MECHANICAL THEOREM PROVING IN
DIFFERENTIAL GEOMETRY

Shang-Ching Chou and Xiao-Shan Gao

Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712-1188

TR-89-08 March 1989
Revision: February 1990
Mechanical Theorem Proving In Differential Geometry

I. Space Curves*

SHANG-CHING CHO and XIAO-SHAN GAO†

Institute for Computing Science
The University of Texas at Austin, Austin, Texas 78712 USA

ABSTRACT With an improved version of Ritt-Wu’s zero decomposition algorithm for differential polynomials, we present two approaches to mechanical proving of geometry theorems in differential geometry. The first approach can be used to prove a theorem when nondegenerate conditions are given explicitly. The second approach can be used to prove a theorem to be generically true. More than fifty nontrivial theorems in the space curve theory have been proved mechanically by our program, in particular, the properties of the Bertrand curves are studied in full detail.

KEYWORDS Mechanical theorem proving, Wu’s method, differential polynomial, Ritt-Wu’s decomposition algorithm, main component, Differential geometry, Bertrand Curves.

* The work reported here was supported in part by the NSF Grant CCR-8702108. The computer facility was supported by the NSF/CER Grant at UT.
† On leave from Institute of Systems Science, Academia Sinica, Beijing.
1. Introduction

In the past decade highly successful algebraic methods for mechanically proving theorems in elementary geometries have been developed. Notably, the method developed by Wu Wen-Tsūn has been used to prove hundreds of hard theorems in Euclidean geometry and non-Euclidean geometries [CH1]. Wu’s method is based on Ritt’s characteristic set (CS) method. The CS method originally developed by J. F. Ritt can also be used to prove theorems in differential geometry, because the CS method is also for differential polynomials. Actually it was Wu who first proposed a method for proving theorems in differential geometry using Ritt’s CS method and also gave several theorems proved by his method [WU1, WU2, WU3]. However, Wu’s work needs further clarification. E.g., it is not clear from Wu’s work that in what sense his method proves theorems. Wu mentioned the notion of “generically (generally) true” for a geometry statement. But his definition of “generally true” needs clarifying. The key problem here is how to understand and handle non-degenerate conditions which are usually implicit and are necessary for a geometry statement to be valid.

Theorems that the CS method addresses are those whose hypothesis and conclusion can be expressed by differential polynomial equations (theorems of equation type). We use the following simple example to illustrate the geometry problems we deal with in this paper.

Example 1.1. Show that the curvature $k$ of a circle is constant.

We adopt a coordinate system in the plane of the circle and choose the center of the circle to be the origin $(0,0)$. We use parametric representation for the circle: let $(x_2, x_3) = (x_2(t), x_3(t))$ be the point on the circle with the radius $x_1$. Note that $x_1$ is a constant, i.e., the derivative of $x_1$ with respect to (ab. wrpt) $t$ is zero. As usual, we use $x_1'$ to denote the derivative of $x_1(t)$, i.e., $\frac{dx_1(t)}{dt}$. Let $x_4$ be the square of the derivative of the arc of the circle wrpt $t$ and $x_5$ be the curvature $k$ of the circle, then the hypothesis can be expressed by the following three equations.

\[
\begin{align*}
H_1 &= x_2^2 + x_3^2 - x_1^2 = 0 \\
H_2 &= x_4 - x_3^2 - x_2^2 = 0 \\
H_3 &= x_2^2 x_3^2 - (x_2' x_3' - x_2' x_3')^2 = 0
\end{align*}
\]

The equation of the circle $c = (x_2, x_3)$.

\[x_4 = (\frac{dx_1}{dt})^2 = |c'|^2, \text{ where } s \text{ is the arc.}\]

The definition of the curvature $k = \frac{|c'|}{|s|}$. The conclusion that $k$ is constant can be expressed by the equation $G = x_5 = 0$. Thus one can ask whether the conclusion $G = 0$ follows from the three hypothesis equations, i.e., whether the following formula

(1.2) \[\forall x_1 \cdots \forall x_5[(H_1 = 0 \land H_2 = 0 \land H_3 = 0) \Rightarrow G = 0]\]

is valid. However, (1.2) is not valid because certain non-degenerate conditions are missing. For example, (1.2) is not valid when $x_1 = 0$, i.e., the circle degenerates to a point. In this paper we propose two approaches to dealing with non-degeneracy.

Let $HS = \{H_1, \ldots, H_r = 0\}$ be the set (conjunction) of the hypotheses and $G = 0$ be the conclusion of a geometry statement, where the $H_i$ and $G$ are differential polynomials (for the definition see Section 2). As we know, the formula

(1.3) \[\forall x[(H_1 = 0 \land \cdots \land H_r = 0) \Rightarrow G = 0]\]

is not accurate because it is valid only under certain non-degenerate conditions. As in elementary geometry, there are two formulations (approaches) for dealing with non-degenerate conditions.
**Formulation F1.** Introduce parameters and the notion of "generally (generically) true" and decide whether (1.3) is generally true, at the same time generating non-degenerate conditions to make (1.3) valid. We will give the precise definition of "generally true" in Section 3.

**Formulation F2.** Explicitly specify non-degenerate conditions as a part of the geometry statement. Let $DS = \{D_1 \neq 0, \ldots, D_l \neq 0\}$ be the non-degenerate conditions thus specified, then this formulation is to decide whether the following formula is valid:

$$\forall x[\left(H_1 = 0 \land \cdots \land H_r = 0 \land D_1 \neq 0 \land \cdots \land D_l \neq 0\right) \Rightarrow G = 0].$$

**Example 1.1.** (Continue). The variables $x_1$ and $x_2$, i.e., the radius of the circle and one coordinate of the point, can be arbitrarily chosen. Thus they can be chosen to be parameters. Once $x_1$ and $x_2$ are fixed, the remaining variables, $x_3$, $x_4$, and $x_5$, are determined by the three hypothesis equations. Thus they are dependent variables. According to Formulation F1, the problem now is to ask whether formula (1.2) is generally true wrpt parameters $x_1$ and $x_2$. In Formulation F2, a natural non-degenerate condition can be $x_1 \neq 0$. Thus we can ask whether

$$\forall x_1 \cdots \forall x_5[(H_1 = 0 \land H_2 = 0 \land H_3 = 0 \land x_1 \neq 0) \Rightarrow g = 0]$$

is valid without adding any additional conditions.

Formulation F2 is easy to understand. However, if one of the necessary non-degenerate conditions is missing and (1.4) is invalid, then we don't have any information about why (1.4) is invalid: it is invalid because of a missing necessary non-degenerate condition or because of the nature of the statement, i.e., it cannot be valid no matter how many reasonable non-degenerate conditions are added. Formulation F1 can answer this question, but it needs more mathematical background. In this paper we will present two methods to prove (differential geometry) theorems according to Formulations F1 and F2, respectively. Our method for Formulation F1 is a further development of Wu's work on the same topic. Our method for Formulation F2 is new.

The basis of our methods is Ritt–Wu's zero decomposition algorithm. In our experience, the original version of Ritt-Wu's algorithm often produces large differential polynomials, thus in many cases making the CS method beyond the computer time and space limits available. To overcome this difficulty, we extend the concepts of weak ascending chain and W-prem for ordinary polynomials presented in [CG1] to the case of differential polynomials, the sizes of polynomials occurring in the decomposition can be reduced. Based on these concepts, an improved version of Ritt-Wu's decomposition algorithm is presented. A program based on the new version of the decomposition algorithm is efficient and has mechanically proved about 100 nontrivial theorems in the theory of space curves.

The methods developed in this paper can also be used to prove theorems in mechanics. For details, see [CG2, CG3].

This paper consists of two parts: an improved version of Ritt–Wu's zero decomposition algorithm (Section 2) and two methods for proving differential geometry theorems based on this algorithm (Section 3). In Section 4, we give several theorems in the space curve theory mechanically proved by our program.

**2. An Improvement of Ritt-Wu's Decomposition Algorithm**
2.1. Preliminary Definitions and Algorithms

A differential field is a field together with a third (unary) operation \( \cdot \) (the differential operation) satisfying the following properties:

\[
(a + b)' = a' + b' \\
(ab)' = a'b + ab'.
\]

Generally, we can work with a computable differential field \( K \) of characteristic zero. But for our purpose of theorem proving, in what follows, we assume that \( K \) is the rational function field \( \mathbb{Q}(t) \) in the variable \( t \) with the differential operation \( d/dt \). Let \( x_1, \ldots, x_n \) be indeterminates. The \( j \)-th \(( j \geq 0)\) derivative of a variable \( x_i \) is denoted by \( x_{i,j} \). Thus \( x_i = x_{i,0}, \ (x_i)' = x_{i,1}, \ (x_i)'' = x_{i,2}, \) etc. An ordinary polynomial \( P \) in variables \( x_{i,j} \) (for \( j \geq 0 \)) and with coefficients in \( K \) is called a differential polynomial (ab. d-pol) in \( x_1, \ldots, x_n \). For example, \( H_1, H_2 \) and \( H_3 \) in Example 1.1 are differential polynomials. As far as the operations plus \( + \) and times \( \cdot \) are concerned, d-pols behave as ordinary polynomials. However, they have the third operation, i.e., the \( \cdot \) operation. The set of all differential polynomials in \( x_1, \ldots, x_n \) is called the differential polynomial ring in \( x_1, \ldots, x_n \) over \( K \) and denoted by \( K\{x_1, \ldots, x_n\} = K\{X\} \).

A non-empty subset \( D \) of \( K\{X\} \) is called an ideal if for any \( g \in D \), \( (i) \ f \in D \Rightarrow f + g \in D; \ (ii) \ f \in K\{X\} \Rightarrow fg \in D; \ (iii) \ g' \in D \). An ideal \( D \) is called a prime ideal if \( fg \in D \Rightarrow f \in D \) or \( g \in D \) for any \( f \) and \( g \) in \( K\{X\} \). An ideal \( D \) is called a radical ideal if \( f^n \in D \Rightarrow f \in D \) for any \( f \) in \( K\{X\} \) and positive integer \( n \). Let \( S \) be a non-empty set in \( K\{X\} \), the minimal ideal \( D \) containing \( S \) is called the ideal generated by \( S \) and denoted by \( \text{Ideal}(S) \); \( S \) is called a set of generators of \( D \). Similarly, we can define \( \text{Radical}(S) \) to be the minimal radical ideal containing \( S \). It is a well known result in [R12] that a radical ideal has a finite set of generators (Raudenbush’s theorem); but this is not true for an ideal. Obviously, \( \text{Ideal}(S) \) is the set of all linear combinations of the d-pols in \( S \) and their derivatives.

Let \( P \) be a d-pol. The class of \( P \), denoted by \( \text{class}(P) \), is the largest \( p \) such that some \( x_{p,i} \) actually occurs in \( P \). If \( P \in K \), \( \text{class}(P) = 0 \). The order of \( P \) wrt \( x_i \) is the largest \( j \) such that \( x_{i,j} \) appears in \( P \). If \( P \) does not involve \( x_i \), the order of \( P \) wrt \( x_i \) is 0. Let a d-pol \( P \) be of class \( p \) and the order of \( P \) wrt \( x_p \) be \( o \), then \( x_p \) and \( x_{p,o} \) are called the leading variable and the lead of \( P \) respectively. Let \( P_1 \) and \( P_2 \) be two d-pols, we say \( P_2 \) is of higher rank than \( P_1 \) in \( x_i \), if either \( P_2 \) is of higher order than \( P_1 \) wrt \( x_i \) or \( P_2 \) and \( P_1 \) are of the same order \( q \) wrt \( x_i \) and \( P_2 \) is of higher degree in \( x_{i,q} \) than \( P_1 \). \( P_2 \) is said to be of higher rank than \( P_1 \), if either \( \text{class}(P_2) > \text{class}(P_1) \) or \( P_2 \) and \( P_1 \) are of the same class \( p \) and \( P_2 \) is of higher rank than \( P_1 \) in \( x_p \). Two d-pols for which no difference in rank is established by the foregoing criteria are said to be of the same rank.

A sequence of d-pols \( ASC = A_1, \ldots, A_p \) is said to be a quasi ascending (ab. asc) chain, if either \( r = 1 \) and \( A_1 \neq 0 \) or \( 0 < \text{class}(A_i) < \text{class}(A_j) \) for \( 1 \leq i < j \). \( ASC \) is called nontrivial if \( \text{class}(A_1) > 0 \). A quasi asc chain \( ASC \) is said to be of higher rank than another quasi asc chain \( ASC' = B_1, \ldots, B_r \), if either (i) there is a \( j \), exceeding neither \( p \) nor \( s \), such that \( A_j \) and \( B_i \) are of the same rank for \( i < j \) and that \( A_j \) is of higher rank than \( B_j \); or (ii) \( s > p \) and \( A_i \) and \( B_i \) are of the same rank for \( i \leq p \). We denote \( ASC > ASC' \). Two quasi asc chains for which no difference in rank is established by the foregoing criteria are said to be of the same rank.

**Lemma 2.1.** Let

\[
ASC_1, ASC_2, \ldots, ASC_i, \ldots
\]
be an infinite sequence of quasi asc chains the ranks of which do not increase. Then there is an index \(i_0\) such that for any \(i > i_0\), \(ASC_i\) and \(ASC_{i_0}\) have the same rank.

**Proof.** See the proof for a similar result in 4 of Chapter I in [RI2].

Let a d-pol \(P\) be of class \(p > 0\) and of order \(m\) in \(x_p\). We call \(\frac{\partial P}{\partial x_{p,m}}\) the separant of \(P\). The coefficient of the highest power of \(x_{p,m}\) in \(P\) considered as a polynomial of \(x_{p,m}\) is called the initial of \(P\). Let \(I\) and \(S\) be the initial and separant of \(P\) respectively. For any d-pol \(G\) we shall define the pseudo remainder of \(G\) wrpt \(P\): \(\text{prem}(G, P)\) as below. Let \(G\) be of order \(h\) in \(x_p\) and \(k_1 = h - m\). If \(k_1 > 0\) then \(P^{(k_1)}\), the \(k_1\)-th derivative of \(P\), will be linear in \(x_{p,h}\) with \(S\) as the coefficient. Note that \(G\) and \(P^{(k_1)}\) can be looked as ordinary polynomials of \(x_{p,h}\). Using the algorithm of pseudo division of ordinary polynomials for \(G\) and \(P^{(k_1)}\), we can find a nonnegative integer \(v_1\) and d-pols \(C_1\) and \(D_1\) such that:

\[
S^{v_1}G = C_1P^{(k_1)} + D_1
\]

where \(D_1\) is of order less than \(h\) in \(x_p\). If \(D_1\) is of order higher than \(P\) in \(x_p\), we repeat the above process for \(D_1\), and so on. Finally we can find a nonnegative integer \(v\) and d-pols \(Q_i\) such that:

\[
S^vG = Q_1P^{(k_1)} + \ldots + Q_sP^{(k_s)} + D
\]

where \(D\) is of order not higher than \(m\) in \(x_p\). If the order of \(D\) wrpt \(x_p\) is less than \(m\) then define \(\text{prem}(G, P) = G\). Otherwise, \(D\) is of order \(m\) wrpt \(x_p\) and both \(D\) and \(P\) can be looked as ordinary polynomials of \(x_{p,m}\). Using the algorithm of pseudo division of ordinary polynomials for \(D\) and \(P\), we have

\[
S^vI^uG = Q_1'P^{(k_1)} + \ldots + Q_s'P^{(k_s)} +QP + R
\]

where \(R\) is a d-pol with lower rank than \(P\) in \(x_p\). We define \(R = \text{prem}(G, P)\).

As an example let us show how to calculate \(\text{prem}(q_2, q_1)\) for \(q_2 = x_3' + x_3\) and \(q_1 = x_3^2 + x_2^2 - x_1^2\).

\[
q_1' = 2x_3x_3' + 2x_2x_2' - 2x_1x_1' \\
q_3 = 2x_3q_2 - q_1' = 2x_3^2 - 2x_2x_2' + 2x_1x_1' \\
q_4 = q_3 - 2q_1 = 2x_1x_1' - 2x_2x_2' + x_1^2 - x_2^2 \\
\text{The differentiation of } q_1. \\
\text{Eliminating } x_3'. \\
\text{Eliminating } x_3.
\]

Let \(R = q_1 = \text{prem}(q_2, q_1)\). We have the remainder formula \(S q_2 = q_1' + 2q_1 + R\), where \(S = 2x_3\) is the separant of \(q_1\).

For a quasi asc chain \(ASC = A_1, \ldots, A_p\) with \(\text{class}(A_i) > 0\), we define the pseudo remainder of \(G\) wrpt \(ASC\) inductively as \(\text{prem}(G, ASC) = \text{prem}(\text{prem}(G, A_p), A_1, \ldots, A_{p-1})\). Let \(R = \text{prem}(G, ASC)\), then there is a product \(J\) of powers of the initials and separatants of d-pols in \(ASC\) and we have the following important remainder formula:

\[
(2.2) \quad JG - R \in \text{Ideal}(A_1, \ldots, A_p).
\]

**Definition 2.3.** Let \(ASC = A_1, \ldots, A_p\) be a quasi asc chain. It is called a weak asc chain, if for each \(i\) \((1 < i \leq p)\) the pseudo remainders of the initial and separant of \(A_i\) are not zero. \(ASC\) is called an asc chain if for each \(1 < i \leq p\), \(A_i\) is of lower rank than \(A_j\) in the leading variable of \(A_j\) \((j = 1, \ldots, i - 1)\). Note that an asc chain is also a weak asc chain.

Now we define a new reduction procedure, the key to our improved algorithm.
Definition 2.4. The weak pseudo remainder, W-prem, of a d-pol $P$ wrpt to a nontrivial quasi asc chain $ASC = A_1, ..., A_p$ is defined inductively as follows. Base case $p = 1$: if $\text{class}(P) = \text{class}(A_1)$ or the pseudo remainder of the initial or separant of $P$ wrpt $A_1$ is zero then $\text{W-prem}(P, A_1) = \text{prem}(P, A_1)$; otherwise $\text{W-prem}(P, A_1) = P$. If $p > 1$, then we have the following four cases:

Case a. $\text{W-prem}(P, ASC) = \text{W-prem}(\text{prem}(P, A_p), A_1, ..., A_{p-1})$ if $\text{class}(P) = \text{class}(A_p)$.

Case b. $\text{W-prem}(P, ASC) = \text{W-prem}(P, A_1, ..., A_{p-1})$ if $\text{class}(P) < \text{class}(A_p)$.

Case c. $\text{W-prem}(P, ASC) = \text{prem}(P, ASC)$, if the pseudo remainder of the separant or the initial of $P$ wrpt $ASC$ is zero.

Case d. Otherwise, $\text{W-prem}(P, ASC) = P$.

If $\text{W-prem}(P, ASC) = P$, we say $P$ is W-reduced wrpt $ASC$. Note that $\text{W-prem}(P, ASC)$ is always W-reduced wrpt $ASC$ and a quasi asc chain $ASC = A_1, ..., A_p$ is a weak asc chain if each $A_i$ is W-reduced wrpt $A_1, ..., A_{i-1}$.

Lemma 2.5. For a d-pol $P$ and a weak asc chain $ASC = A_1, ..., A_p$, if $\text{W-prem}(P, ASC) = 0$ then $\text{prem}(P, ASC) = 0$.

Proof. Use induction on $p$. It is obvious when $p = 1$. Suppose $p > 1$. There are four cases a–d. For cases a and b if $\text{prem}(P, A_p) = 0$ the lemma is true; otherwise the lemma comes from the induction hypothesis. For case c, the lemma is also true because $\text{W-prem}(P, ASC) = \text{prem}(P, ASC)$. For case d, $\text{W-prem}(P, ASC) \neq 0$. Then the lemma is obviously true in this case.

In what follows, whenever we talk about a finite set of d-pols DPS, we always assume it is non-empty and does not contain 0.

Lemma 2.6. For a finite d-pol set DPS, we can find a weak asc chain $ASC$ in DPS which is not higher than other weak asc chains in DPS. Such a weak asc chain is called a weak basic set of DPS.

Proof. Let $B_1$ be a d-pol which has the lowest rank in $P_0 = \text{DPS}$. If $B_1$ is in $K$ then the asc chain $B_1$ satisfies the condition of the lemma. Otherwise, the class of $B_1$ is positive. Let $P_1$ be the set of the d-pols in $P_0$ which are W-reduced wrpt $B_1$. If $P_1$ is empty, then $B_1$ satisfies the condition of the lemma. Otherwise, let $B_2$ be a d-pol of the lowest rank in $P_1$. Then $B_2$ must be of higher class than $B_1$. Repeat the above process, at last we get a weak asc chain $B_1, B_2, ..., B_k$ with the desired property.

Lemma 2.7. If $P$ is W-reduced wrpt a weak basic set of DPS, then a weak basic set of $\text{DPS} \cup \{P\}$ is of lower rank than a weak basic set of DPS.

Proof. Let $BS = B_1, ..., B_p$ be a weak basic set of DPS. If the class of $P$ is not equal to the class of any d-pol in $BS$, let $i_0$ be the last index such that the class of $B_{i_0}$ is less than the class of $P$, then $B_1, ..., B_{i_0}, P$ will be a weak asc chain contained in $\text{DPS} \cup \{P\}$ which has lower rank than $BS$. Otherwise, let $B_{i_0}$ has the same class as $P$. As $P$ is W-reduced to $BS$ then $P$ must be of lower rank than $B_{i_0}$ by (a) of definition 2.4. Then $B_1, ..., B_{i_0-1}, P$ is a weak asc chain contained in $\text{DPS} \cup \{P\}$ which is of lower rank than $BS$. 

For a quasi asc chain \( ASC \), we introduce the following important notation
\[
PD(ASC) = \{ G \mid G \in K \{ X \} \text{ and } \text{prem}(G, ASC) = 0 \}.
\]

For a set of d-pols \( DPS \), let \( E\text{-Zero}(DPS) \) denote the common solutions of the d-pols in \( DPS \) in any extension field \( E \) of \( K \), i.e.,
\[
E\text{-Zero}(DPS) = \{ z \in E^n : P(z) = 0, \forall P \in DPS \}
\]

Let \( RS \) be another set of d-pols, we define \( E\text{-Zero}(DPS/RS) = E\text{-Zero}(DPS) - E\text{-Zero}(RS) \).

**Lemma 2.8.** (Ritt-Wu's Principle) For a given finite set \( DPS \) of d-pols, we can find either a nonzero d-pol \( P \in K \cap \text{Ideal}(DPS) \) or a nontrivial weak asc chain \( ASC \) and an enlarged d-pol set \( DPS' \) of \( DPS \) such that:

(a) \( ASC \) is a weak basic set of \( DPS' \).
(b) \( E\text{-Zero}(DPS) = E\text{-Zero}(DPS') \).
(c) \( E\text{-Zero}(DPS) = E\text{-Zero}(ASC/J) \cup \bigcup_{i \in J} E\text{-Zero}(DPS' \cup \{ i \}) \).
(d) \( E\text{-Zero}(ASC/J) \subset E\text{-Zero}(PD(ASC)) \subset E\text{-Zero}(DPS) \).

where \( J \) is the set of all initials and separators of the d-pols in \( ASC \).

**Proof.** Let \( BS_0 \) be a weak basic set of \( DPS \). If \( BS_0 = B_1 \) and \( B_1 \in K \), then \( B_1 \in K \cap \text{Ideal}(DPS) \). Otherwise, for the d-pols belonging to \( DPS \) but not to \( BS_0 \), we form the weak pseudo remainders and adjoin all the nonzero remainders to \( DPS \) to get an enlarged set of d-pols \( DPS_1 \). As the remainders obtained above are in \( \text{Ideal}(DPS) \), \( DPS \) and \( DPS_1 \) have the same zero. If \( DPS \neq DPS_1 \), by lemma 2.7, \( DPS_1 \) has a basic set \( BS_1 \) with lower rank than \( BS_0 \). Repeating the above process for \( DPS_1 \) and so on, we either get a d-pol \( P \in K \cap \text{Ideal}(DPS) \) or get a sequence of d-pol sets which have the same zeros
\[
DPS \subset DPS_1 \subset \cdots
\]

and a sequence of nontrivial, strictly decreasing weak asc chains:
\[
BS_0 > BS_1 > \cdots
\]

By lemma 2.1, the above iteration must terminate in finite steps, i.e., there is an \( i_0 \) such that \( W\text{-prem}(G, BS_{i_0}) = 0 \) for all \( G \in DPS_{i_0} \). Then \( BS_{i_0} \) and \( DPS_{i_0} \) satisfy (a) and (b). (c) follows from (2.2) and (b). The first inclusion of (d) is an immediate consequence of (2.2). The second inclusion of (d) comes from the fact the pseudo remainders of the d-pols in \( DPS \) wrpt \( BS_{i_0} \) are zero.

\[ \blacksquare \]

2.2. An Improved Ritt-Wu's Zero Decomposition Algorithm

**Algorithm 2.9.** (Ritt-Wu's Zero Decomposition Algorithm: the Coarse Form) For two finite sets of d-pols \( DPS \) and \( RS \), the algorithm either detects the emptiness of \( E\text{-Zero}(DPS/RS) \) or furnishes a decomposition of the following forms:

\[
(2.10) \quad E\text{-Zero}(DPS/RS) = \bigcup_{i=1}^{l_1} E\text{-Zero}(ASC_i/RS \cup J_i)
\]
\[
(2.11) \quad E\text{-Zero}(DPS/RS) = \bigcup_{i=1}^{l_2} E\text{-Zero}(PD(ASC_i)/RS)
\]
where for each $i \leq l$, $ASC_i$ is a weak asc chain such that \( \text{prem}(P, ASC_i) \neq 0 \) for $P \in RS$ and $J_i$ is the set of all initials and separatals of the d-pols in $ASC_i$.

**Proof.** Let $ASC_1$ and $DPS_1$ be the weak asc chain and the enlarged d-pol set obtained from $DPS$ as in Lemma 2.8. If $ASC_1$ is trivial, then $E$-Zero$(DPS/RS)$ is empty. Otherwise, compute the pseudo remainders of the d-pols in $RS$ wrt to $ASC_1$. If one of them is zero, then $E$-Zero$(ASC_1/RS \cup J_1)$ is empty, where $J_1$ is the set of all initials and separatals of $ASC_1$. Thus, by Lemma 2.8, we have

$$E\text{-Zero}(DPS/RS) = \bigcup_{I \in J_1} E\text{-Zero}(DPS_1 \cup \{I\}/RS).$$

Otherwise, we have

$$E\text{-Zero}(DPS/RS) = E\text{-Zero}(ASC_1/RS \cup J_1) \cup \bigcup_{I \in J_1} E\text{-Zero}(DPS_1 \cup \{I\}/RS).$$

For each $I \in J_1$, let $I' = W$-prem$(I, ASC_1)$. We have $E$-Zero$(DPS_1 \cup \{I, I'\}) = E$-Zero$(DPS_1 \cup \{I\})$. Repeating the above process for $DPS_1 \cup \{I, I'\}$, we get another weak asc chain $ASC_2$. Since $\text{prem}(I, ASC_1) \neq 0$, $I'$ is not zero by lemma 2.5. Hence $ASC_2$ must be of lower rank than $ASC_1$ by lemma 2.7. The above process must terminate within a finite number of steps and we will get a decomposition of form (2.10). From the above process, it is clear that the pseudo remainders of the d-pols in $DPS$ wrt to each $ASC_i$ are zero. Thus (2.11) comes from (d) of lemma 2.8.

The above decomposition is not complete in the sense that each $PD(ASC_1)$ is generally not a prime ideal. To give a complete decomposition we need the notion of irreducibility and factorization. Let $ASC = A_1, ..., A_p$ be an asc chain. Let the lead of $A_i$ be $x_{i,0}$. We rename each $x_{i,0}$ to be $z_i$ and rename the remaining $x_{i,j}$ in the $A$ by $v_1, ..., v_l$. With such a renaming, $ASC$ becomes an asc chain of ordinary polynomials: $ASC' = B_1, ..., B_p$ of the $v$ and the $z$. $ASC$ is said to be irreducible if $ASC'$ is irreducible as a polynomial asc chain, i.e., if $B_1$ is irreducible and for each $k > 1, B_k$ is irreducible in the ring $K(v)[z_1, ..., z_{k-1}, z_k]/(B_1, ..., B_{k-1})$, where $(B_1, ..., B_{k-1})$ stands for the polynomial ideal generated by $B_1, ..., B_{k-1}$ in $K(v)[z_1, ..., z_{k-1}]$.

**Theorem 2.12.** (Ritt) $ASC$ is an irreducible asc chain if and only if $PD(ASC)$ is a prime ideal.

**Proof.** See page 97 in [RI2].

**Theorem 2.13.** If asc chain $ASC' = A_1, ..., A_{p-1}$ is irreducible and asc chain $ASC = A_1, ..., A_{p-1}, A_p$ is reducible, then we can find nonzero d-pols $G$ and $F$ which are $W$-reduced wrt $ASC$ and with the same lead as $A_p$ such that $GF \in \text{Ideal}(A_1, ..., A_p)$.

**Proof.** See page 107 in [RI2].

**Lemma 2.14.** Let $ASC_1$ and $ASC_2$ be two weak asc chains, and $ASC_2$ be irreducible. If the pseudo remainders of the d-pols in $ASC_1$ wrt $ASC_2$ are zero and the pseudo remainder of the product of the initials and separatals of $ASC_1$ wrt $ASC_2$ is not zero, then $PD(ASC_1) \subset PD(ASC_2)$.

**Proof.** As $ASC_2$ is irreducible, $PD(ASC_2)$ is a prime ideal by theorem 2.12. We have $ASC_1 \subset PD(ASC_2)$ and $J \notin PD(ASC_2)$ where $J$ is any product of the separatals and initials of the d-pols in $ASC_1$. Let $P \in PD(ASC_1)$, then there exists a product $J_1$ of the separatals and initials of the d-pols in $ASC_1$ such that $J_1 P \in \text{Ideal}(ASC_1)$. Therefore, we have $J_1 P \in PD(ASC_2)$. 

8
Hence \( P \in PD(ASC_2) \) as \( J_1 \) is not in \( PD(ASC_2) \).

**Theorem 2.15.** For a nontrivial weak asc chain \( ASC = A_1, ..., A_p \), let \( ASC' = A'_1, ..., A'_p \) where \( A'_i = A_i \) and \( A'_i = \text{prem}(A_i, A_1, ..., A_{i-1}) \) \((i = 2, ..., p)\). Then either (a) we can find two nonzero d-pols \( G \) and \( H \) which are W-reduced wrpt \( ASC \) such that \( HG \in \text{Ideal}(ASC) \), or (b) \( ASC' \) is an irreducible asc chain and \( PD(ASC) = PD(ASC') \).

**Proof.** Induction on \( p \). If \( p = 1 \), the result is obviously true. Assuming the result is true for \( p = k - 1 \), we want to prove the result is true for \( p = k \). By the induction hypothesis, either (a) or (b) is true for \( ASC_{k-1} \). If (a) is true for \( ASC_{k-1} \), then (a) is also true for \( ASC_k \). Now we suppose (b) is true for \( ASC_{k-1} \), i.e., \( PD(ASC_{k-1}) = PD(ASC'_{k-1}) \) are prime ideals. By definition we have \( A'_k = \text{prem}(A_k, A_1, ..., A_{k-1}) \), then by (2.2) we have

\[
A'_k - JA_k \in \text{Ideal}(ASC_{k-1}) \subset PD(ASC_{k-1})
\]

where \( J \) is a product of the initials and separators of \( A_1, ..., A_{k-1} \). As \( ASC \) is a weak asc chain, \( A'_k \) and \( A_k \) have the same lead and the same degree wrpt the lead. Then \( ASC' \) is an asc chain. If \( ASC' \) is reducible, then according to theorem 2.13, we can find non-zero d-pols \( H \) and \( G \) which are W-reduced wrpt \( ASC' \) such that \( HG \in \text{Ideal}(ASC') \). By (2.16), we have \( HG \in \text{Ideal}(ASC) \). \( H \) and \( G \) are also W-reduced to \( ASC \), as \( PD(ASC_{k-1}) \) is a prime ideal. In this case, (a) is true. Now we assume \( ASC' \) is irreducible. As \( ASC \) is a weak asc chain, the pseudo remainders of the initial and separator of \( A_k \) wrpt \( ASC_{k-1} \), hence wrpt \( ASC'_{k-1} \), are not zero. By (2.16), the pseudo remainder of \( A_k \) wrpt \( ASC' \) is zero. Thus \( PD(ASC) \subset PD(ASC') \) follows from lemma 2.14 and the induction hypothesis. To prove the other direction, let \( P \in PD(ASC') \) and let \( P' = \text{prem}(P, A_k) \). \( P' \in PD(ASC') \) as \( A_k \in PD(ASC') \). Since \( P' \) is of lower rank than \( A'_k \), \( \text{prem}(P', ASC') = \text{prem}(P', ASC_{k-1}) = 0 \). By the induction hypothesis, \( \text{prem}(P', ASC_{k-1}) = 0 \). Hence \( \text{prem}(P, ASC) = 0 \). This proves \( PD(ASC') \subset PD(ASC) \).

In case (b) of Theorem 2.15, we call the weak asc chain \( ASC \) irreducible. Our improved version of the complete Ritt-Wu's decomposition algorithm is as follows.

**Algorithm 2.17.** (Ritt-Wu's Zero Decomposition Algorithm: the Strong Form) The same as algorithm 2.9, except the \( ASC_i \) in (2.10) and (2.11) are irreducible.

**Proof.** Similar to the proof of Algorithm 2.9, let \( ASC_1 \) and \( DPS_1 \) be the weak asc chain and the enlarged d-pol set obtained from \( DPS \) as in Lemma 2.8. If \( ASC_1 \) is irreducible or trivial, then do the same decomposition as algorithm 2.9. Otherwise, by theorem 2.15, we can find two non-zero d-pols \( G \) and \( F \) which are W-reduced wrpt \( ASC \) such that \( GF \in \text{Ideal}(ASC_1) \). We have:

\[
\text{E-Zero}(DPS/RS) = \text{E-Zero}(DPS_1 \cup \{F\}/RS) \cup \text{E-Zero}(DPS_1 \cup \{G\}/RS)
\]

We can repeat the above process for \( DPS_1 \cup \{F\} \) and \( DPS_1 \cup \{G\} \). As \( F \) and \( G \) are W-reduced wrpt \( ASC_1 \), then each weak basic set of \( DPS_1 \cup \{F\} \) or \( DPS_1 \cup \{G\} \) must be of lower rank than \( ASC_1 \). Thus the process will terminate at a finite number of steps.

The difference between the two versions of decompositions 2.9 and 2.17 is that 2.9 does not require factorization, but it is incomplete. On the other hand, 2.17 requires not only multivariate factorization over \( Q \), but also factorization over algebraic extensions of fields of rational functions. In practice, we haven't encountered examples which need factorization over extension fields and multivariate factorization over \( Q \) is enough. Thus the algorithm
implemented in our program is a mixture of 2.9 and 2.17, i.e., whenever a polynomial is reducible over $Q(t)$ at certain steps, we put its factors into polynomial sets.

For a quasi asc chain $ASC = A_1, ..., A_p$, we make a renaming of the variables. If $A_i$ is of class $m_i$, we rename $x_m$ as $x_i$, other variables are renamed as $u_1, ..., u_q$, where $q = n - p$. The variables $u_1, ..., u_q$ are called the parameter set of $ASC$. If $ASC$ is irreducible, $DIM(ASC) = q = n - p$ is defined to be the dimension of $ASC$ and $ORD(ASC) = \sum_{i=1}^{p} o_i$ is defined to be the order of $ASC$ wrt to the given parameter set, where $o_i$ is the order of $A_i$ wrt $x_i$. $DIM(ASC)$ and $ORD(ASC)$ are actually the dimension and order of the prime ideal $PD(ASC)$ respectively [RI2].

Example 2.18. (Continuation of Example 1.1). Let $HS = \{H_1, H_2, H_3\}$, where the $H_i$ are in Example 1.1. Using our algorithm for decomposition we have

$$E\text{-}Zero(HS) = \cup_{i=1}^{5} E\text{-}Zero(ASC_i/J_i) = \cup_{i=1}^{5} E\text{-}Zero(PD(ASC_i))$$

where

$ASC_1 = x_3^2 + x_2^2 - x_1^2, \quad x_4 - x_2^2 - x_4, \quad x_4^3 x_2^2 - (x_2^2 x_3 - x_4 x_4)^2, \quad J_1 = \{2x_3, 2x_4 x_5\};$

$ASC_2 = x_2, \quad x_3^2 + x_2^2 - x_1^2, \quad x_4, \quad J_2 = \{2x_3\};$

$ASC_3 = x_2 + x_1, \quad x_3, \quad x_4, \quad J_3 = \{1\};$

$ASC_4 = x_2 - x_1, \quad x_3, \quad x_4, \quad J_4 = \{1\};$

$ASC_5 = x_1, \quad x_3^2 + x_2^2, \quad x_4, \quad J_5 = \{2x_3\}.$

This decomposition is redundant, i.e., some components may contain others. For example, $PD(ASC_i) \subset PD(ASC_2)$ for $i = 3, 4$ (it is non-trivial to prove this fact). Unlike the case of ordinary polynomials, no methods have been found to delete the redundant components in the above decomposition completely.

2.3. The H-extension

This subsection is needed only when the reader wants to know the completeness problem of our methods in the next section. It can be skipped if the reader only needs to know how our methods works.

An extension field $E$ of $K$ is said to be an H-extension if for any finite variables $y_1, ..., y_t$, each non-unit ideal in $K[y_1, ..., y_t]$ has at least one zero in $E^t$.

Lemma 2.19. For an extension field $E$ of $K$, the following statements are equivalent:

(a) $E$ is an H-extension of $K$.

(b) Let $G, F_1, ..., F_s$ be d-pols in $K\{X\}$. If $G$ vanishes on the E-zeros of $F_1, ..., F_s$, then a power of $G$ is a linear combination of the $F$ and their derivatives.

(c) For a radical ideal $D$ in $K\{X\}$, we have $D = I(E\text{-}Zero(D))$. For $S \subseteq E^n$, we denote the set of d-pols in $K\{X\}$ which vanish on $S$ by $I(S)$.

Proof. (a) $\Rightarrow$ (b). As $G$ vanishes on all E-zeros of $F_1, ..., F_s$, then for a new variable $z$, the ideal $D = \text{ideal}(F_1, ..., F_s, zG - 1)$ has no E-zero. By (a), 1 is in $D$, i.e., 1 is a linear combination of the $F, zG - 1$ and their derivatives, with d-pols in $K\{x_1, ..., x_n, z\}$ as coefficients. Set $z = 1/G$ in this expression and clear the denominators. Note that $z' = -G'/G^2, z'' = (2G'^2 - G'' G)/G^3, ...$,
then some power of $G$ can be expressed as linear combination of the $F$ and their derivatives. This proves (b).

(b) $\Rightarrow$ (c): from the definition of radical ideals.

(c) $\Rightarrow$ (a). Let $D$ be a non-unit ideal. Then $\text{Radical}(D)$ is also non-unit. By (c) $\text{Radical}(D) = I(\text{Zero}(\text{Radical}(D)))$. Thus $\text{Zero}(D) = \text{Zero}(\text{Radical}(D))$ must be non-empty.

From [KO1], we know that for a differential field $K$ of characteristic zero, there always exists an $H$-extension field of $K$. In [RI2], Ritt proved that the field of meromorphic functions over an open region in the complex plane is an $H$-extension of itself. The completeness of our methods in next section is based on the following theorem.

**Theorem 2.20.** Let $ASC$ be an irreducible weak asc chain and $R$ be a d-pol with nonzero pseudo remainder wrpt $ASC$. Then for an $H$-extension field $E$ of $K$, a nonzero d-pol $G$ vanishes on $E(\text{Zero}(PD(ASC))/R)$ if and only if $\text{prem}(G, ASC) = 0$.

**Proof.** The if part is obvious. As $ASC$ is irreducible, $PD(ASC)$ is a prime ideal by theorem (b) of 2.15. Since $G$ vanishes on $E(\text{Zero}(PD(ASC))/R)$, $GR$ vanishes on $E(\text{Zero}(PD(ASC)))$. Then $GR \in PD(ASC)$ by lemma 2.19 (c), because a prime ideal is always a radical ideal. Since $R$ is not in $PD(ASC)$, we have $G \in PD(ASC)$, i.e., $\text{prem}(G, ASC) = 0$.

---

3. The Methods

Now we present two methods to solve the problems raised by Formulations F1 and F2 in Section 1. For a statement $(S)$ in differential geometry, let $HS$, $DS$ and $G$ be the same as in Section 1. We denote such a geometry statement $(S)$ by $(HS, DS, G)$. For Formulation F2, we introduce the following notion:

**Definition 3.1.** A geometry statement $(S) = (HS, DS, G)$ is said to be true (valid) in an extension field $E$ of $K$, if

$$\forall x \in E^n[(H_1 = 0 \land \cdots \land H_r = 0 \land D_1 \neq 0 \land \cdots \land D_l \neq 0) \Rightarrow G = 0].$$

$(S)$ is called universally true (valid) if it is true in any extension of $K$.

**Theorem 3.2.** A geometry statement $(HS, DS, G)$ is universally valid if and only if this statement is valid in an $H$-extension field $\Omega$ of $K$.

**Proof.** Only the if part needs proof. The statement is valid in $\Omega$ means

$$\forall x \in \Omega^n[(H_1 = 0 \land \cdots \land H_r = 0 \land D_1 \neq 0 \land \cdots \land D_l \neq 0) \Rightarrow G = 0]$$

which is equivalent to:

$$\forall x \in \Omega^n \forall z \in \Omega'[H_1 = 0 \land \cdots \land H_r = 0 \land z_1 D_1 - 1 = 0 \land \cdots \land z_l D_l - 1 = 0) \Rightarrow G = 0]$$

for some new variables $z_1, \ldots, z_l$. By lemma 2.19 (b), some power of $G$ is in the ideal generated by $H_1, \ldots, H_r, z_1 D_1 - 1, \ldots, z_l D_l - 1$, which implies the statement is valid in any extension field of $K$. 

---

11
Algorithm 3.3. Decide whether a geometry statement \((S) = (HS, DS, G)\) is universally valid.

Step 1. Using algorithm 2.9, we have:

\[
E\text{-}Zero(HS/DS) = \bigcup_{i=1}^{r} E\text{-}Zero(PD(ASC_i^*))/DS
\]

Step 2. If the pseudo remainders of \(G\) wrpt the \(ASC\) in (3.4) are all zero, then the statement is universally valid.

Step 3. Otherwise, using algorithm 2.17 we have the complete decomposition:

\[
E\text{-}Zero(HS/DS) = \bigcup_{i=1}^{l} E\text{-}Zero(PD(ASC_i))/DS
\]

Step 4. The statement is universally valid if and only if the pseudo remainders of \(G\) wrpt the \(ASC_i^*\) in (3.5) are all zero.

Example 3.6. (Continuation of Example 1.1). If we want to decide whether (1.5) is universally valid, by example 2.18, we can decompose \(E\text{-}Zero(HS/x_1) = \bigcup_{1 \leq i \leq 4} E\text{-}Zero(PD(ASC_i^*))/x_1\). We have \(\text{prem}(G, ASC_1^*) = 0\); however, \(\text{prem}(G, ASC_i^*) \neq 0\) for \(i = 2, 3, 4\). Thus the statement is not confirmed to be valid. The problem here is due to the mistake in choosing non-degenerate conditions. Instead, if we choose \(DS\) to be \(\{x_4\}\), i.e., the arc is not constant, then \(E\text{-}Zero(HS/x_4) = E\text{-}Zero(PD(ASC_4^*))/x_4\). Since \(\text{prem}(G, ASC_1^*) = 0\), the geometry statement

\[
\forall x(H_1 = 0 \land H_2 = 0 \land H_3 = 0 \land x_4 \neq 0 \Rightarrow G = 0)
\]

has been proved to be universally valid.

Now we give a method to prove theorems according to Formulation F1. First we give the definition of general validity in the context of differential polynomials. For a geometric statement with \(HS\) and \(G\), we divide the variables occurring in \(HS\) and \(G\) into two groups: \(u_1, \ldots, u_q\) and \(x_1, \ldots, x_p\) in the sense that in this statement the \(u\) can generally take any values and the \(x\) can be determined as some functions of the \(u\). We call the \(u\) and the \(x\) the parameter and the dependent variables of the geometry statement. Applying algorithm 2.17 to \(HS\) under the variable order \(u_1 < \cdots < u_q < x_1 < \cdots < x_p\), we have

\[
E\text{-}Zero(HS) = \bigcup_{i=1}^{r} E\text{-}Zero(PD(ASC_i^*))/DS \quad U \quad \bigcup_{j=1}^{l} E\text{-}Zero(PD(ASC_j^*))/DS
\]

where the \(ASC_i^*\) are the weak asc chains with the parameters of the statement, i.e., \(u_1, \ldots, u_q\), as their parameter sets. Let \(r = \max_{i=1}^{s} \text{ORD}(ASC_i^*)\). A component \(E\text{-}Zero(PD(ASC_i^*))\) is called a main component of the statement, if \(\text{ORD}(ASC_i^*) = r\), i.e., the main components are represented by the weak asc chains which have the same parameters as the statement and have the highest order. Other components are called degenerate components. The following is a clarification of Wu’s notion of a geometry statement to be generally true.

Definition 3.7. For a geometry statement with \(HS\) and \(G\), suppose the set of parameters is given. The statement is said to be generally true wrpt the parameters, if \(G\) vanishes on all the main components of the statement.

* Depending on the context, \(HS\) and \(DS\) sometimes also denote the d-pol sets \(\{H_1, \ldots, H_r\}\) and \(\{D_1, \ldots, D_l\}\), respectively.
Definition 3.7 actually provides a method to prove a statement to be generally true. But for some examples, we do not need to give a complete decomposition. So we can first use the coarse form of the decomposition algorithm to test whether the statement is generally true. If failed, we use the strong form to give a complete answer.

**Algorithm 3.8.** For a geometry statement with \( HS, G \), and a parameter set \( u_1, \ldots, u_q \), decide whether the geometry statement is generally true wrpt the \( u \).

**Step 1.** Using algorithm 2.9 to \( HS \)

\[
E\text{-}\text{Zero}(HS) = \bigcup_{i=1}^{s} E\text{-}\text{Zero}(PD(ASC_i^*)) \bigcup \bigcup_{j=1}^{r} E\text{-}\text{Zero}(PD(ASC_j))
\]

where the \( ASC_j \) are all the weak asc chains that contain at least a d-pol in the \( u \) alone.

**Step 2.** If \( \text{prem}(G, ASC_i^*) = 0 \) (for \( i \leq s \)), the geometry statement is generally true, as each main component (if there are any) of the geometry statement is contained in some \( E\text{-}\text{Zero}(PD(ASC_i^*)) \).

**Step 3.** If not all the pseudo remainders are zero, then use algorithm 2.17 to get a complete decomposition.

\[
E\text{-}\text{Zero}(HS) = \bigcup_{i=1}^{s} E\text{-}\text{Zero}(PD(ASC_i^*)) \bigcup \bigcup_{j=1}^{r} E\text{-}\text{Zero}(PD(ASC_j))
\]

where the \( ASC_i^* \) are the irreducible weak asc chains with the \( u \) as parameters.

**Step 4.** Let \( r = \max_{i=1}^{s} \text{ORD}(ASC_i^*) \) and let \( MS \) be the set of \( ASC_i^* \) such that \( \text{ORD}(ASC_i^*) = r \).

**Step 5.** The statement is generally true wrpt the \( u \) if and only if the pseudo remainders of \( G \) wrpt the weak asc chains in \( MS \) are all zero.

**Remark 3.9.** For the decomposition in steps 2 and 3, we don’t have to compute the weak asc chains \( ASC_j \) which have at least a d-pol in the \( u \) only. In algorithms 2.9 and 2.17, whenever a d-pol in the \( u \) only occurs, we don’t need to go further because all weak asc chains obtained in this branch will have a d-pol \( D_i \) in the \( u \) only. This is the key to the efficiency of Algorithm 3.8. Let \( D_1, \ldots, D_l \) be all such d-pol in the \( u \) alone. If the statement is proved to be generally true by step 2 of Algorithm 3.8, the following formula is valid:

\[
\forall u \forall x[(H_1 = 0 \land \cdots \land H_r = 0 \land D_1 \neq 0 \land \cdots \land D_l \neq 0) \Rightarrow G = 0].
\]

**Example 3.10.** (Continuation of Example 1.1). By example 2.18, the only main component of \( \text{Zero}(HS) \) is \( \text{Zero}(PD(ASC_1)) \), because other \( ASC_i \) (\( i = 2, \ldots, 5 \)) contain a d-pol in the parameters \( x_1 \) and \( x_2 \) alone. Since \( \text{prem}(G, ASC_1) = 0 \), (1.2) is proved to be generally true wrpt the parameters \( x_1 \) and \( x_2 \). As mentioned in Remark 3.9, we actually don’t have to compute \( ASC_i \) (\( i = 2, \ldots, 5 \)). The d-pol in \( u \) alone collected in the decomposition are \( x_2 - x_1, x_2 + x_1, x_2', \) and \( x_1 \). Thus our method also proves the following formula to be universally true:* 

\[
\forall x[(H_1 = 0 \land H_2 = 0 \land H_3 = 0 \land x_2 - x_1 \neq 0 \land x_2 + x_1 \neq 0 \land x_2' \neq 0 \land x_1 \neq 0) \Rightarrow G = 0].
\]

* Note that the inequations in this formula are not independent. We can use our method again to infer \( x_2' \neq 0 \Rightarrow x_2 \neq x_1 \neq 0 \). Thus only \( x_2' \neq 0 \) and \( x_1 \neq 0 \) are necessary.
We can see that the above algorithms in essence deal with statements in H-extension fields of the base field \( K \) (similar to the algebraic closed field in the polynomial case). A statement is valid in the usual case of real differential geometry means the statement is valid in the field of real analytical functions. So the methods can only confirm theorems in real differential geometry. But, almost all the theorems we encountered in real differential geometry are also valid in complex case. So these geometry statements are actually universally valid and can be confirmed by our methods.

4. Mechanical Theorem Proving For Space Curves

The following lemma is used in the examples to transform an algebraic relation into a differential polynomial equation.

**Lemma 4.1.** For nonzero functions of \( t: x_1, ..., x_n \), there exist arbitrary constants \( a_1, ..., a_n \) such that

\[
a_1 x_1 + ... + a_n x_n = 0
\]

if and only if \( DLR(x_1, ..., x_n) = 0 \). The function \( DLR \) can be defined recursively as follows:

\[
DLR(y_1) = y_1
\]

\[
DLR(y_1, y_2) = y'_1 y_2 - y'_2 y_1
\]

\[
DLR(y_1, ..., y_r) = DLR(DLR(y_1, y_2), ..., DLR(y_{r-1}, y_r))
\]

where the primes here are used for the differentiation operation wrpt \( t \).

**Proof.** we prove it by induction. For \( n = 1 \), as \( a_1 \) is an arbitrary constant then we have \( a_1 x_1 = 0 \) if and only if \( x_1 = 0 \). For \( n = 2 \), \( a_1 x_1 + a_2 x_2 = 0 \) can be written as \( x_1/x_2 = -a_2/a_1 \). This formula is true if and only if \( (x_1/x_2)' = 0 \) or equivalently \( DLR(x_1, x_2) = x'_1 x_2 - x_1 x'_2 = 0 \) as \( x_1 x_2 \neq 0 \). Now assume the theorem for \( r = k \). \( DLR(x_1, ..., x_{k+1}) = 0 \) means \( DLR(DLR(x_1, x_2), ..., DLR(x_{k-1}, x_k)) = 0 \) or equivalently there are some arbitrary constants \( b_1, ..., b_k \) such that \( b_1 DLR(x_1, x_2) + ... + b_k DLR(x_{k-1}, x_k) = 0 \). The last equation is actually \( (b_1 x_2/x_1 + ... + b_k x_{k+1}/x_1)' = 0 \) or equivalently \( b_1 x_2/x_1 + ... + b_k x_{k+1}/x_1 = b_0 \) for a constant \( b_0 \). This proves our lemma.

Consider a space curve \( C = (x, y, z) \) with its length of arc \( s \) as parameter. Let the tangent vector, the principal normal vector, and the binormal vector of \( C \) be \( T = (x', y', z'), N = (n_1, n_2, n_3) \), and \( B = (b_1, b_2, b_3) \) respectively. Let \( k \) be the curvature of \( C \) and \( t \) be the torsion of \( C \). Then we have

\[
x'^2 + y'^2 + z'^2 = 1 = 0
\]

\[
k^2 - x''^2 - y''^2 - z''^2 = 0
\]

\[
k n_1 - x'' = 0
\]

\[
k n_2 - y'' = 0
\]

(4.1) \( kn_3 - z'' = 0 \)

\[
k b_1 - y' z'' + y'' z' = 0
\]

\[
k b_2 + x' z'' - x'' z' = 0
\]

\[
k b_3 + x' y'' + x'' y' = 0
\]

\[
t + n_3 b_3' + n_2 b_2' + n_1 b_1' = 0
\]

where the primes represent the derivation wrpt the length of arc of \( C \), i.e. wrpt \( s \).
Some examples about the classifications of the curves according to their curvature and torsion as functions of their arcs are given below.

**Example 1.** The following statements are equivalent:

(a) \( C \) is a straight line.

(b) \( C' \times C'' \equiv 0 \).

(c) \( k = 0 \).

(d) The tangent lines of \( C \) pass a fixed point.

(a), (b), (c), and (d) can be reduced to:

\[
\begin{align*}
  x'' &= 0 \\
  y'' &= 0 \\
  z'' &= 0 \\
  x' y'' - x'' y' &= 0 \\
  x' z'' - x'' z' &= 0 \\
  y' z'' - y'' z' &= 0 \\
  k &= 0 \\
  DLR(x', y', x'y - y'x) &= x'(x'y'' - x''y')^2 = 0 \\
  DLR(x', z', x'z - z'x) &= x'(x'z'' - z'x')^2 = 0 \\
  DLR(y', z', yz' - z'y) &= y'(y'z'' - z'y')^2 = 0
\end{align*}
\]

respectively. The equivalences of (a) between (4.2) and (d) between (4.5) come from lemma 4.1. (For details, see the appendix of [CG3].) There is no non-degenerate condition for this problem.

We use algorithm 3.3 to prove this statement. Applying algorithm 2.9 to (4.2), we get one component and the pseudo remainders of the d-pols in (4.3) wrpt the weak asc chain representing the component are zero. This proves that (a) implies (b). To prove that (b) implies (a), applying algorithm 2.9 to (4.3)\( \cup \{x'^2 + y'^2 + z'^2 - 1 = 0\} \), we get eight components and the pseudo remainders of the d-pols in (4.2) wrpt the eight weak asc chains representing the eight components are zero. Hence we have proved that (a) and (b) are equivalent. The equivalence of the other statements can be proved similarly. We have proved all the statements are universally valid. Note that, to prove this statement we only use step 1 and 2 of algorithm 3.3 and the complete decomposition algorithm 2.17 is actually not used. This is true for all of the following examples.

From (4.1) we know that if \( k = 0 \), then the vectors \( T, B \) and the torsion \( t \) can not be defined. So in the following examples, we shall exclude the case of straight line.

**Example 2.** For a curve \( C \), not a straight line, the following statements are equivalent:
(a) $C$ is a plane curve.
(b) The tangent lines are perpendicular to a fixed line.
(c) $t = 0$.
(d) The osculating planes of $C$ pass a fixed point.
(e) The binormals are constant.

By lemma 4.1, (a), (b), (c), (d), and (e) can be reduced to

\begin{align}
DLR(1, x, y, z) &= 0 \\
DLR(x', y', z') &= 0 \\
t &= 0 \\
DLR(b_1, b_2, b_3, b_1 x + b_2 y + b_3 z) &= 0 \\
b_1' = 0, b_2' = 0, b_3' &= 0
\end{align}

respectively. The non-degenerate condition is $k \neq 0$. We use algorithm 3.3 to prove this statement. Applying algorithm 2.9 to the d-pol sets of (4.6) $\cup$ (4.1), (4.7) $\cup$ (4.1), (4.8) $\cup$ (4.1), (4.9) $\cup$ (4.1), and (4.10) $\cup$ (4.1) respectively, we find 14, 14, 7, 7, and 22 components respectively under the non-degenerate condition $k \neq 0$. The pseudo remainders of the d-pols in (4.6), (4.7), (4.8), (4.9), and (4.10) wrpt the 64 weak asc chains representing the 64 corresponding components are all zero. This proves that the statements are equivalent universally under the non-degenerate condition $k \neq 0$.

**Example 3.** For a curve, not a straight line, the following statements are equivalent:

(a) The ratio of the torsion to the curvature is a constant.
(b) The curve makes a constant angle with a fixed line.
(c) The principal normals are parallel to a fixed plane.
(d) The binormals make a constant angle with a fixed line.

A curve satisfying these conditions is called a helix.

Bye lemma 4.1, (a), (b), (c), and (d) can be reduced to:

\begin{align}
DLR(k, t) &= k' t - t' k = 0 \\
DLR(1, x', y', z') &= 0 \\
DLR(x'', y'', z'') &= 0 \\
DLR(1, b_1, b_2, b_3) &= 0
\end{align}

respectively. The non-degenerate condition is $k \neq 0$. We use algorithm 3.3 to prove this statement. Applying algorithm 2.9 to the d-pol sets of (4.11) $\cup$ (4.1), (4.12) $\cup$ (4.1), (4.13) $\cup$ (4.1), and (4.14) $\cup$ (4.1) respectively, we find 3, 3, 3, and 5 components respectively under the non-degenerate condition $k \neq 0$. The pseudo remainders of the d-pols in (4.11), (4.12), (4.13), and (4.14) wrpt the 14 weak asc chains representing the 14 components are all zero. This proves the equivalences.
Example 4. For a curve $C$, not a plane curve the following statements are equivalent:

(a) $C$ is a spherical curve.

(b) $rt + (r'/t)' = 0$, where $r = 1/k$.

(c) The normal planes pass a fixed point.

By lemma 4.1, (a), (b), and (c) can be reduced to

\begin{align*}
(4.15) & \quad DLR(1, x, y, x^2 + y^2 + z^2) = 0 \\
(4.16) & \quad rt + (r'p)' = 0 \\
(4.17) & \quad DLR(x', y', z', xx' + yy' + zz') = 0
\end{align*}

respectively, where $rk - 1 = 0, pt - 1 = 0$. The non-degenerate condition is $t \neq 0$. We use algorithm 3.3 to prove this statement. Applying algorithm 2.9 to the d-pol sets of $(4.15) \cup (4.1) \cup \{rk - 1 = 0, pt - 1 = 0\}$, $(4.16) \cup (4.1) \cup \{rk - 1 = 0, pt - 1 = 0\}$, and $(4.17) \cup (4.1) \cup \{rk - 1 = 0, pt - 1 = 0\}$ respectively, we find 3, 4, and 3 components respectively under the non-degenerate condition $t \neq 0$. The pseudo remainders of the d-pols in $(4.15)$, $(4.16)$, and $(4.17)$ wrpt the 10 weak asc chains representing the 10 components are all zero. This proves the equivalences.

More examples can be found in the appendix.

5. Bertrand Curves In Metric Space

A pair of curves having their principal normals in common are said to be associate Bertrand curves. But here we will consider more general problems. Given two curves $C_1$ and $C_2$ let us attach moving frames $(p_1, e_{11}, e_{12}, e_{13})$ and $(p_2, e_{21}, e_{22}, e_{23})$ to $C_1$ and $C_2$ at corresponding points $p_1$ and $p_2$, and let us denote the arc, curvature and torsion of $C_1$ and $C_2$ by $s, k_1, t_1$, and $s', k_2, t_2$ respectively. Following [WU4], let

\begin{align*}
p_2 &= p_1 + a_1 E_{11} + a_2 E_{12} + a_3 E_{13} \\
e_{21} &= u_{11} e_{11} + u_{12} e_{12} + u_{13} e_{13} \\
e_{22} &= u_{11} e_{11} + u_{12} e_{12} + u_{13} e_{13} \\
e_{23} &= u_{11} e_{11} + u_{12} e_{12} + u_{13} e_{13} \tag{5.2}
\end{align*}

Differentiate (5.1) and (5.2) and use the Frenet formulas of $C_1, C_2$, we have:

\begin{align*}
a_2 t_1 - ds'/dsu_{13} + a_3 = 0 \\
a_3 t_1 - a_1 k_1 + ds'/dsu_{12} - a_1' = 0 \\
a_2 k_1 + ds'/dsu_{11} - a_2' - 1 = 0 \\
ds'/dsu_{23} k_2 - u_{12} t_1 - u_{13} = 0 \\
ds'/dsu_{22} k_2 + u_{13} t_1 - u_{11} k_1 - u_{12}' = 0 \\
ds'/dsu_{12} k_2 + u_{12} k_1 - u_{11}' = 0 \\
ds'/dsu_{23} t_2 - ds'/dsu_{13} k_2 - u_{22} t_1 - u_{23}' = 0 \tag{5.3}
\end{align*}
\[
\begin{align*}
\frac{ds'}{ds} u_{22} t_2 - \frac{ds'}{ds} u_{12} k_2 + u_{23} t_1 - u_{21} k_1 - u'_{22} &= 0 \\
\frac{ds'}{ds} u_{32} t_2 - \frac{ds'}{ds} u_{11} k_2 + u_{23} k_1 - u'_{21} &= 0 \\
\frac{ds'}{ds} u_{32} t_2 + u_{32} t_1 + u'_{33} &= 0 \\
\frac{ds'}{ds} u_{22} t_2 - u_{33} t_1 + u_{31} k_1 + u'_{32} &= 0 \\
\frac{ds'}{ds} u_{21} t_2 - u_{32} k_1 + u'_{31} &= 0
\end{align*}
\]

To transform a right-handed orthogonal system \(\{e_{11}, e_{12}, e_{13}\}\) to another right handed orthogonal system \(\{e_{21}, e_{22}, e_{23}\}\), we must have
\[
\begin{align*}
u_{13}^2 + v_{12}^2 + v_{11}^2 - 1 &= 0 \\
v_{23}^2 + v_{22}^2 + v_{21}^2 - 1 &= 0 \\
v_{33}^2 + v_{32}^2 + v_{31}^2 - 1 &= 0 \\
u_{13} u_{23} + u_{12} u_{22} + u_{11} u_{21} &= 0 \\
u_{13} u_{33} + u_{12} u_{32} + u_{11} u_{31} &= 0 \\
u_{23} u_{33} + u_{22} u_{32} + u_{21} u_{31} &= 0 \\
(u_{11} u_{22} - u_{12} u_{21}) u_{33} + (-u_{11} u_{23} + u_{13} u_{21}) u_{32} + (u_{12} u_{23} - u_{13} u_{22}) u_{31} - 1 &= 0 
\end{align*}
\] (5.4)

We add the last equation (5.4) to Wu's original equations to protect the right-handness of the moving system.

5.1. The Case of Identical

Let \(EI_{ij}\) denote the case for which \(e_{2j}\) is identical with \(e_{1i}\) at the corresponding points. At case \(EI_{ij}\), we have:
\[
\begin{align*}
a_{k_1} &= 0 \quad k_1 \neq i \\
u_{ji} &= 1 = 0 \\
u_{jk_1} &= 0 \quad k_1 \neq i \\
u_{k_1} &= 0 \quad k \neq j
\end{align*}
\] (5.5)

For each concrete case \(EI_{i,j,k}\), apply our decomposition algorithm to (5.3), (5.4), and (5.5) under the non-degenerate condition \(k_1 \neq 0, k_2 \neq 0, ds'/ds \neq 0\), i.e. the curves \(C_1\) and \(C_2\) are not lines for which the Frenet moving frames can not be defined and the arc length of \(C_2\) as a function of the length of \(C_1\) is not a constant. Once the decomposition furnished, we may prove or derive formulas from the given arc chain. We always assume the following variable order in this section. \(ds'/ds < u_1 < u_2 < u_3 < u_{11} < u_{12} < u_{13} < u_{21} < u_{22} < u_{23} < u_{31} < u_{32} < u_{33} < k_1 < t_1 < k_2 < t_2\)

We have the following results:

Case \(EI_{11}\). \(C_1\) and \(C_2\) must be identical, i.e. \(p_1 = p_2, e_{11} = e_{21}, e_{12} = e_{22}, e_{13} = e_{23}\) \(r = 1, k_1 = k_2, \) and \(t_1 = t_2\).

Case \(EI_{12}\). We have

a. \(p_2\) and \(p_1\) are both plane curves.

b. \(p_2 = p_1 + a_1 e_{11}\).
c. There are two cases:

\[
\begin{align*}
\epsilon_{21} &= -\epsilon_{12}, \epsilon_{22} = \epsilon_{11}, \epsilon_{23} = \epsilon_{13} \\
a'_1 &= -1, a_1 k_2 = -1 \\
ds' / ds &= -a_1 k_1
\end{align*}
\]

(5.6)

\[
\begin{align*}
\epsilon_{21} &= \epsilon_{12}, \epsilon_{22} = \epsilon_{11}, \epsilon_{23} = -\epsilon_{13} \\
a'_1 &= -1, a_1 k_2 = -1 \\
ds' / ds &= a_1 k_1
\end{align*}
\]

(5.7)

The geometric meaning of the above results can be stated as follows: If \( C_2 \) are the involutes of \( C_1 \) in the strong sense that the principal normals of \( C_2 \) are identical with the tangent lines of \( C_1 \), then both curve must be plane curves, and

(i) \( p_2 = p_1 + (c_0 - s)\epsilon_{11} \) where \( c_0 \) is a constant.

(ii) \( p_1 = p_2 + \frac{1}{k_2} \epsilon_{22} \), i.e \( C_1 \) is the locus of the curvature center of \( C_2 \).

(iii) The arc length of \( C_1 \) between two points equal to the difference of the reciprocal of the curvature of \( C_2 \) at the corresponding points.

**Case** \( EI_{13} \). There exist no curves satisfying \( \epsilon_{11} = \epsilon_{23} \) under the condition \( ds' / ds \neq 0 \).

**Case** \( EI_{22} \). We have

a. The distance from \( p_1 \) to \( p_2 \) is constant.

b. The angle formed by the tangent lines at \( p_1 \) and \( p_2 \) respectively is constant.

c. (Bertrand) There exists a linear relation between \( k_1 \) and \( t_1 \).

d. (Schell) The product of \( t_1 \) and \( t_2 \) is constant.

**Case** \( EI_{23} \). We have

a. The distance from \( p_1 \) to \( p_2 \) is constant.

b. (Mannheim) \( k_1^2 + t_1^2 = c_1 k_1 \)

c. \( t_1 t_2^2 = c_2 (t_1 - t_2) \)

where \( c_1 \) and \( c_2 \) are constants.

**Case** \( EI_{33} \). We have either

a. \( p_1 = p_2, \epsilon_{11} = \epsilon_{21}, \epsilon_{12} = \epsilon_{22}, \epsilon_{13} = \epsilon_{23}, \) and \( k_1 = k_2, t_1 = t_2 \) or

b. \( p_1 \) and \( p_2 \) are both plane curves and \( \epsilon_{11} = \epsilon_{21}, \epsilon_{12} = \epsilon_{22}, \epsilon_{13} = \epsilon_{23}, a'_3 = 0, ds'/ds = 1, k_1 = k_2 \).

In this case, we have either \( C_1 \) and \( C_2 \) are identical or both curves are plane curves and \( C_2 \) is translation of \( C_1 \) with a constant distance along the binormal of \( C_1 \).
Take $EI_{22}$, the classical case of Bertrand as an example. In this case, we have 9 components. The main component is:

\[
\begin{align*}
  a_1 &= 0 \\
  a'_2 &= 0 \\
  a_3 &= 0 \\
  u'_{11} &= 0 \\
  u_{12} &= 0 \\
  u_{13}^2 + u_{11}^2 - 1 &= 0 \\
  u_{21} &= 0 \\
  v u_{22} - 1 &= 0 \\
  u_{23} &= 0 \\
  u_{31} + u_{13} &= 0 \\
  u_{32} &= 0 \\
  u_{33} - u_{11} &= 0 \\
  a_2 k_1 + ds'/ds u_{11} - 1 &= 0 \\
  a_2 t_1 - ds'/ds u_{13} &= 0 \\
  ds'/ds a_2 k_2 - u_{11} + ds'/ds &= 0 \\
  ds'/ds a_2 t_2 - u_{13} &= 0
\end{align*}
\] (5.8)

By lemma 3.10, the four conclusions of $EI_{22}$ are equivalent to

\[
\begin{align*}
  a'_2 &= 0 \\
  u'_{11} &= 0 \\
  DLR(1, k_1, t_1) &= k''_1 t'_1 - t''_1 k'_1 = 0 \\
  (t_1 t_2)' &= 0
\end{align*}
\] (5.9)

respectively. The pseudo remainders of the first two d-pols of (5.9) w.r.t all the nine asc chains are zero, but the last two d-pols are not zero on two components in which we have $a_2 = 0, k_1 = k_2$, and $t_1 = t_2$. At these cases $C_1$ and $C_2$ becomes one curve and hence there is no restriction for their curvature and torsion. Thus the last d-pols of (5.9) can not be zero. Therefore, if we formulate the conclusions of $EI_{22}$ as (5.7), then we must add another non-degenerate condition $a_2 \neq 0$.

On the other hand, we can obtain our results from (5.8) directly. $a'_2 = 0$ and $u'_{11} = 0$ are already in (5.8) Eliminate $ds'/ds$ from the last four equations of (5.8), we have:

\[
\begin{align*}
  a_2 u_{11} t_1 + a_2 u_{13} k_1 - u_{13} &= 0 \\
  a_2^2 t_1 t_2 - u_{13}^2 &= 0 \\
  a_2^2 k_2 + a_2 t_1 - u_{11} u_{13} &= 0
\end{align*}
\] (5.10)

As $a_2, u_{11},$ (and hence $u_{13} = \sqrt{1 - u_{11}^2}$) are constants, the first two formulas of (5.10) actually give the concrete expression of Bertrand's theorem and Schell's theorem. From (5.10) we can find formulas between $k_1, k_2; k_1, t_2; \text{ and } k_2, t_2$ respectively.
\[(1 - a_2 k_1)(1 + a_2 k_2) - u_{11}^2 = 0\]
\[a_2^2 k_1 t_2 - a_2 t_2 + u_{11} u_{13} = 0\]
\[a_2 u_{11} t_2 - a_2 u_{13} k_2 - u_{13} = 0\]  \hspace{1cm} (5.11)

The conclusions in (5.10) and (5.11) are correct at the nondegenerate condition \( k_1 k_2 ds'/ds \neq 0 \).

For \( EI_{23} \), we can find the following concrete expressions for (b) and (c) of \( EI_{23} \):

\[a_2 t_1^2 + a_2 k_1^2 - k_1 = 0\]
\[a_2^2 t_1 t_2^2 - t_2 + t_1 = 0\]

and other algebraic relations among \( k_1, k_2, \) and \( t_2 \):
\[a_2 t_1 t_2 - k_1 = 0\]
\[k_1^2 + t_1^2 - t_1 t_2 = 0\]
\[(a_2^2 k_1 - a_2) t_2^2 + k_1 = 0\]

For \( ds'/ds \), we have:
\[(ds'/ds)^2 = t_1^2 / (t_1^2 + k_1^2)\]
\[(ds' ds)^2 = t_1 / t_2\]
\[ds'/ds = u_{11}\]

Note that \( k_2 \) does not occurred in the above expressions. There are no algebraic relations among \( k_2, k_1, t_1, t_2, \) and \( a_2 \). We have the following formulas for \( k_2 \):
\[2t_1 k_2 + dk_1 / ds' = 0\]
\[a_2 t_2 k_2 - (ds'/ds)' / (ds'/ds)^2 = 0\]

All the above results are true under the nondegenerate condition \( k_1 k_2 ds'/ds \neq 0 \).

5.2. The Case Of Parallel

Let \( EP_{ij} \) denote the case for which vector \( e_{2j} \) is parallel to vector \( e_{1i} \) at the corresponding points. At case \( EP_{ij} \), we have

\[u_{jk} = 0 \quad k \neq i\]
\[u_{ki} = 0 \quad k \neq j\]  \hspace{1cm} (5.12)

For each concrete case \( EP_{tojo} \), apply our decomposition algorithm to (5.3), (5.4) and (5.12) under the non-degenerate condition \( k_1 \neq 0, k_2 \neq 0, ds'/ds \neq 0 \). For \( EP_{11}, EP_{13}, \) and \( EP_{33} \) the following results can be derived automatically.
Case $EP_{11}$. We have four cases:

- \( e_{21} = -e_{11}, e_{22} = e_{12}, e_{23} = -e_{13}, \) and
  \[ \frac{ds'}{ds} = -\frac{k_1}{k_2} = -\frac{t_1}{t_2}. \]

- \( e_{21} = -e_{11}, e_{22} = -e_{12}, e_{23} = e_{13}, \) and
  \[ \frac{ds'}{ds} = -\frac{k_1}{k_2} = -\frac{t_1}{t_2}. \]

- \( e_{21} = e_{11}, e_{22} = -e_{12}, e_{23} = -e_{13}, \) and
  \[ \frac{ds'}{ds} = -\frac{k_1}{k_2} = \frac{t_1}{t_2}. \]

- \( e_{21} = e_{11}, e_{22} = e_{12}, e_{23} = e_{13}, \) and
  \[ \frac{ds'}{ds} = \frac{k_1}{k_2} = \frac{t_1}{t_2}. \]

Case $EP_{13}$. We have four cases:

- \( e_{21} = -e_{13}, e_{22} = -e_{12}, e_{23} = -e_{11}, \) and
  \[ \frac{ds'}{ds} = -\frac{t_1}{k_2} = -\frac{k_1}{t_2}. \]

- \( e_{21} = e_{13}, e_{22} = e_{12}, e_{23} = -e_{11}, \) and
  \[ \frac{ds'}{ds} = -\frac{t_1}{k_2} = \frac{k_1}{t_2}. \]

- \( e_{21} = -e_{13}, e_{22} = e_{12}, e_{23} = e_{11}, \) and
  \[ \frac{ds'}{ds} = \frac{t_1}{k_2} = -\frac{k_1}{t_2}. \]

- \( e_{21} = e_{13}, e_{22} = -e_{12}, e_{23} = e_{11}, \) and
  \[ \frac{ds'}{ds} = \frac{t_1}{k_2} = \frac{k_1}{t_2}. \]

Case $EP_{33}$. We have the same results as $EP_{11}$.

Take $EP_{11}$ as an example. Using our decomposition algorithm to (5.3), (5.4), and \( \{u_{12} = 0, u_{13} = 0, u_{21} = 0, u_{31} = 0\} \) under the following variable order: \( k_1 < t_1 < k_2 < t_2 < \frac{ds'}{ds} < a_1 < a_2 < a_3 < u_{11} < u_{12} < u_{13} < u_{21} < u_{22} < u_{23} < u_{31} < u_{32} < u_{33} \), we find four main components which give the four results respectively.

5. The Conclusion

In this paper, we present an improved version of Ritt-Wu's zero decomposition algorithm and use the algorithm to prove theorems in differential geometry mechanically according to two approaches.

We have implemented a prover using KCL Lisp with enhancement by Schelter in a SUN 3/280 based on both formulations. We use the prover to prove theorems in the space curve theory. Our experiments on the computer shows that a large portion of the theorems in the space curve theory can be proved by our methods. About one hundred theorems in space curve theory have been proved according to Formulation 1 under certain explicitly given non-degenerate conditions. Most of the theorems are also proved to be generally true according to Formulation 2. A description of the prover (input etc.) and most of the examples proved can be found in the appendix of this paper.

REFERENCE


Appendix. Provers For Differential Geometry And More Examples

A.1. Some Geometry Predicates In Differential Geometry

Let \( n = (n_1, n_2, n_3), v_1 = (x_1, y_1, z_1), v_2 = (x_2, y_2, z_2), v_3 = (x_3, y_3, z_3), v_4 = (x_4, y_4, z_4) \), where the \( n, x, y, \) and \( z \) are variables. We define the following predicates.

1. The norm of vector \( v_1 \) is \( p \).
2. Vector \( v_1 \) has constant length.
3. Vector \( v_1 \) is parallel to vector \( v_2 \).
4. Vector \( v_1 \) is parallel to a fixed vector, or equivalently \( v_1 \) has constant direction.
5. Vector \( v_1 \) is perpendicular to vector \( v_2 \), or \( v_1 \) is parallel to the plane with \( v_2 \) as normal vector.
6. Vector \( v_1 \) is perpendicular to a fixed vector, or \( v_1 \) is parallel to a fixed plane.
7. Vector \( v_2 \) is on the line passing \( v_1 \) and parallel to \( n \).
8. The lines passing \( v_1 \) and parallel to \( n \) go through a fixed point.
9. Vectors \( v_1, v_2, \) and \( v_3 \) are on the same line.
10. The lines passing \( v_1 \) and \( v_2 \) go through a fixed point.
11. Vector \( v_2 \) is on the plane passing \( v_1 \) and with \( n \) as its normal vector.
12. The planes passing \( v_1 \) and with \( n \) as its normal vector go through a fixed point.
13. Vectors \( v_1, v_2, \) and \( v_3 \) are parallel to a plane.
14. The planes containing \( v_1, v_2 \) and the origin point go through a fixed point.
15. Vector \( v_1, v_2, v_3, \) and \( v_4 \) are on the same plane.
16. The planes determined by \( v_1, v_2, \) and \( v_3 \) pass a fixed point.
17. The vector \( v_1 \) is a constant vector.

In the following, We shall give the exact representations for the above predicates by differential polynomial equations respectively. The proof of the correctness of these representation can be found in section 2 of this appendix.

The differentiations are w.r.t \( t \). \((v_1, v_2)\) stands for the inner product of \( v_1 \) and \( v_2 \). \((v_1 \ v_2 \ v_3)\) is defined to be \((v_1, v_2 \times v_3)\).

S1. (v-norm \( v_1 \) \( p \)). The square of the norm of vector \( v_1 \) is \( p \).

\[
z_1^2 + y_1^2 + z_1^2 - p = 0
\]

S2. (cons-len \( v_1 \)). Vector \( v_1 \) has constant length.
\[ z_1'z_2' + y_1'y_1' + x_1'x_1' = 0 \]

**S3. (v-para \( v_1 \) \( v_2 \)).** Vector \( v_1 \) is parallel to vector \( v_2 \) if and only if \( v_1 \times v_2 = 0 \) or
\[
\begin{align*}
    y_1z_2 - z_1y_2 &= 0 \\
x_1z_2 - z_1x_2 &= 0 \\
x_1y_2 - y_1x_2 &= 0
\end{align*}
\]

**S4. (cons-dir \( v_1 \)).** Vector \( v_1 \) has constant direction if and only if \( v_1 \times v_1' = 0 \) or
\[
\begin{align*}
    y_1z_1' - y_1'z_1 &= 0 \\
x_1z_1' - x_1'z_1 &= 0 \\
x_1y_1' - x_1'y_1 &= 0
\end{align*}
\]

**S5. (v-perp \( v_1 \) \( v_2 \)).** Vector \( v_1 \) is perpendicular to vector \( v_2 \) if and only if \( (v_1, v_2) = 0 \) or
\[
\begin{align*}
    x_1x_2 + y_1y_2 + z_1z_2 &= 0
\end{align*}
\]

**S6. (perp-fix-line \( v_1 \)) or (para-fix-plane \( v_1 \)).** Vector \( v_1 \) is perpendicular to a fixed line if and only if \( (v_1, v_1', v_1'') = 0 \) or
\[
\begin{align*}
    (x_1y_1' - x_1'y_1)z_1'' + (-x_1y_1'' + x_1'y_1)z_1' + (x_1'y_1'' - x_1''y_1') &= 0
\end{align*}
\]

**S7. (co2-linear \( n \) \( v_1 \) \( v_2 \)).** Vector \( v_2 \) is on the line passing \( v_1 \) and parallel to \( n \) if and only if \( n \times (v_2 - v_1) = 0 \) or
\[
\begin{align*}
    (y_2 - y_1)n_3 + (-z_2 + z_1)n_2 &= 0 \\
    (x_2 - x_1)n_3 + (-z_2 + z_1)n_1 &= 0 \\
    (x_2 - x_1)n_2 + (-y_2 + y_1)n_1 &= 0
\end{align*}
\]

**S8. (fix-co2-linear \( n \) \( v_1 \)).** The lines passing \( v_1 \) and parallel to \( n \) go through a fixed point if and only if the following conditions are generically true.
\[
\begin{align*}
    (DLR \ n_1 \ n_2 \ n_1y_1 - n_2x_1) &= 0 \\
    (DLR \ n_1 \ n_3 \ n_1z_1 - n_3x_1) &= 0 \\
    (DLR \ n_2 \ n_3 \ n_2z_1 - n_2y_1) &= 0
\end{align*}
\]

**S9. (co3-linear \( v_1 \) \( v_2 \) \( v_3 \)).** Vectors \( v_1 \), \( v_2 \), and \( v_3 \) are on the same line if and only if \( (v_2 - v_1) \times (v_3 - v_1) = 0 \) or
\[
\begin{align*}
    (y_2 - y_1)z_3 + (-z_2 + z_1)y_3 + y_1z_2 - z_1y_2 &= 0 \\
    (x_2 - x_1)z_3 + (-z_2 + z_1)x_3 + x_1z_2 - z_1x_2 &= 0 \\
    (x_2 - x_1)y_3 + (-y_2 + y_1)x_3 + x_1y_2 - y_1x_2 &= 0
\end{align*}
\]

**S10. (fix-co3-linear \( v_1 \) \( v_2 \)).** The lines passing \( v_1 \) and \( v_2 \) go through a fixed point if and only if \( (fix-co2-linear \ v_2 - v_1 \ v_1) \) or
\[
\begin{align*}
    (DLR \ (y_2 - y_1 \ (-z_2 + z_1) \ (y_1z_2 - z_1y_2)) &= 0 \\
    (DLR \ (x_2 - x_1 \ (-z_2 + z_1) \ (x_1z_2 - x_1y_2)) &= 0 \\
    (DLR \ (x_2 - x_1 \ (-y_2 + y_1) \ (x_1y_2 - y_1x_2)) &= 0
\end{align*}
\]
A.2. A General Purpose Prover

In this section all d-pols are considered in $Q\{x_1, \ldots, x_n\}$. A geometry statement is defined as
follows:

\[
\begin{align*}
\text{stat} &= \{\text{par-vars} \text{ dep-vars} \text{ pot-list} \\ s_1 & \quad \ldots \\ s_t & \quad \text{conc} \\ [\text{non-deg } d_1 & \ldots d_k] \\ [\text{cons-var } y_1 & \ldots y_l] \}
\end{align*}
\]

(A.2.1)

where par-vars is a subset of \(\{x_1, \ldots, x_n\}\); dep-vars is a subset of \(\{x_1, \ldots, x_n\}\) such that \(\text{par-vars} \cap \text{dep-vars} = \emptyset\); pot-list = \((p_1 (w_1 y_1 z_1) \ldots p_m (w_m y_m z_m))\) in which the \(p\) are some variables other than the \(x\) and the \(w, y, z\) are variables in par-vars and dep-vars; \(s_1, \ldots, s_t, \text{conc}, d_1, \ldots, d_k\) are predicates given in section 1 or some d-pols. \(y_1, \ldots, y_l\) are certain variables in par-vars or dep-vars. We also assume that the variables occurred in the \(s, \text{conc}\), and the \(d\) must be defined in par-vars, dep-vars, or pot-list.

**Definition A.2.2.** A statement as above is true if the following statement

\[
\forall x [(e(s_1) \land \ldots \land e(s_t) \land y'_1 = 0 \land \ldots \land y'_l = 0 \land \lnot e(d_1) \land \ldots \land \lnot e(d_k)] \Rightarrow e(\text{conc})]
\]

is generally true.

Here we actually use a mixture of Formulation F1 and Formulation F2, i.e. to prove a statement generally true under certain non-degenerate conditions. If par-vars is empty, a statement is true according as definition A.2.2 is the same as the statement is universally valid defined in section 3 of the main paper. If \(k = 0\), a statement is true according as definition A.2.1 is the same as the statement is generally true defined in section 3 of the main paper.

**Theorem A.2.3.** For a geometry problem \(\text{stat}\), we have a prover (prove-th \(\text{stat}\)) to decide whether \(\text{stat}\) is true.

We now prove the correctness of the description of the geometry statements in section 1 using our prover Prove-th. S1, S2, S3, S5, S7, S9, S11, S13, S15, and S17 are obviously true. S4 can be reduced to the following two examples

**Example 1.** If \(v_2\) is parallel to a nonzero constant vector \(v_1\) then (cons-dir \(v_2\)) is true.

We need to prove that (prove-th ( ( (x_1 y_1 z_1 x_2 y_2 z_2) (v_1 (x_1 y_1 z_1) v_2 (x_2 y_2 z_2)) (v-para v_1 v_2) (cons-dir v_2) non-deg (v-norm v_1 0) cons-var v_1)) is true.

**Example 2.** If \(v_1\) is a unit vector satisfying (cons-dir \(v_1\)), then \(v_1\) is a constant vector, i.e. \(v_1\) has a constant direction.

The example can be reduced to (prove-th ( ( (x_1 y_1 z_1 x_2 y_2 z_2) (v_1 (x_1 y_1 z_1) v_2 (x_2 y_2 z_2)) (cons-dir v_1) (v-norm v_1 1) (cons-v v_1))) is true.

S6 can be derived from lemma 3.10. By reducing S6 to the following two examples, we can also prove it by our prover.
Example 3. If \( v_2 \) is perpendicular to a nonzero constant vector \( v_1 \) then we have (perp-fix-line \( v_2 \)).

The example is equivalent to (prove-th \( (\bigcup (x_1, y_1, z_1, x_2, y_2, z_2) (v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2)) \) (v-perp \( v_1, v_2 \)) (perp-fix-line \( v_2 \)) non-deg (v-norm \( v_1, 0 \)) cons-var \( v_1 \)) is true.

Example 4. \( v_1 \) satisfies (perp-fix-line \( v_1 \)) does not have constant direction. Then the vector perpendicular to \( v_1 \) and \( v'_1 \) has constant direction.

The example is equivalent to (prove-th \( (\bigcup (x_1, y_1, z_1, x_2, y_2, z_2) (v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2)) \) (v-perp \( v_1, v_2 \)) (v-perp \( v'_1, v_2 \)) (perp-fix-line \( v_1 \)) (cons-dir \( v_2 \)) non-deg (cons-dir \( v_1 \)) is true.

We assume \( v_1 \) does not toward a fixed direction in which case the result is obviously true.

By the following two examples, we know that S8 is generically true.

Example 5. (prove-th \( (\bigcup (n_1, n_2, n_3, x_1, y_1, z_1, x_2, y_2, z_2) (\bigwedge (n_1, n_2, n_3) v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2)) \) (co2-linear \( n, v_1, v_2 \)) (fix-co2-linear \( n, v_2 \)) cons-var \( v_1 \)) is true.

Example 6. (prove-th \( (\bigcup (n_1, n_2, n_3, x_1, y_1, z_1, x_2, y_2, z_2) (\bigwedge (n_1, n_2, n_3) v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2)) \) (co2-linear \( n, v_1, v_2 \)) (fix-co2-linear \( n, v_1 \)) (cons-dir \( v_2 \)) non-deg (para-v \( n, v_1 \) \( p \) cons-var \( x_2, y_2 \)) is true, where \( p = ((n_1'' x_2 n_2' - n_1' n_2 n_3') n_3' + (-2n_1' n_2 n_2' + 2n_1 n_1' n_2') n_3' + ((-n_1'' n_2 n_2'' + 2n_1' n_2') n_3') n_3' + (n_1 n_1' n_2' - 2n_1 n_1' n_2'' + ((-n_1'' + 2n_1') n_2') n_3') n_3'). \) We also assume that \( n \) is not parallel to \( v_1 \), otherwise the result is true obviously.

We can prove S10 by substituting \( n \) for \( v_2 - v_1 \) in S8. For S12, one direction is easy, i.e. we have

Example 7. (prove-th \( (\bigcup (n_1, n_2, n_3, x_1, y_1, z_1, x_2, y_2, z_2) (\bigwedge (n_1, n_2, n_3) v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2)) \) (co2-plane \( n, v_1, v_2 \)) (fix-co2-plane \( n, v_2 \)) cons-var \( v_1 \)) is true.

For another direction, by lemma 3.10 there exist constants \( t_1, t_2, t_3 \) and \( t_4 \) such that

\[ t_1 n_1 + t_2 n_2 + t_3 n_3 + t_4 (n_1 x_1 + n_2 y_1 + n_3 z_1) = 0 \]

If \( t_4 \neq 0 \), the planes passing \( v_1 \) and with \( n \) as its normal vector always pass \( (t_1/t_4, t_2/t_4, t_3/t_4) \). Otherwise, we must have (perp-fix-line \( n_1, n_2, n_3 \)) = 0 which is impossible.

S14 comes immediately from lemma 3.10. But we can also prove S14 using our prover by the two examples below.

Example 8. (prove-th \( (\bigcup (x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3) (v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2) v_3 (x_3, y_3, z_3)) \) (co3-plane \( v_1, v_2, v_3 \)) (fix-co3-plane \( v_2, v_3 \)) non-deg (v-norm \( v_1, 0 \)) cons-var \( v_1 \)) is true.

Example 9. (prove-th \( (\bigcup (x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3) (v_1 (x_1, y_1, z_1) v_2 (x_2, y_2, z_2) v_3 (x_3, y_3, z_3)) \) (co3-plane \( v_1, v_2, v_3 \)) (v-perp \( v_1, v_2, v_3 \)) (fix-co3-plane \( v_1, v_2 \)) (cons-dir \( v_3 \)) non-deg (cons-dir \( v_1, v_2 \)) is true.

S16 comes from S12.

The following examples give some relations among the geometry statements in section 1.

Example 10.

(a) (prove-th \( (\bigcup (x_1, y_1, z_1) (v_1 (x_1, y_1, z_1)) \) (cons-dir \( v_1 \)) (perp-fix-line \( v_1 \)) is true, i.e. if \( v_1 \) is parallel to a fixed direction then \( v_1 \) must be perpendicular to a fixed line.

28
(b) \((n_1, n_2, n_3, x_1, y_1, z_1, n_1, n_2, n_3, v_1, (x_1, y_1, z_1))\) (v-para n v_1) (fix-co2-linear n v_1) is true, i.e. if vectors n and v_1 are parallel then the lines passing v_1 and parallel to n pass a fixed point.

(c) \((x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3, v_1, (x_1, y_1, z_1), v_2, (x_2, y_2, z_2), v_3, (x_3, y_3, z_3))\) (co3-linear v_1, v_2, v_3) (co3-plane v_1, v_2, v_3) is a theorem.

A.3. A Prover For Space Curve

For space curves, we can develop more efficient systems. In the prover, we fix a curve \(C = (x, y, z)\) with its arc s as parameter. Let \(T = (x', y', z')\), \(N = (n_1, n_2, n_3)\), \(B = (b_1, b_2, b_3)\), and \(O = (o_1, o_2, o_3)\) be the tangent vector, principal vector, binormal vector, and the curvature center of \(C\) respectively. Denote the curvature, torsion, and curvature radius of \(C\) by \(k\), \(t\), and \(r\). We have

\[
\begin{align*}
\dot{x'}^2 + \dot{y'}^2 + \dot{z'}^2 - 1 &= 0 \\
k^2 - \ddot{z}^2 - \ddot{y}^2 - \ddot{x}^2 &= 0 \\
k' - 1 &= 0 \\
k n_1 - x'' &= 0 \\
k n_2 - y'' &= 0 \\
k n_3 - z'' &= 0 \\
k b_1 - y' z'' + y'' z' &= 0 \\
k b_2 + x' z'' - x'' z' &= 0 \\
k b_3 - x' y'' + x'' y' &= 0 \\
o_1 - r n_1 - x &= 0 \\
o_2 - r n_2 - y &= 0 \\
o_3 - r n_3 - z &= 0 \\
t + n_3 b_3' + n_2 b_2' + n_1 b_1' &= 0
\end{align*}
\]

(3.1)

(3.2)

Let curve-vars = \{x, y, z, k, r, n_1, n_2, n_3, b_1, b_2, b_3, o_1, o_2, o_3, t\}. Other curves are also considered having s as parameters. Consider the following new predicates.

18. \(k_1\) and \(t_1\) are the curvature and torsion of curve \(v_1\) respectively.

19. \(k_1\) and \(t_1\) are the curvature and torsion of curve \(v_1\) with arc parameter.

20. Give the principal normal vector of curve \(v_1\).

21. Give the binormal vector of curve \(v_1\).

22. The curve \(v_1\) is a straight line.

23. The curve \(v_1\) is a plane curve.

24. The curve \(v_1\) is in a plane passing the origin point.

25. The curve \(v_1\) is a spherical curve.
26. The curve $C$ is a helix.

We can describe the statements as below.

S18. (curve $v_1, k_0, k_1, t_1$)
\[
\begin{align*}
  k_0 - x_1'^2 - y_1'^2 - z_1'^2 &= 0 \\
  k_0^3 k_1^2 - ((v'_1 \times v''_1), (v'_1 \times v'''_1)) &= 0 \\
  k_0^3 k_1^2 t_1 - (v'_1, v''_1, v'''_1) &= 0
\end{align*}
\]

S19. (curve-arc $v_1, k_1, t_1$)
\[
\begin{align*}
  k_1^2 - x_1'''^2 - y_1'''^2 - z_1'''^2 &= 0 \\
  k_1^2 t_1 - (v'_1, v''_1, v'''_1) &= 0
\end{align*}
\]

S20. (curve-norm $v_1$).
\[
\text{(curve-norm $v_1$)} = (v'_1, v''_1) v'''_1 - (v'_1, v''_1) v'_1
\]

S21. (curve-binorm $v_1$).
\[
\text{(curve-binorm $v_1$)} = v'_1 \times (\text{curve-norm $v_1$})
\]

S22. (fix-line $v_1$). The curve $v_1$ is a straight line if and only if $v'_1$ has constant direction, or
\[
\begin{align*}
  y'_1 z''_1 - y''_1 z'_1 &= 0 \\
  x'_1 z''_1 - x''_1 z'_1 &= 0 \\
  x'_1 y''_1 - x''_1 y'_1 &= 0
\end{align*}
\]

S23. (fix-plane $v_1$). The curve $v_1$ is a plane curve if and only if $(v'_1, v''_1, v'''_1) = 0$ or
\[
\begin{align*}
  (x'_1 y''_1 - x''_1 y'_1) z'''_1 + (-x'_1 y'''_1 + x'''_1 y'_1) z'''_1 + (x''_1 y''_1 - x'''_1 y'_1) z''_1 &= 0
\end{align*}
\]

S24. (fix-plane-o $v_1$). The curve $v_1$ is in a plane passing the origin point if and only if (DLR $v_1$) or
\[
\begin{align*}
  (x_1 y'_1 - x'_1 y_1) z''_1 + (-x_1 y''_1 + x''_1 y_1) z''_1 + (x'_1 y''_1 - x''_1 y'_1) &= 0
\end{align*}
\]

S25. (fix-sph $v_1$). The curve $v_1$ is a spherical curve if and only if
\[
\begin{align*}
  x_1^2 + y_1^2 + z_1^2 + fx_1 + gy_1 + hx_1 + e &= 0
\end{align*}
\]

for constants $f, g, h, \text{ and } e$, or equivalently
\[
\begin{align*}
  \text{(DLR } x'_1 y'_1 z'_1, x_1 x'_1 + y_1 y'_1 + z_1 z'_1) &= 0 \\
  \text{(DLR } x'_1 y'_1 z'_1) \neq 0
\end{align*}
\]

S26. (fix-helix $v_1$). The curve $v_1$ is a helix if and only if $(C'', C'''', C''''') = 0$ or
\[
\begin{align*}
  (x'' y''' - x''' y'') z''' + (-x'' y'''' + x''' y'''') z'' + (x''' y''' - x''' y'''') z' &= 0
\end{align*}
\]

S18 and S19 are definitions. S20 and S21 come from S4 and S6 respectively. S22 and S23 come from lemma 3.10. S24 comes from example 4 of the original paper.

Let $\text{stat}$ be a geometry statement as (A.2.1), but the $s$ and $d$ can be the predicates described
in section 1 and in this section of this appendix. Set

\[
stat 1 = \{ \text{par-vars1} \}
\begin{align*}
\text{dep-vars1} \\
\text{pot-list1} \\
s_1 \\
\vdots \\
s_t \\
(3.1) \cup (3.2) \\
\text{conc} \\
\text{non-deg } d_1 \cdots d_k \ k \ z'^2 + y'^2 + x'^2 \\
[\text{cons-var } y_1 \cdots y_t]
\end{align*}
\]

where \text{par-vars1} is the union of \text{par-vars} and a subset of curve-vars; \text{dep-vars1} is the union of \text{dep-vars} and a subset of curve-vars; \text{pot-list1} = \text{pot-list} \cup \{ c (x \ y \ z) n (n_1 \ n_2 \ n_3) o (o_1 \ o_2 \ o_3) \}.

we have the following definition

\textbf{Definition A.3.1} Use the same notation as the above paragraph. The statement \text{stat} is true in the theory of space curve if \text{stat1} is true and we define \text{(prove-curve } \text{stat} \text{)} = \text{(prove-th } \text{stat1}).

Note that in proving theorems in the space curve theory, we always assume the curvature of the curve is not zero, i.e. the curve is not a straight line; because from (3.1) we know when \( k = 0 \) we cannot define \( N, B, O \), and \( t \) at all.

\textbf{A.4. More Examples For Space Curve}

Here are some of the theorems in space curve theory which have been prove mechanically by our prover (prove-curve).

\textbf{Example 11.} (Frenet formula) \( N' = -kC + tB \).

We need to prove \((())()() n'_1 + kx' - tb_1 \ n'_2 + ky' - tb_2 \ n'_3 + kz' - tb_3)\) is true.

\textbf{Example 12.} \(kt = -T'.B'\)

We need to prove \((())()()kt + (C''.B')\) is true.

\textbf{Example 13.} \((C', C'', C''') = k^2 t\)

We need to prove \((())()()k^2 t - (C' \ C'' \ C''' )\) is true.

\textbf{Example 14.} \((C'' C''' C''') = k^5 (t/k)'\).

We need to prove \((())()()k^4 t' - k^3 k't - (C'' \ C''' \ C''')\) is true.

\textbf{Example 15.} \(t^2 = \frac{k^2}{k^2} C'''' - k^2 - (\frac{k^2}{k})^2\).

We need to prove \((())()()k^2 t^2 - (C'''' C''') + k^4 + k'^2\) is true.

\textbf{Example 16.} \(C''' = k' N - k^2 C' + kt B\).
We need to prove \((C'' - k'N + k^2C' = kC')\) is true.

**Example 17.** \(N'' = t'B - (k^2 + t^2)N - k'C'.\)

We need to prove \((N'' + t'B - (k^2 + t^2)N - k'C')\) is true.

**Example 18.** \(B'' = t(kC' - tB) - t'N.\)

We need to prove \((B'' + t(kC' - tB) - t'N)\) is true.

**Example 19.** \((C''C''') = k(k'' - k^3 - kt^2).\)

We need to prove \((C''C''' - k(k'' - k^3 - kt^2))\) is true.

**Example 20.** \((B'B''b''') = t^3(k't - kt').\)

We need to prove \((B'B''b''') = t^3(k't - kt')\) is true.

**Example 21.** The following statements are equivalent

(a) Curve \(C\) is a circle.

(b) \(k \neq 0\) is a constant, and \(t = 0\).

Without loss of generality, we consider a simple case: \(C\) is on the \(z\) plane. We need to prove (prove-curve \(DLR(1,x,y,x^2 + y^2)z(k't)\)) and (prove-curve \(k'tzDLR(1,x,y,x^2 + y^2)\)) are true.

**Example 22.** Show that the tangents to a space curve and the locus of its center of curvature at corresponding points are mutually perpendicular.

The example can be reduced to (prove-curve \((v-perp T O')\)) is true.

**Example 23.** Show that the principal normal of a twisted curve at a point \(P\) is tangent to the locus of the center of the curvature when and only when \(t = 0\) at \(P\).

The example can be reduced to (prove-curve \((v-perp N O')\)) and (prove-curve \((v-perp N O')t)\) are true.

**Example 24.** Show that the principal normal of a twisted curve at a point \(P\) is perpendicular to the locus of the center of the curvature if and only if \(k' = 0\) at \(P\).

The example can be reduced to (prove-curve \((v-perp N O')\)) and (prove-curve \((v-perp N O')k')\) are true.

**Example 25.** If two curves are reflections of one another in a point, their curvatures at corresponding points are equal and their torsions are negatives of one another.

The example can be reduced to (prove-curve \((v_2 + C - v_1)\) (curve \(v_2 k_1 k_2 t_2\) \((t + t_2 k^2 - k^2)\) non-deg \(k_1 k_2\) cons-var \(v_1)\)) is true.

**Example 26.** If two curves are reflections of one another in a plane then their curvatures at corresponding points are equal and their torsions are negatives of one another.

Consider a special case: curves \(v_1\) and \(C\) are reflections of one another in the \(z\)-plane. The
example can be reduced to \( \text{prove-curve} \left( \left( \right) \right) \left( x_1 - x, y_1 - y, z_1 + z, \text{curve} v_1 k_1 k_2 t_2 \right) \left( t_2 + t, k_2^2 - k_2^2 \right) \text{non-deg} k_1 k_2 \)) is true.

**Example 27.** The tangent indicatrix, the principal normal indicatrix, and the binormal indicatrix of the curve \( C \) are the loci represented respectively by the vectors: \( T, N, \) and \( B \). Show that all three indicatrices lie on the sphere of unit radius whose center is at the origin.

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( v\text{-norm} T 1 \right) \left( v\text{-norm} B 1 \right) \left( v\text{-norm} N 1 \right) \right) \)) is true.

**Example 28.** Show that the tangents to the tangent and binormal indicatrices at the points corresponding to a given point \( P \) of a twisted curve \( C \) are parallel to the principal normal of \( C \) at \( P \).

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( v\text{-para} N T' \right) \left( v\text{-para} N N' \right) \right) \)) is true.

**Example 29.** The derivative of the arc of the tangent indicatrix w.r.t the arc of \( C \) is the curvature of \( C \).

The derivative of the arc of a curve \( v_1 \) w.r.t \( s \) is equal to \( \sqrt{x'^2 + y'^2 + z'^2} \). The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{curve} T k_1 k_2 t_2 \right) \left( k_1 - k_2^2 \right) \text{non-deg} \left(k_1, k_2 \right) \right) \)) is true.

**Example 30.** The derivative of the arc of the principal normal indicatrix w.r.t the arc of \( C \) is equal to \( \sqrt{k^2 + t^2} \).

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{curve} N k_1 k_2 t_2 \right) \left( k_1 - t^2 - k_2^2 \right) \text{non-deg} \left(k_1, k_2 \right) \right) \)) is true.

**Example 31.** The derivative of the arc of the binormal indicatrix w.r.t the arc of \( C \) is the torsion of \( C \).

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{curve} B k_1 k_2 t_2 \right) \left( k_1 - t^2 \right) \text{non-deg} \left(k_1, k_2 \right) \right) \)) is true.

**Example 32.** Show that a twisted curve is a helix if and only if the tangent indicatrix is a plane curve.

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{fix-helix} C \right) \left( \text{fix-plane} T \right) \text{non-deg} \left( \text{fix-plane} C \right) \right) \)) and \( \text{prove-curve} \left( \left( \right) \left( \text{fix-plane} T \right) \left( \text{fix-helix} C \right) \text{non-deg} \left( \text{fix-plane} C \right) \right) \)) are true.

**Example 33.** Show that a twisted curve is a helix if and only if the binormal indicatrix is a plane curve.

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{fix-helix} C \right) \left( \text{fix-plane} B \right) \text{non-deg} \left( \text{fix-plane} C \right) \right) \)) and \( \text{prove-curve} \left( \left( \right) \left( \text{fix-plane} B \right) \left( \text{fix-helix} C \right) \text{non-deg} \left( \text{fix-plane} C \right) \right) \)) are true.

**Example 34.** Show that a twisted curve is a helix if and only if the principal normal indicatrix is part of a great circle of the unit sphere.

The example is equivalent to \( \text{prove-curve} \left( \left( \right) \left( \text{fix-plane-o} N \right) \left( \text{fix-helix} C \right) \right) \)) and \( \text{prove-curve} \left( \left( \right) \left( \text{fix-helix} C \right) \left( \text{fix-plane-o} N \right) \right) \)) are true.
Example 35. Show that a curve, not straight line, is a plane curve if and only if the tangent indicatrix is part of a great circle of the unit spherical.

The example is equivalent to (prove-curve ((l) () (fix-plane C) (fix-plane-o T))) and (prove-curve ((l) () (fix-plane-o T) (fix-plane C))) are true.

Example 36. Let $C$ be a twisted curve on the unit sphere with its arc as parameter. Show that $C = -rN - r'pB$, where $r = 1/k, p = 1/t$.

The example is equivalent to (prove-curve ((l) () (v-norm C 1) pt - 1 (C + rN + r'pB) non-deg k, t)) is true.

Example 37. Curve $v_1$ is defined by $v_1 = \int_0^t B(t)dt$. Show that the arc of $C$ is also the arc of $v_1$.

The example is equivalent to (prove-curve ((l) () (v-curve $v_1 k_1 k_2 t_2$) (k_1 - 1) non-deg k_1, k_2)) is true.

Example 38. Curve $v_1$ is defined by $v_1 = \int_0^t B(t)dt$. Let $k_1$ and $t_1$ be the curvature and torsion of $V_1$. Show that $k_1 = \pm t$ and $t_1 = \pm k$.

The example is equivalent to (prove-curve ((l) () (v-curve $v_1 k_1 t_1$) v'_1 - B (k^2 - t^2_1, t^2 - k^2_1) non-deg k_1)) is true.

Example 39. The rectifying planes of a curve pass a fixed point if and only if $t/k = a + b$, where $a$ and $b$ are constants and $s$ is the arc of the curve.

The example is equivalent to (prove-curve ((l) () (tr)'' (fix-co2-plane N C) non-deg (perp-fix-line N))) and (prove-curve ((l) () (fix-co2-plane N C) (tr)'' non-deg (perp-fix-line N))) are true.

Example 40. Let $O$ be the locus of the curvature center of curve $C$ which has constant curvature $k$. Show that the principal normal of $C$ and $O$ are parallel to each other, i.e. $C$ and $O$ consist a Bertrand curve pair.

The example is equivalent to (prove-curve ((l) () (k', (curve O k_1 k_2 t_2)) (v-para N (curve-norm O) non-deg k_1 k_2 cons-var k r)) is true.

Example 41. The radius of spherical curvature of a curve is $R^2 = \frac{1}{k^2} + \frac{1}{t^2}$.

The example is equivalent to (prove-curve ((l) (s_1 s_2 s_3) (s (s_1 s_2 s_3)) pt - 1, s - C - rN - pr'B, (s, s) - r^2 - p^2r'^2)) is true.

Example 42. The radius of spherical curvature of a curve is $R^2 = \frac{1}{k^2} (V'''' C''') - \frac{1}{t^2}$.

The example is equivalent to (prove-curve ((l) (s_1 s_2 s_3) (s (s_1 s_2 s_3)) pt - 1, s - C - rN - pr'B, (s, s) - r^4p^2(C''' C'''') - p^2)) is true.

Example 43. The tangent of the locus of the center of the spherical curvature is parallel to $B$.

The example is equivalent to (prove-curve ((l) (s_1 s_2 s_3) (s (s_1 s_2 s_3)) pt - 1, s - C - rN - pr'B, (v - para B (v - d s 1)))) is true.
Example 44. The principle normal of the locus of the center of the spherical curvature is parallel to $N$.

The example is equivalent to (prove-curve $(l) (s_1 s_2 s_3) (s (s_1 s_2 s_3)) pt \, \text{-} 1, s \, \text{=} \, C \, \text{-} \, r \, N \, \text{-} \, pr' \, B, (v \, \text{-\-} \, \text{para} \, N \, (\text{curve} \, \text{-\-} \, \text{norm} \, s)))$ is true.

Example 45. When the tangents to a curve are normals to another curve, the latter is called an involute of the former. Prove that $C_1 = C + uC'$ is the involute of $C$ if and only if $u' = -1$.

The example is equivalent to (prove-curve $(l) (x_1 y_1 z_1) (c_1 (x_1 y_1 z_1)) c_1 \, \text{-} \, C \, \text{-} \, uC', (v \, \text{-\-} \, \text{para} \, C' \, (\text{curve} \, \text{-\-} \, \text{norm} \, c_1), u + 1)$ and (prove-curve $(l) (x_1 y_1 z_1) (c_1 (x_1 y_1 z_1)) c_1 \, \text{-} \, C \, \text{-} \, uC', u + 1, (v \, \text{-\-} \, \text{para} \, C' \, (\text{curve} \, \text{-\-} \, \text{norm} \, c_1)))$ are true.

Example 46. The involute of a curve $c$ is parallel to the principle normal of $c$.

The example is equivalent to (prove-curve '$((l) (a s x_1 y_1 z_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s) (v \, \text{-} \, d \, c \, 1)))$, $s' \, \text{-} \, 1, (v \, \text{-\-} \, \text{para} \, N \, (v \, \text{-} \, d \, c \, 1)), \text{cons\-var} \, a))$ is true.

Example 47. The derivative of the arc of the involute $c_1 = C + (a - s)C'$ of a curve $C$ is $\frac{ds_1}{ds} = (a - s)k$.

The example is equivalent to (prove-curve $(l) (a s x_1 y_1 z_1 s_1 k_1 t_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s)(v \, \text{-} \, d \, c \, 1))), s' \, \text{-} \, 1, (\text{curve} \, c_1 s_1 k_1 t_1), (p = (pp \, \text{*} s_1 s_1) (pp \, \text{*} (pp \, \text{-} \, a \, s) (pp \, \text{-} \, a \, s) k k)) \text{non-deg} \, (p \, = \, s_2 0 k_2 0) \text{cons\-var} \, a)$ is true.

Example 48. The curvature of the involute $c_1 = C + (a - s)C'$ of a curve $C$ is $k_1 = \frac{k^2 + t^2}{k^2 (a - s)^2}$.

The example is equivalent to (prove-curve $(l) (a s x_1 y_1 z_1 s_1 k_1 t_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s)(v \, \text{-} \, d \, c \, 1))), s' \, \text{-} \, 1, (\text{curve} \, c_1 s_1 k_1 t_1), (p = (pp \, \text{*} k_1 k_1 k (pp \, \text{-} \, a \, s) (pp \, \text{-} \, a \, s) (pp \, \text{*} k k) (pp \, \text{*} (pp \, \text{*} k k) (pp \, \text{*} t t))), \text{non-deg} \, (p \, = \, s_1 0 k_1 0) \text{cons\-var} \, a)$ is true.

Example 49. The torsion of the involute $c_1 = C + (a - s)C'$ of a curve $C$ is $t_1 = \frac{k_1 - k_1't_1}{k_2 (a - s)^2}$.

The example is equivalent to (prove-curve $(l) (a s x_1 y_1 z_1 s_1 k_1 t_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s)(v \, \text{-} \, d \, c \, 1))), s' \, \text{-} \, 1, (\text{curve} \, c_1 s_1 k_1 t_1), (p = (pp \, \text{*} t_1 k (pp \, \text{*} k k) (pp \, \text{*} (pp \, \text{*} k k) (pp \, \text{*} t t))) (pp \, \text{-} \, (pp \, \text{*} k (d t 1)) (pp \, \text{*} t (d k 1))), \text{non-deg} \, (p \, = \, s_1 0 k_1 0) \text{cons\-var} \, a)$ is true.

Example 50. The principal normal of the involute $c_1 = C + (a - s)C'$ of a curve $C$ is parallel to $N'$.

The example is equivalent to (prove-curve $(l) (a s x_1 y_1 z_1 s_1 k_1 t_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s)(v \, \text{-} \, d \, c \, 1))), s' \, \text{-} \, 1, (\text{v\-\text{para} (curve\-\text{-\-}norm c_1) (v\-\text{d} N \, 1))) \text{cons\-var} \, a)$ is true.

Example 51. The binormal of the involute $c_1 = C + (a - s)C'$ of a curve $C$ is parallel to $kB + tC'$.

The example is equivalent to (prove-curve $(l) (a s x_1 y_1 z_1 s_1 k_1 t_1) (c_1 (x_1 y_1 z_1)) (v \, \text{-} \, c_1 C (s \, \text{*} (pp \, \text{-} \, a \, s)(v \, \text{-} \, d \, c \, 1))), s' \, \text{-} \, 1, (\text{v\-\text{para} (curve\-\text{binorm c_1) (v\-\text{d} s\* k B) (s\* t (v\-\text{d} C \, 1))) cons\-var} \, a)$ is true.