Front. Comput. Sci. China 2007, 1(1): 1–8
DOI 10.1007/s11704-007-0001-8
REVIEW ARTICLE

Mathematics mechanization and applications after thirty years

WU Wenjun (Wen-Tsun Wu), GAO Xiaoshan (✉)

Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Academy of Mathematics and System Sciences,
Chinese Academy of Sciences, Beijing 100080, China

Abstract The aim of mathematics mechanization is to develop symbolic algorithms for manipulating mathematical objects, proving and discovering theorems in a mechanical way. This paper gives a brief review of the major advances in the field over the past thirty years. The characteristic set method for symbolic solution of algebraic, differential, and difference equation systems are first introduced. Methods for automated proving and discovering geometry theorems are then reviewed. Finally, applications in computer-aided geometric design, computer vision, intelligent computer-aided design, and robotics are surveyed.

Keywords mathematics mechanization, characteristic set method, automated theorem proving, automated theorem discovering, symbolic equation solving, computer aided geometric design, computer vision, intelligent computer-aided design, robotics

1 Introduction

A major trend in the information age is the mechanization of mental labor with the assistance of computers. Partial mechanization of mental labor allows scientists and engineers to free themselves from tedious and sometimes human unreachable tasks and to concentrate on high-level innovative activities, and hence to greatly enhance social productivity. It was in this background that the first author of this paper began to call for the study of *mathematics mechanization* in the 1970s, which is the effort to mechanize mental labor in the field of mathematics, in particular, theorem proving, discovering, and equation solving.

The first author of the paper started the research on mathematics mechanization around 1976 and published the first paper in 1978, in which he established a method for proving geometry theorems, known as Wu's method. In 1979, the first author of the paper went further to propose the "Program of Mathematics Mechanization" which consists the following aspects:

- "Cover as much as possible the whole of mathematics by domains each of which is sufficiently small to be mechanizable, at the same time also sufficiently large to contain lot of theorems or problems of high mathematical interest."
- Apply the methods of mathematics mechanization to interdisciplinary studies and engineering problem solving.

The past thirty years witnessed the development of mathematics mechanization into an active new research area covering theories, algorithms, and a wide range of applications.

The central theme of mathematics mechanization in the past thirty years is to study effective symbolic methods for solving various equation systems. The reason could be illustrated by the so-called *Descartes Program* [1], which was proposed by Descartes in his posthumous work *Rules for the Direction of the Mind* as a general principle of problem solving:

First, reduce any kind of problem to a mathematical problem.

Second, reduce any kind of a mathematical problem to a problem of algebra.

Third, reduce any problem of algebra to the solution of a single equation.

Although the Descartes program is apparently wrong in many aspects, the importance of Descartes' thought is undisputable. It is well-recognized that algebraic equation solving plays a key role in many kinds of important science and engineering problems, let alone we could include differential, difference, and other types of equations in this program.

On the other hand, developing methods for solving equations is the main concern of mathematics in ancient China [2]. A peak of the work of ancient Chinese mathematicians on equation solving is Szejie Zhu's work in 1303, which gives a quite general method for solving equation systems with four indeterminates. It is along the lines of thought furnished by the classic work of the ancient Chinese mathematics that the first author introduced concepts and techniques from modern mathematics, mainly borrowed from

Received September 5, 2006; accepted December 11, 2006

E-mail: xgao@mmrc.isss.ac.cn

the classical text of Ritt [3], in order to reformulate and to make precise and rigorous the procedure that originated from Szejie Zhu's work. The outcome is a general *characteristic set method* [4, 5], which will be reviewed in Section 2.

Another focus of mathematics mechanization is automated reasoning and computation in geometries. Geometry has always been a model of precise reasoning. It is quite natural that geometry theorem proving was selected as one of the first problems to be experimented with when the field of artificial intelligence (AI) started in the 1950s. But, the progress is slow in the sense that the proposed methods could only prove very simple geometry theorems. Things changed after the appearance of Ref. [6], where a powerful method is introduced, which can be used to prove quite difficult geometry theorems efficiently [5, 6] for the first time. Due to this method, "geometry theorem proving was then fully revived and became one of the most actively researched and successful areas in automated deduction" [7]. In Section 3, we will give a brief introduction to some of the major developments in this area.

Applications and interdisciplinary studies are a major character of mathematics mechanization. The characteristic set method and the methods for geometry reasoning and computation have diverse applications. Theoretically, they may serve as a basis to solve many problems from mathematics, physics, mechanics, chemistry, computer science, etc. They were also applied to many problems from real-world applications, especially problems from IT, including computer vision and image processing [8−11], intelligent computer-aided design (CAD) systems [12], computer-aided geometric design (CAGD) [2, 13−15], hardware verification [16], analysis of robotics and mechanisms [2, 17]. In Section 4, we will review some of these applications.

2 The characteristic set method

The characteristic set method plays a central role in the theory and applications of mathematics mechanization. In this section, we will introduce its main features and applications in equation solving.

2.1 Properties of ascending chains

Let $\mathcal{K}$ be the field of rational numbers, $\mathbb{X}=\{x_1,x_2,\cdots,x_n\}$ a set of indeterminants, and $\mathcal{K}[\mathbb{X}]$ the set of polynomials in $\mathbb{X}$ with coefficients in $\mathcal{K}$. The *universal field* $\mathcal{E}$ over $\mathcal{K}$ is an algebraically closed field containing an infinite number of indeterminants. For a polynomial D and a polynomial set $\mathbb{P} \subset \mathcal{K}[\mathbb{X}]$,

$$\mathrm{Zero}(\mathbb{P}) = \{\eta \in \mathcal{E}^n \mid P(\eta) = 0, \forall P \in \mathbb{P}\}$$

is called a *variety*, and $\mathrm{Zero}(\mathbb{P}/D) = \mathrm{Zero}(\mathbb{P}) \setminus \mathrm{Zero}(D)$ is called a *quasi variety*.

A set $\mathcal{A}$ of polynomials is called an *ascending chain* (or triangular set), or simply a chain, if after renaming the variables $\mathbb{X}$ as $\mathbb{U} = \{u_1,\cdots, u_q\}$ and $\mathbb{Y} = \{y_1,\cdots, y_p\}$, $\mathcal{A}$ can be written as the following form:

$$\begin{aligned} &A_1(\mathbb{U}, y_1) = I_1\, y_1^{d_1} + \text{terms of lower degrees in } y_1,\\ &\qquad\cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (1)\\ &A_p(\mathbb{U}, y_1,\cdots, y_p) = I_p\, y_p^{d_p} + \text{terms of lower degrees in } y_p. \end{aligned}$$

I_i is called the *initial* of A_i. Denote $\mathrm{I}_{\mathcal{A}} = \prod_i I_i$. The *dimension* of $\mathcal{A}$ is defined to be $\dim(\mathcal{A}) = |\mathbb{U}| = q$. The *degree* of $\mathcal{A}$ is defined to be $\deg(\mathcal{A}) = \prod_{i=1}^{p} d_i$.

We could say that the solutions for a chain is basically determined. Intuitively, for a set of given values of the parameters $\mathbb{U}$, the y_i can be determined iteratively by solving univariate equations $A_i = 0$. In order to show the properties of chains, we first introduce several concepts. The *saturation ideal* of $\mathcal{A}$ is defined as below:

$$\mathbf{sat}(\mathcal{A}) = \{P \in \mathcal{K}[\mathbb{X}] \mid \exists k, \mathbf{I}_{\mathcal{A}}^k P \in (\mathcal{A})\}.$$

We may define an ordering among the chains such that any set of chains contains one with the lowest order [2, 5]. A *characteristic set* of a polynomial set $\mathbb{P}$ is any chain contained in $\mathbb{P}$ with lowest ordering.

A chain $\mathcal{A}$ is called *irreducible* if A_1 is irreducible in $\mathcal{K}_1[y_1]$ and A_k is irreducible modulo $A_1,\cdots, A_{k-1}$.

Theorem 2.1 *Let $\mathcal{A}$ be an irreducible chain. Then* $\mathbf{sat}(\mathcal{A})$ *is a prime ideal of dimension* $\dim(\mathcal{A})$ *and degree* $\deg(\mathcal{A})$ *with respect to* $\mathbb{U}$. *Conversely, a characteristic set of a prime ideal is irreducible.*

The following result shows that the dimension and degree of a chain are intrinsic properties.

Theorem 2.2 [18, 19] *Let $\mathcal{A}$ be a chain of form* (1). *If* $\mathrm{Zero}(\mathbf{sat}(\mathcal{A})) \neq \varnothing$, $\mathrm{Zero}(\mathbf{sat}(\mathcal{A}))$ *and* $\mathrm{Zero}(\mathcal{A}/\mathbf{I}_{\mathcal{A}})$ *are unmixed. More precisely, write* $\mathrm{Zero}(\mathbf{sat}(\mathcal{A}))$ *as an irredundant decomposition*: $\mathrm{Zero}(\mathbf{sat}(\mathcal{A})) = \bigcup_{i=1}^{r} \mathrm{Zero}(\mathbf{sat}(\mathcal{C}_i))$. *Then*

(i) $\mathcal{C}_i$ *is also of form* (1). *As a consequence*, $\dim(\mathbf{sat}(\mathcal{C}_i)) = \dim(\mathcal{A})$.

(ii) $\deg(\mathcal{A}) \geqslant \sum_{i=1}^{r} \deg(\mathcal{C}_i)$. *Furthermore*, $\deg(\mathcal{A}) = \sum_{i=1}^{r} \deg(\mathcal{C}_i)$ *iff $\mathcal{A}$ is satured, that is, the initials and separants of $\mathcal{A}$* are *invertible with respect to $\mathcal{A}$*.

To extend Theorems 2.1 and 2.2 to the case of algebraic differential polynomials, we need to assume that the chains are either passive [20] or coherent [21, 22].

Similar results are also proved in the case of algebraic difference polynomials [19, 23]. However, in the difference case, we do not have algorithms to decide whether a chain is regular or irreducible. In order to have a constructive theory, proper irreducible chains are introduced [23]. Also, Theorem 2.2 is proved for proper irreducible chains.

In differential and difference cases, Theorem 2.2 could be strengthened as follows. Let $\mathcal{A}$ be a chain of form (1). Define the *order* of $\mathcal{A}$ to be $\text{ord}(\mathcal{A}) = \sum_i \text{ord}(A_i, y_i)$. Then we further have

Theorem 2.3 [19] *Let* $\text{Zero}(\textbf{sat}(\mathcal{A})) = \bigcup_{i=1}^{r} \text{Zero}(\textbf{sat}(\mathcal{C}_i))$ *be an irredundant decomposition. Then* $\text{ord}(\mathcal{A}) = \text{ord}(\mathcal{C}_i)$.

Other properties of chains, including invertibility with respect to a chain and properties of the saturation ideal [22, 24], factorizations module of a chain [25], and bounds for the coefficients of a chain to represent a zero-dimensional variety [26], were also studied.

2.2 Characteristic set method

The characteristic set method is to decompose the zero set for a polynomial system in general form into the union of zero sets for chains. Since the zero set of a chain is considered to be known, this method gives a general tool to deal with equation systems. The characteristic set method consists of the well-ordering principle, the zero decomposition theorem, and the projection theorem.

Let $\mathbb{P}$ be a finite set of polynomials. Then we can perform the following operations:

$$\begin{array}{llllll} \mathbb{P} = \mathbb{P}_0 & \mathbb{P}_1 & \cdots & \mathbb{P}_i & \cdots & \mathbb{P}_m \\ \mathcal{B}_0 & \mathcal{B}_1 & \cdots & \mathcal{B}_i & \cdots & \mathcal{B}_m = \mathcal{C} \\ \mathbb{R}_0 & \mathbb{R}_1 & \cdots & \mathbb{R}_i & \cdots & \mathbb{R}_m = \varnothing \end{array} \tag{2}$$

where $\mathcal{B}_i$ is the characteristic set of $\mathbb{P}_i$; $\mathbb{R}_i$ is the set of nonzero remainders of the polynomials in $\mathbb{P}_i$ with respect to $\mathcal{B}_i$; and $\mathbb{P}_{i+1} = \mathbb{P}_i \cup \mathbb{R}_i$. In scheme (2), $\mathcal{B}_m = \mathcal{C}$ verifies

$$\text{prem}(\mathbb{P}, \mathcal{C}) = \{0\} \text{ and } \text{Zero}(\mathbb{P}) \subset \text{Zero}(\mathcal{C}), \tag{3}$$

where prem denotes the pseudo-remainder. Any chain $\mathcal{C}$ verifying the property (3) is called a *Wu characteristic set* of $\mathbb{P}$.

Theorem 2.4 (Wu's Well-ordering Principle) [5, 6] *Let* $\mathcal{C}$ *be a Wu characteristic set of a polynomial set* $\mathbb{P}$. *Then*

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\mathcal{C} / \mathbf{I}_{\mathcal{C}}) \bigcup \cup_i \text{Zero}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}),$$

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\textbf{sat}(\mathcal{C})) \bigcup \cup_i \text{Zero}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}),$$

where I_i *are the initials of the polynomials in* $\mathcal{C}$.

Using the well-ordering principle recursively, we obtain the following key result.

Theorem 2.5 (Ritt-Wu's Zero Decomposition Theorem) [3, 5] *There is an algorithm that allows the determination for a given polynomial set* $\mathbb{P}$ *in a finite number of steps a finite set of* (*irreducible*) *chains* $\mathcal{A}_j$ *such that*

$$\text{Zero}(\mathbb{P}) = \cup_j \text{Zero}(\mathcal{A}_j / \mathbf{I}_{\mathcal{A}_j}) = \cup_j \text{Zero}(\textbf{sat}(\mathcal{A}_j)).$$

Let $\mathbb{P}$ be a polynomial set, and $D \in \mathcal{K}[\mathbb{U}, \mathbb{X}]$, where $\mathbb{U} = \{u_1, \cdots, u_m\}$ and $\mathbb{X} = \{x_1, \cdots, x_n\}$. The projection of $\text{Zero}(\mathbb{P}/D)$ to $\mathbb{U}$ is defined as follows:

$$\text{Proj}_{\mathbb{X}} \text{Zero}(\mathbb{P}/D) = \{e \in \mathcal{E}^m \mid \exists a \in \mathcal{E}^n \, s.t. (e, a) \in \text{Zero}(\mathbb{P}/D)\}.$$

Projection for quasi-varieties can be computed with the characteristic set method.

Theorem 2.6 (Projection Theorem) [2, 27] *For a polynomial set* $\mathbb{P} \subset K[\mathbb{U}, \mathbb{X}]$ *and* $D \in K[\mathbb{U}, \mathbb{X}]$, *we can compute chains* $\mathcal{A}_i$ *and polynomials* D_i in $\mathcal{K}[\mathbb{U}]$ such that

$$\text{Proj}_{\mathbb{X}} \text{Zero}(\mathbb{P}/D) = \cup_{i=1}^{l} \text{Zero}(\mathcal{A}_i / D_i \mathbf{I}_{\mathcal{A}_i}).$$

The concept of characteristic set for prime ideals was introduced by Ritt [3]. The Wu-characteristic set, the well-ordering principle, and the current form of zero decomposition theorems were introduced by the first author [2, 4–6].

The complexity of the method was studied in Ref. [28]. Like most general algorithms for polynomial equation solving, the characteristic set method is of exponential complexity in the worst case and developing algorithms with lower complexity is a challenging problem. In order to improve the computation efficiency, new forms of chains such as weak chains [5, 18], regular chains and satured chains [22, 29, 30] were introduced. Hybrid characteristic set methods were introduced in Refs. [31, 32]. New elimination procedures for the characteristic set method were introduced [2, 18, 30, 33–35]. A promising work is to develop a modular characteristic set method [26], where a new equiprojectile decomposition algorithm was proposed.

The characteristic set method for algebraic differential equation systems was also proposed [3, 20–22, 36–38]. A characteristic set method for algebraic difference equation systems was proposed in Refs. [19, 20]. The characteristic set method was also extended to certain analytical functions in Ref. [39].

The characteristic set method was implemented in several software packages, including the MMP [40], Wsolve [41], and Epsilon [42].

2.3 Equation solving with the characteristic set method

When talking about equation solving, most people usually refer to numerical methods such as the Newton-Raphson method. These methods start from certain initial values and apply some limiting processes to converge toward some solution of the given polynomial equations. In general, these methods will give only one solution among the set of all possible solutions and are thus *local* in character. Also, these methods give only solutions in approximate values and suffer from error control as well as stability control.

In contrast to the numerical methods, the symbolic ones give solutions in some acceptable algebraic form and all the possible solutions may be expressed in this way so that the methods are *global* in character. Among such symbolic methods we may cite in particular the Gröbner basis method, which has been proved to be quite successful in the zero-dimensional case. On the other hand, by decomposing the zero set of a polynomial system into the zero sets of polynomial systems in triangular form, the characteristic set method gives a complete way to describe the structure for the zero sets of equation systems for all dimensions [2, 4, 5]. Furthermore, for zero dimensional chains, its real solutions can be computed by methods of root isolation [43]; for algebraic differential equations, formal power series solutions for chains can be computed algorithmically [44].

Most equation systems from applications have parameters. In general, a parametric polynomial equation system in $\mathbb{X}=\{x_1,\cdots,x_n\}$ with parameters $\mathbb{U}=\{u_1,\cdots,u_m\}$ has the following form:

$$\begin{aligned}&P_1(\mathbb{U},\mathbb{X})=0,\ \cdots,P_t(\mathbb{U},\mathbb{X})=0,\\&D_1(\mathbb{U},\mathbb{X})\neq 0,\ \cdots,D_r(\mathbb{U},\mathbb{X})\neq 0.\end{aligned}\tag{4}$$

For an equation system (4), we may ask the following questions: (1) For what values of $\mathbb{U}$, the x_i have solutions? (2) How to compute these solutions for x_i? (3) Determine the number of solutions of the x_i for given values of $\mathbb{U}$. The first problem can be answered by the Projection Theorem 2.6. The second problem is solved by dividing the parametric space into domains and on each domain the solution for x_i can be represented by a chain [45]. The third problem is solved if the equation system has a finite number of solutions for the x_i.

Hybrid characteristic set methods were developed to have the advantages of both the numerical methods and the symbolic methods [11, 13, 32].

3 Automated reasoning with the characteristic set method

After Ref. [6], extensive studies on automated theorem proving were carried out. In this section, we survey some of the major advances.

3.1 Wu's method of automated geometry theorem proving and discovering

A geometry theorem is called a *theorem of equality type*, if after introducing coordinates, the theorem can be expressed in the following form:

$$\forall x_i[(H_1=0\wedge\cdots\wedge H_s=0\wedge D_1\neq 0\wedge\cdots\wedge D_t\neq 0)\Rightarrow(C=0)],\tag{5}$$

where H_i, D_i, C are in $\mathcal{K}[\mathbb{X}]$.

For theorems of equality type, we have the following principles of mechanical theorem proving, which are consequences of Theorems 2.4 and 2.1.

Theorem 3.1 [6] *For a geometry statement of form* (5), *let* $\mathcal{A}$ *be a Wu-characteristic set of* $\{H_1,\cdots,H_s\}$. *If* prem(C, $\mathcal{A}$) = 0, *then the statement is valid under the non-degenerate condition* $\mathbf{I}_{\mathcal{A}}\neq 0$.

Note that the non-degenerate condition $\mathbf{I}_{\mathcal{A}}\neq 0$ is generated automatically by the algorithm.

Theorem 3.2 [5] *Let* $D=\prod_i D_i$. *With Theorem 2.5, we have*

$$\mathrm{Zero}(\{H_1,\cdots,H_s\}/D)=\bigcup_{i=1}^{l}\mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i)/D).$$

If $\mathrm{prem}(C,\mathcal{A}_i)=0,\ i=1,\cdots,l$, *then the statement is true. If* $\mathcal{A}_i$ *is irreducible and* $\mathrm{prem}(C,\mathcal{A}_i)\neq 0$, *then the statement is not valid on* $\mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i)/D)$.

There are two kinds of problems in elementary geometry other than theorem proving. One is finding locus equations, the other is deriving geometry formulas. For a geometric configuration given by a set of polynomial equations $h_1(\mathbb{U},x_1,\cdots,x_p)=0,\cdots,h_r(\mathbb{U},x_1,\cdots,x_p)=0$, we want to find a relation between arbitrarily chosen variables $\mathbb{U}$ (parameters) and a dependent variable, x_1. It is pointed out in Ref. [46] that the characteristic set method can be used to discover such unknown geometric formulas. Many new theorems from elementary and differential geometries were discovered in this way.

The characteristic set method can be used to prove a much wider class of geometry theorems. Let $\mathcal{E}$ e an algebraically closed extension of $\mathcal{K}$, that is, the field of complex numbers. A *first order formula* over $\mathcal{E}$ can be defined as follows:

1. If $P\in\mathcal{K}[\mathbb{X}]$, then $P(\mathbb{X})=0$ is a formula.

2. If f, g are formulas, then $\neg f$, $f\wedge g$, and $f\vee g$ are formulas.

3. If f is a formula, then $\exists x_i\in\mathcal{E}(f)$ and $\forall x_i\in\mathcal{E}(f)$ are formulas.

A formula can always be written as a prefix canonical form:

$$\phi=Q_1y_1\cdots Q_my_m\psi(u_1,\cdots,u_d,y_1,\cdots,y_m),\tag{6}$$

where Q_k is a quantifier $\exists$ or $\forall$ and ψ a formula free of quantifiers. For a first order formula ϕ of form (6), there exists a fundamental problem:

Quantifier Elimination: Find a formula $\theta(u_1,\cdots,u_d)$ such that θ is equivalent to ϕ. If d = 0, we need to decide whether ϕ is valid or not.

Since an existential quantifier can be eliminated with Theorem 2.6, we have the following result, which gives the scope of Wu's method of geometry theorem proving.

Theorem 3.3 *Based on the characteristic set method, we have a decision procedure for the first order theory over a* (*differentially*) *algebraically closed field.*

It turns out that most of the theorems in elementary and differential geometries are of equality type and the Wu's method is capable of proving most of these theorems. Collections of theorems proved with Wu's method can be found in Refs. [18, 47]. Wu's method to prove theorems in elementary geometries was further extended to prove theorems from differential geometry and mechanics [20, 44]. The method is further improved and extended in Refs. [36, 38, 48].

3.2 Coordinate-free approaches to automated reasoning in geometry

Algebraic methods, though powerful, generally can only tell whether a statement is true or not. The proofs generated are generally not readable. Several approaches to produce readable proofs based on geometric invariants were proposed. As expected, these methods can produce shorter proofs than that of the coordinate-based methods. But, this advantage comes with a price: in general, these methods are not complete.

The area method is the first successful method based on geometric invariants [49]. Three basic *geometric quantities*:

the ratio of parallel line segments, the signed area, and the Pythagorean difference are used as the basic geometric quantities. The basic propositions, which formally describe the properties of these quantities, are the deductive basis of the area method. The method involves the elimination of the constructed points from the conclusion using these basic geometry propositions. The area method is powerful enough to solve most of the problems that have been solved with Wu's method and is capable of producing short and readable proofs for a large proportion of them.

One of the earliest efforts to develop coordinate-free methods of geometric reasoning is to use techniques from the bracket algebra such as Cayley factorization and biquadratic final polynomials. The first successful method along this line is proposed in Ref. [50]. In Refs. [51, 52], the techniques of Clifford algebra are combined with Wu's method to prove geometry theorems. The idea is to use several rules of solving vector equations in vector level.

More recently, Li et al. proposed the *conformal geometric algebra* [53], which is a powerful tool for geometric representation and computations. By mapping three-dimensional geometric objects into a five-dimensional space, this algebra provides a unified and compact representation for classical geometric objects and a set of effective algorithms for geometric computation. As a consequence, geometric theorems can be proved and new geometric relations can be discovered effectively [54]. Conformal geometric algebra is also widely used in computer vision and computer graphics.

3.3 AI approaches to automated reasoning in geometry

Geometry theorem proving on computers began in the 1950s with the landmark work of Gelernter et al. [55]. Gelernter's geometry machine uses a *backward chaining approach*, that is, it reasons from the conclusion to the hypotheses and generates a *proof-tree* for a theorem. Several basic ideas of geometric reasoning such as using a numerical model, constructing auxiliary points, and generating geometric lemmas were studied in this work. Most of the other work on the AI approach of geometric reasoning can be considered extensions of this work. The main problem with these approaches is that the search of a proof generally will lead to search space explosions and the methods cannot be used to prove difficult theorems.

In Ref. [56], a *deductive database method* for geometry theorem proving is proposed. The resulting program can be used to find the *fixpoint* for a geometric configuration, i.e., the system can find all the properties of the configuration that can be deduced using a fixed set of geometric rules. This method seems to be the first search-based method capable of proving and discovering a large number of geometric theorems. The idea of the method is to use a structured deductive database to reduce the size of the database and to use a set of powerful deduction rules based on the concept of full-angles.

Generally speaking, the algebraic approaches are decision procedures and are more powerful, while the AI approaches are not decision procedures and are less powerful. But, the AI methods have the following advantages. (1) Exploring search methods may lead to general techniques of theorem proving. (2) Proofs produced by the AI method are generally easy to understand than proofs based on algebraic computations. (3) Using predicates only makes the reaching of fixpoint possible. (4) AI methods allow to produce multiple and shortest proofs for a geometry theorem.

Geometry Expert is a software system that implements Wu's method, the area method, and the deductive database method for proving geometry theorems [57]. It is also a dynamic geometry software system for automated geometric diagram generation.

3.4 Proving theorems involving inequalities

The methods introduced in Section 3.1 are complete only for geometries over complex numbers, although it is quite successful to prove theorems from Euclidean geometry. Historically, Tarski's landmark work on quantifier elimination over the field of real numbers provides a complete method to prove all elementary theorems from Euclidean geometry. However, Tarski's method is too involved to solve any problems in practice. In the 1970s, Collins invented the CAD method, which provides an optimized quantifier elimination algorithm [58]. This general approach is used to prove geometry theorems with limited success. The main difficulty is that in geometry theorems, there are many parameters that increase the computation complexity. An effective method along this line is the quantifier elimination algorithm for linear and quadratic equations proposed in Ref. [59], which has been used to prove a large number of difficult geometry theorems.

The global optimization problem under algebraic constraints was considered [60] and the following result was proved.

Theorem 3.4 (Finite Kernel Theorem) [60] *Let $\mathbb{P}$ be an arbitrary polynomial set and P a polynomial in $\mathcal{R}[\mathbb{X}]$. Then we can construct a finite set of real values K such that the extremal values of P under the constraint $\mathbb{P} = 0$ are contained in K.*

The method was used to prove geometry theorems involving inequalities, to prove trigonometric inequalities, to solve non-linear programming problems, and to solve optimization problems [2].

In Refs. [30, 61], a powerful tool, called the *complete discrimination system* (*CDS*) was introduced, which can be used to give explicit conditions for a univariate polynomial equation $P(x) = 0$ to have a certain given number of solutions. By means of CDS, together with Wu's method and a partial CAD algorithm, a program called *BOTTEMA* was implemented, which is particularly powerful to prove inequalities from triangles [62].

4 Selected applications of the characteristic set method

Equation solving, geometric computation and reasoning are within the heart of many aspects of information technology. Methods developed from mathematics mechanization have been used successfully in some of these problems. In this section, we review several of these applications.

4.1 Applications to computer-aided geometric design

Two kinds of problems from CAGD are extensively studied with the characteristic set method: the surface-fitting problem and the implicitization of rational parametric equations.

The surface-fitting problem is to construct a real implicit surface that intersects a set of given real surfaces along a set of given curves with certain given continuities [2]. Based on the characteristic set method, a general method to solve the above problem was given. As an example, it is shown that there exists a cubic blending surface for two cylinders defined by $y^2+z^2=r_1^2$, $x^2+z^2=r_2^2$ alone the sections given by $x=d_1$, $y=d_2$ iff $r_1^2+d_1^2=r_2^2+d_2^2$. In Ref. [14], a set of similar formulae for blending two quadratic surfaces in general form were given and named the *Wu Wen-tsun formulae*. Blending three or more surfaces with Wu's method was considered in Ref. [31].

To find the implicit form for a set of rational parametric equations is a basic problem in CAGD. Most existing work satisfies with finding the implicit equations. A method was proposed in Ref. [27] to find the defining equations for the image of a set of rational parametric equations. In Ref. [15], Wu's method is used to find a basis for the implicit ideal; to decide whether the parameters are independent, and if not, to re-parameterize the equation so that the new parameters are independent; to decide whether the parametric equation is proper, and for a non-proper equation, find a proper re-parameterization; to decide whether the parametric equation is normal, and if it is not normal, find a normal re-parameterization in some cases.

4.2 Applications to computer vision

Some of the early applications focused on solving constraints raised from computer vision. In Ref. [9], Wu's method is used to perspective viewing in image understanding. Here, the authors considered the problem: under what conditions the images of some geometric objects are in certain particular positions and how to use Wu's method to deduce these conditions automatically. In Ref. [63], Wu's method is used to solve the edge matching constraints and occluding-contour constraints occurring in the global stereo vision problem when the scene consists of polyhedrals.

Another problem studied extensively with Wu's method is the Perspective-*n*-Point (PnP) problem [8, 10, 11]. The problem is to determine the position and orientation of the camera with respect to a scene object from *n* correspondent points. In Ref. [8], the characteristic set method is used to give a complete analytical solution to the P3P problem. A complete solution classification for the P3P equation system is also given, that is, explicit criteria are given for the P3P problem to have one, two, three, and four solutions. Combining the analytical solutions with the criteria, an algorithm is given to find complete and robust numerical solutions to the P3P problem. The characteristic set method is used to prove that the probability for the P4P problem to have one solution is one. In Ref. [11], a hybrid method was proposed, which can be used to find solutions in the singular case.

Due to its ability to represent geometric objects intrinsically, geometric invariant methods are widely used in computer vision. Methods proposed in Refs. [52, 54] were used to study the reconstruction of high dimension objects from their 2D projections. Conformal geometric algebra was used to simplify the solving procedure for monocular vision problems. Spinor and twist representations are used to reduce the number of constraints, which often lead to effective solutions of the pose estimation problem, shape approximation, and curve blending [53].

4.3 Applications to intelligent computer-aided design

Most works on automated geometry reasoning focus on theorem proving and discovering. On the other hand, many problems from engineering applications are about how to draw a geometric diagram automatically. A typical example is computer-aided design where the main task is to draw machine parts and a key feature of the new generation of CAD system is the automatic generation of such design diagrams.

A general framework for automated geometric diagram generation is as follows. First, graphical algorithms are used to decompose a large problem into basic merge patterns, which are the smallest problems that cannot be decomposed further [12]. Second, basic merge patterns are classified and solved with symbolic or numerical methods. Third, merge the solved basic merge patterns to obtain a solution of the original problem. The decomposition is the key step in the solving process, and it is due to this step that a class of large-scale problems can be solved effectively.

The characteristic set method and search methods can be used to solve the basic merge patterns and to simplify the decomposition [12, 17]. Based on Wu's method, a decision procedure for ruler and compass construction for a geometric diagram was proposed.

4.4 Applications to kinematics of robotics

From the viewpoint of structures, there are two major classes of robotics: *serial manipulators* consisting of several links successively and *parallel manipulators* consisting of two platforms connected with several independent links. The *inverse kinematics* of a manipulator is to find the parameters for the links such that the manipulator can reach a given position and an orientation in the space. The *forward kinematics* of a manipulator is to find the position and orientation of one end of the manipulator for given parameters of the links. The inverse kinematics for serial manipulators and the forward kinematics for parallel manipulators are central problems for kinematics of robotics.

It is known that the inverse kinematics for a general serial manipulator has up to 16 solutions. Closed form solutions are not yet found. Using the characteristic set method, a complete analysis for the inverse kinematics of a special type of serial manipulator, Puma560, was given. The analytical solutions, the working range, and the singularities of the inverse kinematics were derived [2].

The general spatial parallel manipulator has six links and is called the *Stewart platform*. It is known that the forward kinematics for the Stewart platform has up to 40 solutions. Closed form formulae for these solutions were found only in some special cases. In Ref. [17], a class of 3850 *generalized Stewart platforms* was introduced, which consists of two rigid bodies connected with six distance and/or angular constraints between six pairs of points, lines and/or planes in the base and the moving platform, respectively. Upper bounds for the number of solutions of the forward kinematics for all the platforms were given. Closed-form solutions and the best upper bounds of real solutions of the forward kinematics for a class of 1120 platforms were given with Wu's method.

Acknowledgements This work was partially supported by the National Key Basic Research Project of China (2004CB318000).

References

1. Pólya G. Mathematical Discovery. Vol 1. John Wiley & Sons, 1962
2. Wu W T. Mathematics Machenization. Beijing: Sience Press/Kluwer, 2001
3. Ritt J F. Differential Algebra. New York: AMS Press, 1950
4. Wu W T. Basic principles of mechanical theorem-proving in elementary geometries. Sys Sci & Math Scis, 1984, 4: 207–235; also in Journal of Automated Reasoning, 1986, 2: 221–252
5. Wu W T. Basic Principle of Mechanical Theorem Proving in Geometries. Beijing: Science Press, 1984 (in Chinese); English translation, Wien: Springer, 1994
6. Wu W T. On the decision problem and the mechanization of theorem-proving in elementary geometry. Scientia Sinica, 1978, 21: 159–172
7. Hsiang J. Herbrand Award for Distinguished Constributions to Automated Reasoning, vi-vii. Automated Deduction-CADE-14. LNAI 1249. Berlin: Springer, 1997
8. Gao X S, Hou X R, Tang J, et al. Complete solution classification for the perspective-three-point problem. IEEE Tran on PAMI, 2003, 25: 930–943
9. Kapur D, Mundy J L. Wu's method and its applications to perspective viewing. Artificial Intelligence, 1988, 37: 15–36
10. Su C, Xu Y, Li H, et al. Application of Wu's method in computer animation. In: Proceedings of Fifth Int'l Conf. CAD/CG. Vol 1. 1997, 211–215
11. Zhi L, Reid G, Tang J. A complete symbolic-numeric linear method for camera pose determination. In: Proceedings of ISSAC'03. New York: ACM Press, 2003, 215–223
12. Gao X S, Lin Q, Zhang G. A C-tree decomposition algorithm for 2D and 3D geometric constraint solving. Computer-Aided Design, 2006, 38: 1–13
13. Chen F, Deng J, Feng Y. Algebraic surface blending using Wu's method. Computer Mathematics. Singapore: World Scientific, 2000, 172–181
14. Wu T, Lei N, Cheng J. Wu Wen-tsun formulae for the blending of pipe surfaces. Northeast Math J, 2002, 17: 383–386
15. Gao X S, Chou S C. Implicitization of rational parametric equations. Journal of Symbolic Computation, 1992, 14: 459–470
16. Mao W, Wu J. Application of Wu's method to symbolic model checking. In: Proceedings of ISSAC'05. New York: ACM Press, 2005, 237–244
17. Gao X S, Lei D, Liao Q, et al. Generalized Stewart-Gough platforms and their direct kinematics. IEEE Trans Robotics, 2005, 21: 141–151
18. Chou S C, Gao X S. Ritt-Wu's decomposition algorithm and geometry theorem proving. In: Proceedings of CADE'10. LNCS, No 449. Berlin: Springer-Verlag, 1990, 207–220
19. Gao X S, Yuan C. Resolvent systems of difference polynomial ideals. In: Proceedings of ISSAC'06. New York: ACM Press, 2006, 101–108
20. Wu W T. Mechanical theorem proving inelementary differential geometry. Scientia Sinica, 1979, 94–102 (in Chinese)
21. Boulier F, Lazard D, Ollivier F, et al. Representation for the radical of a finitely generated differential ideal. In: Proceedings of ISSAC'95. New York: ACM Press, 1995, 158–166
22. Bouziane D, Kandri Rody A, Maârouf H. Unmixed decomposition of a finitely generated perfect differential ideal. Journal of Symbolic Computation, 2001, 31: 631–649
23. Gao X S, Luo Y. A characteristic set method for difference polynomial systems. In: Inter Conf on Poly Sys Sol, Nov 24–26, Paris, 2004; also in MM-Preprints, 2004, 23: 66–91
24. Aubry P, Lazard D, Maza M M. On the theory of triangular sets. Journal of Symbolic Computation, 1999, 25: 105–124
25. Wang D. Elimination Methods. Berlin: Springer, 2000
26. Dahan X, Maza M M, Schost E, et al. Lifting techniques for triangular decompositions. In: Proceedings of ISSAC'05. New York: ACM Press, 2005, 108–115
27. Wu W T. On a projection theorem of quasi-varieties in elimination theory. Chinese Annals of Math B, 1990, 11: 220–226
28. Gallo G, Mishra B. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In: Progress in Mathematics, 94. Boston: Birkhäuser, 1991, 119–142
29. Kalkbrener M. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. Journal of Symbolic Computation, 1993, 15: 143–167
30. Yang L, Zhang J Z, Hou X R. Non-linear Algebraic Equations and Automated Theorem Proving. Shanghai: ShangHai Science and Education Pub, 1996 (in Chinese)
31. Chen F, Yang W. Applications of interval arithmetic in solving polynomial equations by Wu's elimination method. Science in China, Ser A, 2005, 48: 1260–1273
32. Wu W T. On a hybrid method of polynomial equations solving. MM-Preprints, 1993, 9: 1–10
33. Kapur D, Wan H K. Refutational proofs of geometry theorems via characteristic sets. In: Proceedings of ISSAC'90. New York: ACM Press, 1990, 277–284
34. Li B. An algorithem to decompose a polynomial ascending set into irredncible ones. Acta Anal Funct Appl, 2005, 7: 97–105
35. Wang D. An elimination method for polynomial systems. Journal of Symbolic Computation, 1993, 16 (2): 83–114
36. Chou S C, Gao X S. Automated reasoning in differential geometry

and mechanics. Journal of Automated Reasoning, 1993, 10: 161−172

37. Hubert E. Factorization-free decomposition algorithms in differential algebra. Journal of Symbolic Computation, 2000, 29: 641−662
38. Wang D. A method for proving theorems in differential geometry and mechanics. J Univ Comput Sci, 1995, 9: 658−673
39. Richardson D. Wu's method and the Khovanskii finiteness theorem. Journal of Symbolic Computation, 1991, 12: 127−141
40. Gao X S, Wang D K, Qiao Z, et al. Equation Solvings and Theorem Provings−Problem Solvings with MMP. Beijing: Science Press, 2006 (in Chinese)
41. Wang D K. Wsolve: A Maple Package for Solving System of Polynomial Equations. http://www.mmrc.iss.ac.cn/ dwang/wsolve.htm, 2004
42. Wang D. Elimination Practice: Software Tools and Applications. London: Imperial College Press, 2004
43. Lu Z, He B, Luo Y. Real Roots Isolating for Polynomial Systems and Applications. Beijing: Science Press, 2004 (in Chinese),
44. Wu W T. On the foundation of algebraic differential geometry. Sys Sci & Math Scis, 1989, 2: 289−312
45. Gao X S, Chou S C. Solving parametric algebraic systems. In: Proceedings of ISSAC'92. New York: ACM Press, 1992, 335−341
46. Wu W T. A mechanization method of geometry and its applications, I. Distances, areas, and volumes in Euclidean and non-Euclidean Geometries. Kuxue Tongbao, 1986, 32: 436−440
47. Chou S C. Mechanical Geometry Theorem Proving. Dordrecht: D Reidel, 1988
48. Li Z. Mechanical theorem proving of the local theory of surfaces. Ann Math Artif Intell, 1995, 13: 25−46
49. Chou S C, Gao X S, Zhang J Z. Machine Proofs in Geometry. Singapore: World Scientific, 1994
50. Richter-Gebert J. Mechanical theorem proving in projective geometry. Ann Math and AI, 1995, 13: 139−172
51. Li H, Cheng M. Clifford algebraic reduction method for mechanical theorem proving in differential geometry. Journal of Automated Reasoning, 1998, 21: 1−21
52. Li H. Vectorial equation-solving for mechanical geometry theorem proving. Journal of Automated Reasoning, 2000, 25: 83−121
53. Li H, Hestenes D, Rockwood A. Generalized homogeneous coordinates for computational geometry. Geometric Computing with Clifford Algebra. Berlin: Springer, 2000, 27−60
54. Li H, Wu Y. Automated theorem proving in projective geometry with Cayley and bracket algebras. Journal of Symbolic Computation, 2004, 36: 717−762
55. Gerlentner H, Hanson J R, Loveland D W. Empirical explorations of the geometry-theorem proving machine. In: Proceedings of West Joint Computer Conf. 1960, 143−147
56. Chou S C, Gao X S, Zhang J Z. A deductive database approach to automated geometry theorem proving and discovering. Jornal Automated Reasoning, 2000, 25: 219−246
57. Gao X S, Zhang J Z, Chou S C. Geometry Expert. Teipei: Nine Chapters Pub, 1998 (in Chinese)
58. Collins G E. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. LNCS, No 33. Berlin: Springer-Verlag, 1975, 134−183
59. Dolzmann A, Sturm T, Weispfenning V. A new approach for automatic theorem proving in real geometry. Journal of Automated Reasoning, 1998, 21: 357−380
60. Wu W T. On a finiteness theorem about optimization problems. Sys Sci & Math Scis, 1994, 7: 193−200
61. Yang L, Hou X, Zeng Z. Complete discriminant systems. Science in China, Ser E, 1996, 39(6): 628−646
62. Yang L, Hou X, Xia B. A complete algorithm for automated discovering of a class of inequality-type theorems. Science in China, Ser F, 2001, 44: 33−49
63. Xu C, Shi Q, Cheng M. A global stereo vision method based on Wu-solver. In: Proceedings of GMICV'95. 1995, 198−205