In: **Journal of Automated Reasoning**, 10:173-189, 1993,

Automated Reasoning in Differential Geometry and Mechanics Using the Characteristic Set Method[1]

Part II. Mechanical Theorem Proving

Shang-Ching Chou
Department of Computer Science
The Wichita State University
Wichita, KS 67208, USA

Xiao-Shan Gao
Institute of Systems Science
Academia Sinica
Beijing 100080, P.R. China

Abstract We clarify the formulation problem of mechanical theorem proving in differential geometry and mechanics and propose two formulations. We present complete methods of mechanical theorem proving for the two formulations. We also introduce predicates and a language to translate geometry statements into differential polynomial equations. A program based on our methods has proved more than 100 nontrivial theorems in differential geometry and elementary mechanics including various classification theorems for space curves, Bertrand's Theorem, Newton's gravitational laws, etc.

Keywords Mechanical theorem proving, Wu's method, Ritt–Wu's decomposition algorithm, statement of equation type, generally true, universally true, space curve theory, elementary mechanics.

1. Introduction to the Problems

This paper presents two methods for proving theorems in differential geometry based on our first paper of the series [4] (Part I). As we have mentioned in Part I, Wu proposed a method for proving theorems in differential geometry using Ritt's characteristic method (CS) method. Several examples from space curves and mechanics were also given by him [10, 11]. But many problems related to this topic are still not fully studied. First, the formulation problem, i.e., in what sense the method proves theorems. Second, the translation method, i.e., how to translate geometry statements into their algebraic forms. These are the main topics of this second paper.

Similar to the case of elementary geometry, theorems that the CS method addresses are those whose hypotheses and conclusions can be expressed by differential polynomial equations (theorems of equation type). We use the following simple example to illustrate this type of geometry problems.

Example 1.1. Show that the curvature k of a circle is a 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., $x_1' = 0$. Let x_4 be the square of the derivative of the arc of the circle, and x_5 be the curvature k of the circle, then the hypotheses can be expressed by the following equations.

$h_1 = x_3^2 + x_2^2 - x_1^2 = 0$	The equation of the circle $c = (x_2, x_3)$.
$h_2 = x_4 - x_3'^2 - x_2'^2 = 0$	$x_4 = (\frac{ds}{dt})^2 = \lvert c' \rvert^2$, where s is the arc.

[1] The work reported here was supported in part by the NSF Grant CCR-8702108.

$h_3 = x_4^3 x_5^2 - (x_2'' x_3' - x_2' x_3'')^2 = 0$ The definition of the curvature $k = \frac{|c'\ c''|}{|c'|^3}$.

The conclusion that k is constant can be expressed by the equation $C = x_5' = 0$. Thus one can ask whether the conclusion $C = 0$ follows from the three hypothesis equations, i.e., whether

$$\forall x_1 \cdots \forall x_5 [(h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0) \Rightarrow C = 0] \tag{1.2}$$

is true. However, (1.2) is not true because certain non-degenerate conditions are missing. For example, (1.2) is not true when $x_1 = 0$, i.e., the circle degenerates to a point.

As showed by Example 1.1, in the description of a geometry statement, necessary non-degenerate conditions for the statement to be true are often not given explicitly and some of them are not easy to find. The key of the formulation problem is how to handle non-degenerate conditions. As clarified in [5], in elementary geometry there are two formulations dealing with these implicit non-degenerate conditions.

Formulation F1. Introduce parameters and the notion of "generally (generically) true" and decide whether a statement is generally true, at the same time generating non-degenerate conditions to make the statement true (section 2.2).

Formulation F2. Explicitly specify non-degenerate conditions as a part of the geometry statement and prove whether the statement is true without adding any additional conditions (section 2.1).

Formulation F2 is easy to understand. However, if one of the necessary non-degenerate conditions of a geometry statement is missing and the geometry statement is not true, then we don't have any information about why it is not true: it is not true because of a missing 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. If a geometry statement is true according to Formulation F2, it is also generally true according to Formulation F1. For a geometry statement which is not true according to Formulation F2, we have two cases: (i) it is generally true according to Formulation F1, or (ii) it is not generally true according to Formulation F1. In case (i), the statement can be made true according to Formulation F2 by adding more non-degenerate conditions. In case (ii), the statement cannot be true according to Formulation F2 regardless whatever suitable non-degenerate conditions are added. In this sense, Formulation F1 describes the nature of a geometry statement more precisely. On the other hand, the geometry meaning of Formulation F2 is clearer. In Remark 5.6, we show the difference between the two formulations using two examples from mechanics.

In this paper, we extend both formulations to differential geometry and mechanics and present complete methods to prove theorems according to the formulations. Formulation F2 in the differential polynomial case is almost a repetition of Formulation F2 in elementary geometry. However, the extension of Formulation F1 to differential geometry and mechanics is not straightforward.

In elementary geometry, the translation of geometry statements to their algebraic form is relatively easy. But in differential geometry, it is not obvious how to translate a statement such as "The tangent lines of a curve pass a fixed point" to algebraic form. We will see that the key problem here is how to eliminate existential quantifiers. In this paper, we use a method of eliminating existential quantifiers in [8] to develop a translation language for differential geometry.

Theoretically, the methods of theorem proving mentioned above can deal with any geometry statements of equation type involving differentiation. But our experiments are mainly in the space curve theory and plane mechanics. We develop a prover for space curve theory which takes advantage of many special properties of the space curves to enhance efficiency. About 100 non-trivial theorems in space curve theory have been proved by our prover [1, 2]. In mechanics, we have also proved several theorems using our methods [3]. In particular, we use our mechanical method to give a study of the complete logical relationship between Kepler's laws and Newton's gravitational laws.

We assume the reader is familiar with Ritt–Wu's zero decomposition theorem for d-pols a detailed description of which can be found in the first paper of this series [4].

There are other methods to prove theorems mechanically in differential geometry. The elimination theory of Seidenberg [9] (also see [6] for its implementation and applications) is more general than our approach F2 or Algorithm 2.5. But it can not be used to discover necessary nondegenerate conditions as our approach F1 or Algorithm 2.9 does. For example, we can decide whether (1.2) is true using Seidenberg's method. But the problem here is that (1.2) is not true although Example 1.1 is true and our algorithm need to pick up main components carefully (see Example 2.6 and 2.10). So comparing to Seidenberg's general method, our method is a more specialized but different one for geometry theorem proving. [7] uses a quite different approach: in their approach general true means that the conclusion is true on components with maximal dimension. In our point of view, this approach is not appropriate for geometry theorem proving, because there are examples whose main components do not have maximal dimension, e.g. in Example 2.6, $PD(ASC_5)$ is the components with maximal dimension 2 (remember $x_1' = 0$) while $PD(ASC_1)$ with dimension 1 should be the main components (Also see Example 5.3).

The paper is organized as follows. In section 2, we define the two formulations and present methods of mechanical theorem proving for these formulations. In section 3, a language for differential geometry is presented. In section 4, we describe a prover for space curve. Several examples are also given. In section 5, we deal with the Newton-Kepler problems.

2. Methods of Mechanical Theorem Proving

Our methods address a class of geometry statements which can be represented by d-pol equations. Precisely, we have

Definition 2.1. A formula like

$$\forall x_1, ..., \forall x_n[(h_1 = 0 \wedge \cdots \wedge h_r = 0 \wedge d_1 \neq 0 \wedge \cdots \wedge d_t \neq 0) \Rightarrow C = 0]$$

is called a *statement* of equation type (or simply, a statement), where the h, the d, and C are d-pols in $K\{X\}$. Thus a statement of equation type can be represented by a triple $S = (HS, DS, C)$, where $HS = \{h_1, ..., h_r\}$, $DS = \{d_1, ..., d_t\}$.

Before giving methods for statements of equation type, let us note that some other formulas can be reduced to statements of equation type, and hence within the reach of our methods.

Definition 2.2. A *formula with the same quantifier* is a formula like $Qx_1, ..., Qx_n(\phi)$ where Q is $\forall$ or $\exists$; ϕ is a quantifier free formula formed from d-pol equations by Boolean logic operations (such as $\neg$, $\vee$, and $\wedge$); and $x_1, ..., x_n$ are the variables occurring in the d-pols in ϕ.

It is easy to show that a formula with the same quantifier can be reduced to statements of equation type hence can be proved by our methods.

2.1. A Method for Formulation F2

For Formulation F2, we have

Definition 2.3. A statement of equation type $S = (HS, DS, C)$ ($HS = \{h_1, ..., h_r\}$ and $DS = \{d_1, ..., d_t\}$ are in $K\{X\}$) is said to be true in an extension field E of K, if

$$\forall x \in E^n[(h_1 = 0 \wedge \cdots \wedge h_r = 0 \wedge d_1 \neq 0 \wedge \cdots \wedge d_t \neq 0) \Rightarrow C = 0].$$

S is called *universally true* if it is true in any extension of K.

Theorem 2.4. A statement (HS, DS, C) is universally true iff the statement is true in a differential closed extension (see [4]) Ω of K.

Proof. Use the same notations as Definition 2.3. Only the if part needs proof. The statement is true in Ω means

$$\forall x \in \Omega^n[(h_1 = 0 \wedge \cdots \wedge h_r = 0 \wedge d_1 \neq 0 \wedge \cdots \wedge d_t \neq 0) \Rightarrow C = 0]$$

which is equivalent to:

$$\forall x \in \Omega^n \forall z \in \Omega^t[(h_1 = 0 \wedge \cdots \wedge h_r = 0 \wedge z_1 d_1 - 1 = 0 \wedge \cdots \wedge z_t d_t - 1 = 0) \Rightarrow C = 0]$$

for some new variables $z_1, ..., z_t$. By lemma I.5.1 (b) (i.e., Lemma 5.1 in part I), some power of C is in the ideal generated by $h_1, ..., h_r, z_1 d_1 - 1, ..., z_t d_t - 1$, which implies the statement is true in any extension field of K. ∎

Algorithm 2.5. Decide whether a statement $S = (HS, DS, C)$ is universally true.

Step 1. By the coarse form of Ritt-Wu's decomposition algorithm (Theorem I.4.4)

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

Step 2. If $s = 0$ or $\text{prem}(C, ASC_i) = 0$, $i = 1, ..., s$, the statement is universally true.

Step 3. Otherwise, by the refined form of Ritt-Wu's decomposition algorithm (Theorem I.4.5)

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{l} \text{E-Zero}(PD(ASC_i')/DS)$$

Step 4. By Theorem 2.4 and Theorem I.5.2, Jthe statement is universally true iff $l = 0$ or $\text{prem}(C, ASC_i') = 0$, $i = 1, ..., l$. ∎

Example 2.6. (Continuation of Example 1.1). Let $HS = \{h_1, h_2, h_3\}$, where the h_i are in Example 1.1. By Ritt-Wu's decomposition algorithm, we have

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

$$\begin{array}{lllll}
ASC_1 = & x_3^2 + x_2^2 - x_1^2, & x_4 - x_3'^2 - x_2'^2, & x_4^3 x_5^2 - (x_2'' x_3' - x_2' x_3'')^2, & J_1 = \{2x_3, 2x_4^3 x_5\} \\
ASC_1 = & x_3^2 + x_2^2 - x_1^2, & x_4 - x_3'^2 - x_2'^2, & x_4^3 x_5^2 - (x_2'' x_3' - x_2' x_3'')^2, & \\
ASC_2 = & x_2', & x_3^2 + x_2^2 - x_1^2, & x_4, & \\
ASC_3 = & x_2 + x_1, & x_3, & x_4, & \\
ASC_4 = & x_2 - x_1, & x_3, & x_4, & \\
ASC_5 = & x_1, & x_3^2 + x_2^2, & x_4. &
\end{array}$$

Using Formulation F2, we must first figure out the non-degenerate conditions. As mentioned in Example 1.1 that (1.2) is not true when $x_1 = 0$, so one might ask if

$$\forall x_1 \cdots \forall x_5[(h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge x_1 \neq 0) \Rightarrow C = 0] \qquad (2.6.1)$$

is universally true. However, (2.6.1) is still not true. By the above decomposition, we have

$$\text{E-Zero}(HS/x_1) = \cup_{1 \leq i \leq 4} \text{E-Zero}(PD(ASC_i)/x_1)$$

Since $\text{prem}(C, ASC_i) \neq 0$ for $i = 2, 3, 4$, (2.6.1) is not universally true. The necessary non-degenerate condition for this problem is $x_4 \neq 0$, i.e., the arc is not constant. By the above decomposition, we have

$$\text{E-Zero}(HS/x_4) = \text{E-Zero}(PD(ASC_1)/x_4)$$

Since prem$(C, ASC_1) = 0$, the geometry statement $(HS, \{x_4\}, C)$, or

$$\forall x[(h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge x_4 \neq 0) \Rightarrow C = 0]$$

has been proved to be universally true. We see that the selection of correct non-degenerate conditions in this example is not straightforward.

2.2. A Method for Formulation F1

For a statement of equation type $S = (HS, DS, C)$, we divide the variables occurring in HS, DS, and C into two groups: $u_1, ..., u_q$ and $y_1, ..., y_p$ in the sense that in this statement the u can generally take any values and the y can be determined as some functions of the u. We call the u and the y *the parameter* and the *dependent variables* of the statement respectively. Applying the refined form of Ritt-Wu's decomposition algorithm[2] Here we actually only need the existence of the decomposition. We use Ritt-Wu's decomposition algorithm only for convenience. to HS and DS under the variable order $u_1 < \cdots < u_q < y_1 < \cdots < y_p$, we have

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{s}\text{E-Zero}(PD(ASC_i^*)/DS) \bigcup \cup_{j=1}^{l}\text{E-Zero}(PD(ASC_j)/DS) \tag{2.7}$$

where the ASC_i^* are all the irreducible weak asc chains with the u as parameters. Let $r = max_{i=1}^{s} ORD(ASC_i^*)$. A component E-Zero$(PD(ASC_i^*))$ is called *a main component* of the statement, if $ORD(ASC_i^*) = r$, i.e., the main components are represented by the weak asc chains which have the u as the parameter set and have the highest order. Other components are called *degenerate components*. The following is a clarification of Wu's notion of a statement to be generally true.

Definition 2.8. For a statement of equation type $S = (HS, DS, C)$, suppose a set of parameters is given. The statement is said to be *generally true* with respect to (ab. wrpt) the parameters, if C vanishes on all the main components of the statement.

It is obvious that if a statement S of equation type is universally true, S is also generally true.

Algorithm 2.9. For a statement $S = (HS, DS, C)$ where $HS = \{h_1, ..., h_r\}$ and $DS = \{d_1, ..., d_t\}$ are in $K\{u, y\}$, decide whether S is generally true wrpt the u.

Step 1. By the coarse form of Ritt-Wu's decomposition algorithm (Theorem I.4.4)

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{s}\text{E-Zero}(PD(ASC_i')/DS) \bigcup \cup_{j=1}^{l}\text{E-Zero}(PD(ASC_j)/DS)$$

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

Step 2. If prem$(C, ASC_i') = 0$ (for $i \leq s$), S is generally true, as each main component (if there is any) of the geometry statement is contained in some E-Zero$(PD(ASC_i'))$.

Step 3. Otherwise, by the refined form of Ritt-Wu's decomposition algorithm (Theorem I.4.5)

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{t}\text{E-Zero}(PD(ASC_i^*)/DS) \bigcup \cup_{j=1}^{v}\text{E-Zero}(PD(ASC_j)/DS)$$

where the ASC_i^* are all the irreducible weak asc chains with the u as parameters.

Step 4. Let $r = max_{i=1}^{t} ORD(ASC_i^*)$ and MS be the set of asc chains ASC_i^* which satisfy $ORD(ASC_i^*) = r$.

Step 5. By Theorem I.5.1, the statement is generally true wrpt the u iff MS is empty or $\forall ASC \in MS, prem(C, ASC) = 0$. ∎

---

[2] *

Remark For the decomposition in steps 1 and 3, we don't have to compute the weak asc chains ASC_j which contain at least one d-pol in the u only. In the decomposition algorithms, 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. If we use this trick, the decomposition becomes much faster than the complete decomposition.

Example 2.10. (Continuation of Example 1.1). We can take x_1 and x_2 as parameters and ask whether (1.2) or the statement $(HS, \emptyset, C)$ is generally true wrpt x_1 and x_2. By Example 2.6, E-Zero($PD(ASC_1)$) is the only main component, because other ASC_i $(i = 2, ..., 5)$ contain d-pols in the parameters x_1 and x_2 alone. Since prem$(C, ASC_1) = 0$, (1.2) is proved to be generally true wrpt the parameters x_1 and x_2. We can also find the non-degenerate conditions make the statement universally true. Note that x_4 is in ASC_i for $i = 2, ..., 5$ and does not vanish on E-Zero($PD(ASC_1)$), then (1.2) is universally true under an extra condition $x_4 \neq 0$.

Remark We can see that Algorithm 2.5 and 2.9 are complete only for differential closed extension of K. A statement is true in the usual case of real differential geometry means the statement is true in the field of real analytical functions. So the methods can only confirm theorems in real differential geometry. Almost all the theorems we encountered in real differential geometry are universally true and hence within the reach of our methods.

3. A Basic Translation Language

3.1. A Technique to Eliminate Existential Quantifiers

A geometry statement in differential geometry often involves existential quantifiers. For example, the sentence "a vector function $(x(t), y(t), z(t))$ is perpendicular to a fixed line" can be represented as:

$$\forall x \forall y \forall z \exists a \exists b \exists c (ax + by + cz = 0 \wedge a' = 0 \wedge b' = 0 \wedge c' = 0 \wedge (a \neq 0 \vee b \neq 0 \vee c \neq 0)) \tag{3.1.1}$$

(3.1.1) cannot be transformed to statements of equation type. Hence if a geometry statement contains such kind of sentences, generally, we cannot use the algorithms presented in section 2 to prove it. A solution to this kind of problems is given below. We first define a function LD (linear dependence) as follows.

$$LD(y_1, ..., y_r) = \begin{vmatrix} y_1 & y_2 & \cdots & y_r \\ y_{1,1} & y_{2,1} & \cdots & y_{r,1} \\ y_{1,r-1} & y_{2,r-1} & \cdots & y_{r,r-1} \end{vmatrix}.$$

Lemma 3.1. (p.34 [8]) Let E be an extension field of K, then $\tau_1, ..., \tau_n$ in E satisfy $a_1\tau_1 + ... + a_n\tau_n = 0$ for constants $a_1, \cdots, a_n$, not all zero, if and only if $LD(\tau_1, ..., \tau_n) = 0$.

Corollary 3.2. Let E be an extension field of K, then $\tau_1, ..., \tau_n$ in E satisfy $a_1\tau_1 + ... + a_n\tau_n = a_0$ for constants $a_1, \cdots, a_n$, not all zero, if and only if $LD(1, \tau_1, ..., \tau_n) = 0$.

Proof. Note that $a_1\tau_1 + ... + a_n\tau_n = a_0$ for constants $a_0, ..., a_n$ iff $a_1\tau_1' + ... + a_n\tau_n' = 0$, which is equivalent to $LD(\tau_1', ..., \tau_n') = LD(1, \tau_1, ..., \tau_n) = 0$. ▮

By Lemma 3.1, (3.1.1) can be reduced to $LD(x, y, z) = 0$.

3.2. The Basic Predicates

For vectors v_1, v_2, and v_3, let $(v_1\ v_2)$ stand for the inner product of v_1 and v_2. $(v_1\ v_2\ v_3)$ is defined to be $(v_1\ v_2 \times v_3)$.

Definition 3.3. 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_i, the x_i, the y_i, and the z_i are indeterminates. We define the following predicates.

S1. (v-norm v_1 p) means the square of the norm of v_1 is p. Its algebraic equation is
$z_1^2 + y_1^2 + x_1^2 - p = 0$.

S2. (cons-len v_1) means v_1 has constant length. Its algebraic equation is
$z_1 z_1' + y_1 y_1' + x_1 x_1' = 0$.

S3. (v-para v_1 v_2) means v_1 is parallel to v_2. Its algebraic equation is $v_1 \times v_2 = 0$ or
$y_1 z_2 - z_1 y_2 = 0 \wedge x_1 z_2 - z_1 x_2 = 0 \wedge x_1 y_2 - y_1 x_2 = 0$.

S4. (cons-dir $v1$) means v_1 has a fixed direction. Its algebraic equation is $v_1 \times v_1' = 0$ or
$y_1 z_1' - y_1' z_1 = 0 \wedge x_1 z_1' - x_1' z_1 = 0 \wedge x_1 y_1' - x_1' y_1 = 0$.

S5. (v-perp v_1 v_2) means v_1 is perpendicular to v_2. Its algebraic equation is $(v_1\ v_2) = 0$ or
$x_1 x_2 + y_1 y_2 + z_1 z_2 = 0$.

S6. (perp-fix-line v_1) or (para-fix-plane v_1) means that v_1 is perpendicular to a fixed line. Its algebraic equation is $LD(x_1, y_1, z_1) = 0$ or
$(x_1 y_1' - x_1' y_1) z_1'' + (-x_1 y_1'' + x_1'' y_1) z_1' + (x_1' y_1'' - x_1'' y_1') = 0$.

S7. (co2-linear n v_1 v_2) means that v_2 is on the line passing through v_1 and parallel to n. Its algebraic equation is $n \times (v_2 - v_1) = 0$ or
$(y_2 - y_1) n_3 + (-z_2 + z_1) n_2 = 0$
$(x_2 - x_1) n_3 + (-z_2 + z_1) n_1 = 0$
$(x_2 - x_1) n_2 + (-y_2 + y_1) n_1 = 0$

S8. (fix-co2-linear n v_1) means that the lines passing through v_1 and parallel to n pass through a fixed point. Its algebraic equation is
$(\mathrm{LD}\ n_1\ \ n_2\ \ n_1 y_1 - n_2 x_1) = 0$
$(\mathrm{LD}\ n_1\ \ n_3\ \ n_1 z_1 - n_3 x_1) = 0$
$(\mathrm{LD}\ n_2\ \ n_3\ \ n_2 z_1 - n_2 y_1) = 0$

S9. (co3-linear v_1 v_2 v_3) means that v_1, v_2, and v_3 are on the same line. Its algebraic equation is $(v_2 - v_1) \times (v_3 - v_1) = 0$ or
$(y_2 - y_1) z_3 + (-z_2 + z_1) y_3 + y_1 z_2 - z_1 y_2 = 0 \wedge$
$(x_2 - x_1) z_3 + (-z_2 + z_1) x_3 + x_1 z_2 - z_1 x_2 = 0 \wedge$
$(x_2 - x_1) y_3 + (-y_2 + y_1) x_3 + x_1 y_2 - y_1 x_2 = 0$.

S10. (fix-co3-linear v_1 v_2) means that the lines passing through v_1 and v_2 pass through a fixed point. Its algebraic equation is (fix-co2-linear $v_2 - v_1$ v_1) or
$(\mathrm{LD}\ (y_2 - y_1)\ \ (-z_2 + z_1)\ \ (y_1 z_2 - z_1 y_2)) = 0 \wedge$
$(\mathrm{LD}\ (x_2 - x_1)\ \ (-z_2 + z_1)\ \ (x_1 z_2 - z_1 x_2)) = 0 \wedge$
$(\mathrm{LD}\ (x_2 - x_1)\ \ (-y_2 + y_1)\ \ (x_1 y_2 - y_1 x_2)) = 0$.

S11. (co2-plane n v_1 v_2) means that v_2 is on the plane passing through v_1 and with n as its normal vector. Its algebraic equation is $(n\ v_2 - v_1) = 0$ or
$(z_2 - z_1) n_3 + (y_2 - y_1) n_2 + (x_2 - x_1) n_1 = 0$.

S12. (fix-co2-plane n v_1) means that the planes passing through v_1 and with n as their normal vectors pass through a fixed point. Its algebraic equation is

$$(\text{LD } n_1\ n_2\ n_3\ n_1x_1+n_2y_1+n_3z_1)=0 \wedge (\text{perp-fix-line } n)\neq 0.$$

S13. (co3-plane v_1 v_2 v_3) means that v_1, v_2, and v_3 are parallel to a plane. Its algebraic equation is $(v_1\ v_2\ v_3)=0$ or

$$(x_1y_2-y_1x_2)z_3+(-x_1z_2+z_1x_2)y_3+(y_1z_2-z_1y_2)x_3=0.$$

S14. (fix-co3-plane v_1 v_2) means that the planes containing v_1, v_2, and the origin point pass through a fixed point. Its algebraic equation is

$$(\text{LD } \ (y_1z_2-z_1y_2)\ \ (-x_1z_2+z_1x_2)\ \ (x_1y_2-y_1x_2))=0.$$

S15. (co4-plane v_1 v_2 v_3 v_4) means that v_1, v_2, v_3, and v_4 are on the same plane. Its algebraic equation is (co3-plane v_2-v_1 v_3-v_1 v_4-v_1) $=0$ or

$$\begin{aligned}&((x_2-x_1)y_3+(-y_2+y_1)x_3+x_1y_2-y_1x_2)z_4\\&\quad+((-x_2+x_1)z_3+(z_2-z_1)x_3-x_1z_2+z_1x_2)y_4\\&\quad+((y_2-y_1)z_3+(-z_2+z_1)y_3+y_1z_2-z_1y_2)x_4\\&\quad+(-x_1y_2+y_1x_2)z_3+(x_1z_2-z_1x_2)y_3+(-y_1z_2+z_1y_2)x_3=0.\end{aligned}$$

S16. (fix-co4-plane v_1 v_2 v_3) means that the planes determined by v_1, v_2, and v_3 pass through a fixed point. Its algebraic equation is

$$(\text{fix-co2-plane } v_1\times v_2\ \ v_3)=0 \wedge (\text{perp-fix-line } v_1\times v_2)\neq 0.$$

S17. (angle v_1 v_2 p) means that the inner product of v_1 and v_2 is p. Its algebraic equation is

$$x_1x_2+y_1y_2+z_1z_2=p.$$

S18. (fix-angle v_1) means that v_1 forms a constant angle with a constant direction. Its algebraic equation is

$$\begin{aligned}&(\text{LD } (y_1^2+z_1^2)x_1'-x_1(y_1y_1'+z_1z_1'),\\&\quad(x_1^2+z_1^2)y_1'-y_1(x_1x_1'+z_1z_1'),(x_1^2+y_1^2)z_1'-z_1(x_1x_1'+y_1y_1'))=0.\end{aligned}$$

S19. (cons-v v_1) means that v_1 is a constant vector. Its algebraic equation is

$$x_1'=0\wedge y_1'=0\wedge z_1'=0.$$

The above predicates are not independent. We introduce them for convenience. Some of the descriptions are obviously true, e.g. S1, S2, S3 etc. Some are known results, e.g. S4. Some of them, e.g. S6, S8, S10, S12, S14, S16, and S18 seem to be formulated at the present form for the first time. We give the correctness proofs for them in the appendix of [1].

3.3. A Basic Language

Definition 3.4. A *geometry formula of equation type* is a formula like

$$\forall x_1,...,\forall x_n(\Phi) \qquad (3.4.1)$$

where Φ is a quantifier free formula formed from the geometry predicates defined in section 3.2 and $x_1,...,x_n$ are the variables occurring in Φ.

Theorem 3.5. We can decide in a finite number of steps whether a geometry formula of equation type is universally or generally true.

Proof. By the definition of the predicates, (3.4.1) can be translated to statements of equation type. Thus, we can decide whether (3.4.1) is universally or generally true by Algorithm 2.5 or Algorithm 2.9. ∎

As an example, let us show how to prove the correctness of S4 which can be reduced to the following example.

Example 3.6. (a) If v_1 is parallel to a nonzero constant vector n then (cons-dir v_1) is true. (b) If v_1 is a unit vector satisfying (cons-dir v_1), then v_1 is a constant vector, hence v_1 has a constant direction.

Note (a) and (b) can be reduced to

$$\forall v_1, n[(\text{v-para } v_1\ n) \wedge (\text{cons-v } n) \wedge n \neq 0) \Rightarrow (\text{cons-dir } v_1)]$$
$$\forall v_1[(\text{cons-dir } v_1) \wedge (\text{v-norm } v_1\ 1)) \Rightarrow (\text{cons-v } v_1)]$$

respectively, which have been proved to be universally true by a program based on Algorithm 2.5.

4. Proving Theorems in the Space Curve Theory

We use the above general methods to mechanical theorem proving in the space curve theory. A space curve can be expressed as $C(t) = (x(t), y(t), z(t))$ where x, y, and z are functions of the parameter t. In this paper, we treat x, y, and z as indeterminates. The differential operation is d/dt. At first, we introduce some new predicates for space curves.

Definition 4.1. Let $C(t) = (x(t), y(t), z(t))$ be a space curve with parameter t. We define the following predicates:

S20. (curve C κ_0 κ τ) means that κ_0, κ, τ are the square of arc length, the curvature and torsion of C respectively. Its algebraic equations are

$\kappa_0 - (C'\ C') = 0,$

$\kappa_0^3\kappa^2 - ((C' \times C'')\ (C' \times C'')) = 0,$

$\kappa_0^3\kappa^2\tau - (C'\ C''\ C''') = 0.$

S21. (curve-norm C v_1) means that v_1 is the principal normal vector of C. Its algebraic equation is

$v_1 = (C'\ C')C'' - (C'\ C'')C'.$

S22. (curve-binorm C v_1) means that v_1 is the binormal vector of curve C. Its algebraic equation is

$v_1 = C' \times (\text{curve-norm } C).$

S23. (frenet C κ τ N B) means that C has its length of arc as parameter and κ, τ, N, and B are the curvature, the torsion, the principal normal vector, and the binormal vector of C respectively. Its algebraic equations are

$(C'\ C') - 1 = 0,$

$\kappa^2 - (C''\ C'') = 0,$

$\kappa N - C'' = 0,$

$\kappa B - C' \times C'' = 0,$

$\tau + (N\ B') = 0.$

The above predicates are just definitions. The predicate (frenet C κ τ N B) is often used in the following examples, so we give its d-pol equations here. Let $C = (x, y, z)$, $N = (n_1, n_2, n_3)$, and $B = (b_1, b_2, b_3)$. Then we have

$$
\begin{aligned}
&h_1 = z'^2 + y'^2 + x'^2 - 1 = 0 && C \text{ with its arc as parameter}\\
&h_2 = \kappa^2 - z''^2 - y''^2 - x''^2 = 0 && \kappa = |C''|\\
&h_3 = \kappa n_1 - x'' = 0 && \\
&h_4 = \kappa n_2 - y'' = 0 && N = C''/\kappa\\
&h_5 = \kappa n_3 - z'' = 0 && \\
&h_6 = \kappa b_1 - y'z'' + y''z' = 0 && \\
&h_7 = \kappa b_2 + x'z'' - x''z' = 0 && B = C' \times N\\
&h_8 = \kappa b_3 - x'y'' + x''y' = 0 && \\
&h_9 = \tau + n_3 b_3' + n_2 b_2' + n_1 b_1' = 0 && \tau = -(N\ B')
\end{aligned}
$$

Example 4.2. 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 forms a constant angle with a fixed line, i.e., (fix-angle C).

(c) The principal normals are parallel to a fixed plane, i.e., (para-fix-plane N).

(d) The binormals form a constant angle with a fixed line, i.e., (fix-angle B).

A curve satisfying these conditions is called a helix. By Definition 3.3 and Definition 4.1, (a), (b), (c), and (d) are equivalent to

$$h_{31} = LD(\kappa, \tau) = \kappa' \tau - \tau' \kappa = 0$$

$$h_{32} = D(1, x', y', z') = 0$$

$$h_{33} = LD(x'', y'', z'') = 0$$

$$h_{34} = LD(1, b_1, b_2, b_3) = 0$$

respectively. The non-degenerate condition is $\kappa \neq 0$. Thus (a) $\Rightarrow$ (b), (b) $\Rightarrow$ (c), (c) $\Rightarrow$ (d), and (d) $\Rightarrow$ (a) are equivalent to

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{31} = 0 \wedge \kappa \neq 0) \Rightarrow h_{32} = 0]$$

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{32} = 0 \wedge \kappa \neq 0) \Rightarrow h_{33} = 0]$$

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{33} = 0 \wedge \kappa \neq 0) \Rightarrow h_{34} = 0]$$

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{34} = 0 \wedge \kappa \neq 0) \Rightarrow h_{31} = 0$$

respectively. We have proved these statements to be universally true using a program based on Algorithm 2.5. All the statements with $\kappa \neq 0$ dropped have been proved to be generally true wrpt the parameter x.

Example 4.3. For a curve C, not a plane curve, the following statements are equivalent:

(a) C is a spherical curve.

(b) $r\tau + (r'p)' = 0$, where $r = 1/\kappa$, $p = 1/\tau$.

(c) The normal planes pass through a fixed point, i.e., (fix-co2-plane C', C).
Bye Definition 3.3, (a), (b), and (c) are equivalent to

$$h_{41} = LD(1, x, y, z, x^2 + y^2 + z^2) = 0$$

$$h_{42} = r\tau + (r'p)' = 0$$

$$h_{43} = LD(x', y', z', xx' + yy' + zz') = 0$$

respectively, where r and p satisfying $h_{44} = r\kappa - 1 = 0, h_{45} = p\tau - 1 = 0$. The non-degenerate condition is $\tau \neq 0$. Thus (a) $\Rightarrow$ (b), (b) $\Rightarrow$ (c), and (c) $\Rightarrow$ (d) are equivalent to

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{41} = 0 \wedge h_{44} = 0 \wedge h_{45} = 0 \wedge \tau \neq 0) \Rightarrow h_{42} = 0]$$

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{42} = 0 \wedge h_{44} = 0 \wedge h_{45} = 0 \wedge \tau \neq 0) \Rightarrow h_{43} = 0]$$

$$\forall C, N, B, \kappa, \tau[(h_1 = 0 \wedge ... \wedge h_9 = 0 \wedge h_{43} = 0 \wedge h_{44} = 0 \wedge h_{45} = 0 \wedge \tau \neq 0) \Rightarrow h_{41} = 0]$$

respectively. We have proved these statements to be universally true using a program based on Algorithm 2.5. All the statements with $\tau \neq 0$ dropped have been proved to be generally true wrpt the parameter x.

It took less than 5 minutes to complete the proof for each of the above examples on a Symbolics 3600. The description of our prover (input, etc) and more examples can be found in [1] and [2].

5. Proving Theorems in Plane Mechanics

Our experiment on the computer shows that quite a few theorems in elementary mechanics can be proved mechanically by our algorithms [3]. In the following, We extend Wu's work on the Kepler-Newton problem [11], to give a complete, mechanical solution of the logical relationship between these laws. The results on the computer show that

(1) **K1** and **K2** imply **N1** and **N2**

(2) **K2** is equivalent to **N2**.

(3) **N1** and **N2** imply **K1**.

(4) **K1** and **N1** do not imply **K2**.

The mechanical proof of (1) was first given by Wu [11]. Our proof here is based on our two formulations. We first state Kepler's first and second law and Newton's gravitational laws as follows.

K1. Each planet describes an ellipse with the sun in one focus.

K2. The radius vector drawn from the sun to a planet sweeps out equal areas in equal times.

N1. The acceleration of a planet is inversely proportional to the square of the distance from the sun to the planet.

N2. The acceleration vectors of planets are directed towards the sun.

Let the coordinates of the planet be $(x(t), y(t))$ where t is the time. We assume the sun is at the origin $(0, 0)$. The d-pol equations for **K1**, **K2**, **N1**, and **N2** are

$$K_1 = r - p - ex - fy = 0 \wedge p' = 0 \wedge e' = 0 \wedge f' = 0 \tag{5.1}$$

$$y'x - yx' - h = 0 \wedge h' = 0 \tag{5.2}$$

$$n_1 = LD(1, ar^2) = (ar^2)' = 0$$

$$n_2 = x''y - y''x = 0$$

respectively, where a is the magnitude of the acceleration of the planet; r is the length of the radius vector drawn from the sun to the planet. Thus we have

$$h_1 = r^2 - x^2 - y^2 = 0$$

$$h_2 = a^2 - x''^2 - y''^2 = 0$$

As a simple application of lemma 3.2, we show that **K2** and **N2** are equivalent: by Lemma 3.2, (5.2) is equivalent to $LD(1, (x'y - y'x)) = x''y - y''x$, which is exactly the d-pol representing **N2**.

Example 5.3. Show that **K1** and **K2** imply **N1**.

Here we shall adopt a simplification: considering a special coordinate system such that the center of the ellipse is on the x-axis. In this coordinate system, K_1 becomes $K_{11} = r - p - ex$. Now (**K1** $\wedge$ **K2** $\Rightarrow$ **N1**) becomes

$$\forall x, y, p, e, a, r[(K_{11} = 0 \wedge p' = 0 \wedge e' = 0 \wedge n_2 = 0 \wedge h_1 = 0 \wedge h_2 = 0) \Rightarrow n_1 = 0]. \qquad (5.3.1)$$

There are no parameters in this problem. For convenience, we assume $a \neq 0$, in which case the conclusion is obviously true. Using our program based on Ritt-Wu's decomposition algorithm under the variable order: $p < e < f < x < y < r < a$, we have

$$\text{E-Zero}(\{K_{11}, p', e', h_1, h_2, n_2\}/a) = \text{E-Zero}(PD(ASC_1)/a) \cup \text{E-Zero}(PD(ASC_2)/a)$$

where

$ASC_1 =$	$ASC_2 =$
p'	p
e'	e'
$((e^3-1)x^3 + (3e^2-1)px^2 + 3epx + p^3)x'' + pxx'$	$y^2 + (-e^2+1)x^2$
$y^2 - (e^2-1)x^2 - 2pex - p^2$	$r - ex$
$r - p - ex$	$a^2 - y''^2 - x''^2$
$a^2 - y''^2 - x''^2$	

According to section 2.2, ASC_1 representing the main component, and ASC_2 is a degenerate component. The fact $prem(n_1, ASC_1) = 0$ implies (5.3.1) is generally true. But (5.3.1) is not universally true, because prem$(n_1, ASC_2) \neq 0$. By adding $p \neq 0$ (i.e., the ellipse does not degenerate to two lines) to (5.3.1), we obtain a statement

$$\forall x, y, p, e, a, r(K_{11} = 0 \wedge p' = 0 \wedge e' = 0 \wedge n_2 = 0 \wedge h_1 = 0 \wedge h_2 = 0 \wedge ap \neq 0) \Rightarrow n_1 = 0]$$

which is universally true. This has also been proved directly by Algorithm 2.5.

Example 5.4. Show that **N1** and **N2** imply **K1**. By Lemma 3.2, (5.1), i.e., **K1** is equivalent to

$$k_1 = LD(1, x, y, r) = r'''(y''x' - y'x'') + r''(-y'''x' + y'x''') + r'(y'''x'' - y''x''') = 0$$

Now (**N1** $\wedge$ **N2** $\Rightarrow$ **K1**) becomes

$$\forall x, y, a, r[(n_1 = 0 \wedge n_2 = 0 \wedge h_1 = 0 \wedge h_2 = 0) \Rightarrow k_1 = 0]. \qquad (5.4.1)$$

There are no parameters in this problem. Using a program based on Ritt-Wu's decomposition algorithm under the variable order $x < y < r < a$, we have

$$\text{E-Zero}(\{h_1, h_2, n_1, n_2\}/a) = \cup_{i=1}^{3}\text{E-Zero}(PD(ASC_i)/a)$$

where

$$ASC_1 = 9x'''''x''^2x^3 + x''''(-45x'''x''x^3 + 18x''^2x'x^2) + 40x'''^3x^3$$
$$-30x'''^2x''x'x^2 - 6x'''x''^2x'^2x + 18x''^4x'x18 - 4x''^3x'^3,$$
$$y^2(3x''''x''x^2 - 4x'''^2x^2 + 2x'''x''x'x + 6x''^3x + 2x''^2x'^2)$$
$$+x'''^2x^4 + 4x'''x''x'x^3 + 4x''^2x'^2x^2,$$
$$r^2 - x^2 - y^2,$$
$$a^2 - x''^2 - y''^2;$$
$$ASC_2 = \quad xx''' + 2x'x'', xy' - x'y, r^2 - x^2 - y^2, a^2 - x''^2 - y''^2;$$
$$ASC_3 = \quad x, yy''' + 2y'y'', r^2 - x^2 - y^2, a^2 - x''^2 - y''^2.$$

In this problem, ASC_1 represents the main component with order five. The fact $prem(k_1, ASC_1) = 0$ means that (5.4.1) is generally true. Actually (5.4.1) is universally true since $prem(k_1, ASC_2) =$

$prem(k_1, ASC_2) = 0$. The largest d-pol occurring in the computing of prem(k_1, ASC_1) is 5,358 terms.

Example 5.5. Show that **N1** and **K1** do not imply **K2**. Naturally we may ask whether **N2** can be deduced from **N1** and **K1**, i.e., whether

$$\forall x, y, p, e, r, a, [(n_1 = 0 \wedge K_{11} = 0 \wedge p' = 0 \wedge e' = 0) \Rightarrow n_2 = 0)] \quad (5.5.1)$$

is generally true. The answer is negative. To show this, using Algorithm 2.9, we get the following irreducible ascending chain which represents the main component

$$ASC = c_1x''^2 + c_2x'' + c_3, y^2 - (e^2 - 1)x^2 - 2pex - p^2,$$

$$r - p - ex, r^2a - h$$

where c_1, c_2, and c_3 are polynomials of p, e, h, x, and x'. The fact $prem(n_2, ASC) \neq 0$ implies (5.5.1) is generally false.

Remark 5.6. Here we see the obvious distinctions between the two formulations. According to Formulation F2, both (5.3.1) and (5.5.1) are false. But according to Formulations F1, (5.3.1) is generally true and (5.5.1) is generally false. The result we obtained about (5.5.1) according to Formulation F1 is much stronger that the result we obtained by Formulation F2. The general falsity of (5.5.1) means that (5.5.1) can not be true whatever suitable non-degenerate conditions are added.

More examples from kinematics and dynamics can be found in [3].

References

[1] S.C. Chou and X.S. Gao, Mechanical Theorem Proving in Differential Geometry, I. Space Curves, TR-89-08, Computer Sciences Department, The University of Texas at Austin, March 1989.

[2] S.C. Chou and X.S. Gao, Mechanical Theorem Proving in Differential Geometry II. Bertrand Curves, TR-90-09, Computer Sciences Department, The University of Texas at Austin, April, 1990.

[3] S.C. Chou and X.S. Gao, Automated Reasoning In Mechanics Using Ritt-Wu's Method, TR-89-11, Computer Science Department, The Univ. of Texas at Austin, April, 1989.

[4] S.C. Chou and X.S. Gao, Automated Reasoning in Differential Geometry and Mechanics Using Characteristic Method, I. An improved Version of Ritt-Wu's Decomposition Algorithm, *This volume.*

[5] S.C. Chou and Yang Jingen, On the Algebraic Formulation of Certain Geometry Statements and Mechanical Geometry Theorem Proving, *Algorithmica*, Vol. 4, 1989, 237-262.

[6] S. Diop, Elimination in Control Theory, *Math. Control Signals Systems*, 4(1991), 17-32.

[7] G.C. Ferro and G. Gallo, A Procedure to Prove Statements in Differential Geometries, J. Automated Reasoning, pp. 203–209, 1990.

[8] Ritt, J.F., *Differential algebra*, Amer. Math. Sco. Colloquium, (1950).

[9] A. Seidenberg, An Elimination Theory for Differential Algebra, *Univ. California Publication in Math.*, 3 (1956), 31-65.

[10] Wu Wen-tsün, A Constructive Theory of Differential Algebraic Geometry, Lect. Notes in Math., No. 1255, pp 173–189, Springer-verlag, 1987.

[11] Wu Wen-tsün, Mechanical Derivation of Newton's Gravitational Laws from Kepler's Laws, MM Research Preprints, No1, 1987, Ins. of Systems Science.