MM Research Preprints, 6–14
MMRC, AMSS, Academia, Sinica, Beijing
No. 21, December 2002

The Projection of Quasi Variety and Its Application on Geometric Theorem Proving

X.F. Chen & D.K. Wang
Institute of Systems Science, AMSS, Academia Sinica, Beijing 100080, P.R. China
(xfchen,dwang)@mmrc.iss.ac.cn

Abstract.

In this paper, we present an algorithm to compute the projection of a quasi variety over an algebraic closed field. Based on the algorithm, we give a method to prove geometric theorem mechanically, and the non-degenerate conditions that we get by the method are proved to be the "weakest", i.e. the geometric theorem is true if and only if these non-degenerate conditions are satisfied. A method for automatic geometric formula deduction is also proposed based on the algorithm. The algorithm given in this paper has been implemented in computer algebra system Maple.

Keywords: quasi variety, projection, non-degenerate condition, mechanical theorem proving

conclusions about certain variables. At last, we give two examples to show how the method works.

2. Non-degenerate Condition and Projection of Quasi Variety

In this paper, all polynomials are in polynomial ring $K[x_1, \cdots x_n]$, where K is a computable field of character 0. E is an algebraic closed extension field of K. For a geometric theorem, after setting up an appropriate coordinate system, the corresponding geometric configuration of hypothesis can be expressed by a finite set of polynomial equations $PS = 0$ i.e. $PS = \{p_1, \cdots, p_s\}, p_1 = 0, \cdots, p_s = 0, p_i \in K[x_1, \cdots, x_n]$. The geometric configuration of the conclusion can be expressed by a polynomial equation $C = 0$, $C \in K[x_1, \cdots, x_n]$. If $PS = 0 \Rightarrow C = 0$, then the theorem $T = (PS, C)$ is called to be universally true. i.e. $\forall x \in E^n$, $p_1(x) = 0, \cdots, p_s(x) = 0 \Rightarrow c(x) = 0$. In most cases, a geometric theorem is not universally true. It is true only if the non-degenerate condition is satisfied. $g \neq 0$ is called the non-degenerate condition if

$$(1)(\forall x \in K^n)(p_1(x) = \cdots = p_s(x) = 0 \wedge g(x) \neq 0 \Rightarrow c(x) = 0)$$
$$(2)(\exists x \in K^n)(p_1(x) = \cdots = p_s(x) = 0 \wedge g(x) \neq 0)$$

From the above definition, we can see that the non-degenerate condition is a sufficient condition for a geometric theorem to be true.

Wu's non-degenerate condition In Wu's method, the non-degenerate condition is defined as the product of the initials of the characteristic set not equal to zero. Suppose $CS : C_1, \cdots, C_m$ is the characteristic set of PS, $J = \prod_i I_i$ where I_i is the initial of C_i. If the pseudo-remainder of the conclusion polynomial C w.r.t the characteristic set CS is 0, i.e. there are non-negative integers s_i such that $I_1^{s_1} \cdots I_m^{s_m} C = Q_1 C_1 + \cdots + Q_m C_m + 0$, then $J \neq 0$ is the non-degenerate condition for the theorem to be true.

Kapur's non-degenerate condition Let G_1, G_2 be the Grobner basis of ideal (PS) and $(PS \cup \{Cz - 1\})$. if $G_1 \neq \{1\}$ and $G_2 \neq \{1\}$, then the theorem is true when $g_i \neq 0$. If g_i satisfy

(a)$g_i \in G_2 \cap K[x] \wedge g_i \notin (PS)$

(b)$1 \notin \text{GrobnerBasis}(PS \cup \{g_i z - 1\})$

$g_i \neq 0$ is the non-degenerate condition.

Winkler's non-degenerate condition Winkler has proved that all polynomials satisfying (1) constitute an ideal, and among the polynomials in the Grobner basis of the ideal which satisfies (2), there is a polynomial g which has the least leading term, $g \neq 0$ is the simplest non-degenerate condition.

All the non-degenerate conditions mentioned above, are sufficient conditions for a geometric theorem to be true.

To eliminate variables $x_{m+1}, \cdots, x_n$, the map projection is

$$Proj_{x_{m+1}, \cdots, x_n} : E^n \to E^m$$

which sends $(a_1, \cdots, a_n)$ to $(a_1, \cdots, a_m)$. If V is an affine variety in E^n, $Proj_{x_{m+1}, \cdots, x_n}(V)$ may not be a variety in E^m,but it is contained in a variety in E^n.

PS is a finite set of polynomials and D is a polynomial in $K[x_1, \cdots, x_n]$. Let $Zero(PS) \subset E^n$ denote all the common solutions to the polynomials in PS, define $Zero(PS/D)$ as

$$Zero(PS/D) = Zero(PS)/Zero(D)$$

For a polynomial set PS and a polynomial D , we apply projection $Proj_{x_{m+1},\cdots,x_n}$ to $Zero(PS/D)$. Then we have

$$Proj_{x_{m+1},\cdots,x_n} Zero(PS/D) = \{e \in E^m \mid \exists a \in E^{(n-m)} s.t.(e, a) \in Zero(PS/D)\}$$

when $m = 0$, we define $Proj_{x_1,\cdots,x_n} Zero(PS/D) = true$, if $Zero(PS/D) \neq \emptyset$; and $false$ otherwise.

For any finite number of polynomial sets PS_i and polynomials G_i in $K[x_1, \cdots, x_n]$, the set

$$\cup_i \ Zero(PS_i/G_i)$$

is called a quasi variety.

The projection of a quasi variety in E^n to E^m is a quasi variety in E^m. Please see[7] for the details. The projection of a quasi variety has been investigated by Wu[7],Wang[8] and Gao[10].

3. Algorithm to Compute Projection of Quasi Variety

In Wu[7], a method for computing the projection of a quasi variety is given. Before giving a new algorithm, we will give several theorems which are needed for constructing the new algorithm.

Theorem 3.1 Let PS be a polynomial set and D a polynomial , there is an algorithm to decompose PS into a finite set of ascending set AS_i such that

$$Zero(PS/D) = \bigcup_i Zero(AS_i/J_iD)$$

where each AS_i is an ascending set, J_i is the production of the initials of the polynomials in AS_i.

The proof and the algorithm can be found in Wu [1]. In [9], an improved algorithm has been given to decompose a polynomial set into a series of ascending sets.

Lemma 3.2 If $Zero(PS/D) = \bigcup_i Zero(AS_i/J_iD)$, then we have

$$Proj_{x_{m+1},\cdots,x_n} Zero(PS/D) = \bigcup_i Proj_{x_{m+1},\cdots,x_n} Zero(AS_i/J_iD)$$

Proof: It is enough to prove
$Proj_{x_{m+1},\cdots,x_n} \bigcup_i Zero(AS_i/J_iD) = \bigcup_i Proj_{x_{m+1},\cdots,x_n} Zero(AS_i/J_iD)$.
Take any element $a = (a_1, \cdots, a_m) \in E^m$ from $Proj_{x_{m+1},\cdots,x_n} \bigcup_i Zero(AS_i/J_iD)$, then there exists $a' = (a_{m+1}, \cdots, a_n) \in E^{(n-m)}$ such that $(a_1, \cdots, a_n) \in \cup_i Zero(AS_i/J_iD)$, then there exists a i such that $(a_1, \cdots, a_n) \in Zero(AS_i/J_i)$. According to the definition of projection, $(a_1, \cdots, a_m) \in Proj_{x_{m+1},\cdots,x_n} Zero(AS_i/J_i)$, it follows that a

Lemma 3.3 $AS : A_1, \cdots A_s$ is an ascending set w.r.t. variable ordering ($x_1 < x_2 < \cdots < x_n$), $AS' = A_1, \cdots, A_{s-1}$, J' is the product of the initials of polynomials in AS'. I_s is the initial of A_s. $d = degree(A_s, x_n)$, $R = Prem(D^d, A_s, x_n)$.

(1) if $degree(A_s, x_n) \neq 0$, $degree(D, x_n) \neq 0$ then

$$Proj_{x_{m+1},\cdots,x_n} Zero(AS/JD) = Proj_{x_{m+1},\cdots,x_n} Zero(AS'/J'(I_s R))$$

(2) if $degree(A_s, x_n) \neq 0$, $degree(D, x_n) = 0$ then

$$Proj_{x_{m+1},\cdots,x_n} Zero(AS/JD) = Proj_{x_{m+1},\cdots,x_{n-1}} Zero(AS'/J'(I_s D))$$

(3) if $degree(A_s, x_n) = 0$, $degree(D, x_n) \neq 0$ Let $D = \sum_{i=0} D_i x_n^i$, $D_i \in K[x_1, \cdots, x_{n-1}]$, then

$$Proj_{x_{m+1},\cdots,x_n} Zero(AS/JD) = \bigcup_i Proj_{x_{m+1},\cdots,x_{n-1}} Zero(AS'/J'(I_s D_i))$$

(4)If $degree(A_s, x_n) = 0$, $degree(D, x_n) = 0$, then

$$Proj_{x_{m+1},\cdots,x_n} Zero(AS/JD) = Proj_{x_{m+1},\cdots,x_{n-1}} Zero(AS/JD))$$

Proof (1)(2)(4) are obviously according to the definition of projection and the fundamental theorem of algebra. For (3), please see [7] for details.

According to the lemmas given above, we can eliminate one variable. All the variables which will be eliminated can be eliminated successively if we compute it recursively.

PS is a polynomial set in $K[x_1, \cdots, x_n]$. D is a polynomial in $K[x_1, \cdots, x_n]$. If we want to compute $Proj_{x_1,\cdots,x_n} Zero(PS/D)$. The computing process can be divided into two steps. The variable ordering should be $x_n > \cdots > x_{m+1} > x_m > \cdots > x_1$. Under this variable ordering, first we will decompose the polynomial set PS into a series of ascending sets AS_i such that $Zero(PS/D) = \bigcup_i Zero(AS_i/J_i D)$. Each AS_i is an ascending set for the variable ordering $x_n > \cdots > x_{m+1} > x_m > \cdots > x_1$. Then for each $Zero(AS_i/J_i D)$ we can compute its projection. In the following, we will give the algorithms in detail.

step 1. Decompose polynomial set PS into a series of ascending sets AS_i such that

$$Zero(PS/D) = \bigcup_i Zero(AS_i/J_i D)$$

where J_i is the product of the initials of the polynomials in AS_i

Please see [9] for the detail of the algorithm.

step 2. Compute the projection of $Zero(AS/JD)$, AS is an ascending set. J is the product of the initials of the polynomials in AS,D is a polynomial.

ProjectAS(AS, J, D, X, Y)
Input:
AS: an ascending set w.r.t X
D: a polynomial
J: the product of the initials of the polynomials in AS
X: $X := [x_n, \cdots, x_1]$ a variable list, $x_n > \cdots, x_1$
Y: $Y := [x_n, \cdots, x_m]$ a list of variables which will be eliminated

Output:
a list, its element has the form (as, d), as is an ascending set and d is a polynomial.

ProjectAS(AS, J, D, X, Y)
beginproc
y=First(Y), A=Last(AS)
Y'=Y/y, AS'=AS/A
if Y = [] then
result:= $(AS, J * D)$
if $degree(A, y) = 0$ and $degree(D, y) = 0$ then
result:= ProjectAS(AS, J, D, X, Y')
else if $degree(A, y) \neq 0$ and $degree(D, Y) = 0$ then
result:= ProjectAS($AS', J', I * D, X, Y'$)
else if $degree(A, y) = 0$ and $degree(D, y) \neq 0$ then
result:=[];
cf:=coeffs(D,y);
for each c in cf do {
result:= result union ProjectAS(AS,J,c,X,Y') }
else if $degree(A, y) \neq 0$ and $degree(D, y) \neq 0$ then
d:=degree(A,y)
$R := Prem(D^d, A, y)$
result:= ProjectAS($AS', J', I * R, X, Y$)
end if
return result
endproc

In the above algorithm, Y' is a list formed by removing the first element y from the list Y. AS' is a list formed by removing the last element A from the list AS. I is the initial of A. $coeffs(D, y)$ return a list composed of all the coefficients of the polynomial D w.r.t variable y. $Prem(D^d, A, y)$ return the pseudo-remainder of D^d to A w.r.t variable y.

4. Application on geometry theorem proving and formula deduction

Let $K = Q$ be the rational number field. $E = C$ be the complex number field. The corresponding geometric configuration of hypothesis is expressed by a finite set of polynomial equations $PS = 0$ i.e. $PS = \{p_1, \cdots, p_s\}, p_1 = 0, \cdots, p_s = 0, p_i \in Q[x_1, \cdots, x_n]$. The geometric configuration of the conclusion is expressed by a polynomial equation $C = 0 .i.e. . c = 0, c \in Q[x_1, \cdots, x_n]$. We will divide the the variables $x_1, \cdots, x_n$ into two parts $x_1, \cdots, x_m$ and $x_{m+1} \cdots, x_n$. Applying $Proj_{x_{m+1}, \cdots, x_n}$ to the quasi variety $Zero(PS/C)$, the following theorem determines that a geometric theorem is universally true or not. If not, a series of polynomial equations and inequations about the variables $x_1, \cdots, x_m$ are given(i.e. $Proj_{x_{m+1}, \cdots, x_n} Zero(PS/C)$) , which is the sufficient and necessary condition for the theorem to be false.

Theorem 4.1 For polynomial set PS and polynomial C as shown above, then

(1) if $Proj_{x_{m+1}, \cdots, x_n} Zero(PS/C) = \emptyset$ and $Proj_{x_{m+1}, \cdots, x_n} Zero(PS/D) \neq \emptyset$, then the theorem

T is universally true.

(2) if $Proj_{x_{m+1},\cdots,x_n} Zero(PS/C) \neq \emptyset$, $\forall(a_1,\cdots,a_m) \in Proj_{x_{m+1},\cdots,x_n} Zero(PS/C)$, then there is $(a_{m+1},\cdots,a_n)$ such that $PS(a_1,\cdots,a_n) = 0$ and $C(a_1,\cdots,a_n) = 0$

If there is $(a_1,\cdots,a_n)$ such that $PS(a_1,\cdots,a_n) = 0$ and $C(a_1,\cdots,a_n) \neq 0$, then $(a_1,\cdots,a_m) \in Proj_{x_{m+1},\cdots,x_n} Zero(PS/C)$, so that $Proj_{x_{m+1},\cdots,x_n} Zero(PS/C)$ is not empty.

Proof
(1)We claim that $Proj_{x_{m+1},\cdots,x_n} Zero(PS/C) = \emptyset \Leftrightarrow Zero(PS/C) = \emptyset$ It is obviously by the definition of projection. Since $Proj_{x_{m+1},\cdots,x_n} Zero(PS/C) = \emptyset$, it follows that $Zero(PS/C) = \emptyset$, i.e. $Zero(PS) \subseteq Zero(C)$ i.e. $\forall a = (a_1,\cdots,a_n) \in E^n$, $p_1(a) = 0,\cdots,p_s(a) = 0 \Rightarrow c(a) = 0$ so that theorem $T = (PS, C)$ is universally true.
(2) It is obviously by the definition of projection.

Based on the above theorem, we can prove geometric theorem mechanically and give the non-degenerate conditions automatically by computing the projection of a quasi variety .

It's obvious to see that we can predetermine the variables occurring in non-degenerate conditions. So it's convenient for us to observe the range of possible value for any variables. As a rule, we will eliminate all the dependent variables .

Moreover, we can be certain that the conditions found through this method are the weakest compared to the condition obtained by Wu's method and the others based on Grobner basis such as Kapur's and Winkler's approach.

Now we consider the application of projection method on formula deduction.

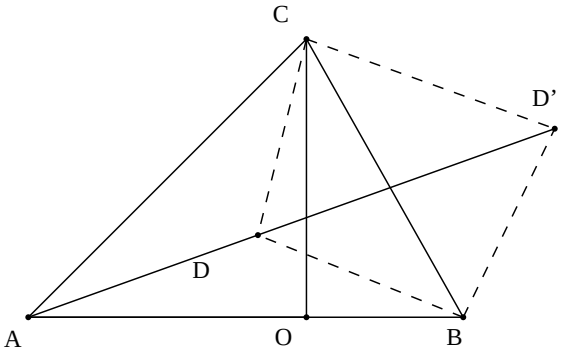
Theorem 4.2 The hypothesis of a geometric statement is expressed by a set of polynomial equations $PS = 0$, then $Proj_{x_{m+1},\cdots,x_n} Zero(PS)$ gives a series of polynomial equations and inequations which involve the variables $x_1,\cdots,x_m$ only.

While deducing the unknown geometric formula by the projection method, all the variables which do not occur in the final formula will be eliminated.

5. Examples

In this section, we will give two examples to show that how the projection method is applied to automatic theorem proving and formula deduction. The first example is taken from Wang [8]. We will prove it by computing the projection of quasi variety and give the non-degenerate conditions and compared the result with Wu's method. The second example is to derive the geometric formula automatically from the given hypothesis.

Example 1
The bisectors of the three angles of an arbitrary triangle,three-to-three, intersect at four points. 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 $\angle C$.



We take the coordinates of the points as $A(x_1, 0), B(x_2, 0), C(0, x_3), D(x_4, x_5)$.
The hypothesis of the theorem consists of the following relations.
$H_1 = x_3[x_5^2 - (x_4 - x_1)^2] - 2x_1x_5(x_4 - x_1) = 0$ (DA is the bisector of $\angle$ CAB)
$H_2 = x_3[x_5^2 - (x_4 - x_2)^2] - 2x_2x_5(x_4 - x_2) = 0$ (DB is the bisector of $\angle$ ABC)

The conclusion to be proved is $C = 0$
$C = [x_1(x_5 - x_3) + x_3x_4][x_3(x_5 - x_3) - x_2x_4] + [x_2(x_5 - x_3) + x_3x_4][x_3(x_5 - x_3) - x_1x_4]$

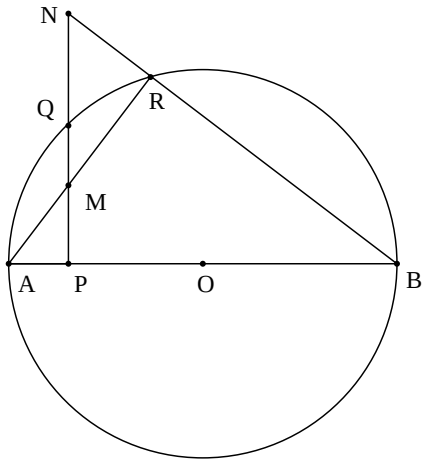
The characteristic set of $\{H_1, H_2\}$ is $CS : [C_1, C_2]$
$C_1 = x_3^3(x_1 - x_2)x_4^4 + lowerterms$
$C_2 = x_3(x_1 - x_2)(x_1 + x_2 - x_4)x_5 + lowerterms$
The pseudo-remainder of the conclusion polynomial C w.r.t the characteristic set CS is 0. The theorem is true under the non-degenerate conditions which are $x_3 \neq 0$,$x_1 \neq x_2$, and $x_1 + x_2 - x_4 \neq 0$ in Wu's sense.

There are three degenerate cases. They are:
Case 1 $x_1 = x_2$. In this case, A and B are coincide, then ABC is not a real triangle anymore.
Case 2: $x_3 = 0$. In this case, C is on the line AB, the ABC is not a real triangle also.
Case 3:$x_1 + x_2 - x_4 = 0$. In this case, the intersection point of the bisectors is on line $x = x_1 + x_2$. In Wu's method, we can't determine the theorem is true or not at this time. If we want to know if the theorem is still true, we should put the polynomial $P = x_1 + x_2 - x_4$ to the original polynomial set $\{H_1, H_2\}$ to form a new polynomial set $\{H_1, H_2, P\}$, compute its characteristic set again , and decide the theorem is true or not under the condition $x_1 + x_2 - x_4 = 0$.

Now we will prove the theorem and give the non-degenerate conditions by computing the projection of the quasi variety. In this example, x_1, x_2, x_3 are the free variables and x_4, x_5 are the dependent variables. We compute the projection of $Zero(\{H_1, H_2\}/C)$ to eliminate the variables x_4, x_5. $Projection_{x_4,x_5} Zero(\{H_1, H_2\}/C) = Zero(\{-x_2 + x_1\}/\{x_3, x_1^2 + x_3^2\}) \bigcup Zero(\{-x_2 + x_1, x_3\}/\{x_1\})$
There are only two degenerate cases. They are
Case 1: $x_2 = x_1$, $x_3 \neq 0$. A is coincidence with B, and C is not on the line $y = 0$.
Case 2: $x_1 = x_2$ and $x_3 = 0$ and $x_1 \neq 0$, A is coincide with B,but A is not coincide with C.
This theorem is false only under these two degenerate cases and it is always true except these two degenerate cases.

Example 2.
Let R be a point on the circle with diameter AB. At a point P(not A or B) of AB a

perpendicular is drawn meeting BR at N, AR at M,the circle at Q, Find the relation among PQ,PM and PN.



First, take the coordinate of the points as $O = (0,0), A = (x_1,0), B = (x_2,0), P = (x_3,0), R = (x_4,x_5), M = (x_3,y_1), Q = (x_3,y_2), N = (x_3,y_3)$ The hypothesis is expressed as following polynomial equations.

$H_1 = x_1 + x_2$	$(AB\ is\ diameter)$
$H_2 = x_1^2 - x_5^2 - x_4^2$	$(\|AO\| = \|RO\|)$
$H_3 = -y_3(x_4 - x_3) - (x_5 - y_3)(x_2 - x_3)$	$(N, R, B\ are\ collinear)$
$H_4 = x_5(x_3 - x_1) - y_1(x_4 - x_1)$	$(A, M, R\ are\ collinear)$
$H_5 = x_1^2 - y_2^2 - x_3^2$	$(\|AO\| = \|QO\|)$

Since we want to derive formula about PQ,PM and PN, it is a formula about the variables about y_3, y_2, y_1. Since $P \neq A$, $P \neq B$ and $A \neq O$, let $D = \{x3 - x1, x3 - x2, x1\}$ in advance. We can eliminate the variables x_5, x_4, x_3, x_2, x_1 by computing the projection of $Zero(\{H_1, H_2, H_3, H_4, H_5\}/D)$.
$Proj_{x_5,x_4,x_3,x_2,x_1} Zero(\{H_1, H_2, H_3, H_4, H_5\}/D)$
$= Zero(\{y_3y_1 - y_2^2\}/\{y_2\}) \cup Zero(\{y_1\}/\{y_2\}) \cup Zero(\{y_3\}/\{y_2\})$

Case 1: $y_3y_1 - y_2^2 = 0$, $y_2 \neq 0$ i.e. When R doesn't coincide with A or B, we have $|PN| * |PM| = |PQ|^2$.
Case 2: $y_1 = 0$,$y_2 \neq 0$ i.e. R coincides with B
Case 3: $y_3 = 0$,$y_2 \neq 0$ i.e. R coincides with A

6. Conclusion

We give an algorithm to compute the projection over an algebraic closed field. Applying this algorithm to automatic theorem proving, we can get the weakest non-degenerate condition for which the theorem is true. In fact, we can get the sufficient and necessary condition for a geometric theorem to be false by computing the projection of a quasi variety. This algorithm also can be applied to automatic geometric formula deduction. There are more

than one hundred geometric theorems which have been proved by this method. Experiments show that the projection of the quasi variety can be computed out if we can get the zero decomposition for the given polynomial system.

References

[1] Wu Wen-tsun, Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J.Sys.Sci. & Math. Scis.,* 4(1984), 207-235.

[2] Shang-Ching Chou, Mechanical geometry theorem proving. D. Reidel, Dordrecht, Boston.

[3] D.Kapur."Using Grobner bases to reason about geometry problems". *Journal of Symbolic Computation*,2(4),399-408,(1986).

[4] Kutzler,B.,Stifter,S. "On the application of Buchberger's algorithm to automatic Geometry theorem Proving.*Journal of Symbolic Computation*,2(4),389-397,(1986).

[5] Chou,S.C.,Schelter,W.F."Automated Geometry Theorem Proving Using Rewrite Rules". Dept of Mathematics, University of Texas, Austin.(1985).

[6] Franz Winkler."Automated Theorem Proving in Nonlinear Geometry", *Advances in Computing Research*, Volume 6, 138-197.(1992).

[7] Wu Wen-tsun, On a Projection Theorem of Quasi-Varieties in Elimination Theory,*MM Research Preprints*, No.4, Ins. of Systems Science, Academia Sinica.

[8] Dongming Wang, Elimination method, Springer 2001.

[9] Dingkang Wang, Zero Decomposition Algorithms for System of Polynomial Equations, Computer Mathematics, P67-70, 2000, World Scientific

[10] X.S.Gao & S.C.Chou, Solving Parametric Algebraic Systems, Proc. of ISSAC'92, 335-341,1992.