A Method to Determine if Two Parametric Polynomial Systems Are Equal

Jie Zhou and Dingkang Wang

KLMM, Academy of Mathematics and Systems Science, CAS, Beijing, China
`jiezhou@amss.ac.cn, dwang@mmrc.iss.ac.cn`

Abstract. The comprehensive Gröbner systems of parametric polynomial ideal were first introduced by Volker Weispfenning. Since then, many improvements have been made to improve these algorithms to make them useful for different applications. In contract to reduced Groebner bases, which is uniquely determined by the polynomial ideal and the term ordering, however, comprehensive Groebner systems do not have such a good property. Different algorithm may give different results even for a same parametric polynomial ideal. In order to treat this issue, we give a decision method to determine whether two comprehensive Groebner systems are equal. The polynomial ideal membership problem has been solved for the non-parametric case by the classical Groebner bases method, but there is little progress on this problem for the parametric case until now. An algorithm is given for solving this problem through computing comprehensive Groebner systems. What's more, for two parametric polynomial ideals and a constraint over the parameters defined by a constructible set, an algorithm will be given to decide whether one ideal contains the other under the constraint.

Keywords: Constructible Set, Quasi-algebraic set, Gröbner Bases, Comprehensive Gröbner System.

1 Introduction

The comprehensive Gröbner systems of parametric polynomial ideal were introduced by Volker Weispfenning in 1992 [12]. Many engineering problems are parameterized and have to be repeatedly solved for different values of parameters. The comprehensive Gröbner systems can give the structure of solution space(finitely many, infinitely many, or the dimension of the solutions), which is similar to the properties of the Gröbner bases.

Let k be a field, $k[U][X]$ be the polynomial ring with the parameters $U = \{u_1, \ldots, u_m\}$ and the variables $X = \{x_1, \ldots, x_n\}$, where U and X are disjoint. K is an algebraically closed field of k, F be a subset of $k[U][X]$. A specialization σ is the homomorphism from $k[U][X]$ to $K[X]$. The comprehensive Gröbner systems for F is a finite set $\mathcal{G} = \{(A_1, G_1), \ldots, (A_l, G_l)\}$, which satisfy $\sigma_{\bar{a}}(G_i)$ is a Gröbner basis for the ideal $\langle \sigma_{\bar{a}}(F) \rangle$ in $K[X]$ for any $\bar{a} \in A_i$ and $i = 1, \ldots, l$.

Many algorithms have been provided for computing the comprehensive Gröbner systems, including CGB (V.Weispfenning, 1992)[12], CCGB(V.Weispfenning,

H. Hong and C. Yap (Eds.): ICMS 2014, LNCS 8592, pp. 537–544, 2014.

2003)[13], ACGB(Y.Sato and A.Suzuki, 2003)[9], SACGB(Y.Sato and A.Suzuki, 2006)[10], HSGB(González-Vega et al., 2005)[2] and BUILDTREE (A.Montes, 2002)[5]. A speed-up of the algorithm was given by Nabeshima [7]. A newest version for computing CSG was provided by Kapur, Sun and Wang by removing redundant segments [3]. There is an related concept of Gröbner cover introduced by Montes and Wibmer in 2010 [6]. In contract to reduced Gröbner bases, which is uniquely determined by the polynomial ideal and the term ordering, however, the comprehensive Gröbner systems do not have such a good property. Different algorithm may output different results. Weispfenning[13], Manubens and Montes[4], Wibmer[14] have done some researches about the canonical Gröbner system. In this paper, we compare two CGS from another aspect.

In ISSAC'09, Suzuki and Sato[8] gave a method to compute the inverses in residue class rings of parametric polynomial ideals. For a given parametric ideal $I \subset k[U][X]$, and a polynomial $f \in k[U][X]$, they first compute a CGS $\mathcal{G}$ of $I + \langle fy - 1\rangle$. For any branch $(A, G) \in \mathcal{G}$. if there is a polynomial which can be expressed as $y - h$, where $h \in k[U][X]$, then f is invertible in $K[X]/(I : f^\infty)$ under the constraint A. In order to judge whether f is invertible in $K[X]/I$, it still need to decide whether I and $I : f^\infty$ are equal under the constraint A. This is the motivation of the paper.

The ideal membership problem of non-parametric case has been totally solved in the past[1]. But there is little research about the problem of parametric case until now. This paper can solve this problem through computing CGS of the parametric polynomial ideal. In the paper, we also give a method to decide whether two comprehensive Gröbner systems are equal. As a consequence, for two parametric polynomial ideals and a constructible set, the method can judge whether one of ideals is contained in the other one under the constraint of the constructible set.

This paper is organized as follow. Section 2 gives some preliminaries about the constructible set and the quasi-algebraic set. In section 3, the method of solving the ideal membership problem is presented. The inclusion and equivalence relation about two parametric ideal are also given in this section. Finally, some conclusions are given in section 4.

2 Notations and Preliminary

2.1 Notations

Let k be a field, K be the algebraic closure of k, R be a polynomial ring $k[U]$ in parameters $U = \{u_1, \ldots, u_m\}$, and $R[X]$ be a polynomial ring over R in variables $X = \{x_1, \ldots, x_n\}$ where X and U are disjoint. Let $PP(X)$ be the sets of power products of X, and $\prec$ be an admissible monomial ordering on $PP(X)$. As before, for a polynomial $f \in R[X] = k[U][X]$, the leading power product, leading coefficient and leading monomial of f w.r.t. the ordering $\prec$ are denoted by $\mathrm{lpp}(f)$, $\mathrm{lc}(f)$ and $\mathrm{lm}(f)$ respectively. Note that $\mathrm{lc}(f) \in k[U]$ and $\mathrm{lm}(f) = \mathrm{lc}(f)\mathrm{lpp}(f)$.

For arbitrary $\bar{a} \in K^m$, a **specialization** of R induced by $\bar{a}$ is a homomorphism $\sigma_{\bar{a}} : R \longrightarrow K$. That is, for $\bar{a} \in K^m$, the induced specialization $\sigma_{\bar{a}}$ is defined as follows:

$$\sigma_{\bar{a}} : f \longrightarrow f(\bar{a}),$$

where $f \in R$. Every specialization $\sigma_{\bar{a}} : R \longrightarrow K$ extends canonically to a specialization $\sigma_{\bar{a}} : R[X] \longrightarrow K[X]$ by applying $\sigma_{\bar{a}}$ coefficient-wise. For a subset F of $k[U][X]$, $\sigma_{\overline{a}}(F) = \{\sigma_{\overline{a}}(f) \mid f \in F\}$.

Definition 1 (Member). *Let F be an subsets of parametric polynomial ring $k[U][X]$, $f \in k[U][X]$. We say f is a* **member** *of the ideal generated by E, if for any $\overline{a}$ in K^m, $\sigma_{\overline{a}}(f)$ is a member of the ideal generated by $\sigma_{\overline{a}}(E)$ in $K[X]$.*

Definition 2 (Contain). *Let E, F be two subsets of the parametric polynomial ring $k[U][X]$. We say E* **contains** *F, if the ideal generated by $\sigma_{\bar{a}}(E)$ contains the ideal generated by $\langle\sigma_{\bar{a}}(F)$ in $K[X]$ for any $\bar{a} \in K^m$. If E contains F, and F contains E, we say E and F are* **equal**.

For any $\bar{a} \in K^m$, if every element in the Gröbner bases of $\langle\sigma_{\bar{a}}(F)\rangle$ is contained in the ideal $\langle\sigma_{\bar{a}}(E)\rangle$, it is obvious that E contains F. For different $\bar{a} \in K^m$, the Gröbner bases of $\langle\sigma_{\bar{a}}(F)\rangle$ may be different, so we need to study the structure of the Gröbner bases of $\langle\sigma_{\bar{a}}(F)\rangle$ with respect to the parametric space K^m. Before that, we introduce the notations about quasi-algebraic set and the constructible set.

For any subset $E = \{e_1, \ldots, e_s\}$ of $k[U]$, the set of common zeros in K^m of E is a Zariski closed set, denoted by $\mathbb{V}(E)$. For a single polynomial h in R, we denote the complement of $\mathbb{V}(h)$ in K^m by $\mathbb{V}(h)^c$, which is a basic Zariski open set. A **quasi-algebraic set** is the intersection of a Zariski closed set with a basic Zariski open set, and a **constructible set** is a finite union of quasi-algebraic set [11]. We denote $\mathbb{V}(E) \cap \mathbb{V}(h)^c$ by $\mathbb{V}(E)\backslash\mathbb{V}(h)$.

In this paper, we only consider the constructible set has a form $\mathbb{V}(E)\backslash\mathbb{V}(N)$, where $E = \{e_1, \ldots, e_s\}$ and $N = \{n_1, \ldots, n_t\}$ are subsets of R. It is obvious that $\mathbb{V}(E)\backslash\mathbb{V}(N) = \cup_{i=1}^{t}(\mathbb{V}(E)\backslash\mathbb{V}(n_i))$. We say a constructible set $\mathbb{V}(E)\backslash\mathbb{V}(N)$ is **consistent** if it is not empty.

Now we can describe the structure of the Gröbner bases of a parametric ideal. For a parametric polynomial system $F \subset R[X]$, a comprehensive Gröbner system of F is defined below.

Definition 3 (*CGS*). *Let F be a subset of $R[X]$, $A_1, \ldots, A_l$ be algebraical constructible subsets of K^m, $G_1, \ldots, G_l$ be subsets of $R[X]$, and S be a subset of K^m such that $S \subset A_1 \cup \cdots \cup A_l$. A finite set $\mathcal{G} = \{(A_1, G_1), \ldots, (A_l, G_l)\}$ is called a* **comprehensive Gröbner system** *on S for F, if $\sigma_{\bar{a}}(G_i)$ is a Gröbner basis for the ideal $\langle\sigma_{\bar{a}}(F)\rangle$ in $K[X]$ for any $\bar{a} \in A_i$ and $i = 1, \ldots, l$. Each (A_i, G_i) is called a branch of $\mathcal{G}$. Particularly, if $S = K^m$, then $\mathcal{G}$ is called a comprehensive Gröbner system for F.*

In above, the constructible set A_i can be expressed as $A_i = \mathbb{V}(E_i) \setminus \mathbb{V}(N_i)$, where E_i, N_i are subsets of $k[U]$.

Notes that, for many algorithm of computing CGS, such as the algorithm given in [3,7], the output of these algorithm has the following property: for any branch (A, G) of a CGS, for each $g \in G$, $\sigma_{\bar{a}}(\mathrm{lc}(g)) \neq 0$ for any $\bar{a} \in A$. So in the paper, we always assume the CGS has the above property.

2.2 Some Preliminaries

Given two polynomial f, g in $k[U][X]$, and a term ordering "$\prec$". If there is a term $c_\alpha X^\alpha$ in f with the coefficient $c_\alpha \neq 0$, and X^α is a multiple of $\mathrm{lpp}(g)$, we say f can be reduced by g, and $r = \mathrm{lc}(g)f - c_\alpha X^\gamma g$ is the remainder of f reduced by g through one step reduction, where $X^\gamma = \frac{X^\alpha}{\mathrm{lpp}(g)}$. Continuing reduce r by g until no term of the remainder is a multiple of $\mathrm{lpp}(g)$, assume the remainder is r_0, we say the r_0 is the **remainder** of f reduced by g.

For a subset F of $k[U][X]$, and a polynomial $g \in k[U][X]$, we can define the reduction of g by F as the following lemma. The pseudo division algorithm in $k[U][X]$ is similar to the division algorithm in $k[X]$, more details about the division algorithm can refer to the book [1].

Lemma 1. *Let $F = \{f_1, \ldots, f_s\}$ be a subset of $k[U][X]$, and "$\prec$" be a term ordering. Then every $g \in k[U][X]$ can be represented as:*

$$\prod_{i=1}^{s} \mathrm{lc}(f_i)^{\delta_i} g = p_1 f_1 + \cdots + p_s f_s + r,$$

for some elements $h_1, \ldots, h_s, r$ in $k[U][X]$, nonnegative integers $\delta_1, \ldots, \delta_s$, such that:

i.) $p_i = 0$ or $\mathrm{lpp}(p_i f_i) \preceq \mathrm{lpp}(g)$,
ii.) $r = 0$ or no term of r is a multiple of any $\mathrm{lpp}(f_i)$, $i = 1, \ldots, s$.

At the end of this part, we review some properties about the constructible set and the quasi-algebraic set.

For a constructible set $A = \mathbb{V}(E) \setminus \mathbb{V}(N)$, where $E, N = \{n_1, \ldots, n_l\}$ are subsets of $k[U]$. We are only interested in those constructible sets which are consistent. Since $A = \mathbb{V}(E) \setminus \mathbb{V}(N) = \bigcup_{i=1}^{l} (\mathbb{V}(E) \setminus \mathbb{V}(n_i))$, we only need to know whether the quasi-algebraic set $\mathbb{V}(E) \setminus \mathbb{V}(n_i)$ is empty, for $i = 1, \ldots, l$.

Lemma 2. *Let $A = \mathbb{V}(E) \setminus \mathbb{V}(h)$ be a quasi-algebraic set, where E is a subset of $k[U]$ and h is a polynomial in $k[U]$. Then A is consistent if and only if h is not in the radical ideal generated by E in $k[U]$.*

In the following lemma, we show any finite intersection of quasi-algebraic set is a quasi-algebraic set.

Lemma 3 ([11]). *Let $A_1 = \mathbb{V}(E_1) \setminus \mathbb{V}(h_1)$, $A_2 = \mathbb{V}(E_2) \setminus \mathbb{V}(h_2)$ be two quasi-algebraic sets, where E_1, E_2 are subsets of $k[U]$, and h_1, h_2 are polynomials in $k[U]$. Then $A_1 \cap A_2$ is also a quasi-algebraic set, and $A_1 \cap A_2 = \mathbb{V}(E_1, E_2) \setminus \mathbb{V}(h_1 h_2)$.*

Given a quasi-algebraic set $A = \mathbb{V}(E)\backslash\mathbb{V}(h) \subset K^m$, and a parametric polynomial $f = c_1X^{\alpha_1} + \cdots + c_tX^{\alpha_t} \in k[U][X]$, $c_i \in k[U]$ for $i = 1, \ldots, t$. If for any $\overline{a} \in A$, the specialization $\sigma_{\overline{a}}(f) = 0$, then A must be a subset of the common zeros of the coefficients, i.e. $A \subset \mathbb{V}(c_1, \ldots, c_t)$. Let $\overline{A}$ be the Zarisiki closure of A,

$$\mathbb{V}(\langle E\rangle : h^\infty) = \overline{\mathbb{V}(\langle E\rangle)\backslash\mathbb{V}(h)} = \overline{A} \subset \overline{\mathbb{V}(c_1, \ldots, c_t)} = \mathbb{V}(c_1, \ldots, c_t),$$

so c_i is in the radical ideal generated by the saturated ideal $\langle E\rangle : h^\infty$ in $k[U]$ for $i = 1, \ldots, t$. On the other hand, we can regard the polynomials in E and h as polynomial in $k[U, X]$, then f is in the radical ideal generated by the saturated ideal $\langle E\rangle : h^\infty$ in $k[U, X]$.

Lemma 4. *Given a quasi-algebraic set $A = \mathbb{V}(E)\backslash\mathbb{V}(h) \subset K^m$, and a parametric polynomial $f \in k[U][X]$. If for any $\overline{a} \in A$, the specialization $\sigma_{\overline{a}}(f) = 0$, then $\langle E, fhv - 1\rangle = \langle 1\rangle = k[v, U, X]$, where v is an auxiliary variable different from X an U.*

3 The Computations about Two Parametric Ideals

In this section, first we give the method to judge whether a parametric polynomial is a member of a parametric polynomial ideal. Then we give the method to determine the inclusion and equivalence relationship about two parametric polynomial ideals. Several examples will be given for illustrating our methods.

3.1 The Membership Problem of Parametric Ideal

Given a subset F of parametric polynomial ring $k[U][X]$, and a parametric polynomial f in $k[U][X]$. If f is a member of the ideal generated by F in $k[U, X]$, it is obvious for any $\overline{a} \in K^m$, $\sigma_{\overline{a}}(f)$ is a member of the ideal generated by $\sigma_{\overline{a}}(F)$. But there are some situations, f is not a member of the ideal generated by F in $k[U, X]$, f is still a member of ideal generated by F. For example, $F = \{a^3b^2x^2 - y^2, ab^2x^2 - b^2xy^2\}, f = abx^2 - b^3y^6$, it is easy to check f is not in the ideal generated by F in $k[a, b, x, y]$. But we will see, for any $(a, b) \in \mathbb{C}^2$, $\sigma_{\overline{a}}(f)$ is a member of the ideal generated by $\sigma_{\overline{a}}(F)$, so f is a member of the ideal generated by F.

In order to check whether a parametric polynomial is a member of a parametric ideal, we have following theorem.

Theorem 4. *Let F be a subset of parametric polynomial ring $k[U][X]$, and f be a parametric polynomial in $k[U][X]$. Assume $\mathcal{G} = \{(A_1, G_1), \ldots, (A_l, G_l)\}$ be a comprehensive Gröbner system of F w.r.t. a term ordering " $\prec$ ". For any branch (A, G) in $\mathcal{G}$, r is the remainder of f reduced by G. If for any $\overline{a} \in A$, $\sigma_{\overline{a}}(r) = 0$, then f is a member of the parametric ideal generated by F.*

We continue the above example to illustrate the result given in Theorem 1.

Example 1. Let $F = \{a^3b^2x^2 - y^2, ab^2x^2 - b^2xy^2\}$ be a subset of $\mathbb{Q}[a,b][x,y]$, and $f = abx^2 - b^3y^6$ in $\mathbb{Q}[a,b][x,y]$. Check whether f is a member of the ideal generated by F.

First, a *CGS* $\mathcal{G}$ of F w.r.t. a lexicographic ordering $x \succ y$ is computed.

$$\mathcal{G} = \{(A_1, G_1), (A_2, G_2), (A_3, G_3)\},$$

where $A_1 = \mathbb{V}(\emptyset)\backslash\mathbb{V}(ab), G_1 = \{ab^2y^4 - y^2, xy^2 - b^2y^6, ab^2x^2 - b^2xy^2\}; A_2 = \mathbb{V}(a)\backslash\mathbb{V}(1), G_2 = \{y^2\}; A_3 = \mathbb{V}(b)\backslash\mathbb{V}(a), G_3 = \{y^2\}$.

For branch (A_1, G_1), f is reduced by G_1 to 0. For branch (A_2, G_2), f is reduced by G_2 to abx^2. Since under the constraint A_2, $a = 0$, so for any $\overline{a} \in A_2$, $\sigma_{\overline{a}}(abx^2) = 0$. For branch (A_3, G_3), f is reduced by G_3 to abx^2. Since under the constraint A_3, $b = 0$, so for any $\overline{a} \in A_3$, $\sigma_{\overline{a}}(abx^2) = 0$. By the Theorem 1, f is a member of parametric ideal generated by F.

3.2 The Equivalence Relationship about Two Parametric Ideal

In this part, we give the method to determine whether a parametric polynomial ideal E contains another parametric polynomial ideal F.

Let $\mathcal{G}_1 = \{(A_1, G_1), \ldots, (A_l, G_l)\}$ be a *CGS* of E w.r.t. a term ordering " $\prec_1$ ", and $\mathcal{G}_2 = \{(B_1, H_1), \ldots, (B_r, H_r)\}$ be a *CGS* of F w.r.t. a term ordering " $\prec_2$ ". For any branch $(A, G) \in \mathcal{G}_1$, if $\sigma_{\overline{a}}(F)$ is contained in $\langle\sigma_{\overline{a}}(E)\rangle$, it is obvious E contains F. We have the following theorem.

Theorem 5. *Let $\mathcal{G}_1, \mathcal{G}_2$ be as above. For any branch $(A, G) \in \mathcal{G}_1$ and $(B, H) \in \mathcal{G}_2$, assume $G = \{g_1, \ldots, g_s\}, H = \{h_1, \ldots, h_t\}$, and r_i be the remainder of h_i reduced by G for $i = 1, \ldots, t$. If for any $\overline{a} \in A \cap B$, $\sigma_{\overline{a}}(r_i) = 0$, then E contains F, where $i = 1, \ldots, t$.*

Remark 1. If we only need to know whether F is contained in E under some constructible set A, we only need to compute a *CGS* of F on A, then use the Theorem 2.

If E contains F and F contains E, E and F are equal. We have the following consequence of Theorem 2.

Corollary 6. *Let $\mathcal{G}_1, \mathcal{G}_2$ be as above. For any branch $(A, G) \in \mathcal{G}_1$ and $(B, H) \in \mathcal{G}_2$, assume $G = \{g_1, \ldots, g_s\}, H = \{h_1, \ldots, h_t\}$, r_i be the remainder of h_i reduced by G w.r.t. " $\prec_1$ " , and q_j be the remainder of g_j reduced by H w.r.t. " $\prec_2$ " . If for any $\overline{a} \in A \cap B$, $\sigma_{\overline{a}}(r_i) = 0$ and $\sigma_{\overline{a}}(q_j) = 0$, then E and F are equal, where $i = 1, \ldots, t$, $j = 1, \ldots s$.*

In the ISSAC'09, Suzuki and Sato give a method to compute the inverse in residue class rings of parametric polynomial ideals. Given a parametric polynomial ideal $I \subset k[U][X]$, and $f \in k[U][X]$, they first compute a *CGS* of $\langle I + fy - 1\rangle$ w.r.t. a block order "$y >> X >> U$" in $k[U][X, y]$. By their method, it only can decide whether f is invertible in $K[X]/(I : f^\infty)$ in every branch directly.

In order to judge whether f is invertible in $K[X]/I$, it still need to compare whether I and $I : f^\infty$ are equal in every branch. The following is the example come from [8].

Example 2. Let $I = \{ax_3^2 + 2x_2x_3 + bx_1^2x_3 + (-b+d)x_1x_3 - dx_3 + ax_2^2 + abx_1^2x_2 + adx_1x_2 + x_1^2 + cx_1 + e, ax_2 + ax_1x_2 + x_1x_3\}$ be a set of parametric polynomials, $f = x_1 + ax_2 + x_3$ be a parametric polynomial in $\mathbb{Q}[U][X]$, where $U = \{a, b, c, d, e\}$ are parameters and $X = \{x_1, x_2, x_3\}$ are variables. We need to check under what specialization σ from $\mathbb{Q}[U]$ to $\mathbb{C}$, $\sigma(f)$ is invertible in $\mathbb{C}[X]/\langle\sigma(I)\rangle$, where $\mathbb{C}$ is the complex field.

Suzuki and Sato computes a CGS of $I + \langle fy - 1\rangle$ in $\mathbb{Q}[a, b, c, d, e][x_1, x_2, x_3, y]$ w.r.t. a lexicographic term ordering $y \succ x_1 \succ x_2 \succ x_3$. There are six branches where f is invertible in $\mathbb{C}[X]/(I : f^\infty)$. We only choose two of them to study whether I and $I : f^\infty$ are equal in these branch.

Branch 1: (A_1, G_1)
$A_1 = \mathbb{V}(a)\backslash\mathbb{V}(e(c + d)(b - c - d + 2))$,
$G_1 = \{(2x_2 - d)x_3 + x_1^2 + cx_1 + e, x_1x_3, (-2x_2 + d)x_3^2 - ex_3, (4x_2^2 + (-2c - 4d)x_2 + dc + d^2)x3 - ex_1 - e^2y - ec\}$;

Branch 6: (A_6, G_6)
$A_6 = \mathbb{V}(e, c + d, b + 2, a - 1)\backslash\mathbb{V}(d)$,
$G_6 = \{-x_3^2 + (-2x_2 + d)x_3 - x_2^2 + (d + 1)x_2, -x_3 - x_2 - x_1 + d, -dy + 1\}$.

In the branch (A_1, G_1), $G_1' = G_1 \cap \mathbb{Q}[U][X] = \{(2x_2 - d)x_3 + x_1^2 + cx_1 + e, x_1x_3, (-2x_2 + d)x_3^2 - ex_3\}$ is the Gröbner basis of $I : f^\infty$ under the constraint of A_1. We first compute a CGS $\mathcal{G}_1$ of I under the constraint A_1,

$$\mathcal{G}_1 = \{\mathbb{V}(a)\backslash\mathbb{V}(e(c+d)(b-c-d+2)), \{(2x_2-d)x_3+x_1^2+cx_1+e, x_1x_3, (-2x_2+d)x_3^2-ex_3\}\}.$$

It is obvious I and $I : f^\infty$ are equal under the constraint A_1, so $\sigma_{\overline{a}}(f)$ is invertible in $\mathbb{C}[X]/\langle\sigma_{\overline{a}}(I)\rangle$ for $\overline{a} \in A_1$.

In the branch (A_6, G_6), $G_6' = G_6 \cap \mathbb{Q}[U][X] = \{-x_3^2 + (-2x_2 + d)x_3 - x_2^2 + (d + 1)x_2, -x_3 - x_2 - x_1 + d\} = \{g_1, g_2\}$ is the Gröbner basis of $I : f^\infty$ under the constraint of A_6. We first compute a CGS $\mathcal{G}_2$ of I under the constraint A_6: $\mathcal{G}_2 = \{\mathbb{V}(e, c+d, b+2, a-1)\backslash\mathbb{V}(d), \{x_2^4 + 4x_2^3x_3 - dx_2^3 - 2x_2^3 + 6x_2^2x_3^2 - 3dx_2^2x_3 - 4x_2^2x_3 + dx_2^2 + x_2^2 + 4x_2x_3^3 - 3dx_2x_3^3 - 2x_2x_3^2 + dx_2x_3 + x_3^4 - dx_3^3, x_1x_3 + x_2^3 + 3x_2^2x_3 - dx_2^3 - 2x_2^2 + 3x_2x_3^2 - 2dx_2x_3 - 2x_2x_3 + dx_2 + x_2 + x_3^3 - dx_3^2, x1x_2 + x_1x_3 + x_2, x_1^2 - dx_1 + x_2^2 + 2x_2x_3 - dx_2 + x_3^2 - dx_3\}\} = \{A_6, \{h_1, h_2, h_3, h_4\}\}$. It is obvious there is no term of $g_1 = -x_3^2 + (-2x_2 + d)x_3 - x_2^2 + (d + 1)x_2$, or $g_2 = -x_3 - x_2 - x_1 + d \in G_6'$ can be reduced by $\{h_1, h_2, h_3, h_4\}$, so the remainder of g_1, g_2 reduced by $\{h_1, h_2, h_3, h_4\}$ are $r_1 = g_1, r_2 = g_2$ respectively. For $\overline{a} = (1, -2, 1, -1, 0) \in A_6$, $\sigma_{\overline{a}}(r_1) = -x_3^2 + (-2x_2 - 1)x_3 - x_2^2 \neq 0$. So I and $I : f^\infty$ are not equal under the constraint A_6. That is, $\sigma_{\overline{a}}(f)$ is invertible in $\mathbb{C}[X]/\langle\sigma_{\overline{a}}(I : f^\infty)\rangle$ but not invertible in $\mathbb{C}[X]/\langle\sigma_{\overline{a}}(I)\rangle$ for $\overline{a} \in A_6$.

4 Conclusions

In this paper, we give the method to solve the membership problem about parametric polynomial ideals, and determine whether two parametric polynomial ideal are equal.

Given a parametric polynomial f and an ideal F in $k[U][X]$, before computing a CGS of F, we can first compute a Gröbner bases G of F in $k[U, X]$ and the remainder of f reduced by G. If the remainder is zero, then f is obvious the member of F. Otherwise, we use the theorem 4 to decide whether f is a member of F. Similarly, for two subset I, J of $k[U][X]$, if the reduced Gröbner bases of I and J in $k[U, X]$ are same, I and J must equal.

The authors are grateful to Professor Y. Sato for his helpful suggestions.

Acknowledgements. This work was supported by National Key Basic Research Project of China (Grant No. 2011CB302400), National Natural Science Foundation of China (Grant No. 11371356, 60970152).

References

1. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms, 3rd edn. Springer, New York (2007)
2. Gonzalez–Vega, L., Traverso, C., Zanoni, A.: Hilbert stratification and parametric Gröbner bases. In: Ganzha, V.G., Mayr, E.W., Vorozhtsov, E.V. (eds.) CASC 2005. LNCS, vol. 3718, pp. 220–235. Springer, Heidelberg (2005)
3. Kapur, D., Sun, Y., Wang, D.K.: A new algorithm for computing comprehensive Gröbner systems. In: Proc. ISSAC 2010, pp. 29–36. ACM Press, New York (2010)
4. Manubens, M., Montes, A.: Minimal canonical comprehensive Gröbner systems. Journal of Symbolic Computation 44(5), 463–478 (2009)
5. Montes, A.: A new algorithm for discussing Gröbner bases with parameters. Journal of Symbolic Computation 33(2), 183–208 (2002)
6. Montes, A., Wibmer, M.: Gröbner bases for polynomial systems with parameters. Journal of Symbolic Computation 45(12), 1391–1425 (2010)
7. Nabeshima, K.: A speed-up of the algorithm for computing comprehensive Gröbner systems. In: Proc. ISSAC 2010, pp. 299–306. ACM Press, New York (2007)
8. Sato, Y., Suzuki, A.: Computation of inverses in residue class rings of parametric polynomial ideal. In: Proc. ISSAC 2009, pp. 311–316. ACM Press, New York (2009)
9. Suzuki, A., Sato, Y.: An alternative approach to comprehensive Gröbner bases. Journal of Symbolic Computation 36(3), 649–667 (2003)
10. Suzuki, A., Sato, Y.: A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In: Proc. ISSAC 2006, pp. 326–331. ACM Press, New York (2006)
11. Sit, W.: Computations on Quasi-Algebraic Sets (2001)
12. Weispfenning, V.: Comprehensive Gröbner bases. Journal of Symbolic Computation 14(1), 1–29 (1992)
13. Weispfenning, V.: Canonical comprehensive Gröbner bases. Journal of Symbolic Computation 36(3), 669–683 (2003)
14. Wibmer, M.: Gröbner bases for families of affine or projective schemes. Journal of Symbolic Computation 42(8), 803–834 (2007)