$ cannot exist in $M$ at all; hence, all pairs of $M$ can be top-reduced by $G_r$, and $G_r$ is a strong Gröbner basis for $M$.

The pair $p = (p, f)$ is covered by $G_r$ when there exists at least one pair such as $p_1 = (p_1, f_1)$ in $G_r$, such that $\text{lt}(p_1)||\text{lt}(p)$ and $\text{tlm}(f_1) < \text{lt}(f)$, where $t = \text{lt}(p)/\text{tlm}(p)$.

**Theorem 2.** Suppose $G_r$ is a special subset of $M$, whose particularity is reflected in for any term $T \in R^n$, there always exist a pair $(p, f) \in G_r$ and monomial $t \in R$ and $a \in V$, such that $T = \text{at}(p)$. Then, $G_r$ is a strong Gröbner basis for $M$ if the factors of the $J$ pairs formed by $G_r$ can always be eventually super top-reduced by the set $G_r$.

Proof. Assume that $t_1(p_1, f_1), t_2(p_2, f_2)$ are the two $J$ pairs formed by $G_r$, and $(p_1, f_1)$ is a factor of $t_2(p_2, f_2)$. Then, $t_1(p_1, f_1)$ can be eventually super-top-reducible by $G_r$, that is, after doing a series of regular top-reduction to $t_1(p_1, f_1)$, it gets to $(p', f')$ where $\text{lt}(p') = t_1 \text{lt}(p_1), \text{lt}(f') < t_1 \text{lt}(f_1)$, besides, $(p', f')$ can be super top-reduced by $G_r$, say $(p, f)$; then, $\text{lt}(p_1) = t_1 \text{lt}(p), \text{lt}(f_1) = t_1 \text{lt}(f_1)$, where $t_1 = (\text{lt}(f')/\text{lt}(f_1))$. Clearly, $t_2(p_2, f_2)$ can be covered by $(p, f)$. It is also correct for the rest of the $J$ pairs and their factors. By Theorem 1, we have that $G_r$ is a strong Gröbner basis for $M$.

According to Theorems 1 and 2, we can discard the $J$ pairs which can be covered by $G_r$ without doing any regular nor super top-reductions. As a consequence, there are four criteria for discarding redundant $J$ pairs.

**Corollary 1.** (Covered criterion) For any $J$ pair $(p, f)$ of $G_r$, it can be discarded if $(p, f)$ is covered by $G_r$.

**Corollary 2.** (Syzygy criterion) If a $J$ pair $(p, f)$ can be top-reduced by a syzygy, then it can be discarded.

**Corollary 3.** (Signature criterion) As for the $J$ pairs with the same signature, we only need to keep the one whose $f$-part is minimal.

**Corollary 4.** (Factor criterion) As for the $J$ pair which has a factor, we just need to keep the factor.

4. Algorithm and Example

According to the theorems and corollaries in Section 3, we can get an algorithm for computing Gröbner bases for the polynomial ideals over valuation domains. We call the algorithm as VD – GVW. The main idea of VD – GVW is analogue to the GVW algorithm of principal ideal domain [23]. First, we form $J$ pairs by the initial pairs $(e_1, g_1), \ldots, (e_m, g_m)$. By Theorems 1 and 2, we just store the $J$ pairs with different signatures. We only consider the $J$ pairs that we store, choose any one of them, denoted as $(p, f)$, and then check whether it satisfies Corollary 1, that is, whether it is covered by $G_r$. If so, discard it. Otherwise, delete all the $J$ pairs whose factor is $(p, f)$ and perform regular top-reductions to it repeatedly until it cannot be regular top-reduced any more, say to get $(p', f')$ finally. If $f' = 0$, then $p'$ is a syzygy in $H$. We add it to $H$ and delete the pairs whose signature is divisible by $\text{lt}(p')$. Otherwise, $(p', f')$ adds to the set $JP$, and we will not stop the process until the set of $J$ pair is empty. In the while-loop, all the $J$ pairs formed from $G_r$ will be top-reduced by the set $G_r$. We describe the algorithm in more detail and accurately with Figure 1. $H$ is used to store the leading terms of syzygies; the Gröbner basis we get is a list of pairs $(T_1, f_1), (T_2, f_2), \ldots, (T_k, f_k)$, where $f_j \neq 0$ for $1 \leq j \leq k$. We store this list as

$$P = [T_1, T_2, \ldots, T_k],$$
$$F = [f_1, f_2, \ldots, f_k].$$

(33)

So the whole list $(T_1, f_1), (T_2, f_2), \ldots, (T_k, f_k)$ is represented by $[P, F]$.

**Theorem 3.** Assume the term orders in $R$ are compatible with which in $R^n$; then, the algorithm shown in Figure 1 will terminate after a finite number of steps and get a strong Gröbner basis for $M$.

Proof. The correctness of our algorithm is obviously according to Theorems 1 and 2. As for the termination of the algorithm, we can refer to the Theorem 1 in [21].

Next, we present our algorithm and use a concrete example to demonstrate the improvement clearly.

**Example 1.** Let $V[x, y] = Z_{(3)}[x \cdot y, y]$, and we consider the Gröbner basis of the ideal $I = \langle f_1, f_2, f_3 \rangle \in V[x, y]$, where

$$f_1 = x^2y - x,$$
$$f_2 = xy^2 - xy,$$
$$f_3 = y^3,$$

and $Z_{(3)}$ is a discrete valuation ring, for each prime $p$ (here is 3); set $\nu_p: Q^*/ Z$ is a function given by $\nu_p(p/a = b) = k$ if $a, b$ are integers relatively prime to $p$.

The term order we set on $V[x, y]$ is the lexicographical ordering, which is defined by $y < x$. Besides, the term order $\prec$ on $V^m[x, y]$ is $x^a e_1 < y^a e_2$ if $i < j$ or $i = j$ and $x^a < y^a$.

First, let $[P, F] = \{(e_1, f_1), (e_2, f_2), (e_3, f_3)\}$; then, $H = \langle y^2 e_1, y e_2, y e_4 \rangle$, which is a set that stands for leading term of principle syzygy.

Choose $(e_1, f_1), (e_2, f_2)$ from $[P, F]$; then, $\text{lcm}(\text{lt}(f_1), \text{lt}(f_2)) = x^2 y^2$. Hence, $t_1 = y, t_2 = x, J$ pair of $(e_1, f_1)$ and $(e_2, f_2)$ is $y(e_1, f_1)$, whose signature cannot be reduced by $H$, and we store it.

Doing the same process, the $J$-pairs set of other pairs in $[P, F]$ is $\langle y^2(e_2, f_1), y(e_2, f_3) \rangle$, but $y(e_1, f_1)$ is a factor of $y^2(e_1, f_1)$, so delete it. Then,

$$JP = \langle y(e_1, f_1), y(e_2, f_2) \rangle.$$ (35)

Selecting $y(e_2, f_2)$ from $JP$, we get $((y + 1)e_2 - xe_1, -xy)$ after a series of regular top-reduction, add it to $[P, F]$, and recalculate the $J$ pairs and
Using the syzygy criterion and factor criterion, we obtain

\[ \text{JP} = \{ y(e_1, f_1), y( (y + 1)e_2 - xe_1, -xy) \}. \]  

Select \( y((y + 1)e_2 - xe_1, -xy) \) from JP; it can be regular top-reduced to \( (y( (y + 1)e_2 - xe_1, 0)) \) and add \( ye_1 \) to \( H \).

5. Conclusions

In this study, we have generalized the GVW algorithm and presented an algorithm to compute Gröbner bases for polynomial ideals over valuation domains. We have also given an example to illustrate our method. All of these could provide useful information for engineers to solve large linear
systems and networked dynamical systems. Valuation domains are special kinds of valuation rings which may have zero divisors. In the future, we want to consider new algorithms for Gröbner bases of ideals over general valuation rings. And we also hope to establish a dynamical Gröbner basis algorithm which combined with the algorithm in the study.

Data Availability
The data used to support the findings of this study are included within the article.

Conflicts of Interest
The authors declare that there are no conflicts of interest.

Acknowledgments
This research was supported by the National Natural Science Foundation of China (11871207).

References