# A Note on Irreducible Decomposition of Algebraic Sets and Automatic Theorem Proving

**Trần Quốc–Nam** *

RISC–Linz

Research Institute for Symbolic Computation

Johannes Kepler University, A–4040 Linz, Austria

E-mail: tqnam@risc.uni-linz.ac.at

August 19, 1996

**Abstract**

In this paper, we present some new results concerning the dimension of the irreducible components of an algebraic set. We also point out that our results are very useful in Computer Aided Geometric Design (CAGD) and Visualization, in particular when the algebraic set is one-dimensional.

In the second part of the paper, we report our experiments on combining results in Automatic Theorem Proving with the computer algebra system CASA - a computer algebra system for Algebraic Geometry.

**Keywords:** Irreducible decomposition, Automatic Theorem Proving .

## 1 Introduction

Irreducible decomposition is widely used in Algebraic Geometry, Computer Aided Geometric Design, etc. In fact, it has been used as the first and requisite step in many constructive computations such as parameterization, genus computation, projection of an algebraic set onto a hypersurface. It is a well-known result that we can algorithmically decompose an algebraic set (in $K^n$, where $K$ is a field) into a union of finitely many irreducible and noncontractive components. The decomposition of an algebraic set is unique up to the order in which the components are written. Algorithms for finding the decomposition can be found in [Her26], [Rit32, Rit50], [MRR88], [Sei74, Sei84], [GTZ88] and [EHV90]. Among them, an efficient method for finding the decomposition is the method of Ritt's based on characteristic set computations (see [Rit50], [Cho88] and [Wu94]). Using Ritt's method, to decompose an algebraic set, we first compute a sequence of irreducible characteristic sets which has the union of their corresponding irreducible algebraic sets to be equal to the original algebraic set. Then to find the corresponding irreducible algebraic set for each irreducible characteristic set, we need to compute a Gröbner basis of a system of equations which includes the characteristic set itself and an extra equation with an extra variable. However, for an algebraic set in higher dimensional spaces, such the Gröbner bases are very expensive to compute from both time and memory space considerations. Meanwhile in practice, for example in Computer Aided Geometric

*Supported by the Austrian Fonds zur Förderung der wissenschaftlichen Forchung, Project HySaX

Design (CAGD) or Visualization, we need only an approximation of the algebraic set, in particular for one-dimensional algebraic sets. In fact, approximation and representation of one-dimensional algebraic sets in higher dimensional space is a fundamental and difficult problem in Computer Aided Geometric Design (CAGD), Visualization and Solid Modeling. For example, the intersection of two parametric surfaces can be seen as a space curve in a 4-dimensional space and the intersection of an implicit surface with an $r$-offset surface of another implicit surface can be seen as a space curve in a 6-dimensional space.

In this paper, we present some new results of the author's concerning the dimension of the irreducible components of an algebraic set. We also show how to use our results to develop hybrid symbolic-numerical algorithms, which aim at the goals of efficiency and reliability, for solving the problem of approximation and representation of one-dimensional algebraic sets in Computer Aided Geometric Design and Visualization.

In the second part of the paper, we report our experiments on combining results in Automatic Theorem Proving with the computer algebra system CASA. CASA is a computer algebra system for constructive Algebraic Geometry which is designed for performing computations and reasoning about geometric objects in classical algebraic geometry, in particular affine and projective algebraic geometry over an algebraically closed field $K$ of characteristic 0. The core of the system is that we can represent an algebraic set in four different representations, namely implicit representation, projected representation, parametric representation and representation by places or Puiseux series. The system also works with the polynomial ideals corresponding to these geometric objects and many other operations such as: dimension computation, rational parameterization, implicitization, transformations of algebraic sets into hyper-surfaces, Puiseux series expansion, Gröbner bases computation over $K[X]^r$-modules and so on.

As it is shown in the second part of the paper, combining the results in Automatic Theorem Proving with a computer algebra system gives us, on the one hand an engine within the computer algebra system for proving theorems in algebraic geometry, in particular theorems in elementary geometry. On the other hand, we benefit from the computer algebra system for improving the efficiency of Automatic Theorem Proving algorithms by using more up-to-date algorithms and methods in the computer algebra system.

The structure of the paper is as follows. In the next section, we summarize some well-known results from Ritt's characteristic set method and the dimension theory. In Section 3, we present our main results. In Section 4, we show the applicability of our results in tracing one-dimensional algebraic sets in higher dimensional space. In Section 5, we report our experiments on combining results in Automatic Theorem Proving with CASA.

# 2 Preliminaries

We assume that the readers are familiar with the dimension theory and Ritt's method to decompose an algebraic set (see [Rit32, Rit50], [Cho88], [CLO92] and [Wu94]). In particular, the following lemmas are used in the proofs of our results.

**Lemma 2.1** *Let* $\mathrm{CS}^{(i)}$ *be the sequence of irreducible extended characteristic sets constructed by applying Ritt's algorithm to a finite set of multivariate polynomials* PS *and* $\mathrm{PD}^{(i)} = \{f : \mathrm{prem}(f, \mathrm{CS}^{(i)}) = 0\}$, *for* $i = 1 \cdots r$. *Then for all* $i$, $\mathrm{PD}^{(i)}$ *is a prime ideal with an irreducible characteristic set* $\mathrm{CS}^{(i)}$. *Moreover, we have*

$$\mathcal{V}(\mathrm{CS}^{(i)}) \setminus \mathcal{V}(J^{(i)}) \subseteq \mathcal{V}(\mathrm{PD}^{(i)}) \subseteq \mathcal{V}(\mathrm{CS}^{(i)}) \quad (1)$$

*and a decomposition of the corresponding algebraic set of* PS

$$\mathcal{V}(\mathrm{PS}) = \bigcup_{i=1}^{r} \mathcal{V}(\mathrm{PD}^{(i)}), \tag{2}$$

**Lemma 2.2** *Let $K$ be an algebraically closed field and $I$ be a homogeneous ideal in $K[x_0, x_1, \ldots, x_n]$. If $f \in K[x_0, x_1, \ldots, x_n]$ is any nonconstant homogeneous polynomial whose class in the quotient ring $K[x_0, x_1, \ldots, x_n]/I$ is not a zero divisor, then*

$$\dim \mathcal{V}(I + \langle f \rangle) = \dim \mathcal{V}(I) - 1$$

# 3 The Dimension of the Irreducible Components

Given an irreducible ascending chain, the difference of the algebraic set defined by the ascending chain from the algebraic set defined by the product of its initials may not be an algebraic set. But the following theorem, which is proposed by the author, shows the Zariski closure of the difference.

**Theorem 3.1** *Let* CS *be an irreducible ascending chain,* PD *be the corresponding prime ideal, i.e.* $\mathrm{PD} = \{f : \mathrm{prem}(f,\ \mathrm{CS}) = 0\}$*, and $J$ be the product of the initials of the polynomials in* CS*. Then $\mathcal{V}(\mathrm{PD})$ is the Zariski closure of $\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)$, i.e.*

$$\mathcal{V}(\mathrm{PD}) = \overline{\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)}.$$

*In other words, $\mathcal{V}(\mathrm{PD})$ is the smallest algebraic set containing $\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)$.*

Proof. Assume that $\mathcal{I}$ is an ideal in $K[u_1, \cdots, u_{k-h}, x_1, \cdots, x_h]$ such that

$$\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J) \subseteq \mathcal{V}(\mathcal{I}).$$

Let $f$ be an arbitrary polynomial in $\mathcal{I}$ and $R$ be the pseudoremainder of $f$ with respect to CS then we have

$$R(P) = 0,$$

for all $P \in \mathcal{V}(\mathrm{CS}) = (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)) \cup (\mathcal{V}(\mathrm{CS}) \cap \mathcal{V}(J))$. By Lemma 2.1, $R$ vanishes in particular at every zero of PD. Since PD is prime, $R$ is a polynomial in PD by Hilbert's Nullstellensatz and hence $R(\zeta) = 0$ where $\zeta$ is an extended zero of CS. That means, $R \equiv 0$ and so $f \in \mathrm{PD}$. Therefore,

$$\mathcal{V}(\mathrm{PD}) \subseteq \mathcal{V}(\mathcal{I}).$$

□

In addition to finding the Zariski closure, by doing some more investigations into the dimension of the algebraic sets, we even get a stronger result as follows.

**Theorem 3.2** *Let* CS*,* PD *and $J$ be as in Theorem 3.1. Then*

$$\dim(\mathcal{V}(\mathrm{PD}) \setminus (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))) = \dim \mathcal{V}(\mathrm{PD}) - 1.$$

Proof. From Theorem 3.1,

$$\mathcal{V}(\mathrm{PD}) = \overline{\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)}.$$

We will now prove that there is only a measure zero set[1] of points which are members of $\mathcal{V}(\mathrm{PD})$ but not $\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)$. Let $P$ be such a point, then $P \in \mathcal{V}(\mathrm{PD})$ and $P \notin \mathcal{V}(\mathrm{CS})$ or $P \in \mathcal{V}(J)$. But the former cannot occur, therefore,

$$P \in \mathcal{V}(\mathrm{PD} + \langle J \rangle) = \mathcal{V}(\mathrm{PD} + \langle I_1 \cdots I_r \rangle).$$

[1] A measure zero set of points with respect to a set $V$ is a set whose dimension is strictly smaller then $\dim V$

In addition, we have

$$\mathcal{V}(\mathrm{PD} + \langle J \rangle) = \mathcal{V}(\mathrm{PD}) \setminus (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)).$$

Homogenize the prime ideal PD obtaining $(\mathrm{PD})^h$ which is a homogenous prime ideal. Since CS is irreducible, for all $j = 1 \dots r$, $I_j \notin \mathrm{PD}$ and then $J \notin \mathrm{PD}$, where $I_j$s are coefficients of polynomials in CS. Since $K[x_0, x_1, \dots, x_n]/(\mathrm{PD})^h$ is an integral domain, the class of $J$ is not zero in $K[x_0, x_1, \dots, x_n]/(\mathrm{PD})^h$ and hence it is not a zero divisor. From Corollary 2.2, we have

$$\dim \mathcal{V}(\mathrm{PD} + \langle J \rangle) = \dim \mathcal{V}(\mathrm{PD}) - 1$$

Therefore,

$$\dim (\mathcal{V}(\mathrm{PD}) \setminus (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))) = \dim \mathcal{V}(\mathrm{PD}) - 1.$$

□

Note that from the following example, we have $\dim \mathcal{V}(\mathrm{CS}) = \dim(\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))$ but we may not have $\dim(\mathcal{V}(\mathrm{CS}) \setminus (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))) < \dim \mathcal{V}(\mathrm{CS})$.

**Example 3.1** *Assume that we have fixed the order $x \prec y \prec z$. Let* CS *be* $\{y^3 - x^4, xz - y^2\}$, *an irreducible ascending chain. Then we have*

$$\dim \mathcal{V}(\mathrm{CS}) = \dim(\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J)) = 1.$$

*But*

$$\dim(\mathcal{V}(\mathrm{CS}) \setminus (\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))) = \dim \mathcal{V}(\mathrm{CS}) = 1.$$

We now introduce the concept of pseudoirreducibility. This is a new idea of the author's which has been first reported in this paper.

**Definition 3.1** *Given an algebraic set $\mathcal{V}$, a set of affine sets $\{\widehat{V^{(1)}}, \dots, \widehat{V^{(r)}}\}$ is called a pseudoirreducible decomposition of $\mathcal{V}$ if for all $i = 1 \dots r$, $\widehat{V^{(i)}}$ coincides with $V^{(i)}$ except at a measure zero set of points (i.e. a set whose dimension is strictly smaller then $\dim V^{(i)}$), where $V^{(1)}, \dots V^{(r)}$ is the irreducible decomposition of $\mathcal{V}$.*

Note that $\widehat{V^{(i)}}$ need not be an algebraic set. We will state and prove the following theorem on the pseudoirreducible decomposition.

**Corollary 3.1** *Given a system* PS *of polynomials with a noncontractible sequence of irreducible extended characteristic sets* $\mathrm{CS}^{(1)}, \mathrm{CS}^{(2)}, \dots, \mathrm{CS}^{(r)}$. *Then*

$$(\mathcal{V}(\mathrm{CS}^{(1)}) \setminus \mathcal{V}(J^{(1)})), \dots, (\mathcal{V}(\mathrm{CS}^{(r)}) \setminus \mathcal{V}(J^{(r)}))$$

*is a pseudoirreducible decomposition of* $\mathcal{V}(\mathrm{PS})$

Proof. From Ritt's theorem, we have

$$\mathcal{V}(\mathrm{PS}) = \bigcup_{i=1}^{r} (\mathcal{V}(\mathrm{CS}^{(i)}) \setminus \mathcal{V}(J^{(i)})).$$

For all $1 \le i \le r$, let $\mathrm{PD}^{(i)} = \{f : \mathrm{prem}(f, \mathrm{CS}^{(i)}) = 0\}$, then $\mathrm{PD}^{(i)}$ is a prime ideal and hence $\mathcal{V}(\mathrm{PD}^{(i)})$ is irreducible. The assertion follows Theorem 3.2. □

**Corollary 3.2** *Let* CS, PD *and $J$ be as in Theorem 3.2. In case of a one-dimensional algebraic set, we have only finitely many points which are members of the irreducible components* $\mathcal{V}(\mathrm{PD})$*s but not members of the pseudoirreducible components* $(\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J))$*s.*

Proof. The assertion follows Theorem 3.2. □

## 4 Applications

We found that the above idea of avoiding heavy computations of generating sets is very useful in Computer Aided Geometric Design and Visualization. In particular for the approximation and representation of one-dimensional algebraic sets in higher dimensional spaces (see [Tra96b, Tra96a]). The advantages of this approach are that:

1. We almost have the irreducible decomposition.
2. The system of equations corresponding to each pseudoirreducible component is very simple. So it is much easier to be traced or evaluated.

The following algorithm can be used for tracing along a one-dimensional algebraic set in higher dimensions.

**Algorithm 4.1**

*Inputs: a one-dimensional algebraic set in higher dimensions defined implicitly by $m$ polynomials $p_1, \ldots, p_m \in \mathbb{Q}[x_1, \ldots, x_n]$. A tolerance $\epsilon$ for precision of the representation.*

*Output: A space "graph" of the algebraic set $V = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : p_1(x_1, \ldots, x_n) = \ldots = p_m(x_1, \ldots, x_n) = 0\}$.*

1. *Compute a pseudoirreducible decomposition of $\mathcal{V}(PS)$ by using Theorem 3.1.*
2. *For each pseudoirreducible component of the algebraic set, find a starting point by using the method in [Tra97] with some of the variables can take complex values.*
3. *From a point on the curve, an approximate value of the next point is obtained by taking a small step size in a direction determined by the local geometry of the curve. Refine the approximate value to a curve point by using the method in [Tra97].*
4. *Represent the space curve.*

We have implemented the algorithm using CASA, a system for constructive algebraic geometry developed at RISC-Linz and based upon the kernel of the Maple language (i.e. we have our own implementation of algorithms for computations such as Gröbner bases for an arbitrary admissible ordering, Puiseux expansions, resultants, etc. See [MWW93] and [TW97] for more details). All the experiments were carried out on an SGI-IRIS workstation under IRIX 5.2 with 64MB RAM using MIPS-RISC 4000A/100MHz CPU.

The following are two examples of one-dimensional algebraic sets which are very tough for other methods. In fact, the computer system would crash if one tries to compute the irreducible decomposition or Gröbner basis of the ideal corresponding to the algebraic sets.

$$\begin{aligned} PS_1 &= \{(x-u)^2 + (y-v)^2 - 1, v^2 - u^3, \\ &\quad 2v(x-u) + 3u^2(y-v), (3wu^2 - 1)(2wv - 1)\} \\ PS_2 &= \{t_1^2 + t_2^2 + t_3^2 - 1, \\ &\quad u_1 t_1 + u_2 t_2 + u_3 t_3, \\ &\quad (u_1 + 3t_3)^2 + u_2^2 + (u_3 - 3t_1)^2 - 1, \\ &\quad (u_1 - 3t_3)^2 + u_2^2 + (u_3 + 3t_1)^2 - 1, \\ &\quad (u_1 - 7t_3 + t_2)^2 + (u_2 - t_1)^2 + (u_3 + 7t_1)^2 - 1, \\ &\quad (u_1 - v_1 t_3 + 2t_2)^2 + (u_2 - 2t_1 + t_3)^2 + \\ &\quad + (u_3 - t_2 + v_1 t_1)^2 - 1\} \end{aligned}$$

Meanwhile, using our method, we are able trace along those one-dimensional algebraic sets. In the Figure 1, we report the time to use for tracing along the algebraic sets with the tolerance of $10^{-15}$. The time for approximation and refining of regular points or near singularities are the average of 1000 tests.

Figure 1: Time Consuming

| | Tracing $PS_1$ (second) | Tracing $PS_2$ (second) |
|---|---|---|
| Starting point | 52.484 | 82.500 |
| Regular points | $\sim 9.384$ | $\sim 24.400$ |
| Near singularities | $\sim 20.150$ | $\sim 26.666$ |

# 5 Combining ATP with Computer Algebra Systems

One of the most successful application of the characteristic set method is in Geometric Theorem Proving by the works of W. T. Wu and his followers (see [Wu84, Wu94], [Cho88], etc. ). In this section, we report our experiments on combining results in Automatic Theorem Proving with the computer algebra system CASA.

CASA is a computer algebra system for constructive Algebraic Geometry which is designed for performing computations and reasoning about geometric objects in classical algebraic geometry, in particular affine and projective algebraic geometry over an algebraically closed field $K$ of characteristic 0. CASA has been developed at RISC-Linz over the last six years, starting in 1990, by a research group under the direction of Doz. Dr. Franz Winkler and currently the system is maintained by the author. The system is built as an enhancement of the traditional and widely used computer algebra system Maple. The core of the system is that we can represent an algebraic set in four different representations. Algebraic sets may be embedded into affine or projective spaces.

- Implicit representation: An algebraic set is the set of common zeros of a system of polynomial equations. To give an algebraic set in implicit form means to give finitely many polynomials.

- Projected representation: As a consequence of the primitive element theorem every irreducible $d$–dimensional algebraic set in $n$–dimensional space is, after a suitable linear transformation of coordinates, birationally projectable onto an irreducible $d$–dimensional algebraic set in $(d+1)$–dimensional space, which can be specified by a single polynomial in $d+1$ variables. This can be generalized to unmixed-dimensional algebraic sets. An algebraic set in projected form is given by a polynomial and a tuple of rational functions (specifying the birational mapping).

- Parametric representation: Some irreducible algebraic sets can be parameterized by rational functions. An algebraic set in parametric form is given by a tuple of rational functions that parameterizes the algebraic set.

- Representation by places or Puiseux series: All algebraic curves can be parameterized by a set of power series that are convergent around a point of the curve. An algebraic set is given by places if for each branch passing through a certain point on the algebraic set a tuple of power series that parameterizes the algebraic set around the point is specified.

The system also works with the polynomial ideals corresponding to these geometric objects. The operations available in CASA include: (1) ideal theoretic operations $+, *, \cap, /$, (2) creating algebraic sets in different representations, (3) generating curves of fixed multiplicities at given points, (4) intersection, union, and difference of algebraic sets, (5) computing tangent cones and tangent spaces, (6) computation of the dimension of an algebraic set, (7) decomposition into irreducible components, (8) transformations of algebraic sets to hyper-surfaces, (9) computation of the genus of a curve, (10) rational parameterization of curves, (11) implicitization of parametrically given algebraic sets, (12) Puiseux series expansions, (13) plotting both explicitly and implicitly given curves and surfaces.

To combine the results in Automatic Theorem Proving with a computer algebra system, on the one hand we construct an engine within the computer algebra system for proving theorems in algebraic geometry. Particularly, for theorems in elementary geometry, the engine will first translate the geometric statements into algebraic ones by using a built-in dictionary.

For checking the validity of theorems in Algebraic Geometry, we use the following propositions.

**Lemma 5.1** *Given a theorem* $\mathrm{PS} \Rightarrow f_c$ *in algebraic form, where* PS *is the set of hypotheses and* $f_c$ *is the conclusion of the theorem. The theorem is* **strictly** *true if* $\mathrm{prem}(f_c, \mathrm{CS}) = 0$ *and* $\mathcal{V}(\mathrm{CS}) \cap \mathcal{V}(J) = \emptyset$*, where* CS *is an extended characteristic set of* PS *and* $J$ *is the product of the initials of the polynomials in* CS.

PROOF. Since CS is an extended characteristic set of PS, $\mathcal{V}(\mathrm{CS}) \setminus \mathcal{V}(J) \subset \mathcal{V}(\mathrm{PS}) \subset \mathcal{V}(\mathrm{CS})$. From the necessary condition of the theorem, $\mathcal{V}(\mathrm{CS}) \subset \mathcal{V}(f_c)$ and therefore $\mathcal{V}(\mathrm{PS}) \subset \mathcal{V}(f_c)$. □

Checking the emptiness of $\mathcal{V}(\mathrm{CS}) \cap \mathcal{V}(J)$ can be done by checking the sum $\langle \mathrm{CS} \rangle + \langle J \rangle$. Note that the theorem $\mathrm{PS} \Rightarrow \{f_{c_1}, \ldots, f_{c_n}\}$ is true if and only if $\mathrm{PS} \Rightarrow f_{c_i}$ is true for $i = 1 \ldots n$. Then for making the presentation simple, we assume that the set of conclusions is a singleton.

**Lemma 5.2** *Given a theorem* $\mathrm{PS} \Rightarrow f_c$ *in algebraic form, where* PS *is the set of hypotheses and* $f_c$ *is the conclusion of the theorem. The theorem is* **strictly** *true if* $\mathrm{prem}(f_c, \mathrm{CS}^{(i)}) = 0$ *for* $i = 1 \ldots h$*, where* $(\mathrm{CS}^{(i)})$ *is a sequence of extended characteristic sets of* PS.

PROOF. Since $\mathrm{prem}(f_c, \mathrm{CS}^{(i)}) = 0$ for $i = 1 \ldots h$, $\mathcal{V}(\mathrm{CS}^{(i)}) \setminus \mathcal{V}(J^{(i)}) \subset \mathcal{V}(f_c)$ for $i = 1 \ldots h$. But $\mathcal{V}(\mathrm{PS}) = \cup_i (\mathcal{V}(\mathrm{CS}^{(i)}) \setminus \mathcal{V}(J^{(i)}))$. Therefore $\mathcal{V}(\mathrm{PS}) \subset \mathcal{V}(f_c)$ □

Subsequently, we prove two theorems concerning with the completeness of theorem proving by using the characteristic set method and Gröbner basis method respectively.

**Theorem 5.1 (Completeness of Theorem Proving)** *Given a theorem* $\mathrm{PS} \Rightarrow f_c$ *in algebraic form, where* PS *is the set of hypotheses and* $f_c$ *is the conclusion of the theorem. Then we can algorithmically decide about the correctness of the theorem. Moreover, the theorem is* **strictly** *true if and only if* $\mathrm{prem}(f_c, \mathrm{CS}^{(i)}) = 0$ *for* $i = 1 \ldots h$*, where* $(\mathrm{CS}^{(i)})$ *for* $i = 1 \ldots h$*, is a sequence of irreducible extended characteristic sets of* PS.

PROOF. The necessary condition follows directly from the previous theorems. For the sufficient condition, suppose that the theorem is true, i.e. $f_c(P) = 0$ for all

$P \in \mathcal{V}(\mathrm{PS})$. Then $\mathcal{V}(\mathrm{PS}) \subset \mathcal{V}(f_c)$. We have $\mathcal{V}(\mathrm{PD}^{(i)})) \subset \mathcal{V}(f_c)$ for $i = 1 \ldots h$, where $\mathrm{PD}^{(i)})$ is the corresponding prime ideal of $\mathrm{CS}^{(i)}$. Since $\mathrm{PD}^{(i)}$ is prime and by Hilbert's Nullstellensatz, $f_c$ is a polynomial in $\mathrm{PD}^{(i)}$. Hence, $prem(f_c, \mathrm{CS}^{(i)}) = 0$ for $i = 1 \ldots h$. $\square$

**Theorem 5.2 (Completeness of Theorem Proving)** *Given a theorem* $\mathrm{PS} \Rightarrow f_c$ *in algebraic form, where* PS *is the set of hypotheses and* $f_c$ *is the conclusion of the theorem. Then we can algorithmically decide about the correctness of the theorem. Moreover, the theorem is* **strictly** *true if and only if* $1 \in \mathrm{GB}(\mathrm{PS}, f_c \cdot z - 1) \subset K[u_1, \cdots, u_{k-h}, x_1, \cdots, x_h, z]$, *where* $z$ *is an extra variable.*

Proof. By Hilbert's Nullstellensatz, $\mathcal{V}(\mathrm{PS}) \subset \mathcal{V}(f_c)$ if and only if $f_c \in \mathrm{radical}(PS)$. But the latter condition is satisfied if and only if $1 \in \mathrm{GB}(\mathrm{PS}, f_c \cdot z - 1)$. $\square$

In particular, for checking the validity of theorems in elementary geometry we use the same scheme as in [Cho88]. That means, we first divide the set of variables into two subsets, namely the set of independent variables and the set of dependent variables. Then for checking the generic validity of a theorem, we just check the validity of the irreducible components of the algebraic set defined by the set of hypotheses and degenerates on which the independent variables are algebraically independent. More precisely, for checking the validity of a theorem in formula F1 by using the Gröbner basis method, we use the following algorithm in which we need only one extra equation and one extra variable.

**Theorem 5.3** *Given a theorem* $\mathrm{PS} \Rightarrow f_c$ *in algebraic form together with a set of non-degenerates* $\{s_1, s_2, \ldots s_r\}$, *where* PS *is the set of hypotheses and* $f_c$ *is the conclusion of the theorem. Then we can algorithmically decide about the correctness of the theorem. Moreover, the theorem is true if and only if* $1 \in \mathrm{GB}(\mathrm{PS}, s_1 \cdot s_2 \cdots s_r \cdot f_c \cdot z - 1) \subset K[u_1, \cdots, u_{k-h}, x_1, \cdots, x_h, z]$, *where* $z$ *is an extra variable.*

Proof. Assume that the theorem is true. Then 1 should be a member of the ideal $\langle \mathrm{PS}, s_1 \cdot s_2 \cdots s_r \cdot f_c \cdot z - 1\rangle$ and therefore a member of $\mathrm{GB}(\mathrm{PS}, s_1 \cdot s_2 \cdots s_r \cdot f_c \cdot z - 1)$. Conversely, let $1 = \sum_1^h a_i \cdot f_i + a_{h+1} \cdot (s_1 \cdot s_2 \cdots s_r \cdot f_c \cdot z - 1)$. We substitute $1/s_1 \cdot s_2 \cdots s_r \cdot f_c$ for $z$ and then multiply both sides with $s_1^N \cdot s_2^N \cdots s_r^N \cdot f_c^N$, where $N$ is the maximum of the degree of $a_i$'s in $z$ for $i = 1 \ldots h$. Then $s_1^N \cdot s_2^N \cdots s_r^N \cdot f_c^N = \sum_1^h \overline{a_i} \cdot f_i$ and therefore $\mathcal{V}(\mathrm{PS}) \setminus \mathcal{V}(s_1 \cdot s_2 \cdots s_r) \subset \mathcal{V}(f_c)$. $\square$

Meanwhile, for checking the generic validity of a theorem in formula F3 by using the Gröbner basis method, we simply check whether $f_c$ is a member of $\mathrm{radical}\langle\mathrm{PS}\rangle \subset K(u_1, \cdots, u_{k-h})[x_1, \cdots, x_h, z]$.

On the other hand, we benefit from the computer algebra system for improving the efficiency of Automatic Theorem Proving algorithms by using more up-to-date algorithms and methods in the computer algebra system. For example, the Automatic Theorem Proving engine in our computer algebra system now can prove as many elementary geometric theorems as in [Cho88] in a reasonable time. Following are some experiments with our combined system. All the experiments were carried out on a SUN-UltraSparc1 workstation under SunOS 5.5 using the kernel of Maple V3. Times are in second.

# 6 Conclusion

We presented some new results of the author's concerning the dimension of the irreducible components of an algebraic set. We also showed how to use our results to develop hybrid symbolic-numerical algorithms, which aim at the goals of

| Theorem | Characteristic Set Method Formula F1 | Characteristic Set Method Formula F3 | Gröbner Basis Method Formula F1 | Gröbner Basis Method Formula F3 |
|---|---|---|---|---|
| Pappus | 0.260 | 0.270 | 0.930 | 0.910 |
| Pappus-point | 1.350 | 1.270 | 1.840 | 2.780 |
| Pascal-conic | 1.110 | 1.170 | 2.060 | 5.270 |
| Gauss-point | 0.790 | 0.790 | 1.550 | 1.720 |
| Gauss-conic | 21.690 | 25.070 | 20.610 | 18.500 |
| Pappus-dual | 0.380 | 0.590 | 0.790 | 1.130 |
| Altitude-dual | 0.130 | 0.130 | 0.350 | 0.330 |
| Simson | 0.150 | 0.150 | 0.420 | 0.590 |

efficiency and reliability, for solving the problem of approximation and representation of one-dimensional algebraic sets in Computer Aided Geometric Design and Visualization. We reported our experiments on combining techniques in Automatic Theorem Proving with CASA, a computer algebra system. We showed that, on the one hand this combination gives us an engine within the computer algebra system for proving theorems in algebraic geometry, in particular theorems in elementary geometry. On the other hand, we benefit from the computer algebra system for improving the efficiency of Automatic Theorem Proving algorithms by using more up-to-date methods.

## References


[Cho88] Shang Ching Chou. *Mechanical Geometry Theorem Proving.* D. Reidel, 1988.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer–Verlag, 1992.

[EHV90] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 1990.

[GTZ88] P. Gianni, B. M. Trager, and G. Zacharias. Gröbner Bases and Primary Decomposition of Polynomial Ideals. *J. Symb. Comput.*, 6: pages 149–167, 1988.

[Her26] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Annalen*, 95:736–788, 1926.

[MRR88] R. Mines, F. Richman, and W. Ruitenberg. *A Course on Constructive Algebra.* Springer-Verlag, New York-Berlin-Heidelberg, 1988.

[MWW93] M. Mnuk, B. Wall, and F. Winkler. Casa reference manual (version 2.1). Technical Report 93–63, RISC, 1993.

[Rit32] J. F. Ritt. *Differential Equations from the Algebraic Standpoint.* Amer. Math. Soc., New York, 1932.

[Rit50] J. F. Ritt. *Differential Algebra*, volume 33. AMS Colloquium Publications, New York, 1950.

[Sei74] A. Seidenberg. Constructions in Algebra. *Trans. Am. Math. Soc.*, 197: pages 273–313, 1974.

[Sei84] A. Seidenberg. On the Lasker–Noether decomposition theorem. *Am. J. Math.*, 106:611–638, 1984.

[Tra96a] Quoc-Nam Tran. *A Hybrid Symbolic-Numerical Approach in Computer Aided Geometric Design (CAGD) and Visualization.* PhD thesis, Research Institute for Symbolic Computation (RISC–Linz), University of Linz, Austria, 1996. dissertation.ps.gz.

[Tra96b] Quoc-Nam Tran. A hybrid symbolic-numerical method for tracing algebraic curves in higher dimensions. In *ICCAM–96 conference, Leuven, Belgium*, 1996.

[Tra97] Quoc-Nam Tran. Extending newton's method for finding the roots of an arbitrary system of equations and its applications. *International Journal of Modeling and Simulation*, 17(4), 1997. To appear.

[TW97] Quoc-Nam Tran and Franz Winkler. Casa reference manual (version 2.3). Technical report, RISC, 1997. Preprint.

[Wu84] W.T. Wu. Basic Principles of Mechanical Theorem Proving in Elementary Geometries. *Journal Sys. Sci. & Math. Scis.*, 4: pages 207–235, 1984.

[Wu94] W.T. Wu. *Basic Principles of Mechanical Theorem Proving in Geometries.* Springer-Verlag, 1994. Translated from Chinese by Xiaofan Jin and Dongming Wang.