Mechanical Theorem Proving of the Local Theory of Surfaces*

ZIMING LI

Research Institute for Symbolic Computation
Johannes Kepler University,
A-4040 Linz, Austria
e-mail: zmli@risc.uni-linz.ac.at

August 10, 1992

Abstract

The present paper applies the characteristic set method of algebraic differential polynomials to give a mechanical procedure which permits us to prove non-trivial theorems in the local theory of surfaces. By this method, we have discovered a new relation between the first and second fundamental forms of a surface in case this surface contains no umbilici. A few examples are given to illustrate the method

In 1989 Wu Wen tsun [Wu, 1989] gave a constructive theory of the characteristic set (abbreviated as char-set) method of general algebraic differential polynomials (abbreviated as d-pols) based on the works of Riquier, Janet, Cartan, Thomas and Ritt. One of the applications of this method is mechanical theorem-proving (abbreviated as MTP) in differential geometries. In the case of a single independent variable, this method is quite similar to the char-set method in the algebraic case. There have been several papers applying it to the MTP of space curves, cf. [Chou & Gao, 1989, 1990]. In the case of two or more independent variables, the char-set method is much more complicated than that of a single variable because of the presence of integrability conditions. Consequently, the MTP of the

*This work is supported by Fonds zur Förderung der wiss. Forschung, Project P9181-TEC POSSO

surface theory becomes rather difficult in practice since the computation of integrability conditions is costly. However, as shown in the rest of this paper, some non-trivial theorems can still be proved mechanically by this method when we translate geometric statements by means of the frames on surfaces.

The paper is organized as follows In Section 1 we give a brief description of the char-set method of d-pols. For more details, please refer to [Wu, 1989] and [Wu, 1991]. In Section 2 some experiments and results of studying the fundamental equations of surface are given. In Section 3 we illustrate this method by means of three examples.

1 A survey of the char-set algorithm of algebraic differential polynomials

We assume that the following polynomials involve two independent variables u and v. In fact, all of statements in this section can be extended to any finite number of variables.

1.1 Ordering of indeterminates

Let K be an algebraic field of characteristic 0 which admits two operations of differentiation, that is, each element a of K has two partial derivatives $\frac{\partial a}{\partial u}$ and $\frac{\partial a}{\partial v}$. These symbols may merely distinguish the derivatives. Each of the two operations satisfies, for any$a, b \in K$,

$$\frac{\partial(a+b)}{\partial u} = \frac{\partial a}{\partial u} + \frac{\partial b}{\partial u},$$
$$\frac{\partial ab}{\partial u} = \frac{\partial a}{\partial u}b + \frac{\partial b}{\partial u}a,$$

where u can be replaced by v, and

$$\frac{\partial}{\partial v}\frac{\partial a}{\partial u} = \frac{\partial}{\partial u}\frac{\partial a}{\partial v}.$$

K is called a *differential field*. For example, K may be $\mathbf{Q}(u, v)$, the field of rational functions in u and v.

We use indeterminates X_1, X_2, ..., X_n. With each X_k are associated symbols

$$\frac{\partial^{i+j} X_k}{\partial u^i \partial v^j},$$

where i and j are non-negative integers. These are the partial derivatives of X_k.

K being given, a d-pol is a polynomial in the derivatives of $X_1, X_2, ..., X_n$ with coefficients over K. We can then introduce partial differentiations satisfying the ordinary rules in the calculus. It is easy to see that the set of all d-pols with ordinary algebraic and differential operations forms a differential polynomial ring which we will denote by $K\{X_1, X_2, ..., X_n\}$.

Notation. For brevity, we denote the partial derivative $\frac{\partial^{i+j} X_k}{\partial u^i \partial v^j}$ by $\partial_\delta X_k$ in which $\delta = (i, j)$.

Let Δ be the set $\{\partial_\delta | \delta = (i, j),\ i \ and \ j \ are \ non-negative \ integers\}$. The set Δ may be regarded as the free commutative monoid generated by $\partial_{1,0}$ and $\partial_{0,1}$ with an identity $\partial_{0,0}$ and the composition of differentiations, namely,

$$\partial_{i,j}\partial_{k,l} = \partial_{i+k,j+l}.$$

In the remainder of this paper we shall write ∂_{ij} instead of $\partial_{i,j}$, for instance, ∂_{23} instead of $\partial_{2,3}$ since no derivative appearing in this paper will have order more than 9.

Definition 1. Let $<$ be an ordering on Δ that is compatible with the monoid structure, i.e.

1. $\partial_{00} < \partial_{lk}$ for all $(l, k) \neq (0, 0)$.

2. $\partial_\alpha < \partial_\beta$ implies that $\partial_\delta\partial_\alpha < \partial_\delta\partial_\beta$ for all $\partial_\alpha, \partial_\beta, \partial_\delta \in \Delta$.

We call such an ordering $<$ an *admissible ordering* on Δ.

Definition 2. Let $\{\partial_\delta X_k | \partial_\delta \in \Delta, k \in \{1, 2, ...n\}\}$ be denoted by $\{X\}$ and $<$ be an ordering on $\{X\}$ that is compatible with differentiation, i.e.

$$\partial_\alpha X_m > \partial_\beta X_k \Longrightarrow \partial_\delta\partial_\alpha X_m > \partial_\delta\partial_\beta X_k.$$

We call such an ordering $<$ an *admissible ordering* on $\{X\}$.

Let the *order* and the *class* of $\partial_{ij} X_k$ be, resp., $i + j$ and k. By fixing an admissible ordering on $\{X\}$, we can write a d-pol P in the form

$$P = I(\partial_\alpha X_k)^d + I_1(\partial_\alpha X_k)^{d-1} + lower\ terms,$$

where $\partial_\alpha X_k$ is the highest derivative occurring in P and d is the degree of P w.r.t. $\partial_\alpha X_k$. We may introduce the following terminologies to describe a d-pol.

Definition 3. Let $<$ be an admissible ordering on $\{X\}$ and P in $K\{X_1, ..., X_n\}$ but not in K,

1. The highest derivative occurring in P is called the *lead* of P, denoted by $\mathrm{ld}(P)$.
2. The order of the lead of P is called the *order* of P, denoted by $\mathrm{ord}(P)$.
3. The class of the lead of P is called the *class* of P, denoted by $\mathrm{class}(P)$.
4. The highest degree of P w.r.t. its lead is called the *degree* of P, denoted by $\deg(P)$.
5. The leading coefficient of P w.r.t. its lead is called the *initial* of P, denoted by $\mathrm{init}(P)$.
6. The formal partial derivative of P w.r.t. its lead is called the *separant* of P, denoted by $\mathrm{sep}(P)$.

Remark 1. One can easily see that $sep(P)$ is the initial of any proper derivative of a d-pol P.

1.2 Ordering of d-pols and ascending sets

We now introduce a partial ordering on $K\{X_1, X_2, ..., X_n\}$ as follows:

Definition 4. Let P and Q be non-zero d-pols, then we say that P is higher than Q or that Q is lower than P if they satisfy either (1) or (2).

1. $Q \in K$, but P not in K.
2. Both Q and P are not in K and either $\mathrm{ld}(P) > \mathrm{ld}(Q)$ or $\mathrm{ld}(P) = \mathrm{ld}(Q)$ and $\deg(P) > \deg(Q)$.

In this case we write $P \succ Q$. If neither $Q \prec P$ nor $P \prec Q$ hold, then we say that P and Q are incomparable in order and write $P \sim Q$.

Definition 5. A non-zero d-pol Q is said to be reduced w.r.t. a d-pol P that is not in K if no proper derivatives of $\mathrm{ld}(P)$ occur in Q, and either ld(P) does not occur in Q or ld(P) occurs in Q with a degree lower than deg(P).

Definition 6. An ascending set Φ is either a single non-zero element in K and is then said to be trivial or a finite sequence of d-pols none of which are in K,

$$\Phi : \quad P_1, \quad P_2 \quad , ..., \quad P_r$$

such that $P_1 \prec P_2 \prec ... \prec P_r$ and each P_i is reduced w.r.t. preceding P_j, for $j < i$.

Definition 7. Given two non-trivial ascending sets

$$\Phi_1 : \quad P_1 \quad P_2 \quad , ..., \quad P_r,$$

$$\Phi_2 : \quad Q_1 \quad Q_2 \quad , ..., \quad Q_s.$$

We shall say that Φ_2 is higher than Φ_1 or that Φ_1 is lower than Φ_2 and write $\Phi_1 \prec \Phi_2$ if either (1) or (2) below holds.

1. There is some $k \leq min(s, r)$ such that $P_i \sim Q_i$ for $i < k$ and $P_k \prec Q_k$.
2. $s < r$ and $P_i \sim Q_i$ for all $i \leq r$.

If neither $\Phi_1 \prec \Phi_2$ and $\Phi_2 \prec \Phi_1$ hold, then we say that Φ_1 and Φ_2 are incomparable in order and write $\Phi_1 \sim \Phi_2$.

Remark 2. Any non-trivial ascending set is said to be higher than any trivial one.

Definition 8. Let Ψ be a set of d-pols. A subset of Ψ is called a basic set of Ψ if it is any lowest ascending set contained in Ψ.

1.3 Remainder

Computing remainders of a d-pol w.r.t. an ascending set is a basic procedure in the char-set method. Let us start with two technical definitions

Definition 9. An *IS-product* of a non-trivial ascending set Φ is any power product of initials and separants of d-pols in Φ.

Remark 3. IS-products of a non-trivial an ascending set play a role in specifying degenerate cases for geometric theorems.

Definition 10. A d-pol R is said to be reduced w.r.t. a non-trivial ascending set Φ if R is reduced w.r.t. each d-pol in Φ.

Remainder Theorem. For any d-pol P and a non-trivial ascending set Φ

$$\Phi : F_1 \;\; F_2, ..., \;\; F_r,$$

there is an IS-product J of Φ such that

$$JP = \sum_{k,\delta_k} A_{k\delta_k} \partial_{\delta_k}(F_k) + R,$$

in which k runs over a finite subset of non-negative integers, δ_k runs over a finite subset of Δ, $A_{k\delta_k}$ is a d-pol, and R is reduced w.r.t.Φ. R is called a remainder of P w.r.t. Φ.

The above formula is then called the remainder formula which is obtained by applying pseudo division successively w.r.t. an admissible ordering on $\{X\}$. In this procedure we have to choose some of the proper derivatives of F_k as divisor polynomials.

1.4 The completion of an ascending set

Given a non-trivial ascending set Φ

$$\Phi : \;\; F_1, \;\; F_2, \;\; ..., \;\; F_r.$$

we shall now define the completion of Φ.

Definition 11.

1. For $1 \le k \le r$, derivatives of leads of F_k in Φ are called the *principal derivatives* of Φ.

2. For $1 \le k \le r$, the leads of F_k in Φ are called *leading derivatives* or *proper principal derivatives* of Φ, while other principal derivatives are called *improper derivatives* of Φ.

3. The derivatives that are not principal are called *parametric derivatives.*

4. $\mathrm{lpair}_p(\Phi)$:=$\{(i,j)|\ \partial_{ij}X_p$ *is a lead of some* F_k *in* $\Phi\}$.

5. $\max_p(\Phi) := (m_1, m_2)$, where m_i is the maximal integer of the ith coordinate of all pairs in $\mathrm{lpair}_p(\Phi)$, for $i = 1, 2$.

6. We say that (i, j) is a multiple of (i_1, j_1) if $i \geq i_1$ and $j \geq j_1$ hold , and in this case write $(i, j) \gg (i_1, j_1)$ or $(i_1, j_1) \ll (i, j)$.

7. $\mathrm{cpair}_p(\Phi) := \{(i, j) | (i_1, j_1) \ll (i, j) \ll \max_p(\Phi), (i_1, j_1) \in \mathrm{lpair}_p(\Phi)\}$

For the pair $(i, j) \in \mathrm{cpair}_p(\Phi) - \mathrm{lpair}_p(\Phi)$, let us form a remainder of $\partial_{ij} X_p$ w.r.t. Φ and denote it by $h_{ij,p}$. Then $J\partial_{ij} X_p - h_{ij,p}$ is a linear combination of derivatives of F_k in Φ, where J is a IS-product of Φ.

Definition 12. The d-pol $J\partial_{ij} X_p - h_{ij,p}$ is called a *derived d-pol* of Φ w.r.t (i, j) and p.

Let the set of all derived polynomials be

$$\{G_1, G_2, ..., G_s\}.$$

Definition 13. The sequence consisting of all F_i $(1 \leq i \leq r)$ and G_j $(1 \leq j \leq r)$ arranged in increasing order

$$(\Phi+) : \ H_1, \ H_2, \ ..., \ H_g$$

$(g = r + s)$ is called the *completion* of Φ.

Remark 4. The initials and separants of H_k in $(\Phi+)$ are all IS-products of Φ.

1.5 The integrability polynomials of an ascending set

Let a non-trivial ascending set

$$F_1, \ \ F_2, \ \ ..., \ \ F_r$$

denoted by Φ be given with its completion

$$(\Phi+) : \ H_1, \ H_2, \ ..., \ H_g.$$

Definition 14. An *M-derivative* M of Φ is a d-pol of the form

$$M = \partial_{i_1 i_2} H_k$$

with $\mathrm{ld}(H_k) = \partial_{j_1 j_2} X_p$, and $i_k = 0$ if $j_k < m_k$ where $k = 1, 2$ and $(m_1, m_2) = \max_p(\Phi)$.

Definition 15. An *M-product* of Φ is a product of d-pols, one of which is an M-derivative.

Definition 16. An *M-polynomial* of Φ is a linear sum of M-products whose coefficients are d-pols in leading and parametric derivatives alone.

Consider any d-pol P in some M-derivatives and other parametric or principal derivatives of Φ. Suppose that among the improper principal derivatives not appearing in M-products of P, the highest one is $\partial_{l_1 l_2} X_p$, then let

$$\max_p(\Phi) = (m_1, m_2),$$

$$(j_1, j_2) = (min(l_1, m_1), min(l_2, m_2)),$$

and

$$(i_1, i_2) = (l_1 - j_1, l_2 - j_2).$$

It is easy to see that $(j_1, j_2) \in \mathrm{cpair}_p(\Phi)$, and if $l_q < m_q$, then $i_q = 0$ for $q = 1, 2$. Hence there exists a H_k in $(\Phi+)$ such that $\mathrm{ld}(H_k) = \partial_{j_1 j_2} X_p$. Moreover $\partial_{i_1 i_2} H_k$ is an M-derivative with the lead $\partial_{l_1 l_2} X_p$. Then we have

$$J_1 \partial_{l_1 l_2} X_p = \partial_{i_1 i_2} H_k + U$$

where J_1 is an IS-product of Φ, and U is a d-pol in parametric and principal derivatives lower than $\partial_{l_1 l_2} X_p$. Replacing $\partial_{l_1 l_2} X_p$ in P by

$$\frac{\partial_{i_1 i_2} H_k + U}{J_1}$$

and clearing denominators, we get a d-pol $P_1 = J_1' P$, J_1' being a power of J_1, in such a form which involves the M-derivatives and the new one $M = \partial_{i_1 i_2} H_k$, and other parametric, proper and improper principal derivatives lower than $\partial_{l_1 l_2} X_p$.

Definition 17. The above procedure for obtaining $P_1 = J_1' P$ from P is called an *M-reduction* of P.

In P there may still be, besides the parametric derivatives, some leading derivatives not yet present in the M-products. Suppose that the highest such leading derivatives $\partial_{j_1 j_2} X_p$, whose corresponding d-pol in Φ is F_i, has degree $d \geq \deg(F_i) = d_i$. By performing pseudo division of $(\partial_{j_1 j_2} X_p)^d$ and F_i w.r.t $\mathrm{ld}(F_i)$, we then have

$$J_2(\partial_{j_1 j_2} X_p)^d = QF_k + V$$

where J_2 is an IS-product of Φ, Q is a d-pol, and V is a d-pol lower than $(\partial_{j_1 j_2} X_d)^{d_i}$. Replacing $(\partial_{j_1 j_2} X_p)^d$ in P by

$$\frac{QF_k + V}{J_2}$$

and clearing denominators, we get a d-pol $P_2 = J_2 P$ in such a form which involves the M-derivatives and a new one F_k, other parametric, improper, and proper principal derivatives lower than $\mathrm{ld}(F_i)^{d_i}$.

Definition 18. The above procedure for obtaining P_2 from P is called an *I-reduction* of the d-pol P.

It is clear that in applying successive M- and I-reductions we will finally arrive at a d-pol

$$JP = M + N$$

possessing the following properties:

1. J is a certain IS-product of Φ.
2. M is a M-polynomial for Φ.
3. N is a d-pol containing parametric and leading derivatives alone.
4. The leading derivatives in M and N not already appearing in the M-derivatives each have a degree less than the degree of those derivatives in the corresponding d-pol F_i of Φ.

Definition 19. In the above formula the d-pols M and N are called resp. the *M-part* and *N-part* of P.

We shall now show how to compute the integrability polynomials of Φ by means of M- and I-reductions. Consider any H_h of $(\Phi+)$ with lead

$\partial_{j_1 j_2} X_p$ such that either $j_1 < m_1$ or $j_2 < m_2$. Without loss of generality, assume that $j_1 < m_1$. Then we have

$$H_h = I(\partial_{j_1 j_2} X_p)^d + lower \;\; terms$$

where $I = \mathrm{init}(H_h)$. Moreover, we get

$$\partial_{10} H_h = S \partial_{(j_1+1) j_2} X_p + U,$$

where $S = \mathrm{sep}(H_h)$, and U is a d-pol lower than $\partial_{(j_1+1) j_2} X_p$. As $j_1 < m_1$, it is clear that

$$(j_1 + 1, j_2) \in \mathrm{cpair}_p(\Phi) - \mathrm{lpair}_p(\Phi).$$

Thus $\partial_{(j_1+1) j_2} X_p$ is the lead of some H_k in $(AS+)$. We then have

$$H_k = I^{'} \partial_{(j_1+1) j_2} X_p + V$$

where $I^{'} = \mathrm{init}(H_k)$ and V is a d-pol lower than $\partial_{(j_1+1) j_2} X_p$. It follows that

$$I^{'} \partial_{10} H_h - S H_k = W_1$$

where W_1 is a d-pol lower than $\partial_{(j_1+1) j_2} X_p$.

We can form W_2 in the same way if $j_2 < m_2$.

Definition 20. The N-part of the above d-pol W_1 (resp., W_2) is called the *integrability d-pol* of Φ of index 1 (resp., index 2)corresponding to H_h.

Definition 21. A non-trivial ascending set is said to be *passive* if all its integrability d-pols are zero.

Passivity Theorem If an ascending set Φ is passive, then all derivatives of any d-pol in $(\Phi+)$, when multiplied by some IS-product of Φ, have their N-parts equal to zero. Moreover, any such derivative, say P, can be written in the form

$$JP = J^{'} M + R$$

where M is an M-derivative having the same lead as that of the given derivative P, while R is an M-polynomial in which all M-derivatives are lower than P.

1.6 The Char-sets of a differential polynomial set

Let Ψ be a finite set of d-pols and $<$ an admissible ordering on $\{X\}$. $Zero(\Psi)$ denotes the differential algebraic set defined by Ψ. For any d-pol G, $Zero(\Psi/G)$ denotes the subset of $Zero(\Psi)$ for which $G \neq 0$. By the following algorithm `Charset`, we can obtain a passive ascending set Φ such that the remainders of all d-pols in Ψ with respect to Φ are zero. This algorithm basically consists of pseudo division, and the M- and I-reductions introduced in the previous sections.

Algorithm `Charset`

INPUT: Ψ (a finite set of d-pols).
OUTPUT: Φ (an ascending set w.r.t. $<$).

(1) [Initialization]
 $\Psi_0 := \Psi$;
 BS_0:= a basic set for Ψ_0;
 RS_0:= the set of all non-trivial remainders of d-pols in Ψ_0 w.r.t. BS_0;
 HS_0:= the set of all non-trivial integrability conditions for Ψ_0
 $i := 0$;
(2) [Loop]
 While $RS_i \neq \emptyset$ or $HS_i \neq \emptyset$ do
  $i := i + 1$;
  $\Psi_i := \Psi_{i-1} \cup RS_{i-1} \cup HS_{i-1}$;
  BS_i:= a basic set for Ψ_i;
  RS_i:= the set of all non-trivial remainders of d-pols in Ψ_i w.r.t. BS_i;
  HS_i:=the set of all non-trivial integrability conditions for Ψ_i
 end{while}
(3) [Done]
 $\Phi := BS_i$;
 Return Φ;

Remark 5. We exit from this algorithm as long as a non-zero element in K appears in either RS_i or HS_i, for $i = 0, 1, \ldots$. In this case the input system Ψ is inconsistent.

Remark 6. In this algorithm the set of d-pols Ψ is enlarged to Ψ_i for $i = 1\,2\ldots$, while the $Zero(\Psi_i) = Zero(\Psi)$ holds throughout the while-loop since each d-pol in RS_{i-1} or HS_{i-1} can be expressed as a linear combination of d-pols in PS_{i-1} and their derivatives.

It can be shown that the basic-sets

$$BS_0 \succ BS_1 \ \ ...$$

are decreasing in order so that the construction should end in a finite number of steps and at a certain stage t we should have both $RS_t = \emptyset$ and $HS_t = \emptyset$.

Definition 22. The corresponding ascending set Φ in Algorithm `Charset` is called a passive (differential) char-set of the given d-pol-set Ψ.

Theorem (Well-Ordering Principle) Let Φ be a passive char-set of the given differential polynomial set Ψ, I_i and S_i the initials and separants of differential polynomials in Φ, and J some IS-product of Φ. Then

$$Zero(\Phi/J) \subset Zero(\Psi) \subset Zero(\Phi), \qquad (I)$$

$$Zero(\Psi) = Zero(\Phi/J) \bigcup (\cup_i Zero(\Psi_i')) \bigcup (\cup_i Zero(\Psi_i'')). \quad (II)$$

In these formulas $\Psi_i' = \Psi \cup \{I_i\}$ and $\Psi_i'' = \Psi \cup \{S_i\}$.

Remark 7. Φ must be passive by the assumption of the well-ordering principle. In fact, it suffices to derive relation (I) and (II) if $RS_k = \emptyset$, for some non-negative integer k in the Algorithm `Charset`.

1.7 A basic principle of MTP

The char-set method is able to prove the theorems whose hypothesis and conclusion can be formulated in terms of d-pols. Hence we have the following definitions.

Definition 23. A theorem consists of a d-pol set called the *hypothesis set* and a d-pol called the *conclusion d-pol.*

Definition 24 Let the hypothesis set and the conclusion polynomial of a theorem T be resp. H and C. Then we say

1. T is *true* if

$$Zero(H) \subset Zero(C).$$

2. T is *generically true* under non-degeneracy conditions

$$G_i \neq 0.$$

for degenerate polynomials G_i if

$$Zero(H/\prod G_i) \subset Zero(C).$$

Remark 8. A zero in $Zero(H)$ is nothing but a geometrical configuration verifying the hypothesis of the theorem T and $Zero(H)$ is just the algebraic differential set of all such geometrical configurations.

Using the notation of Definition 24, we state the following principle.

Principle of MTP (weak form) If the remainder R of C w.r.t. a char-set of HYP is identical to 0, then the theorem T with hypothesis set H is generically true under the non-degeneracy conditions $I_i \neq 0$ and $S_i \neq 0$ where I_i and S_i are the initials and separants of this char-set, respectively.

There are three principles of MTP corresponding to different forms of zero structure theorems for an algebraic differential set. The examples shown in the following sections are only based on the principle mentioned above. Another way to prove theorems mechanically in differential geometries is based on the calculation of differential dimension of differential quasi-algebraic sets, cf. [Ferro & Gallo, 1990].

2 Studying the fundamental equations of surface theory by the char-set method

In this section we shall try to compute a characteristic set of the fundamental equations of surfaces. To do this we first introduce an admissible ordering on the variables to be handled and then apply the algorithm `Charset` to these equations. As shown below, although it is difficult to obtain a char-set for the general form of the fundamental equations of surfaces, some interesting results can still be obtained during this computation.

2.1 The fundamental equations of surface theory

Suppose that a surface S is generated by the movement of the tip of a position vector

$$\vec{r} = \vec{r}(u,v) = (x(u,v), y(u,v), z(u,v))$$

in which $x(u,v)$, $y(u,v)$, and $z(u,v)$ are functions of u and v possessing as many derivatives as may be required. The first fundamental form is defined as follows:

$$I = Edu^2 + 2Fdudv + Gdv^2$$

where $E = \frac{\partial \vec{r}}{\partial u} \cdot \frac{\partial \vec{r}}{\partial u}$, $F = \frac{\partial \vec{r}}{\partial u} \cdot \frac{\partial \vec{r}}{\partial v}$ and $G = \frac{\partial \vec{r}}{\partial v} \cdot \frac{\partial \vec{r}}{\partial v}$. Here " $\cdot$" means the dot product of two vectors.

When the tangent vectors $\frac{\partial \vec{r}}{\partial v}$ and $\frac{\partial \vec{r}}{\partial v}$ at any point $\vec{r}(u,v)$ are not parallel, we may find a unit normal vector $\vec{n}(u,v)$, which is perpendicular to the tangent plane at the point on S, by computing the vector product of partial derivative vectors $\frac{\partial \vec{r}}{\partial v}$ and $\frac{\partial \vec{r}}{\partial v}$ at the point, that is,

$$\vec{n}(u,v) = \frac{\frac{\partial \vec{r}}{\partial u} \times \frac{\partial \vec{r}}{\partial v}}{\mid \frac{\partial \vec{r}}{\partial u} \times \frac{\partial \vec{r}}{\partial v} \mid}$$

The order in which we take the vector product determines the direction of $\vec{n}(u,v)$.

The vectors $\frac{\partial \vec{r}}{\partial u}$, $\frac{\partial \vec{r}}{\partial v}$ and $\vec{n}(u,v)$ constitute a moving frame on S denoted by $[\vec{r}; \vec{r}_u, \vec{r}_v, \vec{n}]$. The second fundamental form is given by

$$II = Ldu^2 + 2Mdudv + Ndv^2$$

where $L = -\frac{\partial \vec{r}}{\partial u} \cdot \frac{\partial \vec{n}}{\partial u}$, $M = -\frac{\partial \vec{r}}{\partial u} \cdot \frac{\partial \vec{n}}{\partial v} = -\frac{\partial \vec{r}}{\partial v} \cdot \frac{\partial \vec{n}}{\partial u}$, and $N = -\frac{\partial \vec{r}}{\partial v} \cdot \frac{\partial \vec{n}}{\partial v}$.

By differentiating the frame $[\vec{r}; \vec{r}_u, \vec{r}_v, \vec{n}]$, we may obtain the fundamental equations of surface theory. Let $u = u^1$, $v = u^2$, $\frac{\partial \vec{r}}{\partial u} = \vec{r}_1$, and $\frac{\partial \vec{r}}{\partial v} = \vec{r}_2$. Then we may write these equations as follows:

$$(2.1) \qquad \begin{cases} \frac{\partial \vec{r}}{\partial u^\alpha} = \vec{r}_\alpha & \alpha = 1\ 2 \\ \frac{\partial \vec{r}_\alpha}{\partial u^\beta} = \sum_{\delta=1}^{2} \Gamma^\delta_{\alpha\beta} \vec{r}_\delta + b_{\alpha\beta} \vec{n} & \alpha,\ \beta = 1\ 2 \\ \frac{\partial \vec{n}}{\partial u^\alpha} = -\sum_{\delta=1}^{2} b^\delta_\alpha \vec{r}_\delta & \alpha = 1\ 2 \end{cases}$$

where the $\Gamma^\delta_{\alpha\beta}$'s are the Christoffel symbols of the second kind which are rational functions of E, F, G and their derivatives, $b_{\alpha\beta}$ and b^δ_α are rational functions of L, M, N, E, F, and G. For the definitions of $\Gamma^{\delta}_{\alpha\beta}$, $b_{\alpha\beta}$ and b^{δ}_{α}, please refer to [Carmo, 1976]. One may observe that the denominators of these rational functions are $EG - F^2$, which is non-zero by its geometric meaning.

2.2 Computing char-sets of the fundamental equations of surface theory

There are two reasons for computing a passive char-set of the fundamental equations of surface. The first is to derive Gauss's theorem mechanically, and the second is to find the general passive char-set of the fundamental equations since we often put some of the fundamental equations or their integrability conditions into the hypothesis set of the theorem to be mechanically proved.

The Gauss's Theorem may be stated as follows:

Theorem (Theorema Egregium) The Gaussian curvature $\frac{LN-M^2}{EG-F^2}$ is determined by the first fundamental form of surface S.

In order to compute the char-set of the fundamental equations, we should first translate (2.1) into d-pols and arrange the variables occurring in (2.1) in a proper order. Since all the coefficients in (2.1) are rational functions of L, M, N, E, F, G and their derivatives, we can order L, M, N, E, F, G and the vectors $\vec{r}$, $\vec{r}_u$, $\vec{r}_v$, $\vec{n}$ as well as their derivatives.

Let

$$\begin{array}{lll} E = X_1, & F = X_2, & G = X_3, \\ L = X_{24} & M = X_{25}, & N = X_{26}, \\ \vec{r}_u = X_{32}, & \vec{r}_v = X_{33}, & \vec{n} = X_{34}. \end{array}$$

Furthermore, let Λ_1 be the set consisting of X_1, X_2, X_3 and their derivatives, Λ_2 the set consisting of X_{24}, X_{25}, X_{26} and their derivatives, and Λ_3 the set consisting of X_{32}, X_{33}, X_{34} and their derivatives. We introduce an admissible ordering on $\Lambda = \Lambda_1 \cup \Lambda_2 \cup \Lambda_3$ as follows:

1. For any two pairs of non-negative integers, (i, j) and (l, k), $\partial_{ij} > \partial_{kl}$ iff either $i + j > k + l$ or $i + j = k + l$ and $j > l$.

2. For any $\partial_{ij}X_p, \partial_{kl}X_q \in \Lambda_i$, where $i = 1, 2, 3$, $\partial_{ij}X_p > \partial_{kl}X_q$ iff either $\partial_{ij} > \partial_{kl}$ or $\partial_{ij} = \partial_{kl}$ and $p > q$.

3. For any $\partial_{ij}X_p \in \Lambda_m$ and $\partial_{kl}X_q \in \Lambda_n$, $\partial_{ij}X_p > \partial_{kl}X_q$ iff $m > n$.

One may easily verify that such an ordering is admissible.

We can now rewrite (2.1) in terms of d-pols in Λ. After removing trivial and extraneous equations, we have

$$
(2.2)\quad \begin{cases}
p_1 = & (\partial_{01}X_{34})(X_3X_1 - X_2^2) + X_{33}X_{26}X_1 - X_{33}X_{25}X_2 \\
& -X_{32}X_{26}X_2 + X_{32}X_{25}X_3 \\
p_2 = & (\partial_{10}X_{34})(X_3X_1 - X_2^2) + X_{33}X_{25}X_1 - X_{33}X_{24}X_2 \\
& -X_{32}X_{25}X_2 + X_{32}X_{24}X_3 \\
p_3 = & 2(\partial_{01}X_{33})(X_3X_1 - X_2^2) - 2X_{34}X_{26}(X_3X_1 - X_2^2) \\
& -X_{33}((\partial_{01}X_3)X_1 + (\partial_{10}X_3)X_2 - 2(\partial_{01}X_2)X_2) \\
& +X_{32}((\partial_{01}X_3)X_2 + (\partial_{10}X_3)X_3 - 2(\partial_{01}X_2)X_3) \\
p_4 = & 2(\partial_{10}X_{33})(X_3X_1 - X_2^2) - 2X_{34}X_{25}(X_3X_1 - X_2^2) \\
& -X_{33}((\partial_{10}X_3)X_1 - (\partial_{01}X_1)X_2) \\
& +X_{32}((\partial_{10}X_3)X_2 - (\partial_{01}X_1)X_3) \\
p_5 = & 2(\partial_{01}X_{32})(X_3X_1 - X_2^2) - 2X_{34}X_{25}(X_3X_1 - X_2^2) \\
& -X_{33}((\partial_{10}X_3)X_1 - (\partial_{01}X_1)X_2) \\
& +X_{32}((\partial_{10}X_3)X_2 - (\partial_{01}X_1)X_3) \\
p_6 = & 2(\partial_{10}X_{32})(X_3X_1 - X_2^2) - 2X_{34}X_{24}(X_3X_1 - X_2^2) \\
& -X_{33}(2(\partial_{10}X_2)X_1 - (\partial_{01}X_1)X_1 - (\partial_{10}X_1)X_2) \\
& +X_{32}((2\partial_{10}X_2)X_2 - (\partial_{01}X_1)X_2 - (\partial_{10}X_1)X_3)
\end{cases}
$$

According to the ordering introduced before, (2.2) is itself an ascending set. We then compute the derived d-pols of (2.2). Note that X_{32}, X_{33} and X_{34} are linearly independent vectors which represents the moving frame $\vec{r}_u$, $\vec{r}_v$ and $\vec{n}$. Therefore, during the computation we may replace any linear homogeneous d-pol in X_{32}, X_{33} and X_{34} by the d-pols obtained from the coefficients of this d-pol w.r.t. X_{32}, X_{33} and X_{34}. Hence we get a d-pol, say F, in the from

$$F = X_{24}X_{26} - X_{25}^2 + F^*$$

where F^* is a d-pol in $\mathbf{Q}[\Lambda_1]$. From Remark 6 in Section 1.6 it follows that F vanishes on the zero set defined by (2.2). In other words, Theorema Egregium has been derived mechanically. Moreover, it is easy to check that $F = 0$ gives us the formula for computing the Gaussian curvature by means of E, F and G and their derivatives.

The intermediate d-pols of this derivation are too lengthy to be shown here. For more details, please refer to [Li, 1991].

We are able to obtain the completion of (2.2) which consists of 9 d-pols. In accordance with our general method described in Section 1, we should compute integrability d-pols of (2.2). But we meet some intermediate polynomials that are too big to manipulate on our computer.

Consider a simple case. Let $X_2 = X_{25} = 0$ ($M = F = 0$), i.e. we suppose that there is no umbilicus point on S. Then the fundamental equations can be expressed in terms of X_1, X_3, X_{24}, X_{26}, X_{32}, X_{33} and X_{34} as follows:

$$(2.3)\quad \begin{cases} pp_1 = & (\partial_{01}X_{34})X_3 + X_{33}X_{26} \\ pp_2 = & (\partial_{10}X_{34})X_1 + X_{32}X_{24} \\ pp_3 = & 2(\partial_{01}X_{33})X_3X_1 - 2X_{34}X_{26}X_3X_1 \\ & -X_{33}(\partial_{01}X_3)X_1 - X_{32}(\partial_{10}X_3)X_3 \\ pp_4 = & 2(\partial_{10}X_{33})X_3X_1 - X_{33}(\partial_{10}X_3)X_1 - X_{32}(\partial_{01}X_1)X_3 \\ pp_5 = & 2(\partial_{01}X_{32})X_3X_1 - X_{33}(\partial_{10}X_3)X_1 - X_{32}(\partial_{01}X_1)X_3 \\ pp_6 = & 2(\partial_{10}X_{32})X_3X_1 - 2X_{34}X_{24}X_3X_1 \\ & +X_{33}(\partial_{01}X_1)X_1 - X_{32}(\partial_{10}X_3)X_1 \end{cases}$$

In the same way we get the derived polynomials of (2.3) as follows:

$$(2.4)\quad \begin{cases} pp_{10} = & 2(\partial_{10}X_{26})X_3X_1 - X_{26}(\partial_{10}X_3)X_1 - X_{24}(\partial_{10}X_3)X_3 \\ pp_{11} = & 4X_{26}X_{24}X_3X_1 + 2(\partial_{20}X_3)X_3X_1 - (\partial_{01}X_3)(\partial_{01}X_1)X_1 \\ & -(\partial_{10}X_3)^2X_1 - (\partial_{10}X_3)X_3(\partial_{10}X_1) + 2X_3(\partial_{02}X_1)X_1 \\ & -X_3(\partial_{01}X_1)^2 \\ pp_{12} = & 8(\partial_{01}X_{24})X_{24}X_3^2X_1 - 4X_{24}^2X_3^2(\partial_{01}X_1) \\ & +2(\partial_{20}X_3)X_3(\partial_{01}X_1)X_1 - (\partial_{01}X_3)(\partial_{01}X_1)^2X_1 \\ & -(\partial_{10}X_3)^2(\partial_{01}X_1)X_1 - (\partial_{10}X_3)X_3(\partial_{01}X_1)(\partial_{10}X_1) \\ & +2X_3(\partial_{02}X_1)(\partial_{01}X_1)X_1 - X_3(\partial_{01}X_1)^3 \end{cases}$$

Please notice that pp_{11} is the formula for computing the Gaussian curvature by means of X_1, X_3 and their derivatives in the case $X_2 = X_{25} = 0$. During the computation of the integrability d-pols of (2.3) with derived polynomials (2.4), it is interesting to note that we obtained an intermediate d-pol, P, with 434 terms. This d-pol can be written as

$$P = X_{24}P^*,$$

in which P^* takes X_{24} as its lead with $\deg(P^*) = 4$, the coefficients of P w.r.t. X_{24} are d-pols involving only X_1, X_2, and X_3. It is clear that P vanishes on $Zero((2.3))$. In consideration of pp_{11} and P, we can conclude that the second fundamental form is *algebraically determined* by the first fundamental form in case there is no umbilic point on S.

Remark 9. If X_{24} is identical to zero, then S is developable.

Unfortunately, the passive char-set of (2.3) has not yet been obtained since we ran out of memory on a Sun-3/50 using REDUCE.

3 Examples

In order to control the size of intermediate expressions, the following strategies are quite helpful.

> Formulate the hypothesis and conclusion of a theorem by means of moving frames on surfaces and put Gauss-Codazzi equations into the hypothesis set.
>
> In the algorithm `Charset`, supposing that RS_i is empty at some stage i, then we try to compute a remainder of the conclusion d-pol w.r.t. the basic set BS_i. If this d-remainder is identical to 0, then this theorem is generically true under some non-degeneracy conditions (See Remark 6 in Section 1.6).

The following examples are chosen from [Chen, 1990].

Example 1. Show that, if a surface $\vec{r} = \vec{r}(u, v)$ has two unequal constant principal curvatures, then the surface is a cylinder.

We may choose the parameters (u, v) as the lines of curvatures since the principal curvatures at every point on the surface are unequal. Hence the first and second fundamental forms are

$$I = Edu^2 + Gdv^2 \quad and \quad II = Ldu^2 + Ndv^2$$

The conclusion can be expressed as

1. v-curves are straight lines, that is,

$$\partial_{01}\vec{r} \times \partial_{02}\vec{r} = 0.$$

2. the curvature of u-curves is a constant, that is,

$$\partial_{10}\left(\frac{|\ \partial_{10}\vec{r} \times \partial_{20}\vec{r}\ |}{|\ \partial_{10}\vec{r}\ |^3}\right) = 0$$

and

$$\partial_{01}(\frac{|\ \partial_{10}\vec{r} \times \partial_{20}\vec{r}\ |}{|\ \partial_{10}\vec{r}\ |^3}) = 0$$

3. the torsion of u-curves is zero, that is,

$$(\partial_{10}\vec{r} \times \partial_{20}\vec{r}) \cdot \partial_{30}\vec{r} = 0.$$

Here $|\quad|$, $\cdot$ and $\times$ mean the length of a vector, dot product, and vector product , respectively.

From the assumption of this example we obtain the hypothesis set as follows

$$(3.1)\quad \begin{cases} p_1 = & num(\partial_{10}(\frac{X_{24}}{X_1})) = 0 \\ p_2 = & num(\partial_{01}(\frac{X_{24}}{X_1})) = 0 \\ p_3 = & num(\partial_{10}(\frac{X_{26}}{X_3})) = 0 \\ p_4 = & num(\partial_{01}(\frac{X_{26}}{X_3})) = 0 \\ p_5 = & 2(\partial_{10}X_{26})X_3X_1 - X_{26}(\partial_{10}X_3)X_1 - X_{24}(\partial_{10}X_3)X_3 \\ p_6 = & 4X_{26}X_{24}X_3X_1 + 2(\partial_{20}X_3)X_3X_1 - (\partial_{01}X_3)(\partial_{01}X_1)X_1 \\ & -(\partial_{10}X_3)^2X_1 - (\partial_{10}X_3)X_3(\partial_{10}X_1) + 2X_3(\partial_{02}X_1)X_1 \\ & -X_3(\partial_{01}X_1)^2 \\ p_7 = & 8(\partial_{01}X_{24})X_{24}X_3^2X_1 - 4X_{24}^2X_3^2(\partial_{01}X_1) \\ & +2(\partial_{20}X_3)X_3(\partial_{01}X_1)X_1 - (\partial_{01}X_3)(\partial_{01}X_1)^2X_1 \\ & -(\partial_{10}X_3)^2(\partial_{01}X_1)X_1 - (\partial_{10}X_3)X_3(\partial_{01}X_1)(\partial_{10}X_1) \\ & +2X_3(\partial_{02}X_1)(\partial_{01}X_1)X_1 - X_3(\partial_{01}X_1)^3 \end{cases}$$

in which $num(R)$ means the numerator of the rational expression R, p_1, p_2, p_3 and p_4 imply that two principal curvatures of this surface are constants, and p_5, p_6, p_7 are the Gauss-Codazzi equations of the surface.

By means of the fundamental equations of surface theory, the conclusion can be expressed in terms of $[\vec{r}; \vec{r_u}, \vec{r_v}, \vec{n}]$ and Christoffel symbols of the second kind. Hence we have the following conclusion polynomials:

$$\begin{aligned} c_1 = &\ X_{15} \\ c_2 = &\ X_{26} \\ c_3 = &\ 2(\partial_{10}X_{24})X_{24}X_1^2 - 2X_{24}^2(\partial_{10}X_1)X_1 \\ & +2(\partial_{10}X_{16})X_{16}X_1 - 3X_{16}^2(\partial_{10}X_1) \\ c_4 = &\ 2(\partial_{01}X_{24})X_{24}X_1^2 - 2X_{24}^2(\partial_{01}X_1)X_1 \\ & +2(\partial_{01}X_{16})X_{16}X_1 - 3X_{16}^2(\partial_{01}X_1) \\ c_5 = &\ \sqrt{X_1}X_{29}X_{24}^2X_3 + \sqrt{X_3}(\partial_{10}X_{24})X_{16} \\ & -\sqrt{X_1}X_{24}X_{18}X_{16}X_3 - \sqrt{X_1}X_{24}(\partial_{01}X_{16})X_3 \\ & -\sqrt{X_1}X_{24}X_{16}X_{12}X_3 + \sqrt{X_3}X_{24}X_{16}X_{12} \end{aligned}$$

in which $X_{12} = \Gamma^1_{11}$, $X_{15} = \Gamma^1_{22}$, $X_{16} = \Gamma^2_{11}$ and $X_{18} = \Gamma^2_{21}$, moreover, we have $X_{29} = b^1_2 = 0$ since $M = F = 0$. In the actual computation we may treat the square root $\sqrt{X}$ as a new indeterminate satisfying $\sqrt{X}^2 - X = 0$. c_1 and c_2 mean that v-curves are straight lines, c_3 and c_4 imply that the curvatures of all u-curves are a single constant, and c_5 implies that u-curves are planar curves.

Let us take the admissible ordering defined in Section 2. We may obtain the following char-set of the hypothesis set in accordance with the algorithm `Charset`

$$(3.2) \quad \begin{cases} p_1 = & X_{26} \\ p_2 = & \partial_{01} X_{24} \\ p_3 = & (\partial_{10} X_{24}) X_1 - X_{24} (\partial_{10} X_1) \\ p_4 = & \partial_{10} X_3 \\ p_5 = & \partial_{01} X_1 \end{cases}$$

All the remainders are identical to zero w.r.t. (3.2). In computing the char-set we remove some factors, e.g. $X_{26}X_1 - X_{24}X_3$, which are non-zero because the two principal curvatures are assumed to be unequal.

Remark 10. We get $p_1 = X_{24}X_{26}$ from the algorithm `Charset`. If $X_{24} = 0$, then we may swap the positions of u and v in the conclusions.

Example 2. Assume that both S_1 and S_2 do not contain any umbilici and have non-zero Gaussian curvatures. There is a map ϕ between S_1 and S_2 which preserves the normal curvature with every tangent at every point. Prove that there exists a rigid motion such that S_1 coincides with S_2.

Suppose that the principal directions at a point on S_1 is in the direction of the parameter lines $u = constant$ and $v = constant$. Hence the first and second fundamental forms of S_1 are, resp.,

$$I_1 = E_1 du^2 + G_1 dv^2$$

and

$$II_1 = L_1 du^2 + N_1 dv^2.$$

Under the correspondence of ϕ, (u, v) is also a regular parametric system of S_2. Furthermore the u-curve and the v-curve of S_2 are also the lines of curvature since ϕ preserves principal curvatures at every point. Thus the first and second fundamental forms of S_2 are, resp.,

$$I_2 = E_2 du^2 + G_2 dv^2$$

and

$$II_2 = L_2 dv^2 + N_2 dv^2.$$

We can then formulate the hypothesis under such a choice of parameters as:

$$\frac{E_1 du^2 + G_1 dv^2}{L_1 du^2 + N_1 dv^2} = \frac{E_2 du^2 + G_2 dv^2}{L_2 du^2 + N_2 dv^2}. \tag{3.3}$$

Let $E_1 = X_1$, $G_1 = X_2$, $E_2 = X_3$, $G_2 = X_4$, $L_1 = X_5$, $N_1 = X_6$, $L_2 = X_7$, and $N_2 = X_8$, then the hypothesis set is as follows

$$\left\{ \begin{array}{ll} p_1 = & X_7 X_1 - X_5 X_3 \\ p_2 = & X_8 X_2 - X_6 X_4 \\ p_3 = & X_6 X_1 + X_7 X_2 - X_6 X_3 - X_5 X_4 \\ p_4 = & X_6(\partial_{01} X_1) X_1 - 2(\partial_{01} X_5) X_2 X_1 + X_5 X_2 (\partial_{01} X_1) \\ p_5 = & 2(\partial_{10} X_6) X_2 X_1 - X_6 (\partial_{10} X_2) X_1 - X_5 (\partial_{10} X_2) X_2 \\ p_6 = & X_8 (\partial_{01} X_3) X_3 - 2(\partial_{01} X_7) X_4 X_3 + X_7 X_4 (\partial_{01} X_3) \\ p_7 = & 2(\partial_{10} X_8) X_4 X_3 - X_8 (\partial_{10} X_4) X_3 - X_7 (\partial_{10} X_4) X_4 \\ p_8 = & 4 X_6 X_5 X_2 X_1 + 2(\partial_{20} X_2) X_1 - (\partial_{01} X_2)(\partial_{01} X_1) X_1 \\ & -(\partial_{10} X_2)^2 X_1 - (\partial_{10} X_2) X_2 (\partial_{10} X_1) \\ & +2 X_2 (\partial_{02} X_1) X_1 - X_2 (\partial_{01} X_1)^2 \\ p_9 = & 4 X_8 X_7 X_4 X_3 + 2(\partial_{20} X_4) X_4 X_3 - (\partial_{01} X_4)(\partial_{01} X_3) X_3 \\ & -(\partial_{10} X_4)^2 X_3 - (\partial_{10} X_4) X_4 (\partial_{10} X_3) \\ & +2 X_4 (\partial_{02} X_3) X_3 - X_4 (\partial_{01} X_3)^2 \end{array} \right. \tag{3.4}$$

where p_1, p_2, and p_3 are equivalent to (3.3), p_4, p_5, p_8 and p_6, p_7, p_9 are the Gauss-Codazzi equations of S_1 and S_2 respectively. By the fundamental theorem of the surface theory, the conclusions expressed in terms of $X's$ are

$$\begin{array}{ll} c_1 = & X_8 - X_6 \\ c_2 = & X_7 - X_5 \\ c_3 = & X_4 - X_2 \\ c_4 = & X_3 - X_1 \end{array} \tag{3.5}$$

A char-set of the hypothesis set consists of seven d-pols of which the largest one has 22 terms. The remainders of all c_i's are identical to zero w.r.t. the char-set. In the computation we remove all the factors X_5, X_6, X_7, and X_8 since the Gaussian curvatures of S_1 and S_2 are non-zero.

Example 3 If T is an isometric correspondence between two planes, then T is a rigid motion.

Assume that the two planes are P_1 and P_2 with the first fundamental forms $I_1 = du^2+dv^2$ and $I_2 = (dX_1)^2+(dX_2)^2$ respectively. The mapping between these two parametric coordinates of P_1 and P_2 induced by T is

$$(3.7) \qquad \begin{cases} X_1 = & X_1(u,v) \\ X_2 = & X_2(u,v) \end{cases}$$

Then the hypothesis set is made up of the following equations.

$$(3.6) \qquad \begin{cases} p_1 = & (\partial_{10}X_2)^2 + (\partial_{10}X_1)^2 - 1 \\ p_2 = & (\partial_{01}X_2)^2 + (\partial_{01}X_1)^2 - 1 \\ p_3 = & (\partial_{10}X_2)(\partial_{01}X_2) + (\partial_{10}X_1)(\partial_{01}X_1) \end{cases}$$

with a non-degenerate condition

$$\frac{\partial(X_1, X_2)}{\partial(u,v)} \neq 0$$

The conclusion d-pols are the nine d-pols

$$c_1 = (\partial_{10}X_1)^2 + (\partial_{10}X_2)^2 - 1,$$

$$c_2 = (\partial_{01}X_1)^2 + (\partial_{01}X_2)^2 - 1,$$

$$c_3 = (\partial_{10}X_2)(\partial_{10}X_1) + (\partial_{01}X_2)(\partial_{01}X_1),$$

$$c_4 = \partial_{20}X_1 \quad c_5 = \partial_{02}X_1 \quad c_6 = \partial_{11}X_1,$$

$$c_7 = \partial_{20}X_2 \quad c_8 = \partial_{02}X_2 \quad c_9 = \partial_{11}X_2,$$

where c_1, c_2 and c_3 imply that the Jacobian matrix of $X_1(u,v)$ and $X_2(u,v)$ is orthogonal. $c_4 \ldots c_9$ imply that each entry of this matrix is a constant.

The char-set of the hypothesis set is $\{(\partial_{01}X_1)^2+(\partial_{10}X_1)^2-1, \partial_{20}X_1, p_1, p_3\}$, in which $\partial_{20}X_1$ is a factor of the following d-pol that is obtained by computing integrability d-pols

$$(\partial_{10}X_1)(\partial_{20}X_1)((\partial_{10}X_1)(\partial_{01}X_2) - (\partial_{10}X_2)(\partial_{01}X_1))$$

The third factor is non-zero since it is just the non-degenerate condition. If the first one is zero, then we get the hypothesis set as follows:

$$(3.9) \qquad \begin{cases} (\partial_{01}X_2)^2 - 1 & = 0 \\ \partial_{10}X_2 & = 0 \\ \partial_{10}X_1 & = 0 \\ (\partial_{10}X_1)^2 - 1 & = 0 \end{cases}$$

Therefore, the theorem holds immediately.

Acknowledgement

The author would like to thank Mark J. Encarnación and the anonymous referee for their help and comments.

References

[Carmo, 1976] Manfredo P. do Carmo *Differential Geometry of Curves and Surfaces, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, (1976) ISBN 0-13-212589-7.*

[Chen, 1990] Chen Weihua, *A First Course in Differential Geometry, Beijing University Press, (1990) (in Chinese).*

[Chou & Gao, 1989] Chou, S. C. & Gao Xiaoshan, *Mechanical Theorem Proving in Differential Geometry, I. Space Curves, MM-Res. Preprints (1989), No.4, 109-124.*

[Chou & Gao, 1990] Chou S. C. & Gao Xiaoshan, *Mechanical Theorem Proving in Differential Geometry, II. Bertrand Curves, TR-90-09, Computer Science Department, The Univ. of Texas at Austin, April, 1990.*

[Ferro & Gallo, 1990] Giuseppa Carrá Ferro & Giovanni Gallo, *A procedure to Prove Statements in Differential Geometry, Journal of Automated Reasoning Vol. 6, No. 2, June 1990, 203-210.*

[Li, 1991] Ziming Li, *Mechanical Theorem-Proving of the Local Theory of Surfaces, MM-Res. Preprints (1991) No. 6, 102-120.*

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

[Wu, 1989] Wu Wen-tsun, *On the Foundation of Algebraic Differential Geometry, Systems Sciences and Mathematical Sciences Vol. 2, No. 4, Oct. (1989), 290-312.*

[Wu, 1991] Wu Wen-tsun, *Mechanical Theorem Proving of Differential Geometries and Some of its Applications in Mechanics, Journal of Automated Reasoning Vol. 7, No. 2 1991, 171-192.*