SOFTWARE DEVELOPMENT IN MMRC

Dingkang WANG & Lihong ZHI
Institute of Systems Science, Academia Sinica
Beijing 100080,P.R. China
(dwang@mmrc.iss.ac.cn lzhi@mmrc.iss.ac.cn)

Abstract

In this paper, we report three packages CSET, SACCS, WSOLVE and one system GPROVE. CSET and SACCS are packages implement characteristic set method. WSOLVE is a package for solving systems of polynomial equations. GPROVE is a system for geometric theorems mechanical proving.

1. Introduction

The characteristic set method which considers the zero structure of polynomial sets was first introduced by J.F.Ritt (see [RITT]) and revived by Wu Wentsun (see [WU1,page 159-172]). Many improvements and modifications of this method have been made since 1978. This method is successfully used in many areas such as mechanical theorem proving in geometries (see [WU2 page 207-235] or [CHOU]), computer aided geometry design(CAGD) (see [WU3, page 1-11]), nonlinear programming (see [WU4 page 1-19]), solving Stewart platform equations (see [W-H, page 181-189]), solving Yang-Baxter equation (see [SHI page 79-89]), etc.

Developing more efficient and practical algorithms for people interested in characteristic set method and its application is very important. CSET and SACCS are provided for this purpose. CSET is written in Maple, SACCS is written in C language by means of the basic subroutines in SACLIB(a library of C programs for computer algebra). These two packages all include algorithms for computing characteristic set of any polynomial set, decomposing polynomial set into ascending sets and irreducible ascending sets, decomposing algebraic varieties into irreducible components, factorizing polynomial over algebraic extension fields and solving system of polynomial equations.

Geometric theorem proving and polynomial equations solving are two main applications of the characteristic set method. GPROVE is a geometric theorem prover, which can be used for proving theorems in Euclidean geometry , non-Euclidean geometry and projective geometry. For a geometric statement of constructive type,

the prover can decide whether the statement is true, at the same time generate the figure and the non-degenerate conditions in geometric form of the statements automatically. It is programmed in C and implemented on Sun SPARC station. WSOLVE is designed specially for solving system of nonlinear algebraic equations, written in Maple.

2. Preliminaries

Let $K[x_1, x_2, \cdots, x_n]$ denote the ring of polynomials in indeterminates $x_1, x_2, \cdots, x_n$ with coefficients in a field K of characteristic 0. Consider a fixed ordering on the set of indeterminates: $x_1 < x_2 < \cdots < x_n$ Let $f \in K[x_1, x_2, \cdots, x_n]$, if f is not a constant, $class(f)$ is the greatest i such that x_i occurs in f, otherwise $class(f) = 0$.

Definition 1. Given two polynomials $f_1, f_2 \in K[x_1, x_2, \cdots, x_n]$, we say f_1 is reduced with respect to f_2. if $deg_{x_c}(f_1) < deg_{x_c}(f_2)$, $c = class(f_2)$.

Definition 2. A sequence of polynomials $AS = \{f_1, f_2, \cdots, f_r\}$ is called an *ascending set* if $r = 1$ and f_1 is not identically zero, or $r > 1$ and $0 < class(f_1) < class(f_2) < \cdots < class(f_r) \leq n$ and each f_i is reduced with respect to the preceding $f_j (1 \leq j < i)$.

Definition 3. Consider an ascending set $AS = \{f_1, \cdots, f_r\}$, $f_i \in K[x_1, \cdots, x_n]$, and a polynomial $g \in K[x_1, \cdots, x_n]$. Let's pseudo-divide g by $f_r, \cdots, f_1$ consider successively as polynomials in $x_{c_r}, \cdots, x_{c_1}$, $c_i = class(f_i)$, and denote the final remainder by R. Then we shall get an expression of the form:

$$I_1^{s_1} \cdots I_r^{s_r} g = \sum_{i=1}^{r} Q_i f_i + R$$

where I_i is the initial of f_i, s_i assumes the smallest possible power achievable. R is called the *pseudo-remainder* of g with respect to AS, denoted as $R = Prem(g, AS)$.

Definition 4 An ascending set CS is called a *characteristic set* of polynomial set PS if CS is contained in the ideal generated by the polynomials in PS and $Prem(f, CS) = 0$ for all f in PS .

3. CSET and SACCS

CSET and SACCS are two packages implement the characteristic set method. The basic structure of algorithms in CSET and SACCS are almost the same. For explicity and convenience, we only describe briefly the algorithms in SACCS and prove the truth of each algorithm. Some techniques are also discussed.

3.1 Description of algorithms

SACCS consists of six main algorithms.Each algorithm implements a function of characteristic method.

3.1.1 Charset

This algorithm computes a characteristic set of any polynomial set.

Well-Ordering Principle: There is an algorithm which permits to determine for any polynomial set PS in a finite number of steps characteristic set CS that satisfies

$Zero(CS/J) \subset Zero(PS) \subset Zero(CS)$

J is the product of initials of polynomial in CS.(see [WU5,page103])

3.1.2 Charser

Programmed here is a function for decomposing any polynomial set into a finite sequence of ascending sets.

Zero-Decomposition theorem D1 : For any polynomial set PS, we shall have the following decomposition in a finite number of steps:

$Zero(PS) = \bigcup_{i=1}^{n} Zero(CS_i/J_i)$

in which each CS_i is ascending set and J_i is the product of all initials of polynomials in CS_i.(see [WU5,page 103])

3.1.3 IRRcharser

This routine computes the decomposition of a polynomial set into a sequence of irreducible ascending sets.

Zero-Decomposition theorem D2: For any polynomial set PS, the following decomposition will be finished in a finite number of steps:

$Zero(PS) = \bigcup_{i=1}^{n} Zero(IRRCS_i/J_i)$

where $IRRCS_i$ is irreducible ascending set and J_i is the product of all initials of polynomials in $IRRCS_i$. (see [WU6,page 11])

3.1.4 IRRvariety

This algorithm decomposes the algebraic variety defined by a polynomial set PS into a sequence of irredundant and irreducible algebraic varieties defined by polynomial set VS_i.

Zero-Decomposition theorem D3: For any polynomial set PS, we can finish in a finite number of steps the zero decomposition:

$Zero(PS) = \bigcup_{i=1}^{n} IRRvar(VSi)$ (see [WU6,page 11])

3.1.5 Pfactor

Pfactor computes the irreducible factorization of a polynomial F over any algebraic extension fields defined by an irreducible ascending set or any polynomial set. It combines modular technique with characteristic method so that improves dramatically the efficiency of the algorithm for factorization. (see [ZHI,page 77-84]).

3.1.6 Psolve

According to Decomposition theorem D1 we have

$Zero(PS) = \bigcup_{i=1}^{n} Zero(CS_i/J_i)$

where CS_i are all of triangular form . We can get the corresponding zero set of an arbitrary system of polynomial equations by solving successively for the leading variables in turn. Psolve use this technique to solve the polynomial equations.

3.2 Some techniques for improving speed

We adopted several strategies in the design and implementation of CSET and SACCS.

3.2.1 Optimization of variable ordering

The efficiency of all the algorithms in SACCS and CSET depends heavily upon the choice of variable ordering. For example

$$PS = \left\{ \begin{array}{l} (4-5x_1+4x_4)^2+4(-5x_1-2x_3)^2-8x_1^2, \\ (2+x_1+4x_4)^2+(4-8x_1-6x_3)^2-16x_1^2, \\ 4x_2^2-4x_1x_2-11x_1^2, \\ 4x_3^2+4x_2^2+4x_1x_2-15x_1^2-4x_1-8x_2+4 \end{array} \right\}$$

$Charset(PS,[x_1,x_2,x_3,x_4])$ Time: 0.21 seconds.

$Charset(PS,[x_2,x_3,x_4,x_1])$ Time: 245.73 seconds.

So it is important to select an optimal variable ordering. In our implementation, if the variable ordering is not given, we choose a heuristic variable ordering according to some laws which abstracted from practical experience. We purpose to pay more attention to this problem in the future.

3.2.2 Controlling the expansion of polynomials

The size of polynomials includes the terms and coefficients may grow quickly while using the characteristic method. (see [WU1,page 104]) Sometimes the number of terms increase to thousands and thousands. Several strategies are given by Wu Wentsun and others.

Wu introduce the concepts of quasi and weak ascending set. (see [WU7,page6]) $CS = \{f_1, f_2, ..., f_n\}$ is a *quasi-ascending set* if either $n = 1$ and $f_i \neq 0$, or $r > 1$ and $class(f_1) \prec class(f_2) \prec \cdots \prec class(f_n)$. A quasi-ascending set is called a *weak-ascending set* if the initial of f_j is reduced with respect to f_i for all $j \geq i$ .In (see [C-G,page 6]) S.C.Chou and X.S.Gao also define the weak ascending set and weak prem. We implemented four options for user to choose.

Polynomial factorization is also an effective tool to control the expansion of polynomial.

During the computation of pseudo-remainder, Some undesirable redundant factors will appear according to the theory of Collins (see [COL page 128-142]). We adopted Linear Equations Method (see [WU5,page 101-110]) to avoid partially the redundant factors.

3.2.3 Removing redundant branches

Because of the recursive property of characteristic method, the number of branches maybe hundreds or even thousands. Some of these branches are redundant so must be cut off.

The following theorem provides a trick to remove the redundant branches (see [C-G1,page 207-220])

Theorem : Let AS_1 and AS_2 be two ascending set. AS_1 is irreducible, if the remainder set of AS_2 with respect to AS_1 is empty and the remainder of J_2 is non-zero, then $Zero(AS_1/J_1) \subset Zero(AS_2/J_2)$, where J_1, J_2 are respectively the product of initials of the polynomials in AS_1 and AS_2, so that AS_1 can be removed.

There are many techniques , we refer to (see [DMW] and [C-G2,page 1-19]).

4. GPROVE

GPROVE is a geometric theorems prover. It is based on Xlib and written in C language. It consists of a main window and two sub-windows. One sub-window is the proving sub-window, the other one is the graphics sub-window. The geometric theorem will be input in natural language, such as English, in the main window. When you press the prove item in the main menu, the proving detail will be shown in the proving sub-window.The users also can use mouse to draw the diagram according to the geometric statements in the graphics sub-window. The user also can move certain points in a diagram smoothly to change the shape and position of diagram to see if it is true when the free points are moved.

There are three main steps to prove the geometric statement in GPROVE. First, the geometric statement will be translated into a normal form so that it can be represented by polynomial equations. The hypotheses will be represented by polynomial equations $PS = 0$ while the conclusion statement will be described by $G = 0$. Second, the characteristic set CS of PS can be got in finite steps according to the Well Ordering Principle. Finally, the pseudo-remainder of polynomial G with respect to the characteristic set CS will be computed, if the pseudo-remainder is zero, then the geometric theorem is generic true.

An example is given to show the proving details.

1. The theorem can be loaded from a file or typed directly in the main window.

```
 The input to the prover:

Example Pappus. Let A, B, and C be three points on a line;
and A1, B1,
and C1, be three points on another line.
  P is the intersection of
line AB1 and line A1B.
 Q is the intersection of lines AC1 and CA1. R
is the intersection of lines BC1 and CB1.
```

```
 Show that P, Q, and R are
collinear.
```

2.The constructive description of the geometry statement will be given.

```
EXAMPLE Pappus
HYPOTHESES:                    HYPOTHESES:
POINT A B A1 B1;                   ;A,B,A1,B1 are free points
ON-LINE C A B;                     ;C,A,B are on the same line
ON-LINE C1 A1 B1;                  ;C1,A1,B1 are on the same line
INTERSECTION-LL P A B1 A1 B;       ;P is the intersection of line AC1 and CA1
INTERSECTION-LL Q A C1 C A1;       ;Q is the intersection of line BC1 and CB1
INTERSECTION-LL R B C1 C B1;       ;R is the in
CONCLUSION:                    CONCLUSION:
COLLINEAR P Q R.                   ;P,R,Q are collinear
```

3. The predicate form of the geometry statement and the non-degenerate conditions will be given.

```
The  HYPOTHESES:               HYPOTHESES
COLL C A B.                         ;C, A and B are collinear
COLL C1 A1 B1.                      ;C1, A1 and B1 are collinear
COLL P A B1.                        ;P, A and B1 are collinear
COLL P A1 B.                        ;P, A1 and B are collinear
COLL Q A C1.                        ;Q, A and C1 are collinear
COLL Q C A1.                        ;Q, C and A1 are collinear
COLL R B C1.                        ;R, B and C1 are collinear
COLL R C B1.                        ;R, C and B1 are collinear
THE CONCLUSION:                CONCLUSION:
COLL P Q R.                         ;P, Q and R are collinear
```

The non-degenerate conditions:

```
LINE AB IS NON-ISOTROPIC.
LINE A1B1 IS NON-ISOTROPIC.
AB1 DOES NOT PARALLEL TO A1B.
AC1 DOES NOT PARALLEL TO CA1.
BC1 DOES NOT PARALLEL TO CB1.
```

4. The coordinates of the points will be given and the geometry statement will be represented by polynomial equations.

```
A: (0 0)   B: (x1 0)  A1: (x2 x3) B1: (x4 x5)
C: (x6 x7) C1: (x8 x9) P: (x10 x11) Q: (x12 x13)
R: (x14 x15)

THE HYPOTHESES:
x1x7 = 0                                ;C, A and B are collinear
(x4-x2)x9+(-x5+x3)x8+x2x5-x3x4 = 0      ;C1, A1 and B1 are collinear
x4x11-x5x10 = 0                         ;P, A and B1 are collinear
(-x2+x1)x11+x3x10-x1x3 = 0              ;P, A1 and B are collinear
x8x13-x9x12 = 0                         ;Q, A and C1 are collinear
(-x6+x2)x13+(x7-x3)x12-x2x7+x3x6 = 0    ;Q, C and A1 are collinear
(x8-x1)x15-x9x14+x1x9 = 0               ;R, B and C1 are collinear
(-x6+x4)x15+(x7-x5)x14-x4x7+x5x6 = 0    ;R, C and B1 are collinear

THE CONCLUSION:
 CONC =                                 ;P, Q and R are collinear
(x12-x10)x15+(-x13+x11)x14+x10x13-x11x12 = 0
```

5. According to the Well-Ordering Principle, the characteristic set TS of the hypotheses polynomial system will be computed.

```
 TS =
(-x6+x4)x15+(x7-x5)x14-x4x7+x5x6 = 0
((x6-x4)x9+(-x7+x5)x8+x1x7-x1x5)x14+(-x1x6+x1x4)x9+(x4x7-x5x6)x8
          -x1x4x7+x1x5x6 = 0
x8x13-x9x12 = 0
((-x6+x2)x9+(x7-x3)x8)x12+(-x2x7+x3x6)x8 = 0
x4x11-x5x10 = 0
((-x2+x1)x5+x3x4)x10-x1x3x4 = 0
(x4-x2)x9+(-x5+x3)x8+x2x5-x3x4 = 0
x7 = 0
```

6. The successive pseudo remainder of CONC w.r.t to TS will be computed. The class, leading degree and terms of the pseudo remainder are given. If the pseudo remainder is 0, It means the theorem is generic true.

```
Index: (15,1,6)
Index: (14,1,10)
Index: (12,1,27)
Index: (10,1,18)
Index: (9,2,12)
Index: (0,0,0)
The statement is true.
```

5. WSOLVE

WSOLVE is a maple package for solving system of polynomial equations. For a given system of polynomial equations $PS = 0$, It will decompose PS into a series of ascending set, which is in a "triangular" form and can be solved easier

Zero Decomposition Theorem

For a polynomial set PS, we have the following zero decomposition theorem

$$Zero(PS) = \sum_i Zero(AS_i/J_i)$$

in which J_i is the product of the leading coefficient of the polynomial in AS_i If PS has only finitely many solutions, we have

$$Zero(PS) = \sum_i Zero(AS_i)$$

where each AS_i is an ascending set.

The specification of WSOLVE is as follows:

$LIST \leftarrow wsolve(PS,X)$
Input:

PS is a list of polynomials;
X is a list of ordered indeterminates.

Output:

$LIST$ is either NIL, which implies $Zero(PS) = \emptyset$, or
a list, which consists of a finite number of ascending set AS_i,
$Zero(PS) = \bigcup_i Zero(AS_i/J_i)$ where J_i is the product of the initials of the polynomials in AS_i. If PS has only finitely many solutions, then $Zero(PS) = \bigcup_i Zero(AS_i)$

For a polynomial system PS, we can get a series of subsystems AS_i, each AS_i is a ascending set so that the zeros of the polynomial system PS are the union of the zeros of the subsystems AS_i. Each subsystem is in a "triangular" form and the leading coefficients of the polynomials in each AS_i are constant so that the numerical solutions of the system can be given easily.

There are many technique and tricks used in WSOLVE to improve the efficiency of the algorithms. Every polynomial produced by the pseudo-remainder algorithm will be factored. This factorization will reduce the amount of the computation greatly. The redundant factors and branches will be cut off in the computing process.

6. Remarks The packages and system together with user's guide are available via anonymous ftp at

mmrc.iss.ac.cn:/pub/software

A new system STAR - A Small Tool for Algebraic Research is being developed in MMRC. It will be written in C++ and provide a symbolic environment for polynomial operations and the computing of the characteristic set.

References

[CHOU] S.C.Chou ,"Mechanical Geometry Theorem Proving" , D.Reidel Publishing Company, Dordrecht, Netherlands (1988).

[C-G1] S.C.Chou & X.S.Gao, "Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving" Proceedings of CADE-10, Lecture Notes in AI, Vol. 449, 1990.

[C-G2] S.C.Chou & X.S.Gao, "An Algebraic System Based on the Characteristic Method ", IWMM'92 , China (1992).

[COL] G.E.Collins, "Subresultants and Reduced Polynomial Sequences", J.ACM, 14 (1967)

[DMW] D.M.Wang, "An Implementation of the Characteristic Set Method in Maple" RISC-LINZ series no.91-25.0 Johannes Kepler University,Austria (1991)

[RITT] J.F.Ritt, "Differential Algebra " , AMS Colloquium Publications, New York,1950.

[SHI] He Shi "On Solving the Yang-Baxter Equations", IWMM'92 . China (1992)

[WU1] Wu Wen-tsun, "On the Decision Problem and the Mechanical Theorem Proving and the Mechanization of Theorem in Elementary Geometry", Scientia Sinica 21(1978).

[WU2] Wu Wen-tsun, "Basic Principles of Mechanical Theorem Proving in Geometries" J.of Sys.Sci.and Math.Sci, China (1984) .

[WU3] Wu Wen-tsun, "On Surface-Fitting Problem in CAGD", Research Preprints, Mathematics-Mechanization No.10, China(1993)

[WU4] Wu Wen-tsun, "On a Finiteness Theorem about Optimization Problems" Research Preprints, Mathematics-Mechanization No.8, China . (1992)

[WU5] Wu Wen-tsun, "On the Char-Set Method and the Linear Equations Method on Non-linear Polynomial Equations-Solving", IWMM'92 , China (1992) .

[WU6] Wu Wen-tsun, "On the Generic Zero and Chow Basis of an Irreducible Ascending Set" Research Preprints, Mathematics-Mechanization No.4, China (1989)

[WU7] Wu Wen-tsun, "A Zero Structure Theorem for Polynomial Equations Solving and Its Applications" , Research Preprints, Mathematics-Mechanization No.1 , China (1987).

[W-H] Wu Wen-da & Yu-zhen Huang , "Kinematic Solution of A Stewart Platform", IWMM'92 , China (1992)

[ZHI] L.H.Zhi, "Factorizing Multivariate Polynomials over Algebraic Extension Fields", Research Preprints, Mathematics-Mechanization No.12, China (1994).