Journal of Universal Computer Science, vol. 1, no. 9 (1995), 658-673
submitted: 10/4/95, accepted: 18/8/95, appeared: 28/9/95,

A Method for Proving Theorems in Differential Geometry and Mechanics

Dongming Wang
(Institut National Polytechnique de Grenoble, France
wang@lifia.imag.fr)

Abstract: A zero decomposition algorithm is presented and used to devise a method for proving theorems automatically in differential geometry and mechanics. The method has been implemented and its practical efficiency is demonstrated by several non-trivial examples including Bertrand's theorem, Schell's theorem and Kepler-Newton's laws.

Key Words: Differential geometry, mechanics, polynomial elimination, theorem proving, triangular system, zero decomposition
Category: I.1.2, I.2.3

1 Introduction

We consider theorems in elementary differential geometry and plane mechanics which can be expressed algebraically in the form

$$(\forall x_1 \cdots \forall x_n)\,[H_1 = 0 \wedge \cdots \wedge H_h = 0 \wedge D_1 \neq 0 \wedge \cdots \wedge D_d \neq 0 \Longrightarrow C = 0], \quad (1)$$

where H_i, D_j and C are differential polynomials in the variables $x_1, \ldots, x_n$ and any number of their derivatives with respect to (abbr. wrt) a variable t with coefficients in $\boldsymbol{K}$, an ordinary differential field of characteristic 0 consisting of functions of t. That the curvature of a circle is constant and that the orbit described by a particle under a central attractive force is an ellipse if the force varies directly as the distance are examples of such theorems. This paper presents a method that decides the validity of any theorem of this type. The decision problem is solved as determining whether the formula (1) is valid, and if not, finding certain subsidiary (non-degeneracy) condition under which it becomes valid.

Proving theorems in differential geometry and mechanics mechanically was initiated in [Wu 79, Wu 82, Wu 87a], followed up in [Carrà Ferro and Gallo 90, Chou and Gao 93a, Li 91]. In particular, several remarkable theorems have been proved or even "discovered" automatically in [Wu 87b, Wu 87c, Wu 91], and many more later in [Chou and Gao 91, Chou and Gao 92, Chou and Gao 93b], using Wu's method with improvements. An approach based on the evaluation of differential dimension (polynomials) has been proposed in [Carrà Ferro 94, Carrà Ferro and Gallo 90]. The method presented in this paper follows similar algebraic approaches of Wu and others, but employs a different algorithm for the involved zero decomposition. This new decomposition algorithm is developed by the author using ideas from Seidenberg's elimination theory [Seidenberg 56]. The method has been implemented in the Maple system and its practical efficiency is demonstrated by several notable examples including theorems named after Bertrand, Mannheim and Schell, and Kepler-Newton's laws. Experiments with these and other theorems indicate that our method is likely to have better performance [see Remark 4]. Yet complexity analysis and more comparisons between this and other relevant methods remain to be carried.

2 Notations

Write the prefix *d-* for the modifier *differential*, *pol* for *polynomial* and *tri* for *triangular*. A *d-pol* is a pol in $x_1, \ldots, x_n$ and any number of their derivatives wrt t with coefficients in $\boldsymbol{K}$. The set of all such d-pols is denoted by $\boldsymbol{K}\{x_1, \ldots, x_n\}$ or $\boldsymbol{K}\{x\}$ for short. Differentiation of functions x_i will be indicated by means of a second subscript as

$$x_{ij} = \frac{d^j x_i}{dt^j},$$

with $x_{i0} = x_i$. Let $P \in \boldsymbol{K}\{x\}$ be a d-pol. The *jth derivative* of P is obtained by differentiating P j times wrt t, regarding $x_1, \ldots, x_n$ as functions of t. For any x_{ij}, denote the degree of P in x_{ij} by $\deg(P, x_{ij})$. The greatest j, if exists, such that $\deg(P, x_{ij}) > 0$ is called the *order* of P wrt x_i, denoted by $\mathrm{ord}(P, x_i)$. If $\deg(P, x_{ij}) = 0$ for any $j \geq 0$, then define $\mathrm{ord}(P, x_i) = -1$. Let

$$q = \mathrm{ord}(P, x_i), \quad d = \deg(P, x_{iq});$$

the pair $\langle q, d\rangle$ is called the *rank* of P wrt x_i, denoted by $\mathrm{rank}(P, x_i)$. We place $\langle q, d\rangle \prec \langle q', d'\rangle$ if $q < q'$ or $q = q'$, and $d < d'$. Fix the variable ordering as

$$t \prec x_1 \prec \cdots \prec x_n,$$

and order $x_{ij} \prec x_{ik}$ if $j < k$. The leading variable of P, denoted by $\mathrm{lvar}(P)$, is defined to be x_l with l the biggest index such that $\deg(P, x_{lj}) > 0$ for some j if $P \notin \boldsymbol{K}$, and t otherwise.

Let P be a d-pol with

$$\mathrm{lvar}(P) = x_p \succ t, \quad \mathrm{rank}(P, x_p) = \langle q, d\rangle,$$

written as

$$P = P_0 x_{pq}^d + P_1 x_{pq}^{d-1} + \cdots + P_d, \quad P_0 \neq 0,$$

where $\mathrm{ord}(P_i, x_p) < q$ for each i. We call x_{pq} the *lead* of P, denoted by $\mathrm{lead}(P)$, P_0 the *initial* of P, denoted by $\mathrm{ini}(P)$, and $P_1 x_{pq}^{d-1} + \cdots + P_d$ the *reductum* of P, denoted by $\mathrm{red}(P)$. The d-pol $\partial P/\partial x_{pq}$ is called the *separant* of P, denoted by $\mathrm{sep}(P)$.

Pseudo-dividing a d-pol Q by P and its derivatives in x_p, one can get a remainder formula of the form

$$\mathrm{sep}(P)^\alpha \mathrm{ini}(P)^\beta Q = A_1 \frac{d^{k_1} P}{dt^{k_1}} + \cdots + A_s \frac{d^{k_s} P}{dt^{k_s}} + R, \tag{2}$$

where α, β, k_j are non-negative integers and R is a d-pol with $\mathrm{rank}(R, x_p) \prec \langle q, d\rangle$ (cf. [Ritt (50), Wu 89]). We call R the (*pseudo-*) *remainder* of Q wrt P and denote it by $\mathrm{prem}(Q, P)$ (which is not necessarily unique).

Throughout the paper, $\tilde{\boldsymbol{K}}$ denotes an algebraic d-closure of $\boldsymbol{K}\{x\}$, the elements of an ordered set are enclosed in square brackets, and $|S|$ stands for the number of elements of a set S.

A *d-pol set* is a finite set of non-zero d-pols in $\boldsymbol{K}\{x\}$. Let $\mathbb{P}$ and $\mathbb{Q}$ be two d-pol sets. Denote, by $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$, the set of all common d-zeros (in $\tilde{\boldsymbol{K}}$) of the d-pols in $\mathbb{P}$ which are not d-zero of any d-pol in $\mathbb{Q}$. Namely,

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \{x \in \tilde{\boldsymbol{K}}^n \mid P(x) = 0, Q(x) \neq 0, \forall P \in \mathbb{P}, Q \in \mathbb{Q}\}.$$

We write $\mathrm{Zero}(P/\mathbb{Q})$ for $\mathrm{Zero}(\{P\}/\mathbb{Q})$ and $\mathrm{Zero}(\mathbb{P}/Q)$ for $\mathrm{Zero}(\mathbb{P}/\{Q\})$, and write $\mathrm{Zero}(\mathbb{P})$ for $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ when $\mathbb{Q} = \emptyset$ or $\mathbb{Q} \subset \boldsymbol{K}$, etc.

By a *d-pol system* we mean a pair $[\mathbb{P}, \mathbb{Q}]$ of d-pol sets, with which $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ is of concern. An element of $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$ is also called a d-zero of $[\mathbb{P}, \mathbb{Q}]$, and

$$\mathrm{Zero}([\mathbb{P}, \mathbb{Q}]) = \mathrm{Zero}(\mathbb{P}/\mathbb{Q}).$$

Definition 1. A finite non-empty ordered set

$$\mathbb{T} = [T_1, T_2, \ldots, T_r]$$

of d-pols is called a *d-tri form* (or *d-tri set*) if

$$t \prec \mathrm{lvar}(T_1) \prec \mathrm{lvar}(T_2) \prec \cdots \prec \mathrm{lvar}(T_r).$$

A pair $[\mathbb{T}, \mathbb{U}]$ is called a *d-tri system* if $\mathbb{T}$ is a d-tri form and $\mathbb{U}$ a d-pol set, possibly empty, such that $\mathrm{ini}(T)$ and $\mathrm{sep}(T)$ do not vanish on $\mathrm{Zero}(\mathbb{T}/\mathbb{U})$ for all $T \in \mathbb{T}$.

Let $\mathbb{T}$ be as above and

$$\mathrm{prem}(Q, \mathbb{T}) = \mathrm{prem}(\cdots \mathrm{prem}(Q, T_r), \ldots, T_1),$$

called the (*pseudo-*) *remainder* of Q wrt $\mathbb{T}$. A d-tri system $[\mathbb{T}, \mathbb{U}]$ is said to be *fine* if $\mathrm{prem}(U, \mathbb{T}) \neq 0$ for any $U \in \mathbb{U}$. $\mathbb{T}$ is said to be *fine* if

$$[\mathbb{T}, \{\mathrm{ini}(T_i), \mathrm{sep}(T_i) \mid 1 \leq i \leq r\}]$$

is fine.

For any d-pol set $\mathbb{P}$, d-pol T and d-tri form $\mathbb{T}$, we define

$$\mathrm{prem}(\mathbb{P}, T) = \{\mathrm{prem}(P, T) \mid P \in \mathbb{P}\}, \quad \mathrm{prem}(\mathbb{P}, \mathbb{T}) = \{\mathrm{prem}(P, \mathbb{T}) \mid P \in \mathbb{P}\}.$$

Moreover, let

$$\mathbb{P}^{(k)} = \mathbb{P} \cap \boldsymbol{K}\{x_1, \ldots, x_k\}, \quad \mathbb{P}^{\langle k \rangle} = \mathbb{P}^{(k)} \setminus \mathbb{P}^{(k-1)}, \quad \mathbb{P}^{[k]} = \mathbb{P} \setminus \mathbb{P}^{(k)}.$$

$\mathbb{P}$ is said to be of *level* k, denoted as $\mathrm{level}(\mathbb{P}) = k$, if

$$\mathbb{P}^{[k-1]} = \mathbb{P}^{\langle k \rangle} \neq \emptyset.$$

3 Decomposition Algorithm

Let $[\mathbb{P},\mathbb{Q}]$ be a d-pol system. The algorithm DECOM described below decomposes $[\mathbb{P},\mathbb{Q}]$ into fine d-tri systems. More precisely, it computes a set Ψ which is either empty, that means $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, or of the form $\{[\mathbb{T}_1,\mathbb{U}_1],\ldots,[\mathbb{T}_e,\mathbb{U}_e]\}$ such that

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i), \tag{3}$$

where each $[\mathbb{T}_i,\mathbb{U}_i]$ is a fine d-tri system.

The algorithm employs an elimination top-down from x_n to x_1 (steps D3–D5) with splitting (whenever pseudo-division is performed – according as the initial and separant of the dividing d-pol vanish or not – step D4). For each x_i a single d-pol T with $\mathrm{lvar}(T) = x_i$ is produced from $\mathbb{S}^{\langle i\rangle}$ when it is non-empty. This is done recursively among the d-pols in $\mathbb{S}^{\langle i\rangle}$ by pseudo-dividing those of higher rank with one of minimal rank wrt x_i.

Algorithm DECOM (Input: $\mathbb{P},\mathbb{Q}$; Output: Ψ).

D1. Set $\Psi \leftarrow \emptyset$ and $\Phi \leftarrow \{[\mathbb{P},\mathbb{Q},\emptyset]\}$. Repeat steps D2–D6 until $\Phi = \emptyset$.

D2. Let $[\mathbb{S},\mathbb{U},\mathbb{T}]$ be an element of Φ and set

$$\Phi \leftarrow \Phi \setminus \{[\mathbb{S},\mathbb{U},\mathbb{T}]\},\quad m \leftarrow \mathrm{level}(\mathbb{S}).$$

Do steps D3–D5 for $i = m,\ldots,1$.

D3. If $\mathbb{S}\cap \boldsymbol{K} \neq \emptyset$ then go to D2. If $|\mathbb{S}^{\langle i\rangle}| > 0$ then repeat step D4.

D4. Select from $\mathbb{S}^{\langle i\rangle}$ a T having minimal rank wrt x_i. If $\mathrm{ini}(T)$ does not occur in $\prod_{U\in\mathbb{U}} U$ as factor then set

$$\Phi \leftarrow \Phi \cup \{[\mathbb{S}\setminus\{T\}\cup\{\mathrm{ini}(T),\mathrm{red}(T)\},\mathbb{U},\mathbb{T}]\},\quad \mathbb{U}\leftarrow\mathbb{U}\cup\{\mathrm{ini}(T)\}.$$

If $\mathrm{sep}(T) \neq \mathrm{ini}(T)$ then set

$$\Phi \leftarrow \Phi \cup \{[\mathbb{S}\setminus\{T\}\cup\{\mathrm{prem}(T,\mathrm{sep}(T)),\mathrm{sep}(T)\},\mathbb{U},\mathbb{T}]\},\quad \mathbb{U}\leftarrow\mathbb{U}\cup\{\mathrm{sep}(T)\}.$$

If $|\mathbb{S}^{\langle i\rangle}| = 1$ then go to D5. Otherwise, compute

$$\mathbb{S}\leftarrow\mathbb{S}^{(i-1)}\cup\{T\}\cup\mathrm{prem}(\mathbb{S}^{\langle i\rangle},T)\setminus\{0\}.$$

D5. Compute $\mathbb{U}\leftarrow\mathrm{prem}(\mathbb{U},T)$. If $0\in\mathbb{U}$ then go to D2. Otherwise, set

$$\mathbb{S}\leftarrow\mathbb{S}\setminus\{T\},\quad \mathbb{T}\leftarrow[T]\cup\mathbb{T}.$$

D6. Set $\Psi\leftarrow\Psi\cup\{[\mathbb{T},\mathbb{U}]\}$.

Proof. Termination: As step D4 repeats, $\text{rank}(T, x_i)$ steadily decreases. Hence, after finitely many repetitions all the non-zero remainders of the d-pols in $\mathbb{S}^{\langle i \rangle}$ wrt T will have leading variables $\prec x_i$. Then $|\mathbb{S}^{\langle i \rangle}|$ becomes 1 and D4 terminates.

Observe that DECOM computes a multi-branch tree on which associated with every node is a triplet $[\mathbb{S}_\alpha, \mathbb{U}_\alpha, \mathbb{T}_\alpha]$. Let $\mathbb{P} = \mathbb{S}_1, \mathbb{S}_2, \ldots, \mathbb{S}_\alpha, \ldots$ be the first components of the triplets associated with one branch of the tree. We want to show that the sequence of d-pol sets $\mathbb{S}_\alpha$ is finite. For this purpose, let us assume that the sequence is infinite and proceed to derive a contradiction.

Any two d-pols F and F' are ordered as $F \prec F'$ if $\text{lvar}(F) \prec \text{lvar}(F')$, or $\text{lvar}(F) = \text{lvar}(F')$ and $\text{rank}(F, \text{lvar}(F)) \prec \text{rank}(F', \text{lvar}(F))$. If neither $F \prec F'$ nor $F' \prec F$, we write $F \sim F'$. Then, any finite set of d-pols can be partially ordered by "$\precsim$" and every steadily decreasing sequence of d-pols is finite.

Let $\mathbb{S}_\alpha$ contain δ_α d-pols, ordered as

$$P_{\alpha 1} \succsim P_{\alpha 2} \succsim \cdots \succsim P_{\alpha \delta_\alpha}, \quad \delta_\alpha \geq 1,$$

for each α. From the enlargement of Φ in DECOM, one sees that each $\mathbb{S}_{\alpha+1}$ is obtained from $\mathbb{S}_\alpha$ by performing some of the following actions:

1. Replace a d-pol T by $\text{ini}(T)$ and $\text{red}(T)$;
2. Replace a d-pol T by $\text{sep}(T)$ and $\text{prem}(T, \text{sep}(T))$;
3. Replace a d-pol by its non-zero remainder (wrt another d-pol of lower rank wrt their common leading variable);
4. Delete a d-pol T (when it has remainder 0 wrt another d-pol of lower rank, or no other d-pol in the set has $\text{lvar}(T)$ as leading variable).

Clearly, the d-pols used to replace T are all $\prec T$. It follows that

$$P_{11} \succsim P_{21} \succsim \cdots \succsim P_{\alpha 1} \succsim \cdots.$$

Thus, there exists an integer β_1 (> 1) such that $P_{\alpha 1} \sim P_{\beta_1 1}$ for all $\alpha \geq \beta_1$.

From the four actions above, it is easy to see that $\delta_\alpha \geq 2$ for any $\alpha \geq \beta_1$. Hence, we are allowed to consider the sequence

$$P_{12} \succsim P_{22} \succsim \cdots \succsim P_{\alpha 2} \succsim \cdots:$$

there exists a β_2 $(\geq \beta_1)$ such that $P_{\alpha 2} \sim P_{\beta_2 2}$ for all $\alpha \geq \beta_2$. Now one has $\delta_\alpha \geq 3$ for any $\alpha \geq \beta_2$.

Continuing this argument, we know that there exists a β_{δ_1} $(\geq \beta_{\delta_1 - 1} \geq \cdots \geq \beta_1)$, renamed α_1, such that $P_{\alpha k} \sim P_{\alpha_1 k}$ for all $\alpha \geq \alpha_1$ and $k = 1, \ldots, \delta_1$.

On the other hand, $\mathbb{S}_{\alpha_1}$ is obtained from $\mathbb{S}_1$ by performing some of the actions 1–4 as well. Hence, there exists an integer γ_1 $(1 \leq \gamma_1 < \delta_1)$ such that

$$P_{11} \sim P_{\alpha_1 1}, \ldots, P_{1\gamma_1 - 1} \sim P_{\alpha_1 \gamma_1 - 1}, \quad \text{while} \quad P_{1\gamma_1} \succ P_{\alpha_1 \gamma_1}.$$

Similarly, there exists an α_2 $(> \alpha_1)$ such that $P_{\alpha k} \sim P_{\alpha_2 k}$ for all $\alpha \geq \alpha_2$ and $k = \gamma_1, \ldots, \delta_{\alpha_1}$, and a γ_2 $(\gamma_1 < \gamma_2 < \delta_{\alpha_1})$ such that

$$P_{\alpha_1 \gamma_1} \sim P_{\alpha_2 \gamma_1}, \ldots, P_{\alpha_1 \gamma_2 - 1} \sim P_{\alpha_2 \gamma_2 - 1}, \quad \text{while} \quad P_{\alpha_1 \gamma_2} \succ P_{\alpha_2 \gamma_2}.$$

In this way, we shall construct an infinite sequence of d-pols as follows

$$P_{1\gamma_1} \succ P_{\alpha_1 \gamma_1} \succ \cdots \succ P_{\alpha_k \gamma_k} \succ \cdots.$$

This leads to a contradiction. Therefore, the sequence of d-pol sets $\mathbb{S}_\alpha$ is finite, and thus any branch of the decomposition tree is finite. According to König's infinity lemma, the tree is finite. This proves that steps D2–D6 only have finitely many iterations.

Correctness: Let the state variables be indexed by b and a respectively for their values *before* and *after* the execution of an iteration of D4. We first prove that

$$\begin{aligned}\mathrm{Zero}(\mathbb{S}_b/\mathbb{U}_b) = \mathrm{Zero}(\mathbb{S}_a/\mathbb{U}_a) \cup \mathrm{Zero}(\mathbb{S}_b \setminus \{T\} \cup \{R, S\}/\mathbb{U}_b \cup \{I\}) \\ \cup\, \mathrm{Zero}(\mathbb{S}_b \setminus \{T\} \cup \{I, \mathrm{red}(T)\}/\mathbb{U}_b),\end{aligned} \tag{4}$$

where

$$\begin{aligned}&\mathbb{S}_a = \mathbb{S}_b^{(i-1)} \cup \{T\} \cup \mathrm{prem}(\mathbb{S}_b^{\langle i\rangle}, T) \setminus \{0\}, \quad \mathbb{U}_a = \mathbb{U}_b \cup \{I, S\},\\ &R = \mathrm{prem}(T, S), \quad I = \mathrm{ini}(T), \quad S = \mathrm{sep}(T), \quad T \in \mathbb{S}_b^{\langle i\rangle}.\end{aligned}$$

Let $\bar{x} \in \mathrm{Zero}(\mathbb{S}_b/\mathbb{U}_b)$; then $d^jT/dt^j(\bar{x}) = 0$ for $j \geq 0$ and $P(\bar{x}) = 0$ for $P \in \mathbb{S}_b$. So by the remainder formula (2) we have $H(\bar{x}) = 0$ for all $H \in \mathbb{S}_a$. Clearly, $U(\bar{x}) \neq 0$ for any $U \in \mathbb{U}_b$. If $I(\bar{x}) = 0$ and thus $\mathrm{red}(I)(\bar{x}) = 0$, then

$$\bar{x} \in \mathrm{Zero}(\mathbb{S}_b \setminus \{T\} \cup \{I, \mathrm{red}(T)\}/\mathbb{U}_b). \tag{5}$$

If $I(\bar{x}) \neq 0$ and $S(\bar{x}) \neq 0$, then $\bar{x} \in \mathrm{Zero}(\mathbb{S}_a/\mathbb{U}_a)$. Otherwise, $I(\bar{x}) \neq 0$ but $S(\bar{x}) = 0$. In this case, let $x_{pq} = \mathrm{lead}(T)$ and $d = \deg(T, x_{pq})$; then $\mathrm{lead}(S) = x_{pq}$, $\deg(S, x_{pq}) = d - 1 > 0$, $\mathrm{ini}(S)(\bar{x}) = dI(\bar{x}) \neq 0$, and the remainder formula for $R = \mathrm{prem}(T, S)$ corresponding to (2) is specialized with $\alpha = 0, s = 1$ and $k_1 = 0$. Hence, $T(\bar{x}) = 0$ if and only if $R(\bar{x}) = 0$. It follows that

$$\bar{x} \in \mathrm{Zero}(\mathbb{S}_b \setminus \{T\} \cup \{R, S\}/\mathbb{U}_b \cup \{I\}). \tag{6}$$

Therefore, the left-hand side of (4) is contained in the right-hand side. To show the opposite, we see that if (5) holds then $T(\bar{x}) = 0$ and thus $\bar{x} \in \mathrm{Zero}(\mathbb{S}_b/\mathbb{U}_b)$. If $\bar{x} \in \mathrm{Zero}(\mathbb{S}_a/\mathbb{U}_a)$, then by the remainder formula we have $P(\bar{x}) = 0$ for all $P \in \mathbb{S}_b$, so $\bar{x} \in \mathrm{Zero}(\mathbb{S}_b/\mathbb{U}_b)$ as well. If (6) holds, then $S(\bar{x}) = 0$ and $I(\bar{x}) \neq 0$. In this case, $R(\bar{x}) = 0$ implies that $T(\bar{x}) = 0$ (as demonstrated above), so $\bar{x} \in \mathrm{Zero}(\mathbb{S}_b/\mathbb{U}_b)$, too. By now (4) is proved.

Let the triplets associated with the nodes of the decomposition tree be $[\mathbb{S}_\alpha, \mathbb{U}_\alpha, \mathbb{T}_\alpha]$. Then

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \textstyle\bigcup_\alpha \mathrm{Zero}(\mathbb{S}_\alpha \cup \mathbb{T}_\alpha/\mathbb{U}_\alpha)$$

holds at any time according to (4), where the set union runs over all leaves of the tree. Eventually, the zero decomposition (3) is established.

As the initial and separant of every d-pol $T \in \mathbb{T}_i$ are adjoined in step D4 to the corresponding $\mathbb{U}$ and subsequently replaced by their (non-zero) remainders wrt other d-pols in $\mathbb{T}_i$, we know that

$$\mathrm{prem}(\mathrm{ini}(T), \mathbb{T}_i),\ \mathrm{prem}(\mathrm{sep}(T), \mathbb{T}_i) \in \mathbb{U}_i.$$

By the remainder formula (2), $\mathrm{ini}(T)$ and $\mathrm{sep}(T)$ do not vanish on $\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$ for all $T \in \mathbb{T}_i$, so $[\mathbb{T}_i, \mathbb{U}_i]$ is a d-tri system.

Since all the d-pols in $\mathbb{U}_i$ are actually the non-zero remainders of some d-pols wrt $\mathbb{T}_i$, $0 \notin \mathrm{prem}(\mathbb{U}_i, \mathbb{T}_i)$ for every i. Hence, each $[\mathbb{T}_i, \mathbb{U}_i]$ is fine and the proof is complete. □

The key step of DECOM is to produce a d-tri system $[\mathbb{T}, \mathbb{U}]$ from an arbitrary d-pol system $[\mathbb{P}, \mathbb{Q}]$ by successively eliminating the variables (from x_n down to x_1) for the d-pols in $\mathbb{P}$ and meanwhile reducing the d-pols in $\mathbb{Q}$. During the computation of $[\mathbb{T}, \mathbb{U}]$, called the *principal d-tri system* of $[\mathbb{P}, \mathbb{Q}]$, other d-pol systems are generated and collected, and to each of them the same procedure is applied recursively.

Remark 1. DECOM has similarities to Seidenberg's original algorithm, Ritt-Wu's and others (e.g., [Chou and Gao 93a, Carrà Ferro 94]). However, it differs from each of them. For any given d-pol system $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$, Seidenberg's algorithm can compute d-pol systems involving fewer variables and equivalent to $\mathfrak{P}$ (wrt solvability), but it does not compute any zero decomposition for $\mathfrak{P}$. In his algorithm, heavy *projection* is always carried out (see below). Compared with Ritt-Wu's, the zero decomposition (3) computed by DECOM looks similar, but in (3) whether $\mathrm{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$ is not verified. DECOM also has different algorithmic structure and steps: in it desired strategies such as top-down elimination and splitting along with pseudo-division are incorporated; some redundant verification and repeated computation are avoided. In our approach, there is no concept analogous to the *d-characteristic set* of a d-pol system.

A d-tri system $[\mathbb{T}, \mathbb{U}]$ is called *perfect* if $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \neq \emptyset$. The d-tri systems computed by DECOM are fine but not necessarily perfect. The perfectness may be ensured when projection is embedded. In other words, one can compute a decomposition of the form (3) with all d-tri systems $[\mathbb{T}_i, \mathbb{U}_i]$ perfect. Moreover, for any $1 \leq k < n$ and $\bar{x}_1, \ldots, \bar{x}_k \in \tilde{\boldsymbol{K}}$, there exist $\bar{x}_{k+1}, \ldots, \bar{x}_n \in \tilde{\boldsymbol{K}}$ such that

$$(\bar{x}_1, \ldots, \bar{x}_n) \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$$

if and only if

$$(\bar{x}_1, \ldots, \bar{x}_k) \in \mathrm{Zero}(\mathbb{T}_i^{(k)}/\mathbb{U}_i^{(k)})$$

for some i (see [Wang 94a] for details). This provides a quantifier elimination procedure and thus a decision procedure for the existential theory of algebraically closed d-fields. Since the practical efficiency of projection is not high enough and the approach based on it is not very appropriate for geometry theorem proving (GTP) due to the occurrence of non-degeneracy conditions (cf. [Wang 95]), we decide not to go further in this direction. Instead, we shall consider the irreducibility of d-tri forms.

A d-tri form $\mathbb{T}$ as well as a d-tri system $[\mathbb{T}, \mathbb{U}]$ is said to be *quasi-irreducible* if every d-pol in $\mathbb{T}$ is irreducible over $\boldsymbol{K}$. Using pol factorization over $\boldsymbol{K}$, one can replace the computation of $\mathrm{prem}(\mathbb{U}, T)$ in step D5 of DECOM by the following as to compute a zero decomposition of the form (3) with each $[\mathbb{T}_i, \mathbb{U}_i]$ quasi-irreducible:

Compute the irreducible factors $F_1, \ldots, F_s$ of T over $\boldsymbol{K}$, set $\bar{\mathbb{Q}} \leftarrow \mathbb{U}$ and do step D5′ for $j = 1, \ldots, s$.

D5′. Compute $\bar{\mathbb{U}} \leftarrow \mathrm{prem}(\bar{\mathbb{Q}}, F_j)$. If $j = 1$ then set $\mathbb{U} \leftarrow \bar{\mathbb{U}}$ and $T \leftarrow F_j$. Otherwise, if $0 \notin \bar{\mathbb{U}}$ then set

$$\Phi \leftarrow \Phi \cup \{[\mathbb{S}, \bar{\mathbb{U}}, [F_j] \cup \mathbb{T}]\}.$$

It is easy to see the termination and correctness of the algorithm obtained with this simple modification.

Let

$$\mathbb{T} = [T_1, T_2, \ldots, T_r]$$

be a fine d-tri form and

$$\mathbb{T}^{\{i\}} = [T_1, T_2, \ldots, T_i], \quad i = 1, \ldots, r.$$

Definition 2. $\mathbb{T}$ is said to be *irreducible* if for every $1 \leq i \leq r$ there do not exist D_i and T_i', T_i'' with

$$\begin{aligned}&\mathrm{lead}(D_i) \prec \mathrm{lead}(T_i), \quad \mathrm{lead}(T_i') = \mathrm{lead}(T_i'') = \mathrm{lead}(T_i),\\ &0 \notin \mathrm{prem}(\{D_i, \mathrm{ini}(T_i'), \mathrm{ini}(T_i'')\}, \mathbb{T}^{\{i-1\}})\end{aligned}$$

such that

$$\mathrm{prem}(D_i T_i - T_i' T_i'', \mathbb{T}^{\{i-1\}}) = 0.$$

A fine d-tri system $[\mathbb{T}, \mathbb{U}]$ is said to be *irreducible* if $\mathbb{T}$ is irreducible.

In fact, $\mathbb{T}$ is irreducible when it is so, considered as a pol tri form (cf. [Ritt (50), p. 107] and [Wu 89]). If $\mathbb{T}$ is reducible, then there exist a k and d-pols D_k and $G_1, \ldots, G_s$ with

$$\begin{aligned}&\mathrm{lead}(D_k) \prec \mathrm{lead}(T_k), \quad \mathrm{lead}(G_1) = \cdots = \mathrm{lead}(G_s) = \mathrm{lead}(T_k),\\ &0 \notin \mathrm{prem}(\{D_k, \mathrm{ini}(G_1), \ldots, \mathrm{ini}(G_s)\}, \mathbb{T}^{\{i-1\}})\end{aligned}$$

such that $\mathbb{T}^{\{k-1\}}$ and

$$\mathbb{T}^{\{k-1\}} \cup [G_j], \quad j = 1, \ldots, s,$$

are all irreducible and

$$\mathrm{prem}(D_k T_k - G_1 \cdots G_s, \mathbb{T}^{\{k-1\}}) = 0.$$

Here the irreducibility and the d-pols $G_1, \ldots, G_s$ can be determined with usual pol factorization (of T_k over the successive algebraic extension field defined by $T_1, T_2, \ldots, T_{k-1}$ – see [Wang 94b]).

Using the factorization of T_k into $G_1, \ldots, G_s$, one can further decompose $\mathbb{T}$ into d-tri forms, and finally into irreducible ones. We omit the involved details of the decomposition procedure and state the result in the form of the following theorem.

Theorem 1. *There is an algorithm which computes, for any given d-pol system* $[\mathbb{P}, \mathbb{Q}]$*, a set which either is empty, that means* $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$*, or consists of finitely many irreducible d-tri systems* $[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]$ *such that the zero decomposition* (3) *holds.*

The proof of this theorem will be given in the sequel of [Wang 94a].

4 Decision Algorithm

On the basis of the zero decomposition method described in the preceding section, we can devise several algorithms for proving theorems and deriving unknown relations automatically in elementary differential geometry and mechanics, which can be formulated in terms of d-pol equations and inequations. In this section we present one of the algorithms for automated theorem proving. Let us first prove two fundamental theorems.

Theorem 2. *Let* $[\mathbb{T}, \mathbb{U}]$ *be a d-tri system and* G *a d-pol. If* $\mathrm{prem}(G, \mathbb{T}) = 0$*, then* $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(G)$*. If* $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(G)$ *and* $\mathbb{T}$ *is irreducible, then* $\mathrm{prem}(G, \mathbb{T}) = 0$*.*

Proof. According to the definition of d-tri systems and the remainder formula (2), the first half of the theorem is obvious. To prove the second half, let

$$\Omega = \{P \in \boldsymbol{K}\{x\} \mid \mathrm{prem}(P, \mathbb{T}) = 0\}.$$

Since $\mathbb{T}$ is irreducible, Ω is a non-trivial prime ideal (cf. [Ritt (50), p. 107]). Clearly,

$$\mathbb{U} \cap \Omega = \emptyset, \quad \mathrm{Zero}(\Omega) \subset \mathrm{Zero}(\mathbb{T}).$$

Let η be a generic zero of Ω; then $U(\eta) \neq 0$ for any $U \in \mathbb{U}$ (cf. [Ritt (50), pp. 25–27] and [Wu 89]). It follows that

$$\eta \in \mathrm{Zero}(\mathbb{T}/\mathbb{U}) \subset \mathrm{Zero}(G).$$

That is, $G(\eta) = 0$, so $G \in \Omega$. Hence, $\mathrm{prem}(G, \mathbb{T}) = 0$ and the theorem is proved. □

Theorem 3. *Let a d-pol system* $[\mathbb{P}, \mathbb{Q}]$ *have zero decomposition of the form* (3) *with each* $[\mathbb{T}_i, \mathbb{U}_i]$ *irreducible. Then*

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q}), \tag{7}$$

where $\mathbb{I}_i = \{\mathrm{ini}(T), \mathrm{sep}(T) \mid T \in \mathbb{T}_i\}$ *for each* i*.*

Proof. As

$$\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i) \subset \mathrm{Zero}(\mathbb{P}/\mathbb{Q}),$$

by Theorem 2 we have

$$\mathrm{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}, \quad 0 \notin \mathrm{prem}(\mathbb{Q}, \mathbb{T}_i)$$

for every i. Thus, according to (2), the right-hand side of (7) is contained in the left-hand side. On the contrary, let $\bar{x} \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. By (3) there is an i such that $\bar{x} \in \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$. Since $[\mathbb{T}_i, \mathbb{U}_i]$ is a d-tri system, $\bar{x}$ is not a zero of any d-pol in $\mathbb{I}$. Hence,

$$\bar{x} \in \mathrm{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q})$$

and thus is contained in the right-hand side of (7). □

Return to (1) and observe that many theorems in differential geometry (space curve theory) and mechanics (cf. [Chou and Gao 91]) can be algebraically formulated in that form. Let

$$\mathbb{H} = \{H_1, \ldots, H_h\}, \quad \mathbb{D} = \{D_1, \ldots, D_d\}.$$

A theorem of the form (1) will be denoted by $\mathfrak{T}(\mathbb{H}, \mathbb{D}, C)$. We call

$$\textstyle\bigwedge_{i=1}^{h} H_i = 0 \wedge \bigwedge_{j=1}^{d} D_j \neq 0$$

the hypothesis and $C = 0$ the conclusion of the theorem.

Algorithm PROVE. Given a theorem

$$\mathfrak{T} = \mathfrak{T}(\mathbb{H}, \mathbb{D}, C),$$

this algorithm decides whether $\mathfrak{T}$ is universally true, and if not, determines a subsidiary condition under which it is true.

P1. Compute $\Psi \leftarrow \mathsf{DECOM}(\mathbb{H}, \mathbb{D})$. If $\Psi = \emptyset$, then the hypothesis of the theorem $\mathfrak{T}$ is self-contradictory and the algorithm terminates.

P2. Compute

$$R_i \leftarrow \operatorname{prem}(C, \mathbb{T}_i) \quad \text{for} \quad [\mathbb{T}_i, \mathbb{U}_i] \in \Psi.$$

If $R_i = 0$ for all i, then $\mathfrak{T}$ is universally true and the algorithm terminates.

P3. Let Δ be the set of all i for which $R_i \neq 0$. Decompose $[\mathbb{T}_i, \mathbb{U}_i]$ into a finite set Ψ_i of irreducible d-tri systems for each $i \in \Delta$.

P4. Compute

$$R_{ij} \leftarrow \operatorname{prem}(C, \mathbb{T}_{ij}) \quad \text{for} \quad [\mathbb{T}_{ij}, \mathbb{U}_{ij}] \in \Psi_i, i \in \Delta.$$

If $R_{ij} = 0$ for all j and i, then $\mathfrak{T}$ is universally true and the algorithm terminates. Otherwise, $\mathfrak{T}$ is not universally true. It is conditionally true, with the *subsidiary* condition determined in step P5.

P5. For each $i \in \Delta$, let Δ_i be the set of all j for which $R_{ij} \neq 0$. Set

$$\mathcal{D} \leftarrow \textstyle\bigwedge_{j \in \Delta_i, i \in \Delta} (\bigvee_{T \in \mathbb{T}_{ij}} T \neq 0 \vee \bigvee_{U \in \mathbb{U}_{ij}} U = 0).$$

Then $\mathcal{D}$ is the subsidiary condition under which $\mathfrak{T}$ is true. If $\mathcal{D}$ can be identified either geometrically or algebraically as *non-degeneracy* conditions, then $\mathfrak{T}$ is *generically* true.

This algorithm terminates obviously. As formula (1) is valid if and only if

$$\operatorname{Zero}(\mathbb{H}/\mathbb{D}) \subset \operatorname{Zero}(C),$$

the correctness follows from Theorem 2. Possible variants of the algorithm and its modification for formula derivation are left out. Some other important issues are also omitted. One of them is to simplify the formula $\mathcal{D}$ algebraically (which is not an easy task) and to identify $\mathcal{D}$ to non-degeneracy conditions. In fact, no definition for "non-degeneracy" and "generically true" is given here. The concepts are due to Wu and may be defined when the variables are separated into parameters and geometric dependents and the notions of dimension and order are introduced. The interested reader is referred to [Carrà Ferro 94, Chou and Gao 93a, Wu 79, Wu 82, Wu 87a] for details.

Remark 2. Step P3 requires algebraic pol factorization which is expensive in general. Nonetheless, the author has implemented rather efficient factoring routines, which work well for pols from GTP, as demonstrated in [Wang 94b]. The factoring times for the pols we have encountered in GTP so far are in the matter of seconds.

5 Examples

To illustrate the method explained in the previous sections and its performance, we now present two examples, using a draft implementation of the algorithms in Maple. The timings mentioned below were obtained from Maple V running on a SUN SparcServer 690/51 and are given in CPU seconds. The examples were studied in detail first in [Wu 87b, Wu 87c, Wu 91] and then in [Chou and Gao 92, Chou and Gao 93a, Chou and Gao 93b] and are among the interesting and difficult ones in differential geometry and mechanics considered so far. Experiments on these and other examples show that our method based on d-tri systems is computationally efficient. Systematic comparisons for the examples will be made later when our implementation of the other methods is completed.

Example 1 (Bertrand curves [Chou and Gao 93b, Wu 87b, Wu 91]). Let C and $\bar{C}$ be a Bertrand pair of curves in one-to-one correspondence with arc lengths $s, \bar{s}$ as parameters in the ordinary metric space. Attach the trihedrals (X, e_1, e_2, e_3) and $(\bar{X}, \bar{e}_1, \bar{e}_2, \bar{e}_3)$ to C and $\bar{C}$ at the corresponding points X and $\bar{X}$, and denote the curvature and torsion of C and $\bar{C}$ by κ, τ and by $\bar{\kappa}, \bar{\tau}$ respectively. We have the following theorems.

Schell's Theorem. The product of τ and $\bar{\tau}$ is a constant.

Bertrand's Theorem. There exists a linear relation between κ and τ with constant coefficients.

Mannheim's Theorem. The cross-ratio of $X, \bar{X}$ and the centers of $\kappa, \bar{\kappa}$ is a constant.

To prove the theorems, let

$$\begin{aligned} &\bar{X} = X + a_1 e_1 + a_2 e_2 + a_3 e_3, \\ &\bar{e}_i = \textstyle\sum_{j=1}^{3} u_{ij} e_j, \ i = 1, 2, 3. \end{aligned}$$

From the Frenet formulae of C and $\bar{C}$, one can easily deduce a set of 12 d-pols (see [Wu 91]). In the classical Bertrand case, $\bar{e}_2 = \pm e_2$. Let us take the positive sign, and similarly for the orthogonality relations between the u_{ij}'s, so that we have

$$\begin{aligned} &a_1 = 0, \ \ a_3 = 0, \ \ u_{12} = u_{21} = u_{23} = u_{32} = 0, \\ &u_{22} = 1, \ \ u_{11} = u_{33}, \ \ u_{13} = -u_{31}, \ \ u_{11}^2 + u_{13}^2 = 1. \end{aligned}$$

Combining these relations with the 12 d-pols, one obtains the following set of 14 d-pols (the primes denoting the derivatives wrt s)

$$
\begin{array}{ll}
H_1 = \bar{s}' u_{11} + a_2\kappa - 1, & H_2 = -a_2', \\
H_3 = \bar{s}' u_{13} - a_2\tau, & H_4 = -u_{11}', \\
H_5 = \bar{s}'\bar{\kappa} - \kappa u_{12} + \tau u_{13}, & H_6 = -u_{13}', \\
H_7 = \bar{s}'\bar{\kappa} u_{11} - \bar{s}'\bar{\tau} u_{31} - \kappa, & H_8 = \bar{s}'\bar{\kappa} u_{13} - \bar{s}'\bar{\tau} u_{33} + \tau, \\
H_9 = -u_{31}', & H_{10} = -\bar{s}'\bar{\tau} - \kappa u_{31} + \tau u_{33}, \\
H_{11} = -u_{33}', & H_{12} = u_{11} - u_{33}, \\
H_{13} = u_{13} + u_{31}, & H_{14} = u_{11}^2 + u_{13}^2 - 1.
\end{array}
$$

With respect to the ordering

$$
\bar{s} \prec a_1 \prec a_2 \prec a_3 \prec u_{11} \prec u_{12} \prec u_{13} \prec u_{21} \prec u_{22} \prec u_{23} \prec u_{31} \prec u_{32} \prec u_{33} \\
\prec \kappa \prec \tau \prec \bar{\kappa} \prec \bar{\tau},
$$

$\mathbb{P} = \{H_1, \ldots, H_{14}\}$ can be decomposed (in 91.4 seconds) into 10 irreducible d-tri systems, with the corresponding d-tri forms given as

$$
\begin{aligned}
\mathbb{T}_1 = {} & [a_2', u_{11}', u_{12} - u_{11}, u_{13}^2 + u_{11}^2 - 1, u_{31} + u_{13}, u_{33} - u_{11}, a_2\kappa + \bar{s}' u_{11} - 1, \\
& a_2\tau - \bar{s}' u_{13}, \bar{s}'\bar{\kappa} + u_{13}\tau - u_{11}\kappa, \bar{s}'\bar{\tau} - u_{11}\tau - u_{13}\kappa], \\
\mathbb{T}_2 = {} & [\bar{s}'', a_2', \bar{s}' u_{11} - 1, \bar{s}'^2 u_{13}^2 - \bar{s}'^2 + 1, u_{31} + u_{13}, u_{33} - u_{11}, \kappa, a_2\tau - \bar{s}' u_{13}, \\
& \bar{s}'\bar{\kappa} + u_{13}\tau, \bar{s}'\bar{\tau} - u_{11}\tau], \\
\mathbb{T}_3 = {} & [a_2', u_{11} - 1, u_{12} - 1, u_{13}, u_{31}, u_{33} - 1, a_2\kappa + \bar{s}' - 1, \tau, \bar{s}'\bar{\kappa} - \kappa, \bar{\tau}], \\
\mathbb{T}_4 = {} & [a_2', u_{11} + 1, u_{12} + 1, u_{13}, u_{31}, u_{33} + 1, a_2\kappa - \bar{s}' - 1, \tau, \bar{s}'\bar{\kappa} + \kappa, \bar{\tau}], \\
\mathbb{T}_5 = {} & [\bar{s}' + 1, a_2', u_{11} + 1, u_{13}, u_{31}, u_{33} + 1, \kappa, \tau, \bar{\kappa}, \bar{\tau}], \\
\mathbb{T}_6 = {} & [\bar{s}' - 1, a_2', u_{11} - 1, u_{13}, u_{31}, u_{33} - 1, \kappa, \tau, \bar{\kappa}, \bar{\tau}], \\
\mathbb{T}_7 = {} & [\bar{s}' - 1, a_2, u_{11} - 1, u_{13}, u_{31}, u_{33} - 1, \kappa, \bar{\kappa}, \bar{\tau} - \tau], \\
\mathbb{T}_8 = {} & [\bar{s}' + 1, a_2, u_{11} + 1, u_{13}, u_{31}, u_{33} + 1, \kappa, \bar{\kappa}, \bar{\tau} - \tau], \\
\mathbb{T}_9 = {} & [\bar{s}' - 1, a_2, u_{11} - 1, u_{12} - 1, u_{13}, u_{31}, u_{33} - 1, \bar{\kappa} - \kappa, \bar{\tau} - \tau], \\
\mathbb{T}_{10} = {} & [\bar{s}' + 1, a_2, u_{11} + 1, u_{12} + 1, u_{13}, u_{31}, u_{33} + 1, \bar{\kappa} - \kappa, \bar{\tau} - \tau]
\end{aligned}
$$

such that

$$
\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{2} \mathrm{Zero}(\mathbb{T}_i/\bar{s}' a_2 u_{13}) \cup \bigcup_{i=3}^{4} \mathrm{Zero}(\mathbb{T}_i/\bar{s}' a_2) \cup \bigcup_{i=5}^{10} \mathrm{Zero}(\mathbb{T}_i).
$$

The conclusions of Schell, Bertrand, and Mannheim's theorems to be proved are

$$
\begin{aligned}
C_S &= (\tau\bar{\tau})' = 0, \\
C_B &= \kappa'\tau'' - \kappa''\tau' = 0, \\
C_M &= [(1 + a_2\bar{\kappa})(1 - a_2\kappa)]' = 0
\end{aligned}
$$

respectively. It is easy to verify that

$$
\begin{aligned}
&\mathrm{prem}(C_S, \mathbb{T}_i) \begin{cases} = 0, & i = 1, \ldots, 6, \\ \neq 0, & i = 7, \ldots, 10; \end{cases} \\
&\mathrm{prem}(C_B, \mathbb{T}_i) \begin{cases} = 0, & i = 1, \ldots, 8, \\ \neq 0, & i = 9, 10; \end{cases} \\
&\mathrm{prem}(C_M, \mathbb{T}_i) = 0, \ i = 1, \ldots, 10.
\end{aligned}
$$

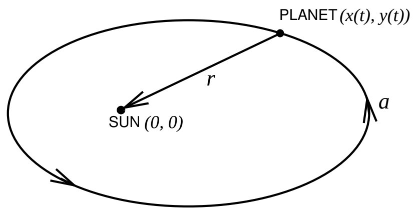
Therefore, the algebraic form of Schell's theorem and of Bertrand's are both conditionally true and of Mannheim's is universally true. The subsidiary conditions for the former may be provided as $\bar{s}' \neq 0$ and $a_2 \neq 0$ (i.e., $C \neq \bar{C}$). The total times of computing the pseudo-remainders for the three theorems are 1.4, 1.7 and 1.9 seconds, respectively.

Note that Bertrand's theorem is also true when $a_2 = 0$ and $\kappa = \bar{\kappa} = 0$ (i.e., $C = \bar{C}$ is a straight line). Mannheim's theorem is considered usually under the condition $\kappa\bar{\kappa} \neq 0$. However, the algebraic form of the theorem is true as well in the degenerate case $\kappa = \bar{\kappa} = 0$.

Remark 3. A relatively large amount of the decomposition time indicated above was spent for verification so that two redundant d-tri systems are removed. The removal of redundancy here is merely to make the list of d-tri systems short. It is not necessary for proving the theorem because the pseudo-remainders of the conclusion d-pols wrt the removed d-tri forms are very easy to compute. This is also true for the following example. Without the verification, the decomposition time can be reduced to 25.7 seconds. The total time needed for proving the three theorems is 31 seconds only.

Example 2 (Kepler-Newton's Laws [Chou and Gao 93a, Wu 87c, Wu 91]). Newton's gravitational laws and Kepler's observational laws play an important role in celestial mechanics. The first two of them may be stated as follows.

K1. Each planet describes an ellipse with the sun at one focus.
K2. The radius vector drawn from the sun to a planet sweeps out equal areas in equal times.
N1. The acceleration of any planet is inversely proportional to the square of the distance from the sun to the planet.
N2. The acceleration vector of any planet is directed to the sun.



There are inference relations between the two groups of laws. For example, K2 is equivalent to N2. We consider two non-trivial relations as illustration for our method: (i) N1 and N2 imply K1 and (ii) K1 and K2 imply N1.

Let the coordinates of the planet be (x, y), depending on the time variable t. Assume that the sun is located at the origin $(0, 0)$. Then the d-pol equations for Newton's two laws are

$$N_1 = (r^2 a)' = 0, \quad N_2 = xy'' - x''y = 0$$

respectively, where a is the acceleration of the planet and r the length of the radius vector from the sun to the planet. Clearly, we have

$$H_1 = r^2 - x^2 - y^2 = 0, \quad H_2 = a^2 - x''^2 - y''^2 = 0.$$

We assume $a \neq 0$; the problem becomes trivial when $a = 0$. Then,

$$\mathfrak{P} = [\{N_1, N_2, H_1, H_2\}, \{a\}]$$

constitutes the hypothesis d-pol system. Kepler's first law to be proved is equivalent to (cf. [Chou and Gao 93a, part II])

$$K_1 = r'''(x'y'' - x''y') - r''(x'y''' - x'''y') + r'(x''y''' - x'''y'') = 0.$$

With the ordering $x \prec y \prec r \prec a$, $\mathfrak{P}$ can be decomposed (in 17.5 CPU seconds) into 6 quasi-irreducible d-tri systems with the corresponding $\mathbb{T}_i, \mathbb{U}_i$ shown below

$$\begin{aligned}
&\mathbb{T}_1 = [T_1, T_2, H_1, H_2], \qquad \mathbb{T}_2 = [xx''' + 2x'x'', xy' - x'y, H_1, H_2],\\
&\mathbb{T}_3 = [x, yy''' + 2y'y'', r - y, a - y''], \quad \mathbb{T}_4 = [x, yy''' + 2y'y'', r - y, a + y''],\\
&\mathbb{T}_5 = [x, yy''' + 2y'y'', r + y, a - y''], \quad \mathbb{T}_6 = [x, yy''' + 2y'y'', r + y, a + y''],\\
&\mathbb{U}_1 = \{x'', xx''' + 2x'x'', y, r, a, S_2,\\
&\qquad 3x^2x''x'''' - 5x^2x'''^2 - 2xx'x''x''' + 6xx''^3 - 2x'^2x''^2\},\\
&\mathbb{U}_2 = \{x'', r, a\}, \quad \mathbb{U}_3 = \cdots = \mathbb{U}_6 = \{y''\},\\
&T_1 = 9x^3x''^2x''''' - 45x^3x''x'''x'''' + 18x^2x'x''^2x'''' + 40x^3x'''^3 - 30x^2x'x''x'''^2\\
&\qquad -6xx'^2x''^2x''' + 18xx'x''^4 - 4x'^3x''^3,\\
&T_2 = 3x^2x''x''''y^2 - 4x^2x'''^2y^2 + 2xx'x''x'''y^2 + 6xx''^3y^2 + 2x'^2x''^2y^2 + x^4x'''^2\\
&\qquad +4x^3x'x''x''' + 4x^2x'^2x''^2,\\
&S_2 = \mathrm{sep}(T_2)/y = 3x^2x''x'''' - 4x^2x'''^2 + 2xx'x''x''' + 6xx''^3 + 2x'^2x''^2.
\end{aligned}$$

It can be verified (in 95.4 seconds) that $\mathrm{prem}(K_1, \mathbb{T}_i) = 0$ for $i = 1, \ldots, 6$, so that Kepler's first law follows from Newton's two laws. The total proving time is 106.5 CPU seconds [see Remark 3].

In fact, the d-tri forms $\mathbb{T}_1$ and $\mathbb{T}_2$ are both reducible. Using our factoring methods (cf. [Wang 94b]), it is easy to verify that $[T_1, T_2, H_1]$ is irreducible and H_2 in both $\mathbb{T}_1$ and $\mathbb{T}_2$ can be factorized algebraically as

$$H_2 \doteq (xa + x''r)(xa - x''r)/x^2. \tag{8}$$

Therefore, $\mathbb{T}_1$ can be further decomposed into two irreducible d-tri forms

$$\mathbb{T}_{11} = [T_1, T_2, H_1, xa + x''r], \quad \mathbb{T}_{12} = [T_1, T_2, H_1, xa - x''r],$$

and $\mathbb{T}_2$ into

$$\begin{aligned}
\mathbb{T}_{21} &= [xx''' + 2x'x'', xy' - x'y, H_1, xa + x''r],\\
\mathbb{T}_{22} &= [xx''' + 2x'x'', xy' - x'y, H_1, xa - x''r]
\end{aligned}$$

such that

$$\mathrm{Zero}(\mathfrak{P}) = \bigcup_{j=1}^{2} \mathrm{Zero}(\mathbb{T}_{1j}/x''yrS_2) \cup \mathrm{Zero}(\mathbb{T}_{2j}/x''r) \cup \bigcup_{i=3}^{6} \mathrm{Zero}(\mathbb{T}_i/y'').$$

The algebraic factorization (8) can be explained as follows. From $H_1 = 0$ and $H_2 = 0$, one knows that the ratio of the length of the radius vector compared with that of the acceleration vector is r/a. Hence, when $N_2 = 0$ is assumed, the ratio of the corresponding vector components may differ from r/a only by sign, i.e.,

$$x/x'' = y/y'' = \pm r/a.$$

This relation is just reflected by (8).

For (ii), consider

$$\mathfrak{P}^* = [\{K_1, K_2, H_1, H_2\}, \{a\}]$$

as the hypothesis d-pol system, where $K_2 = H_2$. We found that $\mathfrak{P}^*$ can also be decomposed (in 28.5 seconds) into 6 quasi-irreducible d-tri systems $[\mathbb{T}_i^*, \mathbb{U}_i^*]$ with

$$\begin{aligned}
&\mathbb{T}_1^* = \mathbb{T}_1, && \mathbb{T}_2^* = [xy' - x'y, H_1, H_2],\\
&\mathbb{T}_3^* = [x, r - y, a - y''], && \mathbb{T}_4^* = [x, r - y, a + y''],\\
&\mathbb{T}_5^* = [x, r + y, a - y''], && \mathbb{T}_6^* = [x, r + y, a + y''],\\
&\mathbb{U}_i^* = \mathbb{U}_i,\ i = 1, \ldots, 6
\end{aligned}$$

(under the same ordering above). The pseudo-remainder of N_1 wrt $\mathbb{T}_i^*$ (computed in 118.7 seconds) is 0 for $i = 1$ and non-zero for $i = 2, \ldots, 6$. Hence, the theorem is conditionally true with the subsidiary condition provided as

$$x(xy' - x'y) \neq 0.$$

Therefore, Kepler's two laws imply Newton's first law under the condition that the ellipse does not degenerate to two lines or points.

If the major axis of the ellipse is taken as the x-axis, then K_1 is simplified to

$$\bar{K}_1 = x'r'' - x''r'.$$

It is somewhat easier to compute a zero decomposition for $[\{\bar{K}_1, K_2, H_1, H_2\}, \{a\}]$, which is the same as that for $\mathfrak{P}^*$, excepting that T_1 and T_2 are replaced by two simpler d-pols – let the first d-tri form so obtained be $\bar{\mathbb{T}}_1$. Then, verifying the 0 remainder of N_1 wrt $\bar{\mathbb{T}}_1$ takes much less time (3.6 seconds). It is also easy to check that the following d-pol

$$N_3 = [x'(xy' - x'y)^2]^2 - [r^2a(xr' - x'r)]^2$$

has 0 remainder wrt $\bar{\mathbb{T}}_1$. $N_3 = 0$ corresponds to the relation

$$r^2a = \pm h^2/p$$

given in [Wu 91]. Thus, one can conclude that, under the assumption of K1 and K2, the third law K3 of Kepler and N3 of Newton are equivalent.

Remark 4. The computing times for this example may demonstrate one aspect about the efficiency of our zero decomposition algorithm in comparison with Ritt-Wu's [Chou and Gao 93a, Ritt (50), Wu 89, Wu 91]. Ritt-Wu's algorithm computes a zero decomposition of the form (7) with $\mathrm{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$ verified for each i. The verification is very time-consuming in most cases. $\mathbb{T}_1$ above is actually a (quasi-) d-characteristic set of $\mathbb{P}$, and verifying $\mathrm{prem}(N_1, \mathbb{T}_1) = 0$ takes 110.1 seconds, which are more than six times the total decomposition time (and eleven times when redundant d-tri systems are not removed) for our algorithm. In the case (ii), the verification of $\mathrm{prem}(K_1, \mathbb{T}_1) = 0$ takes 90.3 CPU seconds.

Using the same method, one can investigate other relations among Kepler's and Newton's laws. As shown by Wu, Chou and Gao that some of the laws can be derived or discovered automatically from the others, our method with modification may be used to formula derivation as well, following a general device introduced in [Wu 87c, Wu 91] and the techniques developed in [Chou and Gao 92].

Acknowledgements

This work has been supported by FWF and CEC under ESPRIT Basic Research Project 6471 (MEDLAR II) and CNRS-MRE under project inter-PRC "Mécanisation de la Déduction."

References

[Carrà Ferro 94] Carrà Ferro, G. An extension of a procedure to prove statements in differential geometry. *J. Automated Reasoning* **12** (1994), 351–358.

[Carrà Ferro and Gallo 90] Carrà Ferro, G. and Gallo, G. A procedure to prove statements in differential geometry. *J. Automated Reasoning* **6** (1990), 203–209.

[Chou and Gao 91] Chou, S. C. and Gao, X. S. Theorems proved automatically using Wu's method – Part on differential geometry (space curves) and mechanics. *MM Research Preprints* 6 (1991), 37–55.

[Chou and Gao 92] Chou, S. C. and Gao, X. S. Automated reasoning in differential geometry and mechanics using characteristic method – III. In: *Automated Reasoning* (Z. Shi, ed.), pp. 1–12. North-Holland: Elsevier Science Publ. (1992).

[Chou and Gao 93a] Chou, S. C. and Gao, X. S. Automated reasoning in differential geometry and mechanics using the characteristic set method – I, II. *J. Automated Reasoning* **10** (1993), 161–189.

[Chou and Gao 93b] Chou, S. C. and Gao, X. S. Automated reasoning in differential geometry and mechanics using the characteristic method – IV. *Syst. Sci. Math. Sci.* **6** (1993), 186–192.

[Li 91] Li, Z. M. Mechanical theorem proving of the local theory of surfaces. *MM Research Preprints* 6 (1991), 102–120.

[Ritt (50)] Ritt, J. F. *Differential Algebra.* New York: Amer. Math. Soc. (1950).

[Seidenberg 56] Seidenberg, A. An elimination theory for differential algebra. *Univ. California Publ. Math.* (N.S.) **3**(2) (1956), 31–66.

[Wang 94a] Wang, D. M. An elimination method for differential polynomial systems I. Preprint, LIFIA–Institut IMAG (1994).

[Wang 94b] Wang, D. M. Algebraic factoring and geometry theorem proving. In: *Proc. CADE-12, Lecture Notes in Comput. Sci.* **814** (1994), pp. 386–400.

[Wang 95] Wang, D. M. Elimination procedures for mechanical theorem proving in geometry. *Ann. Math. Artif. Intell.* (in press).

[Wu 79] Wu, W.-T. On the mechanization of theorem-proving in elementary differential geometry (in Chinese). *Sci. Sinica* Special Issue on Math. (I) (1979), 94–102.

[Wu 82] Wu, W.-T. Mechanical theorem proving in elementary geometry and elementary differential geometry. In: *Proc. 1980 Beijing DD-Symp.*, Vol. 2, pp. 1073–1092. Beijing: Science Press (1982).

[Wu 87a] Wu, W.-T. A constructive theory of differential algebraic geometry. In: *Proc. 1985 Shanghai DD-Symp., Lecture Notes in Math.* **1255** (1987), pp. 173–189.

[Wu 87b] Wu, W.-T. A mechanization method of geometry and its applications – II. curve pairs of Bertrand type. *Kexue Tongbao* **32** (1987), 585–588.

[Wu 87c] Wu, W.-T. Mechanical derivation of Newton's gravitational laws from Kepler's laws. *MM Research Preprints* 2 (1987), 53–61.

[Wu 89] Wu, W.-T. On the foundation of algebraic differential geometry. *Syst. Sci. Math. Sci.* **2** (1989), 289–312.

[Wu 91] Wu, W.-T. Mechanical theorem proving of differential geometries and some of its applications in mechanics. *J. Automated Reasoning* **7** (1991), 171–191.