Proving Geometric Theorems by Partitioned-Parametric Gröbner Bases*

Xuefeng Chen, Peng Li, Long Lin, and Dingkang Wang

Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and System Sciences,
Chinese Academy of Sciences,
Beijing 100080, P.R. China
{xfchen, pli, llin, dwang}@mmrc.iss.ac.cn

Abstract. The notion of partitioned-parametric Gröbner bases of a polynomial ideal under constraints is introduced and an algorithm for constructing partitioned-parametric Gröbner bases is given; the correctness and the termination of the algorithm are proved. We also present a method based on computing partitioned-parametric Gröbner bases for proving geometric theorems mechanically. By this method, besides proving the generic truth of a geometric theorem, we can give the necessary and sufficient conditions on the free parameters for the theorem to be true. An example for proving geometric theorems by the partitioned-parametric Gröbner bases method is given.

1 Introduction

Many geometric statements can be formulated in terms of polynomial equations, and such algebraic formulations usually involve a number of parameters. An important problem concerning proving geometric theorems is to determine whether a geometric statement is valid under a specialization of parameters.

In detail, a geometric statement of equality-type consists of two parts: hypotheses and conclusion. Both hypotheses and conclusion can be expressed in terms of polynomial equations in a number of free arbitrary coordinates $u_1, \ldots, u_m$, which we call parameters, and a number of dependent coordinates $x_1, \ldots, x_n$, which we call variables. Typically, the hypotheses are composed of

$$\begin{cases} h_1(u_1, \ldots, u_m, x_1, \ldots, x_n) = 0, \\ \qquad\cdots\cdots \\ h_r(u_1, \ldots, u_m, x_1, \ldots, x_n) = 0, \end{cases} \tag{1}$$

where the h's are polynomials over a ground field K. The conclusion is

$$g(u_1, \ldots, u_m, x_1, \ldots, x_n) = 0, \tag{2}$$

where g is a polynomial over K. The problem to be considered is:

* Partially supported by a NKBRPC (2004CB318000).

H. Hong and D. Wang (Eds.): ADG 2004, LNAI 3763, pp. 34–43, 2006.

Find all the constraints, viewed as polynomial equations and inequations in u_1, *...,* u_m*, such that (1) implies (2).*

For most geometric theorems, the conclusion does not strictly follow from the hypotheses; there are some so-called degenerate cases. Wu introduced the characteristic set method to prove geometric theorems and the "non-degenerate" conditions can be given automatically [12]. This method has been successfully used to prove many difficult geometric theorems, and to discover new theorems [3, 4, 11]. The application of the Gröbner bases method to geometric theorem-proving has been investigated in [3, 6, 10]. An algorithm based on Gröbner bases is presented in [10] for deriving simplest degeneracy conditions for geometric theorems.

Inspired by the work in [7, 9], in particular, the notion of parametric Gröbner bases in [7], in this paper we introduce the notion of partitioned-parametric Gröbner bases and based on it a method for analyzing the parameters involved in an algebraic formulation of a geometric statement. This method partitions the parametric space into finitely many subsets defined by polynomial equations and inequations (i.e., parametric constraints), and show clearly on which subsets the statement is valid and on which it is invalid. In other wrods, the necessary and sufficient conditions on the parameters for a geometric statement to be true can be given by this method.

Recently, we found that Montes [8] also presented an algorithm for discussing Gröbner bases with parameters.

In the next section, the method for checking the consistency of a polynomial constraint is described. In Section 3, the notion of parametric partition of a constrained polynomial set is introduced and an algorithm for constructing the parametric partition is described. In Section 4, the notion of partitioned-parametric Gröbner bases of an ideal under a constraint is introduced and an algorithm for computing partitioned-parametric Gröbner bases is presented. In Section 5, a partitioned-parametric Gröbner bases method for proving geometric theorems is proposed and an example is given to show how to use this method to prove geometric theorems mechanically.

2 Constraints over the Parameters

Let K be a computable field and E be an algebraically closed field containing K. For simplification, let $u = (u_1, \ldots, u_m)$, where $u_1, \ldots, u_m$ are parameters. $K[u]$ denotes the polynomial ring $K[u_1, \ldots, u_m]$.

A *constraint* is viewed as a set of polynomial equations and inequations over parameters, denoted by

$$C = \{c_1 = 0, \ldots, c_s = 0, d_1 \neq 0, \ldots, d_t \neq 0\},\ c_i, d_j \in K[u], \qquad (3)$$

which is true or false, depending on values in E substituted for parameters appearing in the constraint.

Let C be a constraint over the parameters; a set $S(C) \subset E^m$ is defined as

$$S(C) = \{u' \in E^m | u' \text{ satisfy the constraint } C\}.$$

Especially, $S(C) = E^m$ when C is the empty set.

A constraint C is said to be *consistent* if $S(C)$ is not an empty set.

A Gröbner bases algorithm or a characteristic set algorithm can be used for checking the consistency of a constraint C of form (3).

- **GB method:** by introducing $y_1, \dots, y_t$, let $d'_j = d_j y_j - 1, j = 1, \dots, t$, and $C' = \{c_1, \dots, c_s, d'_1, \dots, d'_t\} \subset K[u, y]$, where $y = (y_1, \dots, y_t)$; then C is consistent if and only if $\{1\}$ is not the reduced Gröbner basis of C'.
- **CS method:** $S(C)$ can be considered as a quasi-variety in E^m. Whether $S(C)$ is an empty set can be detected by computing its projection [2]. Moreover, the methods of regular decomposition or irreducible decomposition of $S(C)$ can also be used to detect its consistency [11, 12].

For a polynomial constraint, the following proposition is obvious.

Proposition 1. *If C is a constraint and p is a polynomial in $K[u]$, then one and only one of the following three cases should be satisfied:*

(a) $C \cup \{p \neq 0\}$ is not consistent, which can be equally described as for each $u' \in S(C)$, $p(u') = 0$, i.e., p can be considered as a zero function under $S(C)$.
(b) $C \cup \{p = 0\}$ is not consistent, which can be equally described as for each $u' \in S(C)$, $p(u') \neq 0$, i.e., p as a function is nonzero on $S(C)$.
(c) Both $C \cup \{p = 0\}$ and $C \cup \{p \neq 0\}$ are consistent.

3 Parametric Partition of a Constrained Polynomial Set

Let $u = (u_1, \dots, u_m)$ and $x = (x_1, \dots, x_n)$. By $K[u, x]$, we denote the polynomial ring with indeterminates u and x over K. Let f be a polynomial in $K[u, x]$ and u' be a specialization of u, and $f(u', x)$ denotes the polynomial obtained by substituting u' for u. Let F be a set of polynomials in $K[u, x]$, and $F(u', x)$ be the set of polynomials obtained by substituting u' for u into the polynomials in F.

In [5], some terminologies about polynomials have been introduced. We will extend them to polynomials with parameters.

Definition 1. *Let f be a nonzero polynomial in $K[u, x]$, where f can be considered as a polynomial in $K[u][x]$, and $f = \sum_\alpha a_\alpha x^\alpha$, where $a_\alpha \in K[u]$. Let $>$ be a monomial order on x.*

(a) The multidegree *of f is*

$$\text{multideg}(f) = \max(\alpha \in Z^n_{\geq 0} : a_\alpha \neq 0).$$

(b) The leading coefficient *of f is*

$$\text{lc}(f) = a_{\text{multideg}(f)} \in K[u].$$

In particular, for $f \in K[u]$, $\text{lc}(f) = f$.

(c) The leading monomial *of f is*

$$\mathrm{lm}(f) = x^{\mathrm{multideg}(f)}.$$

(d) The leading term *of f is*

$$\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f).$$

In paper [7], Kapur defined a constrained polynomial as a pair (C, f), where C is a consistent constraint and f is a polynomial in $K[u, x]$. The constraint polynomial (C, f) is unambiguous if $\mathrm{lc}(f)(u') \neq 0, \forall u' \in S(C)$.

In the following, we will extend constrained polynomial and unambiguous polynomial to constrained polynomial set and unambiguous polynomial set.

Definition 2. *A* constrained polynomial set *is a pair (C, F), where C is a consistent constraint over the parameters u, and F is a finite set of polynomials in $K[u, x]$. A constrained polynomial set (C, F) is an* unambiguous polynomial set *if for all u' in $S(C)$ and for all f in F, $lc(f)(u') \neq 0$.*

For example, $(\{u_1 - u_2 = 0, u_3 = 0, u_1 \neq 0, u_2 \neq 0\}, \{x_1 - u_1, 2u_1u_2x_1 + 1\})$ and $(\{u_1 = 0, u_2 = 0\}, \{1\})$ are two unambiguous polynomial sets.

Now, we define the parametric partition of a constrained polynomial set.

Definition 3. *A set $\{(C_1, F_1), \ldots, (C_s, F_s)\}$ of unambiguous polynomial sets is a* parametric partition *of a constrained polynomial set (C, F) if it satisfies the following conditions:*

(a) $S(C_1), \ldots, S(C_s)$ is a partition of $S(C)$, i.e., $\bigcup_{i=1}^{s} S(C_i) = S(C)$ and $S(C_i) \cap S(C_j) = \emptyset$, for $1 \leq i \neq j \leq s$;

(b) $\forall u' \in S(C)$, if $u' \in S(C_i)$ then $F_i(u', x)$ and $F(u', x)$ generate the same ideal in $K(u')[x]$, where $K(u')$ is the field generated by u' over K.

Let F be a polynomial set; the parametric partition of $(\emptyset, F)$ will be called the parametric partition of F.

Theorem 1. *For any constrained polynomial set, there is an algorithm to compute its parametric partition in finite steps.*

Proof. Let (C, F) be an arbitrary constraint polynomial set. First we will consider the case where F consists of only one polynomial, i.e., suppose that $F = \{f\}$. According to Proposition 1, we know that:

1. If $C \cup \{\mathrm{lc}(f) \neq 0\}$ is not consistent, then $\mathrm{lc}(f)$ is zero on $S(C)$; let $f' = f - \mathrm{lt}(f)$. It is obvious that the parametric partition of $(C, \{f'\})$ is exactly the one of $(C, \{f\})$.
2. If $C \cup \{\mathrm{lc}(f) = 0\}$ is not consistent, then $\mathrm{lc}(f)$ is nonzero on $S(C)$, and $(C, \{f\})$ is the parametric partition of itself.
3. Otherwise, both $C \cup \{\mathrm{lc}(f) = 0\}$ and $C \cup \{\mathrm{lc}(f) \neq 0\}$ are consistent; then the union of $\{(C \cup \{\mathrm{lc}(f) \neq 0\}, \{f\})\}$ and the parametric partition of $(C \cup \{\mathrm{lc}(f) = 0\}, \{f - \mathrm{lt}(f)\})$ is the parametric partition of $(C, \{f\})$.

Since f has a finite number of terms, the above process will terminate in finite steps and the number of the unambiguous polynomial sets in the parametric partition of $(C, \{f\})$ is also finite. It is easy to check that the above process will give the parametric partition of $(C, \{f\})$.

If F has more than one polynomial, then suppose that $F = \{f_1, \dots, f_{k-1}, f_k\}$, and that $\{(C_1, F_1), \dots, (C_t, F_t)\}$ is a parametric partition of $\{f_1, \dots, f_{k-1}\}$. Let $\{(C_{i1}, F_{i1}), \dots (C_{ik_i}, F_{i,k_i})\}$ be the parametric partition of $(C_i, \{f_k\})$; it is easy to check that $(C_{ij}, F_{ij} \cup F_i)$ for $i = 1, \dots, t$, $j = 1, \dots, k_i$ is the parametric partition of (C, F).

For example, $f = vxy + ux^2 + x$, $g = uy^2 + x^2$, $F = \{f, g\}$, assuming a lexicographic order on terms defined by the variable order $y > x$. First, we will construct the parametric partition of $(\emptyset, \{f\})$, It is $\{(C_1, \{f\}), (C_2, \{ux^2 + x\}), (C_3, \{x\})\}$, $C_1 = \{v \neq 0\}$, $C_2 = \{v = 0, u \neq 0\}$, $C_3 = \{v = 0, u = 0\}$. Then, we will construct the parametric partitions of $(C_1, \{g\})$, $(C_2, \{g\})$ and $(C_3, \{g\})$. The parametric partitions of $(C_1, \{g\})$, $(C_2, \{g\})$ and $(C_3, \{g\})$ are $\{(\{v \neq 0, u \neq 0\}, \{g\}), (\{v \neq 0, u = 0\}, \{x^2\})\}$, $\{(C_2, \{g\})\}$ and $\{(C_3, \{x^2\})\}$ respectively. The parametric partition of $(\emptyset, F)$ will be $\{(\{v \neq 0, u \neq 0\}, \{f, g\})$, $(\{v \neq 0, u = 0\}, \{f, x^2\})$, $(C_2, \{ux^2 + x, g\})$, $(C_3, \{x, x^2\})\}$.

4 Partitioned-Parametric Gröbner Bases

Let F be a polynomial set and u' be an element in E; we use I_F to denote the ideal generated by F in $K[u, x]$. Let

$$I_F(u', x) = \{p \mid p \text{ can be written as } f(u', x)/g(u'), f \in I_F, g \in K[u], g(u') \neq 0\};$$

it is easy to check that $I_F(u', x)$ is an ideal in $K(u')[x]$.

Definition 4. *Let (C, F) be a constrained polynomial set; a parametric partition $(C_1, G_1), \dots, (C_s, G_s)$ of (C, F) is called the* (reduced) partitioned-parametric Gröbner basis *of the ideal I_F under the constraint C if: $\forall u' \in S(C)$, if $u' \in S(C_i)$ then $G_i(u', x)$ is the (reduced) Gröbner basis of $I_F(u', x)$.*

The partitioned-parametric Gröbner basis of the ideal I_F under constraint $\emptyset$ will be called the partitioned-parametric Gröbner basis of the ideal I_F.

Two important operations in Gröbner bases computation are that of computing an *S-polynomial* of a pair of distinct polynomials and the *remainder* on division of a polynomial by one polynomial list. Below we extend these two notations to polynomials with parameters.

For a polynomial f in $K[u, x]$, for example $f = u^3x + x^2 + 1$, for a lexicographic order with $u > x$, the leading monomial will be u^3x. u^3x becomes 0 by specifying u to 0, which is different from the leading monomial of $f|_{u=0}$. We will define the following *S-polynomial* in $K(u)[x]$.

Definition 5. *Let f, g be two polynomials in $K[u, x]$. Suppose that* $\mathrm{multideg}(f) = \alpha$, $\mathrm{multideg}(g) = \beta$, *and let $\gamma = (\gamma_1, \ldots, \gamma_n)$, $\gamma_i = \max(\alpha_i, \beta_i)$. The* S-polynomial *of f and g is the combination*

$$\mathrm{spoly}(f, g) = \frac{x^\gamma}{\mathrm{lt}(f)} \cdot f - \frac{x^\gamma}{\mathrm{lt}(g)} \cdot g = \frac{x^\gamma \cdot (f \cdot \mathrm{lt}(g) - g \cdot \mathrm{lt}(f))}{\mathrm{lt}(f) \cdot \mathrm{lt}(g)},$$

which is in $K(u)[x]$.

For example, $f = vxy + ux^2 + x$, $g = uy^2 + x^2$, assuming a lexicographic order on terms defined by the variable order $y > x$,

$$\mathrm{spoly}(f, g) = \frac{u^2x^2y + uxy - vx^3}{uv}.$$

Definition 6. *We will write $\bar{f}^F$ for the* remainder *on division of $f \in K[u, x]$ by the ordered s-tuple $F = (f_1, \ldots, f_s) \subset K[u, x]$; $\bar{f}^F$ can be written as*

$$\bar{f}^F = f - \frac{a_1 f_1}{lc(f_1)} - \frac{a_2 f_2}{lc(f_2)} - \cdots - \frac{a_s f_s}{lc(f_s)},$$

where $a_1, \ldots, a_s$ are in $K[u, x]$. $\overline{f}^F$ is a linear combination with coefficients in $K(u)$, of monomials, none of which is divisible by any of $\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)$.

For example, $F = \{vxy + ux^2 + x, uy^2 + x^2\}$ and $f = vy^2 + ux^3y + y$, assuming a lexicographic order on terms defined by the variable order $y > x$. Then

$$\bar{f}^F = \frac{vuy - v^2x^2 - u^3x^4 - u^2x^3}{uv}.$$

Let f be a polynomial in $K(u)[x]$. We use $\mathrm{num}(f)$ to denote the numerator of f; $\mathrm{num}(f)$ is in $K[u, x]$.

Theorem 2. *The parametric partition $\{(C_1, G_1), \ldots, (C_s, G_s)\}$ of a constrained polynomial set (C, F) is the partitioned-parametric Gröbner basis of I_F under constraint C if and only if for each i, $\forall f, g \in G_i$,* $\mathrm{num}(\overline{\mathrm{num}(\mathrm{spoly}(f, g))}^{G_i})$ *is a zero polynomial on $S(C_i)$.*

Proof. Since f and g are in G_i, the denominator of $\mathrm{spoly}(f, g)$ is the product of $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$ by Definitions 5 and 6. The leading coefficients of the polynomials in G_i will be nonzero on $S(C_i)$, so that the denominator of $\mathrm{spoly}(f, g)$ will be nonzero on $S(C_i)$. For the same reason, the denominator of $\overline{\mathrm{num}(\mathrm{spoly}(f, g))}^{G_i}$ is also nonzero on $S(C_i)$.

By the definition of parametric partition, we know that for each $u' \in S(C_i)$, $G_i(u', x)$ and $F(u', x)$ generate the same ideal in $K(u')[x]$. By Buchberger's S-polynomial criterion of Gröbner bases [1], we know that for each u' in $S(C_i)$, $G_i(u', x)$ is the Gröbner basis of $I_{F(u',x)}$.

Theorem 3. *For any constrained polynomial set, there is an algorithm to compute out its partitioned-parametric Gröbner basis in finite steps.*

We give the algorithm first.

```
Algorithm: PPGB($C, F$)
Input:  $(C, F)$ is a constrained polynomial set;
Output: A partitioned-parametric Gröbner basis of $(C, F)$.
 1. If $F = \{1\}$ then return $(C, F)$.
 2. Let $(C_1, F_1, ), \ldots, (C_s, F_s)$ be the parametric partition of $(C, F)$.
 3. For each $i$, compute the partitioned-parametric Gröbner basis of $(C_i, F_i)$.
     – SP($F_i$)={$\overline{\text{spoly}(f, g)}^{F_i}$ | for each pair $f, g \in F_i$}.
     – If for each $h$ in SP($F_i$), for each $u' \in S(C_i)$, $h(u', x)$ is 0 as a polynomial
       in $K[u', x]$, then $(C_i, F_i)$ is a partitioned-parametric Gröbner basis of
       $(C_i, F_i)$.
     – Otherwise, compute the partitioned-parametric Gröbner basis of ($C_i$, $F_i$
       $\cup$ SP($F_i$)).
 4. Return the union of the partitioned-parametric Gröbner bases of $(C_i, F_i)$.
```

It should be noticed that the polynomials in SP(F_i) will be in $K(u)[x]$, and their denominators will be nonzero on $S(C_i)$. These polynomials can be replaced by their numerators which are in $K[u, x]$.

Proof. The correctness of the algorithm is guaranteed by Theorem 2. Now we prove that the algorithm terminates in finite steps. It is well known that Buchberger's algorithm for computing Gröbner bases terminates in finite steps and the reason is that during the loop of successive iterations through expanding the original polynomial set with the nonzero remainders of S-polynomials, the leading terms of the ever-increasing polynomial set form an ascending chain of ideals. As for the partitioned-parametric case, it becomes a litter more complicated. On the one hand, it is easy to see that the ascending chain of ideals does also exist for the leading coefficients are certainly nonzero under corresponding constraint. On the other hand, in step 2, $(C_1, F_1), \ldots, (C_s, F_s)$ is the parametric partition of (C, F), and s is a finite number. So the algorithm PPGB forms a tree structure of unambiguous polynomial sets, and the two sides prove that the length of the tree is finite and the node number of the same layer is finite respectively. So the number of leaves, which are unambiguous polynomial sets, is finite too. This proves the termination of the algorithm.

5 Proving Geometric Theorem by Partitioned-Parametric Gröbner Bases

The following theorem can solve the radical ideal membership problem.

Theorem 4 (Radical Ideal Membership). *Let F be a finite set of polynomials in $K[x]$ and g be a polynomial in $K[x]$. Then g is in the radical of the ideal I_F if and only if $\{1\}$ is the reduced Gröbner basis of $(F, gy - 1)$.*

Proof. See [1, 5].

We can extend the above theorem to the case of polynomial ideals involving parameters to establish the following theorem, which can solve the parametric radical ideal membership problem.

Theorem 5 (Parametric Radical Ideal Membership). *Let $h_1, \ldots, h_r, g$ be polynomials in $K[u, x]$, $G=\{(C_1, G_1), \ldots, (C_s, G_s)\}$ be the reduced partitioned-parametric Gröbner basis of the ideal generated by $h_1, \ldots, h_r, gy-1$ under constraint C. Then $\forall u' \in S(C_i)$, $g(u', x)$ is in the radical of the ideal generated by $h_1(u', x)$, …, $h_r(u', x)$ in $K(u')[x]$ if and only if $G_i = \{1\}$.*

Proof. It is obvious according to the definition of partitioned-parametric Gröbner bases and Theorem 4.

Based on the above theorem, we propose the following method to prove geometric theorems mechanically.

For a geometric theorem, hypotheses can be expressed by a set of polynomial equations: $\{h_1 = 0, \ldots, h_r = 0\}$, and the conclusion can be expressed by a polynomial equation: $g = 0$. The polynomials h_i and g are in $K[u, x]$, where the u's are parameters and x's are variables. Generally the conclusion $g = 0$ does not strictly follow from the hypotheses $\{h_1 = 0, \ldots, h_r = 0\}$.

Let $F = \{h_1, \ldots, h_r, gy - 1\}$, for any term order on x and y, and let

$$\{(C_1, G_1), \ldots, (C_r, G_r), (C_{r+1}, G_{r+1}), \ldots, (C_s, G_s)\}$$

be the reduced partitioned-parametric Gröbner basis of I_F. Assume that $G_i = \{1\}$ for $i = 1, \ldots, r$ and $G_i \neq \{1\}$ for $i = r+1, \ldots, s$; then the geometric theorem is true under the constraints $C_1, \ldots, C_r$ and the geometric theorem is false under the constraints $C_{r+1}, \ldots, C_s$.

Consider the following example.

Example 1. The bisectors of the three angles of an arbitrary triangle, three-to-three, intersect at four points. In other words, let the triangle be ΔABC, the two bisectors of $\angle A$ and $\angle B$ intersect at point D. We need to show that CD is the bisector of $\angle C$.

To simplify calculation, and without loss of generality, we take the coordinates of the points as $A(u_1, 0), B(u_2, 0), C(0, u_3), D(x_1, x_2)$. The hypotheses of the theorem are expressed as:

$$h_1 = u_3[x_2^2 - (x_1 - u_1)^2] - 2u_1x_2(x_1 - u_1) = 0 \quad (DA \text{ is the bisector of } \angle CAB)$$
$$h_2 = u_3[x_2^2 - (x_1 - u_2)^2] - 2u_2x_2(x_1 - u_2) = 0 \quad (DB \text{ is the bisector of } \angle ABC)$$

The conclusion to be proved is

$$\begin{aligned} g = {} & [u_1(x_2 - u_3) + u_3x_1][u_3(x_2 - u_3) - u_2x_1] \\ & +[u_2(x_2 - u_3) + u_3x_1][u_3(x_2 - u_3) - u_1x_1] = 0. \end{aligned}$$

Compute the partitioned-parametric Gröbner basis of $\{h_1, h_2, gy - 1\}$ with respect to the graded lex order with tie broken by $y > x_2 > x_1$. Here u_1, u_2, u_3

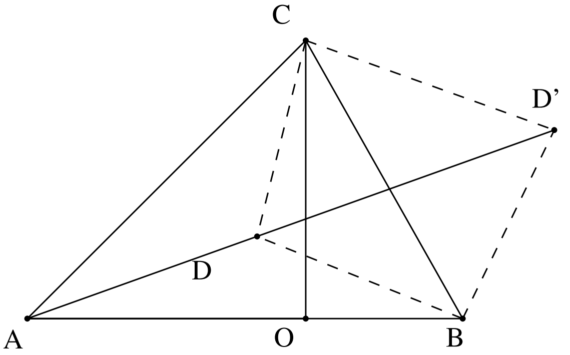

Fig. 1. Three bisectors pass through the same point

are considered as parameters. The partitioned-parametric Gröbner basis is $G = (C_1, G_1), \ldots, (C_7, G_7)$, where

$$
\begin{aligned}
&C_1 = \{u_1 = 0, u_3 = 0\}, \quad G_1 = \{1\};\\
&C_2 = \{-u_2 + u_1 \neq 0, u_3 \neq 0\}, \quad G_2 = \{1\};\\
&C_3 = \{u_3 = 0, -u_2 + u_1 \neq 0, u_1 \neq 0, u_2 \neq 0\}, \quad G_3 = \{1\};\\
&C_4 = \{u_2 = 0, u_3 = 0, u_1 \neq 0\}, \quad G_4 = \{1\};\\
&C_5 = \{u_3^2 + u_1^2 = 0, -u_2 + u_1 = 0, u_3 \neq 0\}, \quad G_5 = \{1\};\\
&C_6 = \{-u_2 + u_1 = 0, u_3 = 0, u_1 \neq 0, u_2 \neq 0\}, \quad G_6 = \{x_1 - u_1, 1 + 2x_2yu_1^3\};\\
&C_7 = \{-u_2 + u_1 = 0, u_3^2 + u_1^2 \neq 0, u_3 \neq 0\},\\
&G_7 = \{u_3x_2^2 - u_3x_1^2 + 2u_3u_1x_1 - u_3u_1^2 - 2u_1x_2x_1 + 2u_1^2x_2,\\
&\qquad 2yu_1u_3^3 + 2yu_3u_1^3 - 2yu_3^3x_1 - 4yu_1x_2u_3^2 - 2u_3x_1yu_1^2 - 4x_2yu_1^3\\
&\qquad + 2yu_3^2x_1x_2 + 2x_1x_2yu_1^2 - 1, 2u_3^5yu_1 + 2u_3^3yu_1^3 - 2u_3^5yx_1 - 2yu_1x_2u_3^4\\
&\qquad - 2yu_1^3x_2u_3^2 + 2x_1yu_3u_1^4 - 4yu_1u_3^3x_1^2 - 4yu_1^3u_3x_1^2 + 2u_3^3yx_1^3\\
&\qquad + 2u_3yx_1^3u_1^2 - u_3^2 - 2u_1^2 - u_3x_2 + 2u_1x_1\}.
\end{aligned}
$$

From this partitioned-parametric Gröbner basis G, one can see that the conclusion $g = 0$ can be deduced from the hypotheses $h_1 = 0, h_2 = 0$ if and only if the free parameters u_1, u_2, u_3 satisfy one of the constraints $C_1, \ldots, C_5$. From

$$C_2 = \{-u_2 + u_1 \neq 0, u_3 \neq 0\}, \quad G_2 = \{1\},$$

we know that the theorem is generically true.

If the variety defined by the hypotheses of a geometric statement is reducible, this method for proving the geometric theorem cannot determine if the conclusion of the geometric statement is true on some components of the hypotheses. For example, when the hypothesis is $x^2 - u^2 = 0$ and the conclusion is $x - u = 0$, the variety defined by $x^2 - u^2 = 0$ is reducible and there are 2 components: one is $x - u = 0$ and the other is $x + u = 0$. We cannot deduce that the conclusion is true on the component $x - u = 0$ by our method.

6 Conclusion

In this paper, for any geometric theorem expressed as an algebraic formulation which involves both parameters and variables, we present a method of partitioned-parametric Gröbner bases to partition the parametric space to finitely many subsets. We can give all the partitions of the parameter space on which the geometric theorem is true.

Our partitioned-parametric Gröbner bases method comes from Kapur's parametric Gröbner bases and has more advantages in the structure and expression. The partitioned-parametric Gröbner bases can be applied for solving many problems about parametric polynomial systems, such as parametric ideal membership, the number of solutions of a parametric polynomial equation system and elimination of quantifier-blocks in algebraically closed fields.

We should thank Z. M. Li for helpful discussions.

References

1. Buchberger, B.: Gröbner Bases: An Algorithmic Method in Polynomial Ideal theorey. In: Multidimensional Systems Theory (N. K. Bose, ed.), D. Reidel Publishing Co., Dordrecht Boston, 184–232 (1985).
2. Chen, X. F., Wang, D. K.: The Projection of Quasi Variety and Its Application on Geometric Theorem Proving and Formula Deduction, In: Automated Deduction in Geometry (F. Winkler, ed.), LNAI **2930**, Springer-Verlag, Berlin Heidelberg, 21–30 (2004).
3. Chou, S.-C.: Mechanical Geometry Theorem Proving. D. Reidel Publishing Co., Dordrecht Boston (1988).
4. Chou, S.-C., Gao, X.-S.: Methods for Mechanical Geometry Formula Deriving. In: Proc. ISSAC '90, ACM Press, New York, 265–270 (1990).
5. Cox, D., Little, J., O'Shea, D.: Ideal, Varieties, and Algorithems. Second Edition, Springer-Verlag, New York (1997).
6. Kapur, D.: Using Gröbner Bases to Reason About Geometry Problems. J. Symbolic Computation **2**(4), 399–408 (1986).
7. Kapur, D.: An Approach for Solving Systems of Parametric Polynomial Equations, In: Principles and Practice of Constraint Programming (Saraswat and Van Hentenryck, eds.), MIT Press, Cambridge (1995).
8. Montes, A.: A New Algorithm for Discussing Gröbner Bases with Parameters. J. Symbolic Computatio **33**(1-2), 183–208 (2002).
9. Weispfenning, V.: Comprehensive Gröbner Bases. J. Symbolic Computation **14**, 1–29 (1991).
10. Winkler, F.: Gröbner Bases in Geometry Theorem Proving and Simplest Degeneracy Conditions. Mathematica Pannonica **1**(1), 15–32 (1990).
11. Wang, D.: Elimination Methods, Springer-Verlag, Wien New York (2001).
12. Wu, W.-T.: Basic Principles of Mechanical Theorem-proving in Elementary Geometries. J. Sys. Sci. & Math. Scis. **4**, 207–235 (1984).