Automated Geometric Reasoning: Dixon Resultants, Gröbner Bases, and Characteristic Sets

Deepak Kapur*

Institute for Programming and Logics
Department of Computer Science
State University of New York
Albany, NY 12222
kapur@cs.albany.edu

Abstract. Three different methods for automated geometry theorem proving—a generalized version of Dixon resultants, Gröbner bases and characteristic sets—are reviewed. The main focus is, however, on the use of the generalized Dixon resultant formulation for solving geometric problems and determining geometric quantities.

1 Introduction

Developing computer programs to prove geometry theorems attracted a great deal of attention in Artificial Intelligence research in its early days. The influential work of Gelernter, in particular, led to a number of key concepts and ideas in automated reasoning which are still used in many artificial intelligence systems employing reasoning. For geometry theorem proving, Gelernter's approach, however, had limited success as it could prove only simple plane geometry theorems whose statements involved lines and angles, and relations among lines and angles [14]. It is difficult to single out any theorem proved by Gelernter's program which could not be easily proved by humans.

It has been well-known that geometry theorem proving falls within the theory of real closed fields for which Tarski gave a decision procedure [55]. But algebraic methods were not successful in proving geometry theorems even with an implementation of a more efficient decision procedure due to Collins [1] for Tarski's geometry. The situation changed dramatically in the late 70's and early 80's when Wu Wen-tsün [62, 63] proposed an algebraic method based on Ritt's characteristic set computation [50] for proving a restricted set of geometry theorems.

For geometry problems involving incidence, congruence and parallelism relations (and not involving the betweenness relations), Wu showed that if a geometric configuration is specified as a finite set of hypotheses translated into polynomials, then conclusions about these relations also expressed as polynomials can be decided. Hypotheses can be transformed into a triangular form, which is then used to check whether the conclusions reduce to 0 using the triangular

* Partially supported by the National Science Foundation Grant no. CCR-9622860.

form. This method can be easily implemented, and can be used for proving many geometry theorems including many nontrivial theorems which even humans do not find easy to prove. Wu's approach and its variations have been experimented by many researchers including Wu himself [63, 64], his students Wang and Gao [61], Chou [4, 5], and Ko and Hussain [41]. A particular mention must be made of Chou's work and his system which has proved nearly 500 geometry theorems [5].

Impressive results achieved using Wu's method sparked a great deal of interest in automatic geometry theorem proving. In particular, Wu's work encouraged researchers to investigate algebraic methods other than the ones based on characteristic set computation for geometry theorem proving. Kapur [28], Chou and Schelter [13], and Kutzler and Stifter [42] independently demonstrated the use of Gröbner basis algorithms for geometry theorem proving.

Wu observed that a good heuristic for studying many Euclidean geometry problems not involving the betweenness relation is to consider these problems over an algebraically closed fields such as the complex numbers, instead of over the reals.[2] Consequently, algorithms for analyzing the zeros of a polynomial set over algebraically closed fields developed in algebraic geometry could be fruitfully used. Wu also demonstrated that Ritt's characteristic set algorithm could be used to prove nontrivial theorems including Morley's theorem and Steiner's theorem [62].

Because of this remarkable but simple insight of Wu, the field of geometry theorem proving has been flourishing with researchers, particularly Chou, Gao and Zhang, developing and experimenting with different heuristics and methods for proving hundreds of theorems in plane and solid Euclidean geometries, as well as in other geometries. Powerful theorem provers have been developed over the last 10 years which have been shown to automatically find proofs of theorems considered difficult by humans as well as discover new geometry theorems. Further, some of these provers can produce succinct, elegant and understandable proofs.

This paper is an attempt to give an overview of my group's research in geometry theorem proving since 1984. The use of Gröbner basis, characteristic set and Dixon resultant methods for algebraic and geometric reasoning as investigated by us is reviewed. In the next section, two commonly-used and related formulations of geometry conjectures are discussed. This is followed by a discussion of two different approaches towards automated geometry theorem proving – the direct approach proposed by Wu and the refutational approach proposed by me. Section 4 reviews three different algebraic methods we have used for geometry theorem proving. Our most recent work using the generalized Dixon resultant formulation is first discussed. The proof by example approach of Hong, Zhang, Yang and Deng is discussed using the Dixon resultants, which can serve as a good heuristic. This is followed by a brief mention of the use of the Gröbner basis method, the first method tried by our group in 1985 lead-

[2] For a geometry theorem involving incidence and parallelism which is true for the reals but not in the algebraically closed field, the reader may consult [16].

ing to the development of the theorem prover *GEometer*. Finally, the use of the characteristic set method investigated in my former student Hoi Wan's M.S. thesis is reviewed. The discussion in this section is focussed mostly on my group's research; other researchers' work is mentioned only briefly, mostly for completeness and comparison purposes. Section 5 discusses the use of Dixon resultants for computing geometric quantities. Section 6 is a brief review of other geometric reasoning problems including implicitization and computing invariants. Section 7 is a mention of a few new promising approaches towards geometry theorem proving which have been successfully investigated by other researchers. Section 8 includes a few comments on techniques for deducing subsidiary conditions and additional hypotheses in case a given geometric conjecture is not valid. These techniques are especially useful for discovering new theorems.

2 Formulating Geometry Problems

Different kinds of geometry problems arise in various application domains. This ranges from proving geometry theorems, computing formulas and quantities, determining whether a geometric construction can be done with a ruler and compass, implicitization of curves and surfaces, parameterization, invariants of geometric configuration with respect to a group of transformation, etc. In this paper, we will briefly review a few such problems, discussing how our research group has attempted to solve these problems over the last 10 years or so. Our experience suggests that no single method is uniformly good for different problems. Instead, different methods must be used for different problems, which calls for a need for developing a geometry reasoning system that supports a variety of elimination algorithms including the characteristic set, Gröbner basis and resultant methods [30].

In most of the recent research for geometry theorem proving, two different but related formulations for geometry statements have been considered. In both formulations, a coordinate system is associated with a geometry configuration, and geometry statements are usually studied in an algebraic closed field, in particular the field of complex numbers.[3]

2.1 Generic Formulation

In the first formulation, henceforth called the *generic formulation*, which was used in Wu's original paper [62, 63], a geometry statement is specified as a finite set of hypotheses translated into polynomials of a finite set of *dependent* and *independent* variables (independent variables are also called *parameters*). A conclusion, which is also a polynomial, is given separately. The objective is to decide whether the conclusion follows from the hypotheses *generically*. If the

[3] In that sense, these approaches are restrictive and serve only as a heuristic for deciding formulas in the quantifier-free subset of Tarski's geometry. For a way to get around this, and an approach for geometry theorem proving over the real closed field, see [20].

answer is yes, then determine also the degenerate cases, if any, which must be ruled out. If the answer is no, then decide a weaker statement, i.e., whether the conclusion is valid for at least one (or more) of the generic configurations specified by the hypotheses, and if so, determine the configurations for which the conclusion is valid as well as list the associated degenerate cases which have to be ruled out. In case the conclusion does not follow at all (it is not valid for any geometric configuration specified by the hypotheses), then declare the conclusion to be false.

Nondegenerate (also called *subsidiary*) conditions such as points being distinct, three distinct points being not collinear, line segments of nonzero lengths, circles of nonzero radii, etc., are left out from this formulation. Instead, they are discovered in case the conclusion follows generically from the hypotheses.

2.2 Logical Formulation

The second formulation, henceforth called the *logical formulation*, is based on a traditional approach taken in developing decision procedures for theories. In this formulation, a geometry statement, which is usually a finite set of hypotheses implying a conclusion, is given and the objective is to decide whether the statement as it is (i.e., without adding any other conditions) is valid. In contrast to the generic formulation above, the hypotheses in this formulation usually include relations ruling out degenerate cases (such as distinctness, noncollinearity, etc.) Variables do not have to be classified into two disjoint categories of parameters (independent) and dependent variables. This formulation was first used by me in [28].

Besides the above two formulations of geometry theorems, many other different geometry problems arise in many application domains. Many of these problems can be formulated as elimination problems. For example, as we shall see later, the problem of determining an implicit representation of a surface from a parameterization representation can be specified as an elimination problem. The problems of determining certain geometric quantities, e.g. Heron's formula – the area of a triangle in terms of its three sides, Brahmagupta's formula on the area of a cyclic quadrilateral in terms of its sides, the maximum volume of a tetrahedron, can also be formulated as elimination problems.

In the first part of the paper, we discuss theorem proving in Euclidean geometry using the generic and logical formulations. Later, we briefly review other geometric reasoning problems.

3 Geometry Theorem Proving: Direct and Refutational Approaches

There have been quite a few approaches proposed for automating geometry theorem proving using the algebraic formulation of geometry problems, prominent about them being the *direct* approach proposed by Wu [62, 64], and the *refutational* approach proposed by Kapur [28]. Below, we briefly review the direct and refutational approaches.

3.1 Parallelogram Example

Let $\mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$ be a polynomial ring over the rationals with variables (indeterminates) $u_1, \cdots, u_k$, $x_1, \cdots, x_l$. Whenever needed, $u_1, \cdots, u_k$ are considered as independent variables (parameters) and $x_1, \cdots, x_l$ as dependent variables; further, we assume a total ordering $x_l > \cdots > x_1 > u_k > \cdots > u_1$.

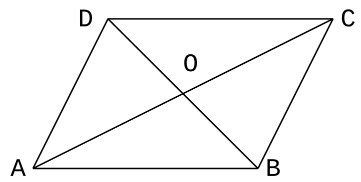

Fig. 1. Midpoint of diagonals in a parallelogram.

As a running example, consider a simple geometry theorem about parallelograms. This example is simple enough that most calculations can even be done by hand to get insight into various methods, and at the same time, the example is quite revealing. Let $ABCD$ be a parallelogram shown in Figure 1; prove that the intersection of the diagonals is the midpoint of a diagonal. The coordinate system chosen is: $A = (0, 0), B = (u_1, 0), C = (u_2, u_3), D = (x_2, x_1), O = (x_3, x_4)$. The hypotheses in polynomial form are:

1. $x_1 - u_3 = 0$	AB is parallel to CD.
2. $x_1(u_2 - u_1) - x_2 u_3 = 0$	BC is parallel to AD.
3. $x_4(x_2 - u_1) - x_1(x_3 - u_1) = 0$	B, O, and D are collinear.
4. $x_3 u_3 - x_4 u_2 = 0$	A, O, and C are collinear.
5. $u_1 \neq 0$	A and B are distinct points.
6. $u_3 \neq 0$	A, B, and C are not collinear.

The conclusion is: 7. $x_3^2 + x_4^2 = (u_2 - x_3)^2 + (u_3 - x_4)^2$, i.e., $|AO|^2 = |OC|^2$.

In the above specification, u_1, u_2, u_3 are independent variables (or parameters), and x_1, x_2, x_3, x_4 are dependent variables.

3.2 Direct Approach

The direct approach for geometry theorem proving, originally in Wu's papers [62, 63, 64, 66], consists of two parts. The hypotheses consisting of polynomial equations are first processed and brought in a *standard* form. Wu and others following his approach used a triangular form, called a *characteristic* set, a concept due to Ritt [50], as well as a finite family of characteristic sets. Chou and Schelter as well as Kutzler and Stifter used a Gröbner basis as a standard form. In the second step, using this standard form, it is decided whether the conclusion follows from the hypotheses. While making this check, degenerate conditions, if any, that must be ruled out, are determined.

For instance, in the parallelogram example, hypotheses 1, 2, 3 and 4 are brought into a standard form. Hypotheses 5 and 6 are not included while attempting a proof of the conclusion 7 using the direct approach; instead, they can be derived.

For computing a characteristic set or a Gröbner basis from the hypotheses, variables appearing in the hypotheses must be classified into independent and dependent variables. This is so because computations are done over the field of rational functions with independent variables as transcendentals. For checking whether a conclusion follows from the hypotheses, any polynomials in independent variables appearing in the denominators of coefficients or as initials of polynomials used in simplification of the conclusion are used as expressing degenerate conditions since those polynomials becoming 0 must be ruled out. Some of these conditions may, however, be unnecessary for the conclusion to follow from the hypotheses.

The main idea is to ensure that the zero set of the conclusion contains the zero set of the hypotheses. Since the conclusion is only required to be *generically* true for the hypotheses, some of the zeros from the zero set of the hypotheses can be excluded insofar as they do not change the generic nature of the geometric problem. This can be ensured by disallowing certain values of independent parameters. For the parallelogram example, it can be assumed that the points A, B, C are not collinear, even if the hypotheses do not explicitly state that; the zeros of the hypotheses corresponding to the case when A, B, C are indeed collinear, do not have to be considered.

Many heuristics can be employed to perform a check for containment of the zero set of the hypotheses in the zero set of a conclusion. The variety defined by the hypotheses can be decomposed into components; the nature of the desired decomposition determines the effort involved. Full decomposition into irreducible components can be, in general, computationally quite expensive. See [56, 39, 5, 58] for such a discussion.

For the parallelogram example, a triangular form can be easily obtained using a characteristic set construction algorithm or a Gröbner basis algorithm (since the hypotheses are linear in the dependent variables). (See below a brief review of Gröbner basis and characteristic sets.) And, it can be easily checked that the conclusion indeed reduces to 0 with respect to the triangular form of the hypotheses.

3.3 Refutational Approach

The second approach discussed in [28] is *refutational*, similar to the resolution method for first-order theorem proving and other refutational methods for reasoning. The conclusion of a conjecture is negated, and the inconsistency (or unsatisfiability) of the negated conclusion and the hypotheses is decided over an algebraically closed field.

If a hypothesis is a polynomial inequation (e.g., 5 and 6 in the parallelogram example), it can be converted into a polynomial equation by introducing a new variable as demonstrated in [28]. By the following theorem proved in [28], the validity of a geometry conjecture is equivalent to checking whether a finite set of polynomial equations generated from the conjecture has a common solution in the field of complex numbers.

Theorem 1 ([28]): Given a quantifier-free formula

$$f = ((p_1 = 0 \wedge \cdots \wedge p_i = 0 \wedge s_1 \neq 0 \wedge \cdots \wedge s_j \neq 0) \Rightarrow c),$$

where $p_1, \cdots, p_i, s_1, \cdots, s_j, c \in \mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$. The conjecture f is valid over an algebraically closed field containing $\mathbb{Q}$ if and only if $\{p_1 = 0, \cdots, p_i = 0, s_1 z_1 - 1 = 0, \cdots, s_j z_j - 1 = 0, cz - 1 = 0\}$ has no solution over the algebraically closed field, where $z, z_1, \cdots, z_j$ are new variables.

For the parallelogram example, the last two hypotheses above can be converted into equations using new variables z_1 and z_2 to give:

$$5'.\ u_1 z_1 - 1 = 0, \quad \text{and} \quad 6.'\ u_3 z_2 - 1 = 0,$$

respectively. The negated conclusion can also be translated to

$$7'.\ z((x_3^2 + x_4^2) - ((u_2 - x_3)^2 + (u_3 - x_4)^2)) - 1 = 0.$$

Checking whether a set of polynomial equations has no common solution in an algebraically closed field can be done by the Gröbner basis or the characteristic set construction, or even using other elimination methods including Dixon resultants.

The number of new variables in the above translation can be reduced to a single variable by combining all the subsidiary conditions together with the negated conclusion. For the above quantifier-free formula f, it thus suffices to require that $\{p_1 = 0, \cdots, p_i = 0, s_1 \cdots s_j cz - 1 = 0\}$ has no solution. Even though the complexity of all the elimination methods grows with the number of variables to be eliminated, we have often found that the Gröbner basis method as well as the characteristic set method work better for many examples when subsidiary conditions and conclusion are separated in the translation using new variables. The Dixon resultant method, of course, work much better with fewer variables. However, the optimized translation using a single extra variable does not seem to help since some of the subsidiary conditions reappear as extraneous factors in a projection operator computed by the Dixon resultant method. Unless these extraneous factors can be explicitly identified, it becomes difficult to discover subsidiary conditions or to check whether the needed subsidiary conditions have been identified.

Generation of Subsidiary Conditions: The refutational approach can also be used for deducing subsidiary conditions when a geometry theorem proving problem is given in generic formulation, as shown in [28]. The hypotheses and the negated conclusion are transformed together to a standard form to see whether the conclusion logically follows from the hypotheses. If yes, then the method terminates affirmatively. If not, then information about additional subsidiary conditions needed, under which the hypotheses logically imply the conclusion, can be extracted from the standard form. The following theorem in [28] serves as the theoretical basis of the method.

Theorem 2 ([28]): Given a quantifier-free formula

$$f = ((p_1 = 0 \wedge \cdots \wedge p_i = 0) \Rightarrow c),$$

where $p_1, \cdots, p_i, c \in \mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$ such that f is not valid over an algebraically closed field containing $\mathbb{Q}$. There is a nonzero polynomial s in the parameters $u_1, \cdots u_k$, such that $f = ((p_1 = 0 \wedge \cdots \wedge p_i = 0 \wedge s \neq 0) \Rightarrow c)$ is valid over an algebraically closed field containing $\mathbb{Q}$ if and only if the elimination ideal of $(p_1, \cdots p_i, cz - 1)$ in the parameters $u_1, \cdots, u_k$, i.e., $(p_1, \cdots p_i, cz - 1) \cap \mathbb{Q}[u_1, \cdots, u_k]$, is different from 0.

The selection of a polynomial from the elimination ideal to serve as a subsidiary condition is an interesting research problem. If the elimination ideal is principal, its unique generator can be a good candidate. Otherwise, a polynomial(s) with a geometric meaning has to be selected. Factoring polynomials in the elimination ideal can lead to identifying simpler subsidiary conditions corresponding to some of the factors. In a later section, we discuss this issue in more detail.

4 Dixon Resultants, Gröbner Bases, and Characteristic Sets

In this section, the generalized Dixon resultant formulation as developed in [35, 38] is first reviewed. It is shown how Dixon resultants can be used to implement the refutational approach to geometry theorem proving. This is followed by a brief review of Gröbner basis and characteristic set methods to implement the direct as well as refutational approaches for geometry theorem proving. For more details, about Dixon resultants, Gröbner basis and characteristic set methods, the reader may consult [31, 30]. A detailed example illustrating the use of Dixon resultants is given later in a subsection on implicitization. It is recommended that the reader read the next subsection along with the subsection on implicitization.

4.1 Dixon Resultants

Let $X = \{x_1, \ldots, x_n\}$ be a set of n variables. Let $P = \{p_1, \cdots, p_{n+1}\}$ be a set of $n + 1$ polynomials in X. Unless otherwise stated, by a polynomial system, we will mean this set of $n + 1$ polynomials in n variables, X. The coefficients of the polynomials in P are assumed to be polynomials from $\mathbb{Q}[U]$, where U is a set of parameters, say $u_1, \cdots, u_k$.

Let I be the ideal generated by P in $\mathbb{Q}[U, X]$. All polynomials in the ideal $J = I \cap \mathbb{Q}[U]$, the elimination ideal of I over U, are known as the **projection**

operators of P with respect to X. Clearly, projection operators of P vanish at all those specializations of A from the algebraic closure, $\bar{\mathbb{Q}}$, of $\mathbb{Q}$, for which P has a common solution in $\bar{\mathbb{Q}}^n$. Note that 0 is trivially always a projection operator of any P. The **resultant** of P is defined to be the unique (up to a scalar multiple) generator of the ideal J. Note that the resultant of P is 0 *if and only if* P has no nonzero projection operator. Also, a nonzero resultant of P must divide all projection operators of P. Finally, any factor ($\in \mathbb{Q}[U]$) of a projection operator of P which is not the resultant of P, is called an **extraneous factor** in that projection operator.

In [19], Dixon proposed a generalization based on Cayley's reformulation of Bezout's resultant for eliminating a single variable from two polynomials.[4] Dixon used it for simultaneously eliminating two variables from three generic bi-degree polynomials, and commented that the generalization would work for a generic n-degree polynomial system as well. A polynomial system P is called **generic** n**-degree** if there exist nonnegative integers $d_1, \ldots, d_n$,

$$p_j = \sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{j,i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \text{ for } 1 \leq j \leq n+1,$$

where each coefficient $a_{j,i_1,\ldots,i_n}$ is a distinct indeterminate. $(d_1, \ldots, d_n)$ is known as their n-degree.

Dixon's method, as discussed in [19], does not work for an arbitrary polynomial system. In fact, it almost always fails if the polynomial system is not generic and even if generic, but of not n-degree.

In [35], we developed a generalization of Dixon's resultant formulation so that it works for a family of polynomial systems that is much larger than systems of generic n-degree polynomials. This method has been experimentally found to be superior in performance on a wide variety of examples, in comparison with other elimination methods including Macaulay resultants, sparse resultants [21], the characteristic set construction, and the Gröbner basis construction. The method takes less time, less space, as well as the extraneous factors seem to be fewer (except in the case of the Gröbner basis method which gives the exact resultant) [38, 37]. Recently, we have also been able to show that if the polynomial system consists of polynomials with the same set of terms (an **unmixed** system), the Dixon formulation, in fact, implicitly exploits the sparse structure of the polynomial system, i.e., its computational complexity is governed by the Newton polytope of the unmixed system, not by the Bezout bound [36].

Below, we first briefly review the generalized Dixon formulation for computing a projection operator of P. From now on, by a projection operator, we mean the projection operator as computed by the extended Dixon resultant formulation. Later, we discuss its application to geometric reasoning.

Let $\bar{X}$ be the set of n new variables $\{\bar{x}_1, \ldots, \bar{x}_n\}$. The **Cancellation matrix**

[4] See [30] for more historical details.

C_P of P is defined to be the following $(n+1) \times (n+1)$ matrix:

$$C_P = \begin{bmatrix} p_1(x_1, x_2, \ldots, x_n) & \cdots & p_{n+1}(x_1, x_2, \ldots, x_n) \\ p_1(\bar{x}_1, x_2, \ldots, x_n) & \cdots & p_{n+1}(\bar{x}_1, x_2, \ldots, x_n) \\ p_1(\bar{x}_1, \bar{x}_2, \ldots, x_n) & \cdots & p_{n+1}(\bar{x}_1, \bar{x}_2, \ldots, x_n) \\ \vdots & \cdots & \vdots \\ p_1(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) & \cdots & p_{n+1}(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \end{bmatrix},$$

where $p_i(\bar{x}_1, \cdots, \bar{x}_k, x_{k+1}, \ldots, x_n)$ stands for uniformly replacing x_j by $\bar{x}_j$ for all $1 \leq j \leq k \leq n$ in p_i.

Since for all $1 \leq i \leq n$, $(x_i - \bar{x}_i)$ is a zero of $|C_P|$, $\prod_{i=1}^{n}(x_i - \bar{x}_i)$ divides $|C_P|$. The **Dixon polynomial** δ_P of P is defined as:

$$\delta_P = \frac{|C_P|}{\prod_{i=1}^{n}(x_i - \bar{x}_i)}.$$

Dixon Matrix and Rank Submatrix Computation: Let V be a column vector of all monomials in X which appear in δ_P, when δ_P is viewed as a polynomial in X. Similarly, let W be a row vector of all monomials in $\bar{X}$ which appear in δ_P, when δ_P is viewed as a polynomial in $\bar{X}$. The **Dixon matrix**, D_P, of P is defined to be the matrix for which $\delta_P = V\, D_P\, W$. The entries of the Dixon matrix of P are polynomials in U.

If the Dixon matrix is square and non-singular, then its determinant is a projection operator of P. The vanishing of the projection operator of P is a necessary condition for the system P to have a common solution.

It is possible for the Dixon matrix to be rectangular, or even if it is square, to be singular. In that case, the *rank submatrix construction*, *RSC*, described in [35] can be used to extract identically non-zero projection operators from D_P. The construction works as follows: if the removal of the column labeled with the monomial 1 reduces the rank of the Dixon matrix, then any maximal minor of the Dixon matrix gives a projection operator. Often, there can be constraints on the variables being eliminated, e.g. variables being nonzero. Then, if the removal of any column from the Dixon matrix, that is labeled by a monomial constrained to be nonzero, leads to a smaller rank matrix, then any maximal minor of the Dixon matrix produces a projection operator.

This method has been successfully used to compute projection operators for elimination problems arising in many different application domains; the reader may consult [35, 38, 52] for details.

Below, we first discuss how the generalized Dixon resultant formulation can be used for geometry theorem proving. Later, we discuss the application of the method for other geometric reasoning problems.

Refutational Approach: In [34], we reported on our preliminary investigation on the use of the generalized Dixon method to implement the refutational approach for geometry theorem proving. This method has been further developed and experimented with. Below, we discuss this method.

As discussed earlier, in the generic formulation of a geometry conjecture, there are as many hypotheses as dependent variables. The negated conclusion introduces an extra variable, say z, which must be nonzero. The generalized Dixon formulation is used to eliminate the dependent variables from the hypotheses and the negated conclusion. The resulting projection operator includes factors expressing conditions under which the hypotheses and the negated conclusion have common zeros.

Theorem 3: Given a quantifier-free formula $f = ((p_1 = 0 \wedge \cdots \wedge p_l = 0) \Rightarrow c)$, where $p_1, \cdots, p_l, c \in \mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$, and $u_1, \cdots, u_k$ are independent parameters. If the projection operator as computed by the generalized Dixon resultant of $\{p_1, \cdots, p_l, cz - 1\}$ obtained by eliminating $x_1, \cdots, x_l$ is of the form cz^k, where c is a rational number, then f is valid over an algebraically closed field containing $\mathbb{Q}$.

A projection operator being cz^k, where c is a number and z is assumed to be nonzero, implies that the hypotheses and the negated conclusion do not share any common zero, so the conclusion follows from the hypotheses.

In general, a projection operator may have additional factors, some of which may even be extraneous. We have a more general version of the above theorem:

Theorem 4: Given a quantifier-free formula $f = ((p_1 = 0 \wedge \cdots \wedge p_l = 0) \Rightarrow c)$, where $p_1, \cdots, p_l, c \in \mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$, and $u_1, \cdots, u_k$ are independent parameters. If the projection operator as computed by the generalized Dixon resultant of $\{p_1, \cdots, p_l, cz - 1\}$ obtained by eliminating $x_1, \cdots, x_l$ is of the form $cz^k s_1^{k_1} \cdots s_j^{k_j}$, where $s_1, \cdots, s_j$ are polynomials in $u_1, \cdots, u_k$, then f is generically valid over an algebraically closed field containing $\mathbb{Q}$.

In addition to cz^k, which is nonzero, if the projection operator includes only polynomials in the independent parameters as the other factors, this means that the negated conclusion shares common zeros with the hypotheses only for certain values of the independent parameters. If those cases can be ruled out as subsidiary conditions, then the conclusion follows from the hypotheses under those subsidiary conditions. In other words, the conclusion generically follows from the hypotheses, much like the direct approach used in Wu's method. A factor in the independent parameters corresponds to the subsidiary conditions that must be ruled out.

For the parallelogram example, when the Dixon resultant method is tried on polynomials $1, 2, 3, 4$, and the negated conclusion $7'$ and variables x_1, x_2, x_3, x_4 are eliminated, a projection operator is:

$$8u_1 u_3^4 (u_2^2 + u_3^2)^2 z^2.$$

It can be thus declared that the conclusion generically follows from the hypotheses. The above polynomial must vanish on every common zero, if any, of the hypotheses and negated conclusion. It is clear that for the parallelogram to be non-degenerate, both u_1 and u_3 be nonzero. Further, $u_2^2 + u_3^2$ should be also nonzero, implying that the point C be distinct from A. (Note that u_3 being nonzero does not guarantee that $u_2^2 + u_3^2$ is nonzero over the field of complex numbers.)

The above method has been successfully tried on almost all examples discussed in [28, 39], including Simson's theorem, Pappus' theorem, Desargues' theorem, Gauss' theorem, nine point circle theorem. Our experiments suggested that the Dixon method compared much more favorably with the Gröbner basis method for deducing subsidiary conditions, but it is slower than the characteristic set method on problems that can be formulated using linear relations. Again like the characteristic set method, the Dixon method produced more subsidiary conditions than necessary. Some of these conditions may even correspond to extraneous factors present in a projection operator.

Logical Formulation: The generalized Dixon method was also tried on geometry statements expressed using the logical formulation in which the subsidiary conditions are included in the problem statement. For every subsidiary condition, a new variable is used to convert an inequation into an equation, and each of these new variables is assumed to be nonzero. All dependent variables and some of the independent parameters constrained by the subsidiary conditions are eliminated from the hypotheses, subsidiary conditions and the negated conclusion. If the projection operator is a polynomial in the new nonzero variables used to express negated conclusion and subsidiary conditions (z, z_1, z_2 for the parallelogram example, for instance), such that if these variables take nonzero values, then the projection operator is also nonzero, then the conjecture is valid; otherwise the conjecture is not valid. That would be the case if a projection operator is of the form $cz^k z_1^{k_1} \cdots z_j^{k_j}$, where $z, z_1, \cdots, z_j$ are the new nonzero variables.

Let us illustrate this on the parallelogram example again. When variables $x_1, x_2, x_3, x_4, u_1, u_3$ are eliminated from polynomials $1, 2, 3, 4, 5', 6'$ and $7'$, the generalized Dixon resultant gives:

$$32u_2^6(z_2^2u_2^2 + 1)z_1^7 z_2^4 z^7$$

as the projection operator. So, it cannot be said that the conclusion follows the hypotheses and the two subsidiary conditions. If we add an additional subsidiary condition

$$8'. \;\; u_2 * z_3 - 1 = 0,$$

to stand for $u_2 \neq 0$, and then eliminate u_2 as well, the resulting projection operator is:

$$128(z_2^2 + z_3^2)z_1^{10} z_2^7 z_3^9 z^{10},$$

implying that the conclusion still does not follow from the hypotheses under the subsidiary conditions of $u_1, u_2, u_3 \neq 0$. However if instead of $8'$, the subsidiary condition:

$$8''. \;\; (u_2^2 + u_3^2) * z_3 - 1 = 0,$$

the projection operator produced by the generalized Dixon resultant is:

$$65536 z_1^{14} z_2^{12} z_3^{14} z^{14},$$

thus implying that the modified conjecture is valid.

As the above example illustrates, even for a geometry conjecture given in logical formulation that does not turn out to be valid, it may be possible to extract additional degenerate conditions from the projection operator which must be ruled out to make the conjecture true.

Our experiments on plane Euclidean geometry theorems including Simson's theorem, Butterfly theorem, Ptolemy's theorem, suggest that the Dixon method works reasonably well on geometry conjecture in the logical formulation, but it is much slower than the Gröbner basis method as well as the characteristic set method for detecting inconsistency. This is so because more variables (including both dependent and some of the independent variables) must be eliminated if a logical formulation is used. The complexity of the Dixon resultant method is determined by the volume of the Newton polytope, which is dependent upon the number of variables to be eliminated.

A main limitation in the use of the generalized Dixon resultants for geometry theorem proving is due to the extraneous factors generated when the projection operator is computed. It becomes necessary to distinguish between extraneous factors and the subsidiary conditions relevant for the configuration. That is why the statements of the above theorems are only in one direction. Extraneous factors are, however, not peculiar to Dixon resultants. They arise in all other elimination methods based on multivariate resultants - successive applications of Sylvester resultants, Macaulay resultants or sparse resultants. In fact, we have experimentally observed that the generalized Dixon formulation produces the least extraneous factors. For more details on extraneous factors in the projection operator computed by the generalized Dixon resultant formulation, refer to [37].

For the parallelogram example, instead of $5', 6', 8''$ and $7'$, subsidiary conditions can be combined together with the negated conclusion to have a single polynomial:

$$7''.\ \ u_1 u_3 (u_2^2 + u_3^2)((x_3^2 + x_4^2) - ((u_2 - x_3)^2 + (u_3 - x_4)^2))z - 1 = 0.$$

If the Dixon resultant method is attempted on $1, 2, 3, 4$ and $7''$, the resulting projection operator is:

$$8 u_3^6 u_1^3 (u_2^2 + u3^2)^4 z^2,$$

still including the subsidiary conditions as extraneous factors.

Proving by Example: In [34], we also reported the use of the Dixon resultants on a generic formulation of a geometry conjecture, using a method of theorem proving by example. The Dixon resultant formulation performed very well. Geometry conjectures could be proved in a few milliseconds since the Dixon matrix entries are mostly numbers when the method of theorem proving by example is used. And, the rank submatrix computation can be performed very quickly in that case.

To our knowledge, Zhang, Yang and Deng were the first one to develop a geometry prover based on the idea of theorem proving by example [72] using the characteristic set construction. Their approach is based on an idea proposed by Hong [26]; see also [57]. For a generic formulation of a geometry conjecture, randomly select a specific geometric configuration by choosing particular values of independent parameters, and use the configuration for proving a theorem. If the conclusion indeed follows from the hypotheses, then argue based on genericity and randomness, that the theorem is generically true. Many instances of the conjecture can be tried in parallel. In [70, 72], Zhang et. al. showed how many interesting and nontrivial geometric theorems could be easily proved even on a 386 personal computer in a few seconds, e.g., Thebault's theorem, Morley trisector theorem, etc.

Using this approach of proving by example, Rege [48] has implemented a geometry prover employing Sylvester resultants and Wu's characteristic set method.

4.2 Gröbner Basis Construction

A Gröbner basis of a set of polynomials is a special basis of their ideal which has the property that (i) every polynomial in the ideal *reduces* to 0 with respect to the basis, and (ii) every polynomial has a unique normal form (canonical form) with respect to the basis. The concept of a Gröbner basis of an ideal was introduced by Buchberger in [3], where he also gave an algorithm for computing a Gröbner basis of a polynomial ideal from its finite basis in the case when the coefficients of polynomials are from a field such as the rationals. Since then, Gröbner bases and algorithms for computing them have been extensively studied, analyzed and generalized [2].

There are two key ideas used in the construction of a Gröbner basis of an ideal specified by a finite set of polynomials: (i) reduction of a polynomial by another polynomial such that the reduction process always terminates, and (ii) inclusion of new polynomials from the ideal into its basis from a pair of polynomials already in the basis using *S-polynomial* construction (also called *critical pair* construction in the rewriting literature). First, an admissible term ordering on terms is selected; some commonly used orderings are degree, lexicographic and reverse lexicographic, as well as block orderings. Terms in a polynomial are sorted with respect to the term ordering. Simplification of a polynomial by another polynomial is done based on whether the first polynomial has terms that are multiple of the highest (leading) term of the second polynomial. If yes, the appropriate multiple of the second polynomial is subtracted from the first polynomial. If not, the first polynomial cannot be reduced by the second polynomial. For S-polynomial computation, the smallest term, say t, that is a multiple of the highest terms of the two polynomials (but not a product) is used to determine the terms with which each polynomial must be multiplied; the two resulting polynomials are subtracted to get a new polynomial whose leading term is smaller than t.

This process of simplification of a polynomial by another polynomial as well as generation of new polynomials from the ideal is continued until it is no more possible to generate new polynomials in the basis. And, this process is guaranteed to stop because of Hilbert's basis theorem. The result is a Gröbner basis of the input ideal.

Refutational Approach: In [28, 29], a Gröbner basis algorithm was used to implement the refutational approach for proving geometry theorems. To determine whether a set of polynomial equations has a common solution, the ideal of the polynomials must be nontrivial, i.e., different from 1, and this can be checked by computing a Gröbner basis of the ideal.

For the parallelogram example, the Gröbner basis algorithm on $1, 2, 3, 4, 5', 6'$, and $7'$ results in 1 as the Gröbner basis implying that the conjecture is true.

In these papers, it was also shown that in case the hypotheses do not imply the conclusion, from a Gröbner basis of the hypotheses and the negated conclusion, subsidiary conditions under which the hypotheses imply the conclusion, can be extracted.

For both problems, it is not necessary to classify variables into parameters and dependent variables. For finding subsidiary conditions, it is however useful to specify the variables in which such conditions must be expressed. In that case, as stated above, a Gröbner basis of the elimination ideal in the parameters can be computed from the hypotheses and the negated conclusion. The smallest polynomial in a Gröbner basis of an elimination ideal is often a good candidate for expressing the simplest subsidiary conditions. This method of deducing subsidiary conditions appears to yield the weakest subsidiary condition under which the hypotheses imply the conclusion, in contrast to the characteristic set method and the resultant method.

For the parallelogram example, the Gröbner basis method, when attempted on $1, 2, 3, 4$ and $7'$, gives $u_1 \neq 0, u_3 \neq 0$ as the subsidiary conditions, whereas the Dixon resultant method as well as the characteristic set method discussed below produce subsidiary conditions in addition to these two conditions which are sufficient.

In [28, 29], many examples are discussed and details about implementing the refutational approach are provided. A theorem prover, *GEometer* based on these ideas is discussed in [18, 15]

Direct Approach: In [13] as well as in [42], the direct approach is employed using a Gröbner basis algorithm. A Gröbner basis of the hypotheses polynomials is first computed without taking into account the conclusion. This computation is done viewing polynomials as multivariate polynomials in the dependent variables with their coefficients being polynomials in the independent parameters. In other words, the computation is performed over the field of rational functions expressed in terms of parameters. In the method used by [13, 42], it is thus essential to classify the variables in the geometry problem formulation into dependent variables and independent parameters.

As stated before, once a Gröbner basis is computed from the hypotheses, the conclusion is simplified with respect to the Gröbner basis. If the conclusion simplifies to 0 (i.e., the conclusion polynomial is in the ideal of the hypotheses polynomials), then it follows from the hypotheses under the assumption that the leading coefficients of polynomials of the Gröbner basis used in the simplification are non-zero. Those leading coefficients, which are polynomials in the independent variables, not being zero are the subsidiary conditions.

Strictly speaking, the membership of the conclusion polynomial should be checked in the radical ideal of the hypotheses polynomials. However, for most geometry problems, checking whether the conclusion polynomial is in the ideal of the hypotheses turns out to be a fairly effective heuristic. For more details, the reader can refer to [13, 42].

The subsidiary conditions produced by this method often turn out to be more complicated than the ones found using the refutational approach discussed in the previous subsection. Further, some of these subsidiary conditions can be unnecessary.

4.3 Characteristic Set Construction

The key primitive operation used in characteristic set computation is that of *pseudo-division* of a multivariate polynomial by another multivariate polynomial (see [40] for more details about pseudo-division). Pseudo-division is different from the reduction used in a Gröbner basis computation. Firstly, the recursive representation of polynomials is used: a multivariate polynomial is considered as a univariate polynomial in its highest variable. Division is performed between two univariate polynomials, but the initial of the divisor, which is its leading coefficient when the divisor is viewed as a univariate polynomial, can be used to multiply the dividend. Reduction is defined using pseudo-division.

A polynomial p is *reduced with respect to* another polynomial q if (a) the highest variable, say x_i, of p is $<$ the highest variable, say x_j, of q, or (b) the degree of x_j in q is $>$ the degree of x_j in p. If p is not reduced with respect to q, then p *reduces* to r by pseudo-dividing by q, i.e., by multiplying p with the *lowest* power, say e, of the initial I_q of q and dividing the result by q such that

$$I_q^e p = sq + r,$$

where r is reduced with respect to q.

It is easy to see that (i) the pseudo-remainder r is in the ideal of p and q, (ii) the common zeros of p and q are also the zeros of remainder r, and (iii) if $r = 0$, then the common zeros of p and q are the same as the zeros of q insofar as they are not the zeros of I, the initial of q. These properties are crucial in the proof of Ritt's theorem below.

The following definition and theorem from [64] are attributed to Ritt and serves as the basis of the characteristic set construction:

Definition: Given a finite set Σ of polynomials in $\mathbb{Q}[u_1, \cdots, u_k, x_1, \cdots, x_l]$, a *characteristic set* Φ of Σ is defined to be either (i) $\{g_1\}$, where g_1 is a polynomial in $\mathbb{Q}[u_1, \cdots, u_k]$ or (ii) $\{g_1, \cdots, g_l\}$, where g_1 is a polynomial in $\mathbb{Q}[u_1, \cdots, u_k, x_1]$ with initial I_1, g_2 is a polynomial in $\mathbb{Q}[u_1, \cdots, u_k, x_1, x_2]$, with initial I_2, $\cdots$, g_l is a polynomial in $Q[u_1, \cdots, u_k, x_1, \cdots, x_l]$ with initial I_l, such that (a) any zero of Σ is a zero of Φ, and (b) any zero of Φ that is not a zero of any of the initials I_i is a zero of Σ.

In the above definition, $u_1, \cdots, u_k$ are the independent parameters, and $x_1, \cdots, x_l$ are the dependent variables. In contrast to a Gröbner basis, a characteristic set includes at most one polynomial for every dependent variable.

Theorem 5 (Ritt): Given a finite set Σ of polynomials in $x_l, \cdots, x_1, u_1, \cdots, u_k$, there is an algorithm which computes a *characteristic set* Φ of Σ.

An algorithm for computing a characteristic set is given in [64]; this algorithm is based on the description of how a characteristic set can be constructed in Ritt's book. Since then, many modifications and heuristics to improve the performance of this algorithm have been proposed; an interested reader may consult [64, 5, 6, 39].

Even though the characteristic set of Σ is small, intermediate computations can swell, leading to large polynomial sets. The worst case complexity of computing a characteristic set is doubly exponential in the degree of the input polynomials.

Wu had a remarkable insight into the theory of characteristic sets. Wu relaxed a main requirement from Ritt's definition of a characteristic set, particularly, that every polynomial in an ideal need not have to be pseudo-divided to 0 with respect to its characteristic set. Wu demonstrated that without this property, a characteristic set can be computed much more easily, since there is no need to require a characteristic set to be **irreducible**. The modified definition works as a good heuristic for geometry theorem proving. For more details about the differences between Ritt's and Wu's definition of a characteristic set, the reader may consult [30].

Direct Approach: A characteristic set is first constructed from the hypotheses. Then the conclusion is pseudo-divided using the polynomials in the characteristic set. If the conclusion pseudo-divides to 0, then the conclusion generically follows from the hypotheses. The initials of the polynomials in the characteristic set used to pseudo-divide the conclusion to 0 correspond to the degenerate conditions which must be ruled out.

For the above parallelogram example, a characteristic set can be easily constructed from the hypotheses. Pseudo-division of hypothesis 3 by hypothesis 4 gives a remainder which serves as the polynomial introducing x_3, whereas hypotheses 1, 2 and 4 serve as introducing x_1, x_2, x_4 respectively. Using these polynomials. the conclusion pseudo-divides to 0, implying that the conclusion generically follows from the hypotheses.

In case a conclusion does not pseudo-divide to 0, then it cannot be declared that the conclusion does not generically follow from the hypotheses since Wu had relaxed one condition on his definition of a characteristic set. Instead, additional work must be done. The characteristic set must be checked for *irreducibility*; see [62] for a definition. It must be checked whether each polynomial included in the characteristic set factors over the extension field defined by the smaller polynomials in the characteristic set; this is an expensive computation. If yes, then the polynomial must be factored, and each factor must be considered separately, thus giving rise to a **family** of characteristic sets. Such decomposition corresponds to a possible ambiguity in the formulation of a geometric problem, giving rise to many geometric configurations, e.g., corresponding to in-circles and out-circles of a triangle, interior angles and exterior angles between two lines, etc [66].

The conclusion is pseudo-divided with respect to each characteristic set in a family of irreducible characteristic sets generated from the input hypotheses (which corresponds to all possible geometric configurations implied by the hypotheses). If the conclusion pseudo-divides to 0 in all cases, then again, the conclusion generically follows from the hypotheses. If the conclusion pseudo-divides to 0 for a subset of characteristic sets, then the conclusion follows from the hypotheses only for the corresponding geometric configurations. If the conclusion does not pseudo-divide to 0 in any case, then the conclusion does not follow from the hypotheses at all for any case.

The direct approach has been successfully used by Wu, Chou, Gao, and Wang to prove hundreds of geometry theorems, including many nontrivial theorems in Euclidean geometry such as Steiner's theorem, Morley's theorem, Thebault's theorem, as well as discover new theorems in Euclidean geometry. Chou's first book is an excellent source for the information about all the theorems proved using this method [5]. As the reader would notice, for proving most geometric theorems, factoring over extension fields is not needed; the heuristic of computing a characteristic set (a la Wu) from the hypotheses works well. In [5], an algorithm for factoring polynomials, in which the degree of variables does not exceed 2, over extension fields is developed. This algorithm has been used by Chou and his colleagues to prove nontrivial theorems including Thebault's theorem. An interested reader may also consult [69] where a different method that attempts to avoid factoring over extension fields is given; see also [59].

The direct approach has also been shown to work for other geometries including solid geometry, non-Euclidean geometry, as well as differential geometry.

Refutational Approach: In [56, 39], we showed how the characteristic set construction can also be employed to implement the refutational approach. It was shown that for many geometry problems, this method turns out to be superior in performance to the Gröbner basis method for the refutational approach. The following theorem serves as the basis of the refutational method for geometry theorem proving using the characteristic set construction.

Theorem 6: Given a finite set Σ of polynomials, if its characteristic set includes a constant, then Σ does not have a common zero.

The converse of the theorem does not hold; however, the following holds:

Theorem 7: Given a finite set Σ of polynomials, if its characteristic set Φ is irreducible and does not include a constant, then Σ has a common zero.

Much like the refutational approach implemented using the Gröbner basis method, to check the validity of a geometry conjecture, a characteristic set is computed from the hypotheses and the negated conclusion. If the characteristic set includes a constant, then the hypotheses and the negated conclusion do not have a common zero, implying that the conclusion indeed follows from the hypotheses. The method works on the generic as well as the logical formulations.

For the parallelogram problem, the characteristic set of $\{1, 2, 3, 4, 5', 6', 7'\}$ includes 1, implying the validity of the conjecture.

If the computed characteristic set does not include a constant, it does not mean that the hypotheses and the negated conclusion have common zeros. For example, consider $\{(x-1)^2 = 0, (x-1) \neq 0\}$ which clearly does not have a common zero. If we replace the inequation by an equation, we get

$$\Sigma = \{(x^2 - 2x + 1) = 0, (x-1)z - 1 = 0\}.$$

Under the ordering $z > x$, Σ is also a characteristic set. (However, under the ordering $x > z$, the characteristic set of Σ includes 1.)

There are a number of possibilities if a characteristic set computed from the hypotheses polynomials and the negated conclusion does not include a constant. (i) Φ is reducible and each of the irreducible characteristic sets of Φ includes a constant. (ii) Φ includes a polynomial in $u_1, \cdots, u_k$, which can serve as an additional subsidiary condition to modify the conjecture to make it valid, or (iii) the geometry conjecture is false.

In [39], an implementation of the above approach is discussed which is based on detecting a constant being included in a characteristic set. However, if case (ii) above is identified in which a polynomial in independent variables (whenever such variables are identified) is in a characteristic set, then it suggests that a subsidiary condition in the hypotheses may be missing. The original geometry statement is not a theorem but it can be modified to include the new subsidiary condition to obtain a geometry theorem.

For decomposing a reducible characteristic set, factorization over extension fields has to be performed. With reducibility check by factorization over extension field, the refutational method using characteristic set computation is complete just like the refutational method using the Gröbner basis method [62, 28].

For the refutational approach, the characteristic set method compares favorably with a method using Gröbner basis algorithm. This method was also tried for deducing subsidiary conditions. When no subsidiary conditions are given in a problem formulation, the method turned out to be quite slow. Moreover, the subsidiary conditions found were usually too complicated. In that sense, the method using the Gröbner basis algorithm is superior than this method. However, when an incomplete set of subsidiary conditions were provided, then this method could identify additional subsidiary conditions quickly. In [39], a table comparing different methods on a number of geometry conjectures is given, along with heuristics to improve the performance of the method as well as different algorithms for computing a characteristic set.

5 Computing Geometric Quantities

Many geometry problems involve computing an expression in terms of other parameters, for example, computing the area of a triangle in terms of its sides – Heron's formula, computing the area of a cyclic quadrilateral in terms of its sides, etc. Such problems can be easily formulated as variable elimination problems. For illustration, we discuss how to determine the area of a cyclic quadrilateral in terms of its sides, also known as Brahmagupta's formula.

Let A, B, C, D be four distinct points on a circle, forming a cyclic quadrilateral. Without any loss of generality, assume $A = (0,0), B = (a,0), C = (x_1, x_2), D = (x_3, x_4)$, with $|BC| = b$, $|CD| = c$, $|AD| = d$. Let k stand for the area of the cyclic quadrilateral $ABCD$. The objective is to compute k in terms of a, b, c, d, the lengths of the four sides of the cyclic quadrilateral. The hypotheses correspond to:

1. $x_2^2 + x_1^2 - 2ax_1 - b^2 + a^2$, $|BC| = b$.
2. $x_4^2 + x_3^2 + x_2^2 + x_1^2 - 2x_2x_4 - 2x_1x_3 - c^2$, $|CD| = c$.
3. $x_4^2 + x_3^2 - d^2$, $|AD| = d$.
4. $x_2x_4^2 + x_4(-x_2^2 - x_1^2 + ax_1) + x_2x_3^2 - ax_2x_3$, A, B, C, D are on a circle.
5. $x_1x_4 - x_2x_3 + ax_2 - 2k$, k is the area of the quadrilateral.

The area k in terms of a, b, c, d can be computed by eliminating x_1, x_2, x_3, x_4 from the above 5 polynomials. The projection operator computed by the Dixon resultants includes two factors:

$$k^2 - (\frac{p}{2} - a)(\frac{p}{2} - b)(\frac{p}{2} - c)(\frac{p}{2} - d), \text{and}$$

$$k^2 - \frac{p}{2}(\frac{p}{2} - a - b)(\frac{p}{2} - a - c)(\frac{p}{2} - a - d),$$

where $p = a + b + c + d$. These two factors correspond to the two possible areas depending upon where the fourth point D is in relation to the other three points of the cyclic quadrilateral.

In [65], Wu discussed the use of the characteristic set method for computing such geometric quantities, including Heron's formula, the volume of a tetrahedron in terms of the six edges, etc. Chou and Gao [7] also used the characteristic set method for deriving such geometric formulas. Using a variation of the characteristic set method, Gao and Wang [22] solved an open problem about determining the three sides of a triangle in terms of its angle bisectors. Their approach, however, took a long time and seemed quite inefficient. They reported that their method took about 7 hours of computation time on a SUN 4/470. Below, we review the use of the generalized Dixon resultant formulation for solving the same problem as well as a few other problems that involve computing geometric formulas.

5.1 Side in Terms of Bisectors

Below, we illustrate how determining the side of a triangle in terms of its bisectors can be done easily and much faster using the generalized Dixon's formulation. Here are the three polynomials relating the lengths of one internal bisector a_i, and two external bisectors a_e, b_e, in terms of the lengths of the three sides a, b, c. The objective is to eliminate b, c from these polynomials to get an expression for a in terms of a_i, a_e, b_e.

$$\begin{aligned}
p_1 &= a_i^2(b+c)^2 - cb(c+b-a)(c+b+a), \\
p_2 &= a_e^2(c-b)^2 - cb(a+b-c)(c-b+a), \\
p_3 &= b_e^2(c-a)^2 - ac(a+b-c)(c+b-a).
\end{aligned}$$

This problem can be completely solved using the Dixon resultant formulation in less than 6 minutes on a Sun Sparc10 using our interpolation software for computing determinants of matrices with polynomial entries [38, 52]. Even using Maple's linear algebra package, the problem can be done in less than 17 minutes on SUN 4 and less than 9 minutes on a Sparc10. This shows the advantage of using the generalized Dixon resultant formulation over the characteristic set method.

The resulting expression has 330 terms, the same as reported in [22]. It is a polynomial of degree 20 in a, implying using a result reported in Herstein's book that the triangle cannot be constructed using a compass and a rule from the bisectors.

5.2 Maximum Volume Tetrahedron

Here is another interesting problem for computing a geometric quantity taken from [23]. The objective is to compute the maximum volume that a tetrahedron can have in terms of the areas a, b, c, d of its faces. It has been shown in [23] that if there exist parameters x, y, z and w satisfying the following equations, then the tetrahedron is orthocentric and hence with maximum volume with those face areas.

$$\begin{aligned}
p_1 &= yz + zw + wy - a, \\
p_2 &= zx + xw + wz - b,
\end{aligned}$$

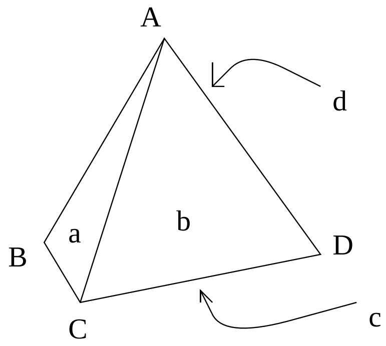

Fig. 2. Orthocentric Tetrahedron.

$$p_3 = wx + xy + yw - c,$$
$$p_4 = xy + yz + zx - d,$$
$$p_5 = 2(xyz + yzw + zwx + wxy) - 9\,T.$$

Polynomial p_5 above relates the square of the volume T to x, y, z, w.

Using the generalized Dixon resultants, the problem can be solved in 76 seconds using interpolation software, and 110 seconds using Maple's linear algebra package. This problem is not easy to do by other methods.

5.3 Gothic Architecture

It is not surprising to know that in the design of cathedrals, geometry was extensively used and there are nice geometric quantities arising there. As an example, consider the design of the top of a catholic church take from [54] (p. 266). There are a collection of arcs drawn in the diagram below: P, Q are centers of the arcs CB, AC, respectively; arcs ED, DF are drawn with R, S as centers, respectively, and AQ as the radius. Further, $AQ = BP = \frac{5}{6}AB$. The goal is to find the radius of the circle O'' tangent to arcs EA, ED, HM, KM as a function of AB.

Only a few of the geometric relations are needed to determine the radius. Assume the origin to be point M so the center of the circle (by symmetry) is on the y-axis. Two tangency points of the inner circle with other arches suffice to completely characterize the inner circle. Let r be the radius of the inner circle and $s = |AB|$. So one point of tangency, say (x_1, y_1), is with arch AHM with A as the center and AM as radius; this is expressed by polynomial q_1, q_3 below. Further this point is collinear with A and O'', expressed by q_2. The second point of tangency, say (x_2, y_2) is with the outer arch AEC with Q as the center and AQ as the radius; this is expressed by q_4, q_6. Further, this point is collinear with Q and O'', expressed by q_5.

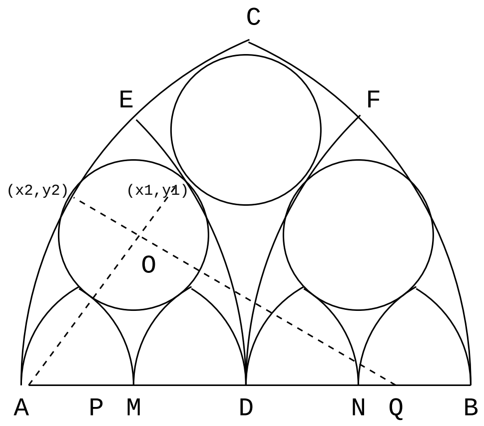

Fig. 3. Top of a Cathedral.

$$
\begin{aligned}
q_1 &= 2y_1^2 + sx_1 + 2x_1^2, \\
q_2 &= 4y_3x_1 + sy_3 - sy_1, \\
q_3 &= r^2 - x_1^2 - y_3^2 - y_1^2 + 2y_1y_3, \\
q_4 &= 17s^2 - 48y_2^2 + 56sx_2 - 48x_2^2, \\
q_5 &= 7sy_2 - 7sy_3 + 12x_2y_3, \\
q_6 &= r^2 - x_2^2 - y_3^2 - y_2^2 + 2y_2y_3.
\end{aligned}
$$

By eliminating x_1, x_2, y_1, y_2, y_3, using the Dixon resultant method, a relationship between r and s can be computed which is: $r = \frac{17}{104}s$, as a factor in the projection operator.

The book [54] is full of such problems from the architectural design, and a great source of entertainment for those interested in geometry; it is a highly recommended reading.

Perhaps the main reason the generalized Dixon resultant formulation is efficient on elimination problems is because it implicitly exploits the sparse structure of the polynomial system. For more details, an interested reader can consult [36] as well as [52].

6 Other Geometric Problems

In addition to geometry theorem proving and computing geometric quantities, algebraic methods including resultants, Gröbner basis and characteristic set constructions, have been successfully used for other problems including implicitization, object recognition and camera calibration in image understanding, object modeling where geometry plays an important role. Below, we briefly review the use of the Dixon resultant formulation for implicitization, invariant computation and an image understanding problem. For further details as well as the use of the Dixon formulation to other related problems, the reader may consult [38, 52].

6.1 Implicitization

We illustrate the use of Dixon resultants for the implicitization problem. Given a variety expressed in a parametric form, e.g.

$$
\begin{aligned}
x_1 \;\; g_1(t_1, \cdots, t_k) &= f_1(t_1, \cdots, t_k), \\
&\vdots \\
x_n \;\; g_n(t_1, \cdots, t_k) &= f_n(t_1, \cdots, t_k),
\end{aligned}
$$

the objective is to find an implicitization (or implicit representation) of the variety as a polynomial in $x_1, \cdots, x_n$. This can be formulated as an elimination problem if there are enough equations – one more equation than the number of parameters.

As an example, consider generating an implicit representation of a torus from its parametric representation. The constraints defining the torus are.

$$
\begin{aligned}
&1.\;\; x = r\;\; cos(u)\; cos(t) + R\;\; cos(t), \\
&2.\;\; y = r\;\; cos(u)\; sin(t) + R\;\; sin(t), \\
&3.\;\; z = r\;\; sin(u).
\end{aligned}
$$

Quantities r and R are the inner and outer radii, respectively, of a torus. The two trigonometric identities relating sin and cos are:

$$
\begin{aligned}
&4.\; cos(u)^2 + \sin(u)^2 = 1, \\
&5.\; \cos(t)^2 + \sin(t)^2 \;\; = 1.
\end{aligned}
$$

The objective is to compute an implicit representation of the torus in terms of $x, y, z,\ r$, and R. This can be achieved by eliminating $\cos(t)$, $\sin(t)$, $\sin(u)$ and $\cos(u)$ from the above equations.

The Dixon polynomial for this example is given below. Symbols c_u, c_t, s_u, s_t are used instead of $cos(u), cos(t), sin(u), sin(t)$, respectively, and $\bar{c}_u, \bar{c}_t, \bar{s}_u, \bar{s}_t$ are the new variables substituted for c_u, c_t, s_u, s_t, respectively, for formulating the Dixon resultant.

$$
\begin{aligned}
&\left(r^3 {c_t}^2 - r^3 + r^3 {s_t}^2\right) \bar{c}_u^3 + \left(-r^3 c_u\, c_t + x r^2 - R c_t\, r^2\right) \bar{c}_u^2 \bar{c}_t \\
&+ \left(-r^3 c_u\, s_t + r^2 y - r^2 R s_t\right) \bar{c}_u^2 \bar{s}_t + \left(-r^3 c_t\, s_u + r^2 c_t\, z\right) \bar{c}_u\, \bar{s}_u\, \bar{c}_t \\
&+ \left(-r^3 s_t\, s_u + r^2 s_t\, z\right) \bar{c}_u\, \bar{s}_u\, \bar{s}_t + \left(x r^2 c_t + r^2 {c_t}^2 R + r^2 y s_t - 2\, r^2 R - r^3 c_u + R r^2 {s_t}^2\right) \bar{c}_u^2 \\
&+ \left(-r^3 {c_t}^2 s_u + r^2 {s_t}^2 z + r^2 {c_t}^2 z - r^3 {s_t}^2 s_u\right) \bar{c}_u\, \bar{s}_u \\
&+ \left(r x R + r^2 c_t\, z s_u + x r^2 c_u - r R^2 c_t - r^3 c_t - 2\, r^2 c_u\, c_t\, R\right) \bar{c}_u\, \bar{c}_t \\
&+ \left(-r^3 s_t - r R^2 s_t - 2\, r^2 R s_t\, c_u + R r y + r^2 y c_u + r^2 s_t\, z s_u\right) \bar{c}_u\, \bar{s}_t \\
&+ \left(r c_t\, R z - r^2 c_t\, R s_u\right) \bar{s}_u\, \bar{c}_t + \left(R r s_t\, z - R r^2 s_t\, s_u\right) \bar{s}_u\, \bar{s}_t
\end{aligned}
$$

$$+ \left(-r^3 {s_t}^2 + r^2 {c_t}^2 z s_u + r x R c_t + R r y s_t - 2\, r^2 R c_u - r^3 {c_t}^2 + x r^2 c_u\, c_t\right) \bar{c}_u$$
$$+ \left(r^2 y c_u\, s_t - r R^2 + r^2 {s_t}^2 z s_u\right) \bar{c}_u + \left(R r {s_t}^2 z + r {c_t}^2 R z - r^2 {c_t}^2 R s_u - R r^2 {s_t}^2 s_u\right) \bar{s}_u$$
$$+ \left(r c_t\, R z s_u + r x R c_u - R c_t\, r^2 - r R^2 c_t\, c_u\right) \bar{c}_t + \left(-r^2 R s_t + R r y c_u + R r s_t\, z s_u - r R^2 s_t\, c_u\right) \bar{s}_t$$
$$+ R r {s_t}^2 z s_u + R r y c_u\, s_t - R r^2 {s_t}^2 + r {c_t}^2 R z s_u + r x R c_u\, c_t - r^2 {c_t}^2 R - r R^2 c_u.$$

The (16×12) Dixon matrix is:

$$\begin{array}{cc}
 & \begin{array}{cccccccccccc} 1 & c_u & c_t & s_t & c_t^2 & s_t^2 & c_t c_u & s_u c_t^2 & s_u c_t & s_t c_u & s_u s_t^2 & s_u s_t \end{array} \\
\begin{array}{c} 1 \\ \bar{c}_u \\ \bar{c}_u \bar{s}_t \\ \bar{c}_u^2 \\ \bar{c}_u \bar{c}_t \\ \bar{s}_u \\ \bar{c}_t \\ \bar{s}_t \\ \bar{c}_u^3 \\ \bar{s}_t \bar{c}_u^2 \\ \bar{c}_t \bar{c}_u^2 \\ \bar{s}_u \bar{c}_u \\ \bar{c}_t \bar{s}_u \bar{c}_u \\ \bar{c}_t \bar{s}_u \\ \bar{s}_t \bar{s}_u \bar{c}_u \\ \bar{s}_t \bar{s}_u \end{array} &
\begin{pmatrix}
0 & -rR^2 & 0 & 0 & -r^2R & -r^2R & rxR & rRz & 0 & Rry & rRz & 0 \\
-rR^2 & -2r^2R & rxR & Rry & -r^3 & -r^3 & xr^2 & r^2z & 0 & r^2y & r^2z & 0 \\
Rry & r^2y & 0 & -r^3-rR^2 & 0 & 0 & 0 & 0 & 0 & -2r^2R & 0 & r^2z \\
-2r^2R & -r^3 & xr^2 & r^2y & r^2R & r^2R & 0 & 0 & 0 & 0 & 0 & 0 \\
rxR & xr^2 & -r^3-rR^2 & 0 & 0 & 0 & -2r^2R & 0 & r^2z & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & rRz & rRz & 0 & -r^2R & 0 & 0 & -r^2R & 0 \\
0 & rxR & -r^2R & 0 & 0 & 0 & -rR^2 & 0 & rRz & 0 & 0 & 0 \\
0 & Rry & 0 & -r^2R & 0 & 0 & 0 & 0 & 0 & -rR^2 & 0 & rRz \\
-r^3 & 0 & 0 & 0 & r^3 & r^3 & 0 & 0 & 0 & 0 & 0 & 0 \\
r^2y & 0 & 0 & -r^2R & 0 & 0 & 0 & 0 & 0 & -r^3 & 0 & 0 \\
xr^2 & 0 & -r^2R & 0 & 0 & 0 & -r^3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & r^2z & r^2z & 0 & -r^3 & 0 & 0 & -r^3 & 0 \\
0 & 0 & r^2z & 0 & 0 & 0 & 0 & 0 & -r^3 & 0 & 0 & 0 \\
0 & 0 & rRz & 0 & 0 & 0 & 0 & 0 & -r^2R & 0 & 0 & 0 \\
0 & 0 & 0 & r^2z & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -r^3 \\
0 & 0 & 0 & rRz & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -r^2R
\end{pmatrix}
\end{array}$$

. Its rank is 10, and the projection operator is

$$r^{23} R(-z^2 - R^2 + r^2)(4R^2(r^2 - z^2) - (x^2 + y^2 + z^2 - R^2 - r^2)^2)$$

and the factor $4R^2(r^2-z^2)-(x^2+y^2+z^2-R^2-r^2)^2$ is the implicit representation of torus.

6.2 Computing Invariant Relations

Geometric invariants appear to play an important role in object recognition as an aid to building model libraries of objects. Building model-based object recognition system using geometric invariants has recently become an active research area. Invariants of various objects (or their models) can be stored in a model library [46]. Invariants of image features can be used to index the model library to prune the search space for objects being recognized in an image.

Invariant relations are expressions relating model features to image features, and they can be computed using elimination techniques. In [32], the use of the generalized Dixon formulation and the Gröbner basis method are discussed for computing invariant relations, and then invariants, using a separability algorithm.

Object features, e.g., coordinates of points in an object, are related to image features, e.g., coordinates of points in an image through the camera parameters which can be specified using various geometric transformations (depending upon the approximation of the camera viewing used), e.g. affine, scaled orthographic and projective transformations. Given enough object features, transformation parameters can be eliminated from these relations by elimination. From the projection operator thus computed, an invariant relation specifying the relation between object and image features and independent of any transformation parameters can be recovered. In many cases, this invariant relation can be separated, resulting in purely a property of an object, or image(s), which remains invariant under camera viewing.

6.3 Recovering Camera Motion from Two Images

In [21], a camera motion reconstruction, a basic problem in photogrammetry, is formulated as an elimination problem. Given the coordinates of corresponding points in two images under perspective projection on calibrated cameras, an objective is compute the displacement of the camera between two positions Let a_i, a'_i be 3-dimensional vectors corresponding to the images of a point in each image frame. Let $q =< q_1, q_2, q_3 >$ and $d =< d_1, d_2, d_3 >$ be two 3-dimensional vectors corresponding to the camera displacement. The equations describing the camera motion reconstruction can be specified as:

$$
\begin{aligned}
p_1 &= (a_1^T\, q) * (d^T\, a'_1) + (a_1^T\, a'_1) + ((a_1 \times q)^T\, a'_1) + ((a_1 \times q)^T\, (d \times a'_1)) + (a_1^T\, (d \times a_1)),\\
p_2 &= (a_2^T\, q) * (d^T\, a'_2) + (a_2^T\, a'_2) + ((a_2 \times q)^T\, a'_2) + ((a_2 \times q)^T\, (d \times a'_2)) + (a_2^T\, (d \times a_2)),\\
p_3 &= (a_3^T\, q) * (d^T\, a'_3) + (a_3^T\, a'_3) + ((a_3 \times q)^T\, a'_3) + ((a_3 \times q)^T\, (d \times a'_3)) + (a_3^T\, (d \times a_3)),\\
p_4 &= (a_4^T\, q) * (d^T\, a'_4) + (a_4^T\, a'_4) + ((a_4 \times q)^T\, a'_4) + ((a_4 \times q)^T\, (d \times a'_4)) + (a_4^T\, (d \times a_4)),\\
p_5 &= (a_5^T\, q) * (d^T\, a'_5) + (a_5^T\, a'_5) + ((a_5 \times q)^T\, a'_5) + ((a_5 \times q)^T\, (d \times a'_5)) + (a_5^T\, (d \times a_5)),\\
p_6 &= 1 - (d^T\, q).
\end{aligned}
$$

The objective is to eliminate d_2, d_3, q_1, q_2, q_3 to get a polynomial in d_1 for a given set of values substituted for a_i and a'_i.

The projection operator is a 10^{th} degree polynomial in d_1, which can be computed in 40 milliseconds on a sparc10; the set up for constructing the Dixon matrix, which has to be done only once, is less than 3 seconds.

It thus appears that the camera motion reconstruction can be done on-line in real time using the generalized Dixon resultants.

6.4 Kinematics: Stewart's Platform

The Stewart platform problem is a well-known benchmark from robotics and kinematics [27, 43, 45, 21]. It is a parallel manipulator with six prismatic joints connecting two platforms, in which the base platform is fixed, while the top platform, or end-effector, is moving in 3-dimensional space, controlled by the lengths of the joints.

The quaternion formulation of the Stewart platform presented below is by Emiris [21]. It contains 7 polynomials in 7 variables. Let $x = [x_0, x_1, x_2, x_3]$ and $q = [1, q_1, q_2, q_3]$ be two unknown quaternions, which are to be determined. Let $q^* = [1, -q_1, -q_2, -q_3]$. Let a_i and b_i, for $i = 2, \ldots, 6$, be ten known quaternions, and let α_i, for $i = 1, \ldots, 6$, be six predetermined scalars. The seven polynomials for solving the Stewart platform problem are:

$$\begin{aligned} f_1 &= x^T x - \alpha_1 q^T q, \\ f_i &= b_i^T (xq) - a_i^T (qx) - (q b_i q^*)^T a_i - \alpha_i q^T q, \;\; i = 2, \ldots, 6, \\ f_7 &= x^T q^*. \end{aligned}$$

Out of the 7 variables, $x_0, x_1, x_2, x_3, q_1, q_2, q_3$, any six can be eliminated to compute the resultant as a polynomial in the seventh.

The generalized Dixon resultant formulation can be used to compute a projection operator. Using our implementation of the generalized Dixon method running on a sparc10 station with 64MB memory, we successfully computed the projection operator from the above formulation in total computer time of less than 10 minutes (273.5 seconds to construct the Dixon matrix and 256.79 seconds to interpolate a projection operator from it). The projection operator is a polynomial of degree 40, consistent with similar results reported in [51, 43, 45]. The generalized Dixon resultant formulation is thus able to compute the exact resultant, without any extraneous factors.

To our knowledge, our results are the first successful attempt to compute the resultant for the Stewart platform problem using multivariate elimination methods in which no a priori processing or ad hoc techniques are employed.

The solution to the Stewart platform problem illustrates an interesting aspect of multivariate elimination methods. Even though in a multivariate formulation, variables are eliminated simultaneously, there is an implicit ordering on variables used in different methods, for example, in the Dixon resultants, the order in which original variables to be eliminated are substituted by new variables in the cancellation matrix. This ordering affects significantly the computational performance of the methods as well as extraneous factors generated in the projection operators. These aspects of resultant methods are not understood, and should be investigated. In [37], it is shown that for the Stewart platform problem, for certain orderings, the generalized Dixon method computes the projection operator quite fast, but at the cost of including numerous extraneous factors. On the other hand, we have identified a particular ordering that gives the exact resultant for the Stewart platform problem, without any extraneous factors, but the computation time is much longer. An interesting research issue is to find an ordering on variables that leads to minimal extraneous factors as well as the fastest computation of a projection operator from the Dixon matrix constructed from a polynomial system.

7 New Promising Approaches

The approaches discussed above share one common aspect in the formulation of geometry problems – associating coordinates with points and expressing geometric relations as polynomials. There are, however, other methods currently being investigated, including vector-based approaches discussed in [53, 9], an invariant based approach proposed in [49, 10], the area method discussed in [11] and more recently, the logical approach revived in [12].

A special mention must be made of the *area* method popularized by Prof. Zhang of Academia Sinica. Chou, Gao and Zhang have developed an impressive prover, Euclid, based on this method using which they have shown how hundreds of theorems in plane and solid geometry can be easily proved. An important advantage of this method is that the proofs generated by the prover are short and readable. In the area method, geometric relations are usually expressed in terms of areas of triangles. A proof is typically generated using the heuristic of successively eliminating points. See their excellent book [11] for details. Earlier, Chou, Gao and Zhang had proposed the use of fourteen basic geometry propositions expressing three kinds of geometry quantities: ratios of lengths, areas of triangles and Pythagoras difference for eliminating points [10]

Recently, Chou, Gao and Zhang have been using a classical approach for searching for proofs of Euclidean geometry theorems, based on a data base of useful geometric lemmas, more in the spirit of Gelernter's geometry machine. They have developed an impressive prover based on this idea, which they are planning to use for educational purposes. For details, the reader may consult a forthcoming paper by them [12].

Crapo and Richter-Gebert developed a system based on bracket algebras and invariants for geometry theorem proving in Euclidean, affine and projective geometries. Bracket expressions representing determinants are used to express incidence relations. Proving a theorem amounts to using bracket relations to prove that a conclusion expressed as a bracket expression follows from the hypotheses, also expressed using bracket expressions [49, 17].

Recently, Li and Cheng have developed a modification of Wu's method based on Clifford algebra techniques for proving theorems in Euclidean as well as differential geometries [44]. Clifford algebra techniques are closely related to vector representations of points in Euclidean geometry [53, 9].

8 Subsidiary Conditions and Discovering Geometry Theorems

An interesting byproduct of Wu's approach has been a discussion of the role of degenerate cases of the hypotheses in geometry theorem proving. In [68], Wu said, "almost all theorems in ordinary geometry (i.e., ordinary Euclidean geometry) are only *generically true,* or true only under some non-degenerate conditions usually not explicitly described in the statement of the theorem. This fact is quite fatal to make the usual Euclidean fashion of proving theorems rigorous as one believes to be so, since it is difficult to state clearly the non-degeneracy conditions to be observed and to verify that the previous theorems to be applied in the proof of the theorem in question do not fall into the degeneracy cases under which the previous theorems to be applied might not be true." Wu went on to add that the fact that his approach is able to automatically discover the non-degeneracy conditions is "the crucial point which is responsible for the high efficiency of our method in proving quite non-trivial theorems without the defect pointed above" about theorem proving in the Euclidean fashion.

As discussed in earlier sections, both in the refutational and direct approaches, subsidiary conditions of the form $s \neq 0$ can be derived from the hypotheses and the conclusion of a geometric conjecture using any of the three methods discussed above.

A theoretical justification for this derivation is Theorem 2 in section 3.3 taken from [28, 29] about the elimination ideal of the hypotheses and the polynomial corresponding to the negated conclusion, just in the parameters, being different from 0. In that case, it is possible to find such an s, a polynomial in the parameters whose zeros must be ruled out of the common zeros of the hypotheses for the conclusion to follow from the hypotheses. And, one way to compute the elimination ideal of the hypotheses and the negated conclusion is to use a Gröbner basis algorithm, as discussed in [28, 29].

What if the elimination ideal of the hypotheses and the negated conclusion is 0, i.e., it does not have any polynomials in the parameters? Then it is not possible to find a subsidiary condition $s \neq 0$ (also called *negative* hypothesis below to contrast with *positive* hypotheses of the form $t = 0$) such that the hypotheses along with the subsidiary condition imply a given conclusion. In that case, one can look for an additional positive hypothesis of the form $t = 0$ such that along with this positive additional hypothesis, the conclusion follows (after degenerate cases have been ruled out).

Using this approach, Recio and Velez-Melon [47] have recently developed an educational package for teaching algebraic geometry by mechanically discovering geometry theorems. A geometric conjecture is first tested for validity. In case the conjecture is not true, a subsidiary condition (negative hypothesis) is looked for, possibly ruling out degenerate cases as discussed earlier. If no negative hypothesis can be identified (which will be the case if the elimination ideal is 0), then they propose analyzing the elimination ideal generated from the hypotheses and the conclusion for positive additional hypotheses of the form $t = 0$ in the parameters. Conditions on parameters can be identified in this way which would be true in case the hypotheses imply the conclusion. If such a positive additional hypothesis is identified, the number of parameters is reduced (since the additional hypothesis is a polynomial in the parameters). It is then checked whether the conclusion follows from the augmented set of hypotheses. As before, some inequations may have to be deduced to rule out the degenerate cases of the modified conjecture, or alternatively, the modified conjecture may have to be further strengthened by adding more positive hypotheses.

For instance, consider dropping one of the hypotheses in the parallelogram example, namely, that AB is parallel to CD. Under the condition that two of the sides of a quadrilateral are parallel (i.e., the quadrilateral is a trapezoid), the objective is to find whether the intersection O of the two diagonals AC and BD is the midpoint of AC. In this modified formulation, along with u_1, u_2, u_3, one of x_1 and x_2 (say, x_1) is also an independent parameter. The ideal of polynomials $2, 3, 4,$ and $7'$ does not include any polynomial in x_1, u_1, u_2, u_3. This implies that no inequation in x_1, u_1, u_2, u_3 can be found such that the hypotheses and the inequation would imply the conclusion.

But if the elimination ideal of polynomials 2, 3, 4 and 7 in u_1, u_2, u_3, x_1 is analyzed, it includes among other things, the polynomial:

$$(x_1 - u_3)u_1u_3(u_2^2 + u_3^2).$$

This implies that if the hypotheses and the conclusion are to hold together (i.e., if a quadrilateral with two parallel sides has the intersection point of its diagonals to be the midpoint of one of its diagonal), then the above polynomial in the independent parameters must be 0. The cases of $u_1, u_3, (u_2^2 + u_3^2)$ being zero correspond to the quadrilateral being degenerate. If they are ruled out, the interesting additional constraint on the quadrilateral for the conclusion to hold is:

$$x_1 - u_3,$$

implying that AB is parallel to CD.

Ideas similar to the above have also been successfully tried using the characteristic set method. As stated earlier, Wu [65] discussed how the characteristic set construction can be used for computing geometric formulas. That observation can be viewed as a particular application of the use of a characteristic set construction for multi-variable elimination; for other such uses of the characteristic set method as an elimination technique, the reader may consult [31, 30]. Particularly, the characteristic set method can be used for deducing positive additional hypotheses as well. Chou [4], for instance, used it to discover a generalization of Simson's theorem in this way. A similar idea was also used by Kapur and Mundy [33] to deduce conditions on object features from the properties of images features and vice versa in applying the characteristic set method to image understanding problems. The key idea is summarized below.

Once a characteristic set is computed from the hypotheses, the conclusion is pseudo-divided using the characteristic set. If the conclusion pseudo-divides to 0, then it is said to follow from the hypotheses under certain conditions. If the remainder is nonzero, the remainder can be analyzed to identify an additional positive hypothesis which must be included so that the conclusion follows from the augmented set of hypotheses. Typically the remainder is factored, and if one of the factors is a polynomial in the parameters and has a geometric meaning, then that polynomial can serve as an additional hypothesis.

It is easy to see that the pseudo-remainder of a polynomial p by another polynomial q is in the ideal generated by p and q. Thus, the polynomials in a characteristic set computed without using factorization are in the ideal generated by the hypotheses. The pseudo-remainder obtained by pseudo-dividing the conclusion by the characteristic set generated from the hypotheses is in the ideal of the characteristic set (and hence of the hypotheses, since the ideal generated by the characteristic set is a subideal of the ideal generated by the hypotheses) and the conclusion. We thus get the effect of analyzing certain polynomials in the elimination ideal of the hypotheses and the conclusion.

Analyzing the elimination ideal of the hypotheses and the conclusion in the parameters is equivalent to considering all possible inferences that can be made about a geometric configuration in which the hypotheses and the desired conclusion hold.

A different approach for mechanically generating subsidiary conditions is discussed in [8]. For a family of geometry statements defined to be of constructive type in [8], subsidiary conditions are generated along with the construction of the geometric configuration. It is proved that for a geometry statement of such constructive type to be valid, subsidiary conditions so generated suffice.

9 Concluding Remarks

We have discussed the use of three different algebraic methods for automated geometry theorem proving. Each of these methods has its advantages and disadvantages. If the hypotheses in a geometric problem are linear (or even quadratic) as is typically the case in most Euclidean geometry problems involving lines and points, the characteristic set construction works particularly well. The characteristic set construction is less efficient with hypotheses expressed by quadratics, as is the case with configurations involving distances and circles. For complicated problem formulations, the refutational approach using the Gröbner basis algorithm works particularly well if the conjecture is valid. That is perhaps due to the fact that the zero dimensional ideals can be more easily analyzed using the Gröbner basis and resultant constructions, in contrast to the characteristic set constructions.

A great deal of progress has been made in developing computer programs prove nontrivial geometry theorems, moving towards one of the milestones of the AI research. The main reason perhaps why research in geometry theorem proving has been tremendously successful is because (i) algebraic representations turns out to be an efficient and succinct way to represent all the information about a geometric problem, (ii) algebraic representation can be manipulated efficiently using simple primitive operations which can be implemented well, and (iii) heuristics can be easily incorporated. Of course, the speed of computers have increased significantly since the 50's and 60's, and memory has not been a problem, and these advances in hardware have helped a great deal.

In addition to geometry theorem proving, we have also briefly reviewed other geometric reasoning problems arising in various application domains including solid and geometric modeling, robotics and kinematics, image understanding. We can envision general purpose as well as special purpose software being developed to support geometric reasoning needed in different application domains. As of now, there does not exist a single uniform method that works well for all geometric reasoning problems. Instead, our experience suggests that different methods behave differently on different types of geometric problems.

For elimination problems, the generalized Dixon formulation is especially effective because it implicitly exploits the sparse structure, if any, of the problem. But it becomes necessary to separate extraneous factors in a projection operator from the resultant. On the other hand, the Gröbner basis algorithm, whenever it works, gives the exact resultant. However, for most problems, the Gröbner basis approach is too expensive.

Lots of research and analysis still need to be done. One of our long term goals has been to develop algorithms and their implementations so as to enable off-line and on-line reasoning for object recognition and other image understanding tasks in computer vision. Despite considerable progress, it is still not possible to automatically compute invariants of geometric configurations [46]. When invariant computation is formulated as an elimination problem, it becomes too difficult to manage by currently implemented elimination techniques. With the generalized Dixon resultant formulation, invariants for only simple geometric configurations can be computed automatically [32]. Otherwise, considerable human interaction and guidance are required.

It is still not possible to recover shape from images and camera parameters on-line from the algebraic formulation of shape recovery problems. Elimination techniques must be specialized to such applications, as well as it is necessary to effectively integrate symbolic methods with numerical and approximate methods that are less sensitive to noise and error in data.

Acknowledgments: The generalization of Dixon resultants was developed by the author jointly with Lu Yang and Tushar Saxena. The use of Dixon resultants for geometry theorem proving was explored jointly with Tushar Saxena. Thanks to Dongming Wang for useful comments on an earlier draft of this paper.

References

1. Arnon, D.S., Collins, G.E., and McCallum, S., Cylindrical algebraic decomposition I: The basic algorithm; II: An adjacency algorithm for the plane. *SIAM J. of Computing* 13, 1984, 865-877, 878-889.
2. Becker T., Weispfenning V., in cooperation with Kredel H., *Gröbner Bases, A Computational Approach to Commutative Algebra.* Springer-Verlag, New York, 1993.
3. Buchberger B., Gröbner bases: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory* (ed. Bose), D. Reidel Publ. Co., 1985, 184-232.
4. Chou, S.-C., *Proving and Discovering Theorems in Elementary Geometry using Wu's Method.* Ph.D. Thesis, Dept. of Mathematics, University of Texas, Austin, 1985.
5. Chou, S.-C., *Mechanical Geometry Theorem Proving.* D. Reidel Publishing Company, Dordrecht, Netherlands, 1988.
6. Chou, S.-C., and Gao, X.-S., Ritt-Wu's decomposition algorithm and geometry theorem proving. Proc. *10th Intl. Conf. on Automated Deduction (CADE-10),* Kaiserslautern, LNCS 449, July 1990, 207-220.
7. Chou, S.-C., and Gao, X.-S., Mechanical formula derivation of elementary geometries. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC),* Tokyo, 1990, 265-270.
8. Chou, S.-C., and Gao, X.-S., Proving constructive geometry statements. Proc. *11th Intl. Conf. on Automated Deduction (CADE-11),* Saratoga Springs, Springer LNAI 607, 1992, 20-34.

9. Chou, S.-C., Gao, X.-S., and Zhang, J.-Z., Automated geometry theorem proving by vector calculations. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Kiev, 1993, 284-291.
10. Chou, S.-C., Gao, X.-S., and Zhang, J.-Z., Automated production of traditional proofs for constructive geometry theorems. Proc. *8th Annual IEEE Symp. on Logic in Computer Science (LICS),* Montreal, June 1994, 48-56.
11. Chou, S.-C., Gao, X.-S., and Zhang, J.-Z., *Machine Proofs in Geometry: Automated Production of Readable Proofs for Geometry Theorems.* World Scientific Press, 1994.
12. Chou, S.-C., Gao, X.-S., and Zhang, J.-Z., A deductive database approach to automated geometry theorem proving and discovering. Accepted for publication in *J. of Automated Reasoning.*
13. Chou, S.-C., and Schelter, W.F., Proving geometry theorems with rewrite rules. *J. of Automated Reasoning* 2 (3), 1986, 253-273.
14. Coelho, H., and Pereira, L.M., Automated reasoning in geometry theorem proving with PROLOG. *J. of Automated Reasoning* 2 (4), 1986, 329-390.
15. Connolly, C.I., Kapur, D., Mundy, J.L., and Weiss, R., GEometer: A System for modeling and algebraic manipulation, Proc. *DARPA Workshop on Image Understanding,* Palo Alto, May 1989, 797-804.
16. Conti, P., and Traverso, C., A case of automatic theorem proving in Euclidean geometry: The Maclane 8_3 theorem. Proc. *AAECC,* LNCS 948, Paris, 1995, 183-193.
17. Crapo, H., Automatic proofs of geometry theorems: The synthetic approach, Presented at the *Intl. Workshop on Automated Deduction in Geometry,* Toulouse, Sept 1996.
18. Cyrluk, D.A., Harris, R.M., and Kapur, D., GEometer: A theorem prover for algebraic geometry. Proc. *9th Intl. Conf. on Automated Deduction (CADE-9)*, Argonne, IL, LNCS 310, May 1988. 770-771.
19. Dixon, A. L., The eliminant of three quantics in two independent variables. Proc. *London Mathematical Society* 6, 1908, 468-478.
20. Dolzmann, A., Sturm, T., and Weispfenning, V., A new approach for automatic theorem proving in real geometry. Accepted for publication in *J. of Automated Reasoning.*
21. Emiris I., *Sparse Elimination and Applications in Kinematics.* Ph.D. Thesis, Computer Science Division, University of Calif., Berkeley, 1994.
22. Gao, X.-S., and Wang, D.-K., On the automatic derivation of a set of geometric formulae. *J. of Geometry,* 53, 1995, 79-88.
23. Gerber, L., The orthocentric simplex as an extreme simplex. *Pacific J. of Mathematics* 56, 1975, 97-111.
24. Herstein, I. N., *Topics in Algebra - Second Edition.* John Wiley & Sons, Inc., USA, 1975.
25. Heymann, W. Problem der Winkehalbierenden. *Ztschr. f. Math. and Phys.* 35, 1890.
26. Hong, J., Proving by example and the gap theorems. Proc *27th Annual Symp. on Foundations of Computer Science (FOCS),* Toronto, Oct. 1986, 107-116.
27. Huang, Y.Z., and Wu, W.D., Kinematic solution of a Stewart platform. Proc. *1992 Intl. Workshop on Mathematics Mechanization* (eds. Wu and Cheng), Intl. Academic Publishers, 1992, 181-188.

28. Kapur, D., Geometry theorem proving using Hilbert's Nullstellensatz. Proc. *1986 Symposium on Symbolic and Algebraic Computation (SYMSAC 86)*, Waterloo, 1986, 202-208.
29. Kapur, D., A refutational approach to geometry theorem proving. *Artificial Intelligence,* 37, 1988, 61-94.
30. Kapur, D., Algorithmic elimination methods. Tutorial Notes, *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Montreal, July 1995.
31. Kapur, D., and Lakshman, Y., Elimination methods: An introduction. *Symbolic and Numerical Computation for Artificial Intelligence* (eds. Donald, Kapur and Mundy), Academic Press, 1992, 45-87.
32. Kapur, D., Y.N., Lakshman, and Saxena, T., Computing invariants using elimination methods. Proc. *IEEE Intl. Symp. on Computer Vision*, Coral Gables, Florida, November 1995.
33. Kapur, D., and Mundy, J.L., Wu's method and its application to perspective viewing. *Artificial Intelligence,* 37, 1988, 15-26.
34. Kapur, D., and Saxena, T., Automated geometry theorem proving using the Dixon resultants. Invited Talk, *IMACS-95*, Albuquerque, New Mexico, May 1995.
35. Kapur, D., and Saxena, T., Comparison of various multivariate resultant formulations. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Montreal, July 1995, 187-194.
36. Kapur, D., and Saxena, T., Sparsity considerations in the Dixon resultant formulation, Proc. *ACM Symposium on Theory of Computing (STOC)*, Philadelphia, May 1996, 184-191
37. Kapur, D., and Saxena, T., Extraneous factors in the Dixon resultant formulations. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Hawaii, July 1997, 141-148.
38. Kapur D., Saxena T. and Yang L., Algebraic and geometric reasoning using Dixon resultants. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Oxford, July 1994, 99-107.
39. Kapur, D., and Wan, H., Refutational proofs of geometry theorems via characteristic set computation. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC),* Tokyo, August 1990, 277-284.
40. Knuth, D.E., *Seminumerical Algorithms: The Art of Computer Programming.* Vol. 2, Second Edition, Addison Wesley, 1980, 407-408.
41. Ko, H.P., and Hussain, M.A., A study of Wu's method—A method to prove certain theorems in elementary geometry. Proc. *1985 Congressus Numerantium,* 1985,
42. Kutzler, B., and Stifter, S., Automated geometry theorem proving using Buchberger's algorithm. Proc. *1986 Symposium on Symbolic and Algebraic Computation (SYMSAC 86)*, Waterloo, 1986, 209-214.
43. Lazard D., Generalized Stewart platform: How to compute with rigid motions? *Proc. IMACS-SC*, Lille, June 1993, 85-88.
44. Li, H., and Cheng, M., Proving theorems in elementary geometry with Clifford algebraic method. Preprint, MMRC, Academia Sinica, China, 1995.
45. Mourrain B., The 40 "generic" positions of a parallel robot. *Proc. ACM Intl. Symp. on Symbolic and Algebraic Computation (ISSAC)*, Kiev, July 1993.
46. Mundy, J., L., Zisserman, A., Towards a new framework for vision. *Geometric Invariance in Computer Vision* (eds. Mundy and Zisserman), MIT Press, 1992, 1-39.

47. Recio, T., and Velez-Melon, M.P., Automatic discovery of theorems in elementary geometry. Presented at the *Workshop on Automated Deduction in Geometry,* Toulouse, Sept 1996.
48. Rege, A., A complete and practical algorithm for geometric theorem proving. Proc *11th Annual Symp. on Computational Geometry,* Vancouver, June 1995, 277-286.
49. Richter-Gebert, J., Mechanical theorem proving in projective geometry. *Algebraic Approaches to Geometric Reasoning* (eds. Hong, Wang, and Winkler), A special issue of Annals of Mathematics and Artificial Intelligence, 1995.
50. Ritt, J.F., *Differential Algebra.* AMS Colloquium Publications, 1950.
51. Ronga F., and Vust T., Stewart platforms without computer. *Preprint,* Department of Mathematics, University of Geneva, 1992.
52. Saxena, T., *Efficient Variable Elimination using Resultants.* Ph.D. Thesis, Dept. of Computer Science, State University of New York, Albany, Nov. 1996.
53. Stifter, S., Geometry theorem proving in vector spaces by means of Gröbner bases. Proc. *Intl. Symp. on Symbolic and Algebraic Computation (ISSAC),* Kiev, July 1993, 301-310.
54. Sykes, M., *A Source Book of Problems for Geometry, based upon Industrial Design and Architectural Ornament.* Boston, Allyn and Bacon, 1912.
55. Tarski, A., A Decision Method for Elementary Algebra and Geometry. U. of Calif. Press, 1948; 2nd edition, 1951.
56. Wan, H., *Refutational Proofs of Geometry Theorems using the Characteristic Set Method.* MS project, RPI, Troy, NY, 1987.
57. Wang, D., Proving-by-examples method and inclusion of varieties. *Kexue Tongbao,* 33, 1988, 1121-1123.
58. Wang, D., A new theorem discovered by computer prover. *J. of Geometry,* 36, 1989, 173-182.
59. Wang, D., Algebraic factoring and geometry theorem proving. Proc. *12th Intl. Conf. on Automated Deduction (CADE-12),* Nancy, LNAI 814, 1994, 386-400.
60. Wang, D., Geometry machines: From AI to SMC. Proc. *Intl. Conf. on Artificial Intelligence and Symbolic Mathematical Computation (AISMC-3),* Steyr, Austria, 1996, LNCS 1138, 213-239.
61. Wang, D., and Gao, X.-S., Geometry theorems proved mechanically using Wu's method—Part on Euclidean geometry. *MM Research Preprints,* 2, 1987, 75-106.
62. Wu, W., On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica* 21 (1978) 150-172. Also in *Automated Theorem Proving: After 25 Years, Contemporary Mathematics* 29 (eds. Bledsoe and Loveland), 1984, 213-234.
63. Wu, W., Some recent advances in mechanical theorem proving of geometries. *Automated Theorem Proving: After 25 Years, Contemporary Mathematics* 29 (eds. Bledsoe and Loveland), 1984, 235-241.
64. Wu, W., Basic principles of mechanical theorem proving in geometries. *J. of System Sciences and Mathematical Sciences* 4 (3), 1984, 207-235. Also in *J. of Automated Reasoning* 2, 1986, 221-252.
65. Wu, W., A mechanization method of geometry and its applications. *J. of System Sciences and Mathematical Sciences* 6 (3), 1986, 204-216.
66. Wu, W., On reducibility problem in mechanical theorem proving of elementary geometries. *Chinese Quart. J. Mathematics,* 2, 1987, 1-20.
67. Wu, W., On zeros of algebraic equations—An application of Ritt's principle. *Kexue Tongbao,* 31 (1), 1986, 1-5.

68. Wu, W., *Mechanical Theorem Proving in Geometries: Basic Principles.* Translated from Chinese by Jin and Wang, Springer Verlag, 1994.
69. Yang, L., Zhang, J.-Z., and Hou, X.-R., An efficient decomposition algorithm for geometry theorem proving without factorization. Proc. *ASCM'95,* Beijing, August 1995, 33-41.
70. Yang, L., Zhang, J.-Z., and Li, C.-Z., A prover for parallel numerical verification of a class of constructive geometry theorems. Proc. *Intl. Workshop on Mechanization of Mathematics* (ed. Wu and Cheng), Beijing, China, July 1992, 244-250.
71. Zhang, J.-Z., Chou, S.-C., and Gao, X.-S., Automated production of traditional proofs for theorems in Euclidean geometry I. *Algebraic Approaches to Geometric Reasoning* (eds. Hong, Wang, and Winkler), A special issue of Annals of Mathematics and Artificial Intelligence, 1995, 109-137.
72. Zhang, J.-Z., Yang, L., and Deng, M.-K., The parallel numerical method of mechanical theorem proving. *Theoretical Computer Science,* 74, 1990, 253-271.