Hindawi
Journal of Mathematics
Volume 2022, Article ID 7049980, 6 pages
https://doi.org/10.1155/2022/7049980

Research Article

Computing Independent Variable Sets for Polynomial Ideals

Zhuoran Yang and Chang Tan

College of Science, Northeast Forestry University, Harbin 150040, China

Correspondence should be addressed to Chang Tan; tanchang@nefu.edu.cn

Received 13 May 2022; Revised 15 July 2022; Accepted 21 July 2022; Published 19 September 2022

Academic Editor: Niansheng Tang

Computing independent variable sets for polynomial ideals plays an important role in solving high-dimensional polynomial equations. The computation of a Gröbner basis for an ideal, with respect to a block lexicographical order in classic methods, is huge, and then an improved algorithm is given. Based on the quasi-Gröbner basis of the extended ideal, a criterion of assigning independent variables is gained. According to the criteria, a maximal independent variable set for a polynomial ideal can be computed by assigning indeterminates gradually. The key point of the algorithm is to reduce dimensions so that the unit of computation is one variable instead of a set, which turns a multivariate problem into a single-variable problem and turns the computation of rational function field into that of the fundamental number field. Hence, the computation complexity is reduced. The algorithm has been analysed by an example, and the results reveal that the algorithm is correct and effective.

1. Introduction

Solving systems of algebraic equations is a main subject in mathematics. In the theory researches and practical problems of many disciplines, it is frequently related to solving high-dimensional equations, whose key point is to know the independent variables of equations. During the research on the ideal of polynomials, the Hilbert-basis theory provides researchers with the direction of computing basis of the ideal. Then, Buchberger [1] and Möller and Mora [2] presented Gröbner basis with good properties.

As noticed in [3], the method of testing whether a subset of indeterminates is independent modulo an ideal aims to compute the Gröbner basis with respect to a block lexicographical order. Moreover, combining results given by Carra-Ferro [4] and Gröbner basis with the definition of strong independent modulo an ideal, it is concluded that the algorithm is correct with respect to any arbitrary admissible term order. Zhang and Feng [5] proposed a different approach to compute the independent variable sets of an ideal. The idea is to compute quasi-Gröbner basis instead of Gröbner basis. Shang et al. [6] used this method to compute independent variable sets for computing rational representation of positive-dimensional ideals. It is noticeable that all computations are in the rational function field. In particular, computations are huge when the number of variables is large, which means it is hard to realize the algorithm. Besides, Bernasconi et al. [7] and Kratzer [8] turned deciding whether variables are independent modulo an ideal to decide whether there is a nontrivial solution for homogeneous equations.

Among the existing algorithms, the whole variables are considered as a unit of computation. Therefore, based on [5], we will propose a descending dimension algorithm. We choose only one variable at a time and assign it a value according to the assigning criteria, which guarantees that there is at least one variable set independent modulo, not only the assigned ideal but also the extended ideal. Then, one independent variable can be selected and added to the independent variable set. Thus, the dimension of algebraic variety will be reduced gradually. Based on this algorithm, computations in the rational function field with several variables are turned to computations with only one variable, which reflects that the algorithm is easy to realize to some extent.

The rest of this paper is organized as follows. In Section 2, we give some basic definitions and results. Section 3 is devoted to introducing the definition of quasi-Gröbner basis

of ring. According to the definition, we propose the assignment criteria. Then, we demonstrate how to gain the maximal independent variable sets based on the criteria and prove the algorithm. In Section 4, we give an example and analyse it through the algorithm given in Section 3.

2. Preliminary

Let K be a field with characteristic 0, and $X = \{x_1, x_2, \ldots, x_n\}$ a finite set of indeterminates. The polynomial ring in $x_1, x_2, \ldots, x_n$ is denoted by $K[X]$, whose coefficients are in the field K. We call $T(x_1, x_2, \ldots, x_n)$ the set, including all power products of variables in X and $>_T$, an arbitrary admissible term order on $T(x_1, x_2, \ldots, x_n)$. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[X]$, and then $T(f) = \{x^\alpha | a_\alpha \neq 0\}$. The multidegree of f is $\text{multideg}(f) = \max_{>_T}\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}$, where $\mathbb{Z}$ stands for the integer set. We denote by $LC(f)$ the leading coefficient of f, $LM(f)$ the leading monomial of f, and $LT(f) = LC(f)LM(f)$.

Definition 1. Let $I \subset K[x_1, x_2, \ldots, x_n]$ be an ideal. For any set $U = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\} \subset \{x_1, x_2, \ldots, x_n\}$, U is an independent modulo I if $I \cap K[U] = \{0\}$; otherwise, U is dependent modulo I. Moreover, if U is an independent variable set modulo I and V is a dependent modulo I for any $U \subsetneq V \subseteq \{x_1, x_2, \ldots, x_n\}$, then we call U a maximal independent set modulo I. Let $|U|$ be the number of indeterminates in U. The dimension of I, denoted by $\dim I$, is the maximal $|U|$, where U is an independent modulo I.

Let S be an integral ring with unit and $f_1, f_2, \ldots, f_m$ be polynomials in $S[X]$, a polynomial ring in X with coefficients in S. $I = \langle f_1, f_2, \ldots, f_m \rangle$ denotes the ideal generated by polynomials $f_1, f_2, \ldots, f_m$. Similarly, we can define the independent variable set modulo I in $S[X]$.

Definition 2. Let $I \subset S[x_1, x_2, \ldots, x_n]$ be an ideal. For any set $U = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\} \subset \{x_1, x_2, \ldots, x_n\}$ independent modulo I, U is a maximal independent modulo I if V is a dependent modulo I for any set V, which satisfies that $U \subsetneq V \subseteq \{x_1, x_2, \ldots, x_n\}$. Let $|U|$ be the number of indeterminates in U. The dimension of I, denoted by $\dim I$, is the maximal $|U|$, where U is independent mod I.

The idea of Gröbner basis of an ideal I in a field plays an important role in solving many a problem of algebraic system. When it turns to focus on a polynomial ring, there is a definition called quasi-Gröbner basis, which is much the same.

Lemma 1. *Let $G = \{g_1, g_2, \ldots, g_m\}$ be a subset of $S[x_1, x_2, \ldots, x_n]$ and f a polynomial in $S[x_1, x_2, \ldots, x_n]$. Then, there are $s_1, s_2, \ldots, s_m \in \mathbb{Z}_{\geq 0}$, $q_1, q_2, \ldots, q_m$, and $r \in S[x_1, x_2, \ldots, x_n]$ such that*

$$\left(\prod_{i=1}^{m} [LC(g_i)]^{s_i}\right) f = \sum_{i=1}^{m} q_i g_i + r, \tag{1}$$

where $\deg(q_i g_i) \leq \deg(f)$ and for any $u \in T(r)$ and $g_i \in G$, u is not the multiple of $LM(g_i)$.

Based on Lemma 1, we introduce a quasi-Gröbner basis of an ideal I in $S[X]$ *[5]* and review a theorem guaranteeing its existence.

Definition 3 (see [5]). Let I be an ideal in $S[x_1, x_2, \ldots, x_n]$. Suppose that $G = \{g_1, g_2, \ldots, g_m\} \subset I$ satisfies that there are $s_1, s_2, \ldots, s_m \in \mathbb{Z}_{\geq 0}$ and $q_1, q_2, \ldots, q_m \in S[x_1, x_2, \ldots, x_n]$ such that

$$\left(\prod_{i=1}^{m} [LC(g_i)]^{s_i}\right) f = \sum_{i=1}^{m} q_i g_i, \deg(q_i g_i) \leq \deg(f), \tag{2}$$

we call G a quasi-Gröbner basis of I.

Theorem 1 (see [5]). *Let I be an ideal in $S[x_1, x_2, \ldots, x_n]$ and $>_T$ an arbitrary admissible term order on T. Then, there is a finite set $G \subset I$, such that G is a quasi-Gröbner basis of I with respect with $>_T$.*

There is also some preparation for proving the correctness of the algorithm given in the following section. In the rest of this section, we assume that L is the algebraic closure of K. Let L^n be the set $\{(a_1, a_2, \ldots, a_n) | \forall a_1, a_2, \ldots, a_n \in L\}$. We consider $f_1, f_2, \ldots, f_m \in K[X]$ *and* $I = \langle f_1, f_2, \ldots, f_m \rangle$. *The* zero set of I *in* L^n, $\{(a_1, a_2, \ldots, a_n) \in L^n | \forall f \in I, f(a_1, a_2, \ldots, a_n) = 0\}$, is denoted by $\mathbf{V}_L(I)$.

Definition 4. Let $V \subset L^n$ be a K-affine variety. If there are no K-affine varieties, V_1 and V_2, such that $V = V_1 \cup V_2$, then we call V an irreducible K-affine variety.

Proposition 1 (see [9]). *A K-affine variety, $V \subset L^n$, is irreducible if and only if the vanished ideal of V, $I(V)$, is prime. In other words, for all f and $g \in K[X]$, if $fg \in \mathbf{I}(V)$, then it is concluded that f belongs to $\mathbf{I}(V)$ or g belongs to $\mathbf{I}(V)$.*

Proposition 2 (see [9]). *If a K-affine variety, $V \subset L^n$, can be written in the form of $V = \cup_{i=1}^{m} V_i$, where each variety V_i is irreducible and m is finite, then we call the form the irreducible decomposition of V.*

3. The Algorithm of the Maximally Independent Set Modulo An Ideal

In our algorithm, computing quasi-Gröbner basis of extended ideal is inevitable. For more details, we refer the readers to [10–12].

3.1. The Algorithm for Computing the Quasi-Gröbner Basis. We will make some preparations correlated to the computation of a quasi-Gröbner basis. First, the definition of extended ideal and some properties are introduced.

Definition 5. Let U be the set $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$, V the set $X/U = \{x_{i_{m+1}}, x_{i_{m+2}}, \ldots, x_{i_n}\}$, and $K(U)$ the rational function field in U with coefficients in K. The ring of quotients of $K[X]$ with respect to U, denoted by $K(U)[V]$, is the

polynomial ring in V with coefficients in $K(U)$. Let I be an ideal in $K[X]$, and then we define extended ideal of I to $K(U)[V]$, denoted by I^e, as the ideal generated by the set I in $K(U)$. For any ideal J in $K(U)[V]$, contraction ideal of J to $K[X]$, denoted by J^c, is defined as $J^c = J \cap K[X]$.

Proposition 3 (see [10]). *Let I be an ideal in $K[x_1, x_2, \ldots, x_n]$, and then the extended ideal generated by I in $K(U)[V]$ is as follows:*

$$I^e = \left\{ \frac{f}{g} \% | f \in I, 0 \neq g \in K\left[x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right] \right\}. \tag{3}$$

The reduction of polynomials in the ring is necessary for getting a quasi-Gröbner basis.

Definition 6. Let S be an integral ring, $f, g, p \in S[x_1, x_2, \ldots, x_n]$ with $p \neq 0$, and P be a finite subset of $S[X]$. Then, we say that

(i) If $g = LC(p)f - Coef(f,t)sp$ for some $t \in T(f)$ satisfying $LM(p)|t$ and $t = LM(p)s$, where $\mathrm{Coef}(f,t)$ is the coefficient of t in f, then we say that f generally reduces to g modulo p.

(ii) If f generally reduces to g modulo p for some $p \in P$, then we say that f generally reduces to g modulo P .

(iii) If f generally reduces to g modulo p for some $g \in S[X]$, then we say that f is generally a reducible modulo p.

(iv) If f generally reduces to g modulo P for some $g \in S[X]$, then we say that f is generally a reducible modulo P.

According to the preparations above, we will show a relationship between a Gröbner basis and a quasi-Gröbner basis next.

Theorem 2 (see [5]). *Let Q_s be the quotient field of integral ring S and $>_T$ an arbitrary admissible term order on $T(x_1, x_2, \ldots, x_n)$. I is an ideal in $S[x_1, x_2, \ldots, x_n]$, and it is easy to know that the extended ideal of I to $Q_s[X]$ is $I^e = \{(1/a)f | f \in I, a \in S/\{0\}\}$. For any subset G of I, G is the quasi-Gröbner basis of I, if and only if G is the Gröbner basis of I^e.*

We can gain a quasi-Gröbner basis of an ideal I in a polynomial ring. The details are in the following definition and theorem.

Definition 7. Let K be a field with characteristic 0, $U = \left\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right\}$, and $V = X/U$. For any f and $g \in K[U](V)$, we define the *ES*-polynomial of f and g as

$$\begin{aligned} \mathrm{ES}(f,g) = \mathrm{LC}(g)\frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(f)} \\ f - \mathrm{LC}(f)\frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(g)}g, \end{aligned} \tag{4}$$

where $\mathrm{LC}(f), \mathrm{LC}(g) \in K[U]$, and $\mathrm{LM}(f), \mathrm{LM}(g) \in T(V)$.

Theorem 3 (see [12]). *Let S be an integral ring and I an ideal of $S[x_1, x_2, \ldots, x_n]$. $G = \{g_1, g_2, \ldots, g_m\}$ is a basis of I, then G is a quasi-Gröbner basis of I, if and only if the remainder of $ES(g_i, g_j)$ modulo G is 0 with respect to the reduction in Definition 6 for any $i \neq j, i, j = 1, 2, \ldots, m$.*

3.2. Main Algorithm. We first demonstrate the correctness of the following algorithm.

Theorem 4 (see [5]). *Let S be an integral ring, I an ideal in $S[x_1, x_2, \ldots, x_n]$, and G quasi-Gröbner basis of I. Then, $I \cap (S/\{0\}) = \emptyset$, if and only if $G \cap (S/\{0\}) = \emptyset$.*

Proposition 4 (see [10]). *Let $U = \left\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right\}$, $V = \left\{x_{i_{m+1}}, x_{i_{m+2}}, \ldots, x_{i_n}\right\} = X/U$, and $>_v$ an admissible term order on $T(V)$. I is an ideal in $K[x_1, x_2, \ldots, x_n]$, and $G \subset I$ is a Gröbner basis of the extension I^e of I to $K(U)[V]$ with respect to $>_v$. Then, we have the following:*

(i) U is a maximal independent modulo I, if and only if I^e is a zero-dimensional proper ideal in $K(U)[V]$.

(ii) For any $g \in G$, let $LC(g)$ be the leading coefficient of g with respect to $>_v$, where g is regarded as a polynomial in $K(U)[V]$ and $f = LCM\{LC(g)|g \in G\}$. Then, the contraction ideal of I^e is $I^{ec} = I\colon f^\infty = \{g \in I | \exists s \in N, gf^s \in I\}$, where I^e is the extended ideal of I to $K(U)[V]$.

The next theorem shows the correctness of our algorithm.

Theorem 5 *Let I be an ideal in $K[x_1, x_2, \ldots, x_n]$. $U = \left\{x_{i_1}\right\}$ is an independent modulo I, and $V = X/U$. I^e is the extended ideal of I to $K(U)[V]$ and G is a Gröbner basis of I^e with respect to $>_v$. Let $LC(g)$ be the leading coefficient of g with respect to $>_v$, where g is regarded as a polynomial in $K(U)[V]$ and $f(x_{i_1}) = LCM\{LC(g)|g \in G\}$. Suppose that $a \in K$ satisfies $f(a) \neq 0$ and $I_1 = I|_{x_{i_1}=a}$. If $U_2 = \left\{x_{i_2}, x_{i_3}, \ldots, x_{i_m}\right\}$ is independent mod I_1, then $U_1 = \left\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right\}$ is an independent mod I.*

Proof. We assume that $U_1 = \left\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right\}$ is a dependent mod I, which means there is a polynomial h such that h is in $I \cap (K[U_1]/\{0\})$. If $h|_{x_{i_1}=a}$ is not equal to 0, then $h|_{x_{i_1}=a}$ belongs to $K[U_2]/\{0\}$ because h is in $K[U_1]$. h belongs to I, and thus $h|_{x_{i_1}=a}$ is in I_1, which means there is a polynomial $h|_{x_{i_1}=a}$ such that $h|_{x_{i_1}=a}$ belongs to $I_1 \cap (K[U_2]/\{0\})$. This contradicts the fact that U_2 is an independent modulo I_1; otherwise, $h|_{x_{i_1}=a}$ equals 0. Then, it is concluded that $(x_{i_1} - a)|h$, which means that there exists a polynomial $u \in S[U_1]$ such that $h = u(x_{i_1} - a)^q, q \in Z_{\geq 1}$, and $u|_{x_{i_1}=a} \neq 0$. Let I^{ec} be the contraction ideal of I^e to $K[x_1, x_2, \ldots, x_n]$. By Proposition 3, $u = (h/(x_{i_1} - a)^q) \in I^e$. Moreover, $u \in K[x_1, x_2, \ldots, x_n]$, and hence, $u \in I^{ec}$. Based on Proposition 4, $I^{ec} = I\colon f^\infty = \{w \in I | \exists s \in N, wf^s \in I\}$, and then $\exists s_0 \in N$ such that $uf^{s_0} \in I$. As a result of the fact that f is in $K[U]$, uf^{s_0} belongs to $K[U_1]$. Also, under the given

condition that $f(a) \neq 0$, $uf^{s_0}|_{x_{i_1}=a} \neq 0$. It follows that $uf^{s_0}|_{x_{i_1}=a}$ is in $I_1 \cap (K[U_2]/\{0\})$, which contradicts that U_2 is an independent modulo I_1. In conclusion, $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$ is the independent modulo I. □

Remark 1. According to Theorem 5, suppose that $\{x_{i_1}\}$ is an independent modulo I and $a \in K$ satisfies $f(a) \neq 0$. If $U_2 = \{x_{i_2}, x_{i_3}, \ldots, x_{i_m}\}$ is an independent mod I_1, then $U_1 = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$ is the independent mod I. Conversely, if $f(a) = 0$, the conclusion of Theorem 5 may not be true. For instance, $I = \langle xy - x, xz\rangle \subset \mathbb{C}[x, y, z]$, where $\mathbb{C}$ is the complex field. It is concluded that x is the independent modulo I and $f(x) = x$, correspondingly. If $x = 0$, let$I_1 = I|_{x=0} = \langle 0\rangle$. Obviously, $\{y\}$ is an independent mod I_1, but $\{x, y\}$ is a dependent mod I. If x_{i_1} is an independent mod I, let $V_1 = X/x_{i_1}$. Then, consider I as the ideal in $K(x_{i_1})[V_1]$, and compute G_1, the quasi-Gröbner basis of I with respect to an admissible term order $>_{v^1}$ (based on Theorem 3, we can compute the quasi-Gröbner basis of I with respect to the admissible term order $>_{v^1}$). Let $f_1(x_{i_1}) = \mathrm{LCM}\{\mathrm{LC}(g)|g \in G_1\}$. Next, choose $a_1 \in K$ such that $f_1(a_1) \neq 0$, and then $I_1 = I|_{x_{i_1}=a_1}$. For simplicity, we call the value polynomial of I with respect to x_{i_1}. Repeat these steps gradually until x_{i_m} is the independent modulo $I_{m-1}(m \geq 2)$ and I_{m-1} is a zero-dimensional ideal, which means $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$ is an independent modulo I. In the end, we can check whether $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$ is a maximal independent modulo I by Proposition 4. If not, specify $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$ the proper values and repeat the steps as before, a maximal independent variable set modulo I can be gained in finite steps.

The following algorithm is the main algorithm in our paper where we describe the main steps to compute maximal independent variable sets.

4. Experiment

4.1. Example

Example 1. Considering the system in the complex field $\mathbb{C}$,

$$\begin{cases} f_1 = z^3 - z^2 y + xy - xz + y - z = 0, \\ f_2 = w^2 - y^2 + 1 = 0. \end{cases} \tag{5}$$

Let $I = \langle f_1, f_2\rangle = \langle z^3 - z^2 y + xy - xz + y - z, w^2 - y^2 + 1\rangle$.Show a maximal independent variable set modulo I.

The detailed steps according to our algorithm to solve this problem are as follows:

(i) Let $G = (f_1, f_2)$. Firstly, choose variable z. Then, consider I as the ideal in $C(z)[w, x, y]$, and compute the quasi-Gröbner basis of I with respect to graded reverse lexicographic order, an admissible term order on $T(w, x, y)$. The result is $G = (f_1, f_2)$. $G \cap (C[z]/\{0\}) = \varnothing$. Therefore, z is an independent mod I.

(ii) Compute the value polynomial of I with respect to variable z. The result is $h(z) = \mathrm{LCM}(1, 1) = 1$. Because $h(0) = 1 \neq 0$, let $z = 0$. Then, I turns to $I_1 = \langle xy + y, w^2 - y^2 + 1\rangle$. The dimension of I_1 is not 0, and hence choose one variable again.

(iii) Firstly, choose variable x. Then, consider I_1 as the ideal in $C(x)[w, y]$, and compute the quasi-Gröbner basis of I_1 with respect to graded reverse lexicographic order, an admissible term order on $T(w, y)$. The result is $G' = ((x + 1)y, w^2 - y^2 + 1)$. $G' \cap (C[x]/\{0\}) = \varnothing$, and thus $\{x\}$ is an independent mod I_1.

(iv) Compute the value polynomial of I_1 with respect to variable x, and the value polynomial is $\tilde{h}(x) = \mathrm{LCM}(x + 1, 1) = x + 1$. Choose $x = 1$ because $\tilde{h}(1) = 2 \neq 0$. Then, I_1 turns to $I_2 = \langle f_1', f_2'\rangle = \langle 2y, w^2 - y^2 + 1\rangle$. Also, the dimension of I_2 is 0.

(v) Consider I as the ideal in $C(z, x)[w, y]$ and compute the quasi-Gröbner basis of I with respect to graded reverse lexicographic order, an admissible term order on $T(w, y)$. The result is $G\prime\prime = ((1 + x - z^2)y + (z^3 - xz - z), w^2 - y^2 + 1)$. The dimension of I^e is 0, and hence a maximal independent set mod I is $\{x, z\}$.

Regarding Algorithm 1, there is one thing to notice that is described as follows.

Remark 2. By Algorithm 1, one maximal independent variable set modulo I can be computed. If the ideal I is prime, which means the variety $V_L(I)$ is irreducible; the rest of maximal independent variable sets can be obtained by exchanging the order of variables selected in each step. Otherwise, in the case that I is not a prime ideal, we can only get all the maximal independent variable sets for one irreducible component of $V_L(I)$ by Algorithm 1. For example, assume that $I = \langle xy - x, xz\rangle \subset \mathbb{C}[x, y, z]$. The sets $\{x\}$ and $\{y, z\}$ are all the maximal independent variable sets modulo I. According to Algorithm 1, if the variable x that is an independent modulo I is selected firstly, it is concluded that $f_1(x) = x$. Let $x = 1$, then the ideal $I_1 = I|_{x=1} = \langle y - 1, z\rangle \subset \mathbb{C}[y, z]$ is zero-dimensional. Thus, the set $\{x\}$ is a maximal independent modulo I. Moreover, in order to get another maximal independent set $\{y, z\}$, two methods can be considered. One way is exchanging the order of variables selected in each step as before. For instance, choose the variable y, which is an independent modulo I, firstly. Compute the value polynomial of I with respect to variable y. The result is $f_1(y) = y - 1$. Set $y = 0$, then $I_1 = I|_{y=0} = \langle -x, xz\rangle \subset \mathbb{C}[x, z]$. Next, we choose the variable z that is an independent modulo I_1. The value polynomial $f_2(z)$ of I_1 with respect to z is z. Let $z = 1$, then $I_2 = I_1|_{z=1} = \langle -x, x\rangle$, which is zero-dimensional in $\mathbb{C}[x]$. Thus, the maximal independent variable set $\{y, z\}$ is obtained. Another way is continuing the algorithm for the new ideal $I\prime = \langle xy - x, xz, f_1(x)\rangle \subset \mathbb{C}[x, y, z]$. We can also obtain the maximal independent set $\{y, z\}$.

Input: $I := \langle f_1, f_2, \ldots, f_m \rangle$.
(i) $j := 1, W := \varnothing, X_0 := X, I_0 := I$.
(ii) Compute the dimension of I. If it is zero, then stop; otherwise, do (iii).
(iii) Choose randomly $x_{i_j} \in X/W, U_j = \{x_{i_j}\}$, and $V_j = X_{j-1}/U_j$. Then, consider I_{j-1} as an ideal in $K(U_j)[V_j]$ and compute G_j, the quasi-Gröbner basis of I_{j-1} with respect to an admissible term order $> v^j$. Next, check whether $G_j \cap (K[U_j]/\{0\})$ is $\varnothing$. If true, it is concluded that x_{i_j} is an independent modulo I, and then do (iv). Otherwise, repeat (iii) until choosing a variable x_{i_j} independent modulo I_{j-1}.
(iv) Compute $f_j(x_{i_j}) = \mathrm{LCM}\{\mathrm{LC}(g) | g \in G_j\}$. Choose randomly $a_j \in K$ such that $f_j(a_j) \neq 0$, and then $I_j := I_{j-1}|_{x_{i_j}=a_j}$.
(v) $W := W \cup \{x_{i_j}\}$. If the dimension of I_j is zero, then do (vi). Otherwise, $X_j := X_{j-1}/\{x_{i_j}\}$, $j := j + 1$, and return to (iii).
(vi) Consider I as the ideal in $K(W)[X/W]$ and compute G, the quasi-Gröbner basis of I with respect to an admissible term order $>_{X/W}$. If $I^e \subset K(W)[X/W]$ is a zero-dimensional proper ideal, the algorithm stops. In other words, W is a maximal independent modulo I. Otherwise, enter the next step.
(vii) Compute $f(x_{i_1}, x_{i_2}, \ldots, x_{i_j}) = \mathrm{LCM}\{\mathrm{LC}(g) | g \in G\}$. Choose $p = (p_1, p_2, \ldots, p_j) \in K^j$ such that $f(p_1, p_2, \ldots, p_j) \neq 0$, $I_j := I|_{(x_{i_1}=p_1, x_{i_2}=p_2, \ldots, x_{i_j}=p_j)}$, and $j := j + 1$. Return to (iii).
Output: W.

Algorithm 1

In each step of Algorithm 1, the variable x_{i_j} selected randomly needs to be assigned $a_j \in K$ such that $f_j(a_j) \neq 0$. The values of a_j satisfying $f_j(a_j) = 0$ are finite in K, so the "correct value" for a_j can be obtained in finite steps. For example, suppose that the degree of the polynomial f_j is d, then there is at least one value in the set $\{0, 1, 2, \ldots, d\}$, which satisfies $f_j(a_j) \neq 0$. Therefore, Algorithm 1 is terminated in finite steps.

4.2. Algorithm Analysis. In the existing algorithms of computing the independent variable sets of an ideal, all variables are regarded as a unit, and computations are all in the rational function field, which might lead to high complexity. Compared with those algorithms, the algorithm given in this paper chooses one variable once, and thus it turns a multivariate problem into a single-variable problem. Moreover, the algorithm reduces the number of variables by assigning them some values, which avoids the redundancy of computation and effectively reduces the complexity of the algorithm to some extent.

5. Conclusions

This paper gives an improved algorithm for computing the maximally independent variable set modulo an ideal. An assignment criterion is proposed, by which the problem of extended ideals is converted into that of assignment ideals gradually. In other words, the computations in rational function field are turned to computations in the fundamental number field. We reduce the dimension of ideal by assigning variables and prefer to choose one variable each time, avoiding increasing the number of considered variables, which realizes the change from a multivariable problem to a single-variable problem. This is the mainly improved aspect with respect to classical algorithms, by which we could reduce the computation complexity to some extent. Although the computations of our algorithm will be smaller than some of the classical algorithms, it is not the perfect one. We compute quasi-Gröbner basis by ES-polynomial in ring whose computations are still large. Therefore, computing quasi-Gröbner basis in ring can be improved.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Fundamental Research Funds for the Central Universities under Grant no. 2572016CB06.

References

[1] B. Buchberger, *Ein algorithmic zum auffinden der basiselemente des restklassrings nach einem nulldimensionalen polynimial*, Ph.D. thesis, University of Insbruck, Insbruck, Australia, 1965.
[2] H. M. Möller and F. Mora, "The computation of the hilbert function," *Computer Algebra in EUROCAL'83*, vol. 162, pp. 157–167, 1983.
[3] H. Kredel and V. Weispfenning, "Computing dimension and independent sets for polynomial ideals," *Journal of Symbolic Computation*, vol. 6, no. 2-3, pp. 231–247, 1988.
[4] G. Carrà Ferro, "Some properties of the lattice points and their application to differential algebra," *Communications in Algebra*, vol. 15, no. 12, pp. 2625–2632, 1987.
[5] C. L. Zhang and G. C. Feng, "Deciding variables set for polynomial ideal," *Numerical Mathematics A Journal of Chinese University*, vol. 3, pp. 17–19, 1998.

[6] B. X. Shang, S. G. Zhang, C. Tan, and P. Xia, "A simplified rational representation for positive-dimensional polynomial systems and SHEPWM equations solving," *Journal of Systems Science and Complexity*, vol. 30, no. 6, pp. 1470–1482, 2017.
[7] A. Bernasconi, E. W. Mayr, M. Mnuk, and M. Raab, "Computing the dimension of a polynomial ideal," 2002, https://www14.informatik.tu-muenchen.de/personen/raab/.
[8] M. Kratzer, "Computing the dimension of a polynomial ideal and membership in low-dimensional ideals," M.Sc. thesis, Technische Universität München, Munchen, Germany, 2008.
[9] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Springer Verlag, Berlin, Germany, 1985.
[10] T. Becker and V. Weispfenning, *Groebner Bases*, Springer Verlag, New York, NY, USA, 1993.
[11] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, New York, NY, USA, 4th edition, 2015.
[12] J. L. Zhang, "Deciding variables set for polynomial ideal," *Journal of Mathematics*, vol. 3, pp. 222–224, 2003.