MECHANICAL THEOREM PROVING IN RIEMANN GEOMETRY*

Shang-Ching Chou and Xiao-Shan Gao†

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

TR-90-03 February 1990

Abstract

This paper studies the mechanical theorem proving in Riemann geometry using algebraic methods. We establish a theorem which can reduce a geometry statement in Riemann geometry to several substatements which are much easier to prove. For a class of constructive geometry statements, we present a method to generate sufficient non-degenerate conditions in geometric form mechanically. We also prove that an irreducible constructive statement is generally true if and only if it is universally true under the non-degenerate conditions generated by our method. More than 20 theorems other than those in projective geometry have been proved by our program.

Keywords: Mechanical geometry theorem proving, Wu's method, the Gröbner basis method, universally true, generally true, Riemann geometry, projective space, geometry statement of constructive type, non-degenerate conditions.

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

† On leave from Institute of Systems Science, Academia Sinica, Beijing.

1. Introduction

In [WU1], Wu Wen-tsün introduced an algebraic method which can be used to prove quite non-trivial theorems in Euclidean geometry that do not involve betweenness. Hundreds of theorems from Euclidean geometry have been proved with Wu's method [CH2], [GW1]. Quite a few theorems from various non-Euclidean geometries have also been proved by the method [CK1], [GA1]. Inspired by Wu's work, people also presented methods based on the Gröbner basis method to prove the same class of geometry theorems which Wu's method addresses [CH2, KA1, KU1]. From theoretic point of view, Wu's method as well as the Gröbner basis method can also be used to prove theorems in other elementary geometries including Riemann geometry, as showed by Wu in [WU2]. But to develop an efficient and comparatively complete prover for a special geometry, a lot of detailed work still need to be done. In this paper, we establish a theorem which can be used to reduce the proof of a geometry statement in Riemann geometry to some special cases which are much easier to prove. We also present a method to generate sufficient non-degenerate conditions in geometric form for a class of constructive geometry statements. These results make the mechanical theorem proving in Riemann geometry much clearer and easier.

We adopt a model for Riemann geometry and propose the general geometry statements which can be mechanically proved by Wu's or the Gröbner basis method. In this model the algebraic translation of a geometry statement involving segment congruence is always reducible and the proof of the statement can be reduced to many subcases. We prove a theorem which states that we need only to check some of the subcases. In most of the examples we encountered we need only check one of the subcases.

In the usual description of a geometry statement, necessary non-degenerate conditions for the statement to be true are usually not given explicitly and some of them are not easy to find. There are two approaches to dealing with these implicit non-degenerate conditions in mechanical theorem proving using algebraic methods. The first approach is to prove a statement to be generally true at the same time gives certain non-degenerate conditions in algebraic form to make the statement true. The second approach is to prove a statement to be true under certain non-degenerate conditions given explicitly as a part of the geometry statement. A detailed discussion of the formulation problem can be found in [CY1]. As mentioned above, the first approach can generate non-degenerate conditions automatically, but there is no general method to transform these conditions to geometry form. The second approach actually needs people to find the non-degenerate conditions. But generally, it is not easy to find the sufficient non-degenerate conditions for some statements. So it is very important that we can generate non-degenerate conditions in geometric form automatically from the usual description of a geometry statement so that the statement is true in the usual sense iff it is true under these non-degenerate conditions. If certain non-degenerate conditions satisfy this condition, we say they are sufficient (for the precise meaning, see section 4.). Wu has done these for a class of geometry statements [WU3]. In his thesis, the first author extended the result to a larger class in metric geometry [CH1]. In [CG2], we prove, for a class of geometry statements, the non-degenerate conditions (in geometric form) generated by our method are also sufficient for a statement to be true in Euclidean geometry.

In this paper, we extend the results in [CG2] to Riemann geometry: we describe a class of geometry statements of constructive type, and for statements in this class we present a method of generating sufficient non-degenerate conditions in geometric form from the construction of the statement. For a class of irreducible statements, we establish a theorem to connect the two approaches to dealing with non-degenerate conditions, i.e., an irreducible statement is generally true iff it is universally true under the geometric non-degenerate conditions generated by our method.

In section 2, we give a model for Riemann geometry and prove a theorem which can be used to reduce the proof of a statement to some easy cases. In section 3, a class of constructive statements is presented, and a method of generating non-degenerate conditions is also given. Section 4 proves the completeness of the non-degenerated conditions generated by our method. Section 5 provides some examples to illustrate our method.

2. Mechanical Theorem Proving in Riemann Geometry

2.1. A Model for Riemann Geometry

Let $\langle x, y\rangle$ and $x \times y$ be the inner product and vector product in the real space of dimension three $\mathbf{R}^3$ for x, y in $\mathbf{R}^3$. We denote $\|x\| = \langle x, x\rangle$ and $|x| = \sqrt{\langle x, x\rangle}$ for $x \in \mathbf{R}^3$. Let

$$\mathbf{S2} = \{X = (x, y, z) \in \mathbf{R}^3 / x^2 + y^2 + z^2 = 1\}$$

be the unit sphere in $\mathbf{R}^3$. Regarding a pair of antipodal points of $\mathbf{S2}$ as the same point, we get the real projective plane:

$$\mathbf{P2} = \{\{X, -X\} / X \in \mathbf{S2}\}$$

which is a model for Riemann geometry. Let $\pi : \mathbf{S2} \to \mathbf{P2}$ be the mapping that sends each $X \in \mathbf{S2}$ to $\{X, -X\} \in \mathbf{P2}$. If $A = \pi(x, y, z)$, we say (x, y, z) is a *coordinate* for A. A point A on $\mathbf{P2}$ has two coordinates (x, y, z) and $(-x, -y, -z)$. One of them is called the *antipodal point* of the other.

Two points $A = \pi(x_1, y_1, z_1)$ and $B = \pi(x_2, y_2, z_2)$ on $\mathbf{P2}$ are equal iff $(x_1, y_1, z_1) = (x_2, y_2, z_2)$ or $(x_1, y_1, z_1) = -(x_2, y_2, z_2)$, or equivalently iff $(x_1, y_1, z_1) \times (x_2, y_2, z_2) = 0$. Thus $A \neq B$ iff $(x_1, y_1, z_1) \times (x_2, y_2, z_2) \neq 0$.

A line in $\mathbf{P2}$ is a set of the form $\pi(l)$, where l is the intersection of $\mathbf{S2}$ and a plane passing the origin. Thus, the equation of a line in $\mathbf{P2}$ can be expressed as:

$$\langle U, X\rangle = u_1x_1 + u_2x_2 + u_3x_3 = 0$$

where $U = (u_1, u_2, u_3) \neq 0$ is the normal vector of the line and $X = \pi(x_1, x_2, x_3)$ is an arbitrary point on the line. Two lines are equal if their normal vectors are parallel. Two lines are perpendicular if the inner product of their normals is zero.

Note that a point P in $\mathbf{P2}$ determines a unique line l in $\mathbf{P2}$ whose normal vector is a coordinate of P. P is called the *pole* of l and l is called the *polar* of P.

We define the length of segment XY as:

$$D(X, Y) = \arccos(|\langle x, y\rangle|)$$

where $X = \pi(x)$ and $Y = \pi(y)$. We assume that all distances are $\leq \pi/2$. The definition is well-defined for the choices of coordinates of X and Y.

We consider four kinds of straight lines in **P2**.

(1) $l = P(A)$ is the polar line of point A on **P2**. The equation of line $P(A)$ is:

$$\langle A, X \rangle = 0$$

(2) $l = L(AB)$ is the line joins points A and B in **P2**. The equation of line $L(AB)$ is:

$$\langle A \times B, X \rangle = 0$$

(3) $l = T(C, AB)$ is the line passes through C and is perpendicular to line $L(AB)$ for points A, B, and C in **P2**. The equation of line $T(C, AB)$ is:

$$\langle C \times (A \times B), X \rangle = 0$$

(4) $l = B(AB)$ is the perpendicular-bisector of segment AB for points A and B in **P2**. The equation of line $B(AB)$ is:

$$\langle A - B, X \rangle \langle A + B, X \rangle = 0$$

Note that $B(AB)$ consists of two lines. It is not difficult to verify that the lines are well defined, i.e., their definition does not dependent on the selection of coordinates of the points. Unless stated otherwise, a straight line mentioned below belongs to one of the above four kinds of lines.

A circle h in **P2** is a pair of a point O and a segment AB: $h = (O, AB)$ which represents the set of points the distances between which and O equal to the length of AB, i.e., h is the circle with O as center and segment AB as radius. Two circles are equal if their centers are equal and their radii have the same length.

Let Π be a set of points on **P2**, then a line or a circle is said in Π if the points occurred in the definition of the line or the circle are in Π.

We define the measure of angle formed by line $L(AB)$ and line $L(CD)$ as:

$$\angle(AB, CD) = \arccos(|\langle \frac{a \times b}{|a \times b|}, \frac{d \times c}{|d \times c|} \rangle|)$$

where $\pi(a) = A, \pi(b) = B$, $\pi(c) = C$, $\pi(d) = D$. We assume that all angles are $\leq \pi/2$.

A complete description of this model can be found in [RY1].

2.2. The Basic Predicates and Mechanical Theorem Proving

For points A, B, C, D, X, Y, and Z, let a, b, c, d, x, y, and z be points on **S2** such that $\pi(a) = A$, $\pi(b) = B$, $\pi(c) = C$, $\pi(d) = D$, $\pi(x) = X$, $\pi(y) = Y$, and $\pi(z) = Z$. We define the following predicates*.

(1). Predicate polar(A, B) means A is on the polar line of B. Its algebraic equation is

$$\langle A, B \rangle = 0.$$

* Strictly speaking they are geometric relations as they can be deduced from the definition of the model.

(2). Predicate coll(A, B, C) means A, B, and C are on the same line. Its algebraic equation is

$$\langle a, b \times c\rangle = 0.$$

(3). Predicate perp(A, B, C, D) means that $A = B$, or $C = D$, or line $L(AB)$ is perpendicular to line $L(CD)$. Its algebraic equation is

$$\langle a \times b, c \times d\rangle = 0.$$

(4). Predicate cong(A, B, C, D) means the length of AB equals to the length of CD. Its algebraic equation is

$$\langle a, b\rangle^2 = \langle c, d\rangle^2.$$

(5). Predicate acong$(A, B, C; X, Y, Z)$ means that angle XYZ is congruent to angle ABC. Its algebraic equation is

$$\frac{\langle x \times y, z \times y\rangle^2}{\|x \times y\| \cdot \|z \times y\|} = \frac{\langle a \times b, c \times b\rangle^2}{\|a \times b\| \cdot \|c \times b\|}.$$

(6). Predicate pole(A, B, C) means $B = C$ or A is the pole of $L(BC)$. Its algebraic equation is

$$a \times (b \times c) = 0.$$

(7). Predicate para(A, B, C, D) means $A = B$ or $C = D$ or A, B, C, and D are on the same line. Its algebraic equation is

$$(a \times b) \times (c \times d) = 0.$$

(8). Predicate cperp(A, B, C, X, Y) means para(B, C, X, Y) or A is on the co-perpendicular line of $L(BC)$ and $L(XY)$. Its algebraic equation is

$$(a \times (b \times c)) \times (a \times (x \times y)) = 0.$$

For a predicate P, let $E(P)$ be the polynomials representing P, then P is true iff $E(P) = 0$, i.e., the polynomials in $E(P)$ are all zero. The correctness of these predicates comes from the definitions in section 2.1. Note that predicates pole and para can be represented by other predicates.

pole(A, B, C) is equivalent to (perp(A, B, B, C) and perp(A, C, B, C)).

para(A, B, C, D) is equivalent to [$A = B$ or $C = D$ or (coll(A, B, C) and coll(A, B, D) and coll(A, C, D) and coll(B, C, D))])

For the proof, see Appendix B.

Definition 2.1. (a). A geometry statement of equation type (or simply a geometry statement) in Riemann geometry is a triple (HS, DS, G) where $HS = \{P_1, ..., P_k\}$ and $DS = \{Q_1, ..., Q_m\}$ for predicates P_i and Q_i, and G is a predicate.

(b). A geometry statement (HS, DS, G) is true if

$$\forall P \in \Pi((P_1 \wedge ... \wedge P_k \wedge \neg Q_1 \wedge ... \wedge \neg Q_m) \Rightarrow G)$$

where Π is the set of points occurring in the P, the Q, and G.

HS is called the *equation part* of the hypothesis. DS is called the *inequation part* of the hypothesis. Note that Definition 2.1 is for simplicity, actually the predicates in the statement can be any geometric relation whose algebraic translation is a polynomial equation. For instance, see Example 5.2.

Definition 2.2. (a). An algebraic statement of equation type (or simply an algebraic statement) is a triple (ES, IS, C) where $ES = \{H_1, ..., H_s\}$, $IS = \{D_1, ..., D_t\}$ are polynomial sets, and C is a polynomial.

(b). An algebraic statement (ES, IS, C) is true in the real number case if

$$\forall x \in \mathbf{R}((H_1 = 0 \wedge ... \wedge H_s = 0 \wedge D_1 \neq 0 \wedge ... \wedge D_t \neq 0) \Rightarrow C = 0)$$

where the x are the variables occurring in the polynomials in (ES, IS, C), and $\mathbf{R}$ is the real number field.

(c). An algebraic statement (ES, IS, C) is universally true if

$$\forall x \in \mathbf{C}((H_1 = 0 \wedge ... \wedge H_s = 0 \wedge D_1 \neq 0 \wedge ... \wedge D_t \neq 0) \Rightarrow C = 0)$$

where the x are the variables occurring in the polynomials in (ES, IS, C), and $\mathbf{C}$ is the complex number field.

Thus if a statement is universally true then it is also true in the real number case. We have.

Theorem 2.3. We can decide whether an algebraic statement is universally true using Ritt-Wu's decomposition method or the Gröbner basis method.

Proof. See for example [CG1,CS1,KA1]. ∎

Let (HS, DS, G) $(HS = \{P_1, ..., P_k\}$ and $DS = \{Q_1, ..., Q_m\})$ be a geometry statement. For points occurring in (HS, DS, G), we assign coordinates such that no variables in the coordinates of different points can be the same. Then (HS, DS, G) can be transformed to an algebraic statement $(HS', DS', E(G))$ where $HS' = \bigcup_{1 \leq i \leq k} E(P_i)$ and $DS' = \{E(Q_1), ..., E(Q_m)\}$*. $(HS', DS', E(G))$ is called the *algebraic version* of (HS, DS, G). Thus a geometry statement is true iff its algebraic version is true in the real number case. We define that (HS, DS, G) is universally true if $(HS', DS', E(G))$ is universally true. By Theorem 2.3, we can decide whether a geometry statement is universally true.

As mentioned in the introduction, there is another approach of mechanical theorem proving. At first we have the following definition.

Definition 2.4. For a polynomial set $ES = \{H_1, ..., H_s\}$ and a polynomial C, we say (ES, C) or

$$\forall x((H_1 = 0 \wedge \cdots \wedge H_s = 0) \Rightarrow C = 0)$$

is generally true wrpt a set of variables $u_1, ..., u_q$, if there is a polynomial D of the u such that $Zero(ES) \subset Zero(CD)$.

* When $E(Q_i) = \{f_1, ..., f_p\}$ contains more than one polynomials, we can also use the following trick to transform $\neg(E(Q_i) = 0)$ to an inequation of a single polynomial: $\exists z(z_1 f_1 + \cdots + z_p f_p \neq 0)$ for new variables z_i.

A detailed discussion of generally true can be found in [WU2,CY2]. We have

Theorem 2.5. Given a polynomial set ES, a polynomial C, and a set of variables $u_1, ..., u_p$, we can decide whether (ES, C) is generally true wrpt $u_1, ..., u_p$ using Ritt-Wu's decomposition method or the Gröbner basis method.

Proof. See [WU2,CH2]. ▮

For a geometry statement (HS, DS, G) $(HS = \{P_1, ..., P_k\})$ with $DS = \emptyset$, let $(HS', \emptyset, E(G))$ be its algebraic version. We can divide the variables occurring in HS' and $E(G)$ into two groups: $u_1, ..., u_p$ and $x_1, ..., x_q$ such that the variables $u_1, ..., u_p$ can take arbitrary value and once their values are fixed the x can be generally determined by the hypothesis HS'. We call the u the parameters of the statement. We define that (HS, DS, G) is generally true wrpt the u if $(HS', E(G))$ is generally true wrpt the u. By Theorem 2.5, we can decide whether a geometry statement with empty inequation part is generally true.

2.3. The Reducibility Problem in Riemann Geometry

Note that the algebraic translation for the predicate cong is reducible. A statement involving this predicate can be divided into many subcases and the statement is true if and only all the subcases are true.

Example 2.6. In any triangle the three perpendicular-bisectors of the three sides are concurrent.

Let $A = \pi(0, 0, 1)$, $B = \pi(0, x_1, x_2)$, $C = \pi(x_3, x_4, x_5)$, and $O = \pi(x_6, x_7, x_8)$.

The hypotheses are:

$h_1 = x_2^2 + x_1^2 - 1 = 0$ $\qquad B \in \mathbf{P2}.$

$h_2 = x_5^2 + x_4^2 + x_3^2 - 1 = 0$ $\qquad C \in \mathbf{P2}.$

$h_3 = x_8^2 + x_7^2 + x_6^2 - 1 = 0$ $\qquad O \in \mathbf{P2}.$

$h_4 = x_8^2 - (x_1 x_7 + x_2 x_8)^2 = 0$ $\qquad \mathrm{cong}(O, A, O, B).$

$h_5 = (x_6 x_3 + x_7 x_4 + x_8 x_5)^2 - x_8^2 = 0$ $\qquad \mathrm{cong}(O, A, O, C).$

The conclusion is:

$c = (x_7 x_1 + x_8 x_2)^2 - (x_6 x_3 + x_7 x_4 + x_8 x_5)^2 = 0$ $\qquad \mathrm{cong}(O, B, O, C).$

Note that $h_4 = h_4' h_4''$ and $h_5 = h_5' h_5''$, where $h_4' = x_8 - (x_1 x_7 + x_2 x_8)$, $h_4'' = x_8 + (x_1 x_7 + x_2 x_8)$, $h_5' = x_6 x_3 + x_7 x_4 + x_8 x_5 - x_8$, and $h_5'' = x_6 x_3 + x_7 x_4 + x_8 x_5 + x_8$. Then the above geometry statement is true if and only if

$$\forall x((h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge h_4' = 0 \wedge h_5' = 0) \Rightarrow c = 0)$$
$$\forall x((h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge h_4'' = 0 \wedge h_5' = 0) \Rightarrow c = 0)$$
$$\forall x((h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge h_4' = 0 \wedge h_5'' = 0) \Rightarrow c = 0)$$
$$\forall x((h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge h_4'' = 0 \wedge h_5'' = 0) \Rightarrow c = 0)$$

are true.

To deal with this problem generally, we introduce two new predicates. (Strictly speaking, they are not predicates, because their algebraic translations depend on the selection of the coordinates of the points.)

(1). cong1(A,B,C,D) means

$$x_1x_2 + y_1y_2 + z_1z_2 = x_3x_4 + y_3y_4 + z_3z_4$$

(2). cong2(A,B,C,D) means

$$x_1x_2 + y_1y_2 + z_1z_2 = -(x_3x_4 + y_3y_4 + z_3z_4)$$

where $A = \pi(x_1, y_1, z_1)$, $B = \pi(x_2, y_2, z_2)$, $C = \pi(x_3, y_3, z_3)$, and $D = \pi(x_4, y_4, z_4)$.

A *substatement* of a geometry statement (HS, DS, G) is a statement (HS', DS, G) where HS' is obtained by replacing the predicate cong in HS by cong1 or cong2. If there are m predicates cong occurring in the equation part a geometry statement, then the truth of the statement is equivalent to the truth of 2^m substatements. We actually need not to check all of these substatements. In the following, we prove a theorem which can be used to reduce the number of substatements needed to check drastically.

Note that cong1 and cong2 are not independent of the choices of the coordinates of the points. If point A occurs one or three times in cong1(A,B,C,D), then cong1(A,B,C,D) changes to cong2(A,B,C,D) when replacing a coordinate of A with its antipodal. If point A occurs two or four times in cong1(A,B,C,D), then cong1(A,B,C,D) changes to itself when replacing a coordinate of A with its antipodal. Thus we can define an equivalent relation among the substatements: two substatements of a geometry statement are *equivalent* if one of them can be changed to the other by replacing the coordinates for some points in the predicates by their antipodals.

Theorem 2.7. Let (HS', DS, G) and (HS'', DS, G) be two equivalent substatements of a statement (HS, DS, G), then (HS', DS, G) is (universally) true if and only if (HS'', DS, G) is (universally) true.

Proof. Let $HS' = \{P_1, ..., P_k\}$, $DS = \{D_1, ..., D_l\}$. Then the substatement (HS', DS, G) is true iff

(2.8) $\quad \forall x \in \mathbf{R}(E(P_1) = 0 \wedge ... \wedge E(P_k) = 0 \wedge E(D_1) \neq 0 \wedge ... \wedge E(D_l) \neq 0 \Rightarrow E(G) = 0)$

Let $HS'' = \{P_1', ..., P_k'\}$. The substatement (HS'', DS, G) is true iff

(2.9) $\quad \forall x \in \mathbf{R}(E(P_1') = 0 \wedge ... \wedge E(P_k') = 0 \wedge E(D_1) \neq 0 \wedge ... \wedge E(D_l) \neq 0 \Rightarrow E(G) = 0)$

As the two substatements are equivalent, $E(P_i) = E(P_i')$ for $i = 1, ..., k$ when replacing the coordinates for some points by their antipodals in one substatement, i.e., when replacing some variables x_i by $-x_i$, (2.8) becomes (2.9). Thus (2.8) is true if and only if (2.9) is true. By changing the $\mathbf{R}$ in (2.8) and (2.9) to $\mathbf{C}$, we can get the result about the universally true. ∎

Theorem 2.10. In a statement (HS, DS, G), if for each predicate cong(P_1, P_2, P_3, P_4) in HS there is a point P_i which occurs in this predicate one or three times and does not occur in other cong predicates in HS, then the statement (HS, DS, G) is true iff one of its substatements is true.

Proof. If P_1 occurs in cong(P_1, P_2, P_3, P_4) one or three times, cong1(P_1, P_2, P_3, P_4) changes to cong2(P_1, P_2, P_3, P_4) when replacing a coordinate of P_1 by its antipodal. As for each segment congruence predicate there is a point which occurs in this predicate one or three times and does not occur in other segment congruence predicates, then in a substatement of (HS, DS, G) each predicate cong1 (cong2) can be changed to cong2 (cong1) separately by replacing the coordinates of this point by their antipodal. Such all the substatements are equivalent to each other. Now the theorem comes from theorem 2.7. ∎

From Theorem 2.10 we know that for Example 2.6, we need only check one of its substatements as point B occurs in cong(O, A, O, B) only and point C occurs in cong(O, A, O, C) only.

3. A Class of Geometry Statements of Constructive Type

3.1. The Constructions

Definition 3.1. A construction is one of the six operations.

Construction 1. Taking an arbitrary point P in **P2**.

Construction 2. Taking an arbitrary point P on a line l in **P2**.

Construction 3. Taking an arbitrary point P on a circle h in **P2**.

Construction 4. Taking the intersection P of two lines l_1 and l_2 in **P2**.

Construction 5. Taking an intersection P of a line l and a circle h in **P2**.

Construction 6. Taking an intersection P of two circles h_1 and h_2 in **P2**.

The point P in each of the above constructions is said to *be introduced by the construction.*

In the following, we shall give the exact geometric meaning in terms of geometry predicates and the algebraic translation for each of the above constructions. The algebraic translation of a construction consists of two parts: the *equation part HS* and the *inequation part DS*.

All the points introduced are in **P2**. For any point P in **P2**, we use its lowercase p to represent a point in **S2** such that $\pi(p) = P$ and $||p|| = 1$. In the following descriptions, we do not give the condition $||p|| = 1$ clearly.

Construction 1. Taking an arbitrary point P.

$$HS = \emptyset, DS = \emptyset.$$

Construction 2. Taking an arbitrary point P on a line l. We have four cases as there exist four kinds of lines.

Case 2.1. $l = P(P_1)$.

$$HS = \{\text{polar}(P, P_1)\}$$
$$DS = \{\}$$

Case 2.2. $l = L(P_1 P_2)$.

$$HS = \{\text{coll}(P, P_1, P_2)\}$$
$$DS = \{||p_1 \times p_2|| \neq 0\}$$

In the real number case DS is equivalent to $P_1 \neq P_2$.*

Case 2.3. $l = T(P_3, P_1P_2)$.

$HS = \{\text{perp}(P, P_3, P_1, P_2)\}$
$DS = \{\|p_3 \times (p_2 \times p_1)\| \neq 0\}$
In the real number case DS is equivalent to $\neg\text{pole}(P_3, P_1, P_2)$.

case 2.2.1. $l = T(P_1, P_1P_2)$.

$HS = \{\text{perp}(P, P_1, P_1, P_2)\}$
$DS = \{\|p_1 \times (p_1 \times p_2)\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq P_2$.

Case 2.4. $l = B(P_1P_2)$.

$HS = \{\text{cong}(P, P_1, P, P_2)\}$
$DS = \{\|p_2 - p_1\|\|p_2 + p_1\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq P_2$.

Construction 3. Taking an arbitrary point P on a circle $h = (O, AB)$.

$HS = \{\text{cong}(O, P, A, B)\}$
$DS = \emptyset$

Construction 4. Taking the intersection P of two lines l_1 and l_2. We have ten types of intersections. Generally speaking the non-degenerate condition for all types of intersection is that l_1 is not the same as l_2.

Case 4.1. $l_1 = P(P_1)$ and $l_2 = P(P_2)$.

$HS = \{\text{polar}(P, P_1), \text{polar}(P, P_2)\}$
$DS = \{\|p_1 \times p_2\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq P_2$.

Case 4.2. $l_1 = P(P_1)$ and $l_2 = L(P_2, P_3)$.

$HS = \{\text{polar}(P, P_1), \text{coll}(P, P_2, P_3)\}$
$DS = \{\|p_1 \times (p_2 \times p_3)\| \neq 0\}$
In the real number case DS is equivalent to: $\neg\text{pole}(P_1, P_2, P_3)$.

Case 4.3. $l_1 = P(P_1)$ and $l_2 = T(P_2, P_3, P_4)$.

$HS = \{\text{polar}(P, P_1), \text{perp}(P, P_2, P_3, P_4)\}$
$DS = \{\|p_1 \times (p_2 \times (p_3 \times p_4))\| \neq 0\}$
In the real number case DS is equivalent to: $\neg\text{pole}(P_2, P_3, P_4)$ and
$(\neg\text{polar}(P_1, P_2)$ or $\neg\text{coll}(P_1, P_3, P_4))$.

Case 4.4. $l_1 = P(P_1)$ and $l_2 = B(P_2, P_3)$.

$HS = \{\text{polar}(P, P_1), \text{cong}(P, P_2, P, P_3)\}$
$DS = \{\|p_1 \times (p_2 \pm p_3)\| \neq 0\}$

* The proof of this result can be found in Appendix B. The same for the following constructions.

In the real number case DS is equivalent to:
$\neg\mathrm{coll}(P_1, P_2, P_3)$ or $\neg\mathrm{cong}(P_1, P_2, P_1, P_3)$ (P_1 is not the middle point of P_2P_3).

Case 4.5. $l_1 = L(P_1P_2)$ and $l_2 = L(P_3P_4)$.

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{coll}(P, P_3, P_4)\}$
$DS = \{\|(p_1 \times p_2) \times (p_3 \times p_4)\| \neq 0\}$

In the real number case DS is equivalent to: $\neg\mathrm{para}(P_1, P_2, P_3, P_4)$.

case 4.5.1. $l_1 = L(P_1P_2)$ and $l_2 = L(P_1P_3)$.

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{coll}(P, P_1, P_3)\}$
$DS = \{\|(p_1 \times p_2) \times (p_1 \times p_3)\| \neq 0\}$

In the real number case DS is equivalent to: $\neg\mathrm{coll}(P_1, P_2, P_3)$.

Case 4.6. $l_1 = L(P_1P_2)$ and $l_2 = T(P_3, P_4P_5)$.

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{perp}(P, P_3, P_4, P_5)\}$
$DS = \{\|(p_1 \times p_2) \times (p_3 \times (p_4 \times p_5))\| \neq 0\}$

In the real number case DS is equivalent to: $\neg\mathrm{pole}(P_3, P_4, P_5)$ and
$(\neg\mathrm{coll}(P_1, P_2, P_3)$ or $\neg\mathrm{perp}(P_1, P_2, P_4, P_5))$.

case 4.6.1. $l_1 = L(P_1P_2)$ and $l_2 = T(P_3, P_1P_2)$. (The foot from P_3 to $L(P_1, P_2)$.)

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{perp}(P, P_3, P_1, P_2)\}$
$DS = \{\|(p_1 \times p_2) \times (p_3 \times (p_1 \times p_2))\| \neq 0\}$

In the real number case DS is equivalent to: $\neg\mathrm{pole}(P_3, P_1, P_2)$.

Case 4.7. $l_1 = L(P_1P_2)$ and $l_2 = B(P_3P_4)$.

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{cong}(P, P_3, P, P_4)\}$
$DS = \{\|(p_1 \times p_2) \times (p_4 \pm p_3)\| \neq 0\}$

In the real number case DS is equivalent to:
$P_1 \neq P_2$ and $(\neg\mathrm{cong}(P_1, P_3, P_1, P_4)$ or $\neg\mathrm{perp}(P_1, P_2, P_3, P_4))$.

case 4.7.1. $l_1 = L(P_1P_2)$ and $l_2 = B(P_1P_2)$. (The middle point of P_1P_2.)

$HS = \{\mathrm{coll}(P, P_1, P_2), \mathrm{cong}(P, P_1, P, P_2)\}$
$DS = \{\|(p_1 \times p_2) \times (p_1 \pm p_2)\| \neq 0\}$

In the real number case DS is equivalent to: $P_1 \neq P_2$.

Case 4.8. $l_1 = T(P_1, P_2P_3)$ and $l_2 = T(P_4, P_5P_6)$.

$HS = \{\mathrm{perp}(P, P_1, P_2, P_3), \mathrm{perp}(P, P_4, P_5, P_6)\}$
$DS = \{\|(p_1 \times (p_2 \times p_3)) \times (p_4 \times (p_5 \times p_6))\| \neq 0\}$

In the real number case DS is equivalent to: $\neg\mathrm{pole}(P_1, P_2, P_3)$ and
$\neg\mathrm{pole}(P_4, P_5, P_6)$ and $(P_1 \neq P_4$ or $\neg\mathrm{cperp}(P_1, P_2, P_3, P_5, P_6))$ and
$(\neg\mathrm{perp}(P_1, P_4, P_2, P_3)$ or $\neg\mathrm{perp}(P_1, P_4, P_5, P_6))$.

Case 4.9. $l_1 = T(P_1, P_2P_3)$ and $l_2 = B(P_4P_5)$.

$HS = \{\mathrm{perp}(P, P_1, P_2, P_3), \mathrm{cong}(P, P_4, P, P_5)\}$
$DS = \{\|(p_1 \times (p_2 \times p_3)) \times (p_5 \pm p_4)\| \neq 0\}$

In the real number case DS is equivalent to:
$\neg$pole(P_1, P_2, P_3) and ($\neg$cong(P_1, P_4, P_1, P_5) or $\neg$cperp$(P_1, P_2, P_3, P_4, P_5)$).

Case 4.10. $l_1 = B(P_1P_2)$ and $l_2 = B(P_3P_4)$.

$HS = \{\text{cong}(P, P_1, P, P_2), \text{cong}(P, P_3, P, P_4)\}$
$DS = \{\|(p_2 \pm p_1) \times (p_4 \pm p_3)\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq P_2$ and $P_3 \neq P_4$ and ($\neg$cong(P_1, P_3, P_2, P_4) or $\neg$cong(P_1, P_4, P_2, P_3)).

Construction 5. Taking an intersection P of a line l and a circle $h = (O, Q_1Q_2)$. We have four cases.

Case 5.1. $l = P(P_1)$ and $h = (O, Q_1Q_2)$.

$HS = \{\text{polar}(P, P_1), \text{cong}(P, O, Q_1, Q_2)\}$
$DS = \{\|p_1 \times o\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq O$.

Case 5.2. $l = L(P_1P_2)$ and $h = (O, Q_1Q_2)$.

$HS = \{\text{coll}(P, P_1, P_2), \text{cong}(P, O, Q_1, Q_2)\}$
$DS = \{\|o \times (p_1 \times p_2)\| \neq 0\}$
In the real number case DS is equivalent to: $\neg$pole(O, P_1, P_2).

case 5.2.1. $l = L(P_1P_2)$ and $h = (P_1, Q_1Q_2)$.

$HS = \{\text{coll}(P, P_1, P_2), \text{cong}(P, P_1, Q_1, Q_2)\}$
$DS = \{\|p_1 \times (p_1 \times p_2)\| \neq 0\}$
In the real number case DS is equivalent to: $P_1 \neq P_2$.

Case 5.3. $l = T(P_1, P_2P_3)$ and $h = (O, Q_1Q_2)$.

$HS = \{\text{perp}(P, P_1, P_2, P_3), \text{cong}(P, O, Q_1, Q_2)\}$
$DS = \{\|(p_1 \times (p_2 \times p_3)) \times o\| \neq 0\}$
In the real number case DS is equivalent to: $\neg$pole(P_1, P_2, P_3) and ($\neg$polar(P_1, O) or $\neg$coll(O, P_2, P_3)).

Case 5.4. $l = B(P_1P_2)$ and $h = (O, Q_1Q_2)$.

$HS = \{\text{cong}(P, O, Q_1, Q_2), \text{cong}(P, P_1, P, P_2)\}$
$DS = \{\|(p_2 \pm p_1) \times o\| \neq 0\}$
In the real number case DS is equivalent to:
$\neg$coll(O, P_1P_2) or $\neg$cong(O, P_1, O, P_2) (O is not the middle point of P_1P_2).

Construction 6. Taking an intersection P of two circles $h_1 = (O_1, P_1P_2)$ and $h_2 = (O_2, Q_1Q_2)$.

$HS = \{\text{cong}(P, O_2, Q_1, Q_2), \text{cong}(P, O_2, P_1, P_2)\}$
$DS = \{\|o_1 \times o_2\| \neq 0\}$
In the real number case DS is equivalent to: $O_1 \neq O_2$.

We see that the equation part HS of a construction is in geometric form, but its inequation part DS is in algebraic form and can be transformed in to geometry predicates in the real number case.

3.2. Geometry Statements of Constructive Type

Definition 3.2. A construction sequence is a sequence of constructions such that for each construction in the sequence the point introduced by it must be different from the points introduced by the previous constructions and the lines and circles occurring in this construction must be in the set of points introduced by the previous constructions.

Definition 3.3. A geometry statement of constructive type is a pair (CS, G) where CS is a construction sequence and G is a predicate.

For a statement of constructive type (CS, G), we give different and non-zero coordinates for different points. Then (CS, G) can be transformed to an algebraic statement $(ES, IS, E(G))$ where $ES = \{H_1, ..., H_s\}$ is the set of polynomials in the equation part of the construction sequence; $IS = \{D_1, ..., D_t\}$ is the set of polynomials in the inequation part of the construction sequence. We call $(ES, IS, E(G))$ the *algebraic version* of (CS, G).

Definition 3.3. Let $(ES, IS, E(G))$ be the algebraic version of a constructive statement (CS, G). We say (CS, G) is true in Riemann geometry if $(ES, IS, E(G))$ is true in the real number case and (CS, G) is universally true if $(ES, IS, E(G))$ is universally true.

By Theorems 2.3 and 2.5, we can decide whether a constructive statement is universally true or generally true.

In the real number case, we can transform a statement of constructive type to a geometry statement of equation type. Let $HS = \{P_1, ..., P_s\}$ be the predicates in the equation part of the statement, and $DS = \{Q_1, ..., Q_t\}$ be the predicate formulas which are equivalent to the inequation part of the statement in the real number case. Then the statement (CS, G) is equivalent to the geometry statement (HS, DS, G) in the real number case, i.e., (HS, DS, G) is true in Riemann geometry iff (CS, G) is true in Riemann geometry. We call (HS, DS, G) the *real version* of the statement (CS, G).

4. The Completeness of the Non-degenerate Conditions

In this section, we shall prove the non-degenerate conditions generated by section 3.1 for a statement of constructive type (CS, G) are sufficient. For the precise meaning, see section 4.1 and section 4.2. Section 4.1 treats the general case. Section 4.2 treats a special case for which connections can be established for the two approaches to dealing with non-degenerate conditions.

In this section, we assume the reader is familiar with Ritt-Wu's decomposition algorithm. A complete description for the decomposition algorithm can be found in [RI1, WU2, CH2], or our newly improved version in [CG1]. The following notions are needed frequently in this section.

Let ES and DS be polynomial sets in $Q[x_1, ..., x_n]$. For an extension field K of Q, let

$$Zero(ES) = \{x = (x_1, ..., x_n) \in K^n \mid \forall P \in ES, P(x) = 0\}$$

and $Zero(ES/DS) = Zero(ES) - Zero(DS)$. We use $RZero(ES/DS)$ and $CZero(ES/DS)$ to denote the $Zero(ES/DS)$ when K is $\mathbf{R}$ or $\mathbf{C}$ respectively. For an ascending chain (depending on text some times maybe a triangular form) ASC and a polynomial P, let $prem(p, ASC)$ be the *pseudo remainder* of P wrpt ASC. For an ascending chain, we use the following notation:

$$PD(ASC) = \{P \in Q[X] \mid prem(P, ASC) = 0\}$$

Some properties about the irreducible ascending chains needed in this section can be found in Appendix A of the paper. We have.

Ritt-Wu's Zero Decomposition Theorem For two finite polynomial sets ES and IS, we can either detect the emptiness of $Zero(ES/IS)$ or furnish a decomposition of the following form

$$Zero(ES/IS) = \cup_{i=1}^{l} Zero(PD(ASC_i)/IS)$$

where (a). for each $i \leq l$, ASC_i is an irreducible ascending chain such that $prem(P, ASC_i) \neq 0$ for $\forall P \in IS$; (b). there are not $i \neq j$ such that $PD(ASC_i) \subset PD(ASC_j)$.

We call such a decomposition an *irredundant decomposition*, and call $Zero(PD(ASC_i)/IS)$ the *irreducible components* of $Zero(ES/IS)$.

4.1. The General Case

Definition 4.1. An algebraic statement (ES, IS, C) is called trivially true if its hypothesis is contradict, i.e, $CZero(ES/IS)$ is empty.

Definition 4.2. An algebraic statement $S = (ES, IS, C)$ is called unmixed if S is not trivially true and we have the following decomposition

$$Zero(ES/IS) = \cup_{1 \leq i \leq k} Zero(PD(ASC_i)/IS)$$

where the ASC_i are irreducible ascending chains with the same parameter set $\{u_1, ..., u_p\}$.

The variable set $\{u_1, ..., u_p\}$ in Definition 4.2 is called a *parameter set* of the unmixed statement. Note that Definitions 4.1 and 4.2 only depend on the equation part and inequation part of the statement, i.e., they are independent of the conclusion of the statement.

If point P is introduced by a construction CO, then a *parameter set of* CO consists of

two of the variables in a coordinate of P, if CO is Construction 1;
one of the variables in a coordinate of P, if CO is Construction 2 or 3;
$\emptyset$, if CO is Construction 4 or 5 or 6.

For a statement of constructive type, the union of all the parameter sets of the constructions in the construction sequence of the statement is called a *parameter set of the statement.* Let n_1, n_2, n_3 be the numbers of the constructions 1-3 occurring in the construction sequence of the statement respectively. Then each parameter set of the statement has $d = 2n_1 + n_2 + n_3$ variables. We define d to be the *dimension of the statement.* Note that in a statement of constructive type, the variables in a set of parameters can take arbitrary value and once their values are fixed other variables can be generally determined by the geometric hypothesis. It is in this sense, we call them parameters.

The following theorem is the main result of this subsection and the completeness of the non-degenerate conditions can be deduced from this theorem.

Theorem 4.3. Let $S = (ES, IS, C)$ be the algebraic version of a statement of constructive type and $\{u_1, ..., u_q\}$ be a parameter set for the statement, then we can decide in a finite number of steps that either S is trivially true or S is an unmixed statement with the u as its parameter set.

The sufficiency of the non-degenerate conditions generated by the constructions can be described in two two aspects. First, (CS, G) is true in the usual sense (or it is a theorem in the text books) iff it is also universally true under these non-degenerate conditions. Roughly speaking, they are the conditions under which the configurations of the hypothesis of the statements are normal. For example, when we take a point on a straight line we assume the line is well-defined; when we take the intersection of two lines we assume the two lines are well defined and they have normal intersection, i.e., they do not coincide. In the traditional proof of a geometry theorem, we actually always assume the same conditions as above. For the second meaning of the sufficiency, we first have.

Theorem 4.4. If P dose not vanish on any irreducible component of $Zero(ES/IS)$, then for any polynomial C, the algebraic statement $S = (ES, IS, C)$ is universally true iff the new statement $S' = (ES, IS \cup \{P\}, C)$ is universally true.

Proof. Let

$$Zero(ES/IS) = \cup_{1 \leq i \leq k} Zero(PD(ASC_i)/IS)$$

be an irredundant decomposition of $Zero(ES/IS)$. By Lemma A.5, S is universally true iff $prem(C, ASC_i) = 0$ for $i = 1, ..., k$. Since $prem(P, ASC_i) \neq 0$ for $i = 1, ..., k$, we have the following irredundant decomposition

$$Zero(ES/IS \cup \{P\}) = \cup_{1 \leq i \leq k} Zero(PD(ASC_i)/IS \cup \{P\})$$

Hence S' is universally true iff $prem(C, ASC_i) = 0$ for $i = 1, ..., k$, i.e., iff S is universally true. ▮

Theorem 4.4 actually means if the newly added non-degenerate condition does not delete any irreducible component of the original statement, then the new statement is universally true iff the original statement is universally true. For a statement S of constructive type, by Theorem 4.3 as all the components are normal in the sense that they are with a parameter set of the statement as their parameter set, then Theorem 4.4 implies if $S = (ES, IS, C)$ is not universally true a new statement $S = (ES, IS \cup \{P\}, C)$ (P is a polynomial) can not be universally true if $P \neq 0$ does not delete any normal component, or equivalently if $P \neq 0$ does not make the statement more special or more degenerate.

In the following, we shall give a proof for Theorem 4.3. Those who are not interested in the technique details may go to section 4.2 directly. We first give some lemmas.

Lemma 4.5. Let EP and IP be the equation part and the inequation part of a construction, then we have a decomposition of the following form:

$$Zero(EP/IP) = \cup_{i=1}^{l} Zero(ASC_i/IP \cup J_i)$$

where (a). each ASC_i is a (weak) ascending chain with a parameter set of the construction as its parameter set and J_i is the set of initials for ASC_i. (b). $ASC_i \subset Ideal(EP)$. (c). For i and $j \leq l$, the pseudo remainders of the polynomials in ASC_i wrpt ASC_j are zero.

Proof. We shall prove the lemma for each of the construction types.

Construction 1. Taking an arbitrary point. Let $P = \pi(x, y, z)$. Then the algebraic equation of construction 1 is:

$$\begin{aligned}&EP_1 = \{h_1 = x^2 + y^2 + z^2 - 1 = 0\}\\&IP_1 = \emptyset\end{aligned}$$

Let $l = 1$ and $ASC_1 = h_1$. The lemma is obviously true for construction 1.

Construction 2. Taking an arbitrary point P on a line l. Let $P = \pi(x, y, z)$ and the normal vector of l be $n = (n_1, n_2, n_3)$. As mentioned in section 2.1, we can reduce the line $B(AB)$ to two linear cases. Then the algebraic equations for the four types of lines can be summed up as:

$$\begin{aligned}&EP_2 = \{h_1, h_2\}\\&h_1 = n_1x + n_2y + n_3z = 0\\&h_2 = x^2 + y^2 + z^2 - 1 = 0\\&IP_2 = \{d = n_1^2 + n_2^2 + n^2 \neq 0\}\end{aligned}$$

Note that $Zero(n_1^2 + n_2^2, n_1^2 + n_3^2, n_2^2 + n_3^2) \subset Zero(d)$. Using lemma A.8, we have:

$$\begin{aligned}Zero(EP_2/IP_2) = Zero(EP_2/IP_2 \cup \{n_1^2 + n_2^2\})\cup\\ Zero(EP_2/IP_2 \cup \{n_1^2 + n_3^2\}) \cup Zero(EP_2/IP_2 \cup \{n_2^2 + n_3^2\})\end{aligned} \tag{4.6}$$

Using lemma A.8 to each of the component on the right side of (4.6) again, we have:

$$\begin{aligned}&Zero(EP_2/IP_2) =\\&Zero(EP_2/IP_2 \cup \{n_1, n_1^2 + n_2^2\}) \cup Zero(EP_2/IP_2 \cup \{n_2, n_1^2 + n_2^2\})\cup\\&Zero(EP_2/IP_2 \cup \{n_1, n_1^2 + n_3^2\}) \cup Zero(EP_2/IP_2 \cup \{n_3, n_1^2 + n_3^2\})\cup\\&Zero(EP_2/IP_2 \cup \{n_2, n_2^2 + n_3^2\}) \cup Zero(EP_2/IP_2 \cup \{n_3, n_2^2 + n_3^2\})\end{aligned} \tag{4.7}$$

Let

$$h_3 = prem(h_2, h_1; x) = (n_2^2 + n_1^2)y^2 + (n_3^2 + n_1^2)z^2 + 2n_2n_3yz - n_1^2$$

Under the variable order: $z < y < x$, we have an ascending chain $ASC_1 = \{h_3, h_1\}$ and the first component of (4.7) becomes:

$$Zero(EP_2/IP_2 \cup \{n_1, n_1^2 + n_2^2\}) = Zero(ASC_1/IP_2 \cup J_1)$$

where $J_1 = \{n_1, n_1^2 + n_2^2\}$ is the set of initials for ASC_1. Other components in (4.7) can be treated similarly. At last we have:

$$Zero(EP_2/IP_2) = \cup_{i=1}^6 Zero(ASC_i/IP_2 \cup J_i)$$

(a) is obviously true. (b) comes from the computation of the ASC_i. (c) can be obtained by calculating the pseudo remainders.

Construction 3. Taking an arbitrary point P on a circle (O, DE). Let $P = \pi(x, y, z)$, $O = \pi(x_1, y_1, z_1)$, $D = \pi(x_2, y_2, z_2)$, and $E = \pi(x_3, y_3, z_3)$. We have:

$$EP_3 = \{h_1, h_2\}$$

$h_1 = x_1x + y_1y + z_1z - x_2x_3 - y_2y_3 - z_2z_3 = 0$
$h_2 = x^2 + y^2 + z^2 - 1 = 0$
IP_3 is empty.

At first let $IP_3 = \{d = x_1^2 + y_1^2 + z_1^2 \neq 0\}$. Similar as construction 2, we have a decomposition like (4.7) with vector (x_1, y_1, z_1) in the position of vector n. Note that $d = x_1^2 + y_1^2 + z_1^2 = 1$ then the decomposition is also true for $IP_3 = \emptyset$.

Construction 4. Taking the intersection P of line l_1 and line l_2. Let $P = \pi(x, y, z)$ and the normals of l_1 and l_2 be $n = (n_1, n_2, n_3)$ and $m = (m_1, m_2, m_3)$ respectively. Use the reducibility of predicate cong, all the cases can be summed up as the following form. (For case 4.1, we need the following identity: $\|(A \times B) \times (C \times D)\| = \|A \times B\| \cdot \|C \times D\| - \langle A \times B, C \times D\rangle^2$.)

$EP_4 = \{h_1, h_2, h_3\}$ where
$h_1 = n_1x + n_2y + n_3z = 0$
$h_2 = m_1x + m_2y + m_3z = 0$
$h_3 = x^2 + y^2 + z^2 - 1 = 0$

$IP_4 = \{d = \|(n \times m)\| \neq 0\}$

Note $n \times m = (n_2m_3 - n_3m_2, n_3m_1 - n_1m_3, n_1m_2 - n_2m_1)$. By lemma A.8, we have:

$$\begin{aligned}(4.8)\qquad & Zero(EP_4/IP_4) = Zero(EP_4/IP_4 \cup \{n_2m_3 - n_3m_2\})\cup \\ & Zero(EP_4/IP_4 \cup \{n_3m_1 - n_1m_3\}) \cup Zero(EP_4/IP_4 \cup \{n_1m_2 - n_2m_1\})\end{aligned}$$

Let ASC_1 be the following ascending chain:

$dx^2 - n_2^2m_3^2 + 2n_2n_3m_2m_3 - n_3^2m_2^2$
$(n_2m_3 - n_3m_2)y + (n_1m_3 - n_3m_1)x$
$(n_2m_3 - n_3m_2)z + (-n_1m_2 + n_2m_1)x$

By direct calculation, we have $prem(h_i; ASC_1) = 0, i = 1, 2, 3$. We can also prove using the Gröbner basis method that $ASC_1 \subset Ideal(EP_4)$. Then we have

$$Zero(EP_4/IP_4 \cup \{n_2m_3 - n_3m_2\}) = Zero(ASC_1/IP_4 \cup J_1)$$

where $J_1 = \{n_2m_3 - n_3m_2, d\}$ is the initial set for ASC_1. Other components in (4.8) can be treated similarly. At last we have:

$$Zero(EP_4/IP_4) = \cup_{i=1}^3 Zero(ASC_i/IP_4 \cup J_i)$$

(a) and (b) have been proved above. (c) can be proved by direct calculation.

Construction 5. Taking the intersection P of a line l and a circle $h = (O, DE)$. Let $P = \pi(x, y, z)$, $O = \pi(x_1, y_1, z_1)$, $D = \pi(x_2, y_2, z_2)$, and $E = \pi(x_3, y_3, z_3)$, and the normal vector of l be $N = (n_1, n_2, n_3)$. The four cases can be summed up as:

$EP_5 = \{h_1, h_2, h_3\}$ where
$h_1 = n_1x + n_2y + n_3z = 0$ $\qquad$ P is on the line.
$h_2 = x_1x + y_1y + z_1z - x_2x_3 - y_2y_3 - z_2z_3 = 0$ $\qquad$ P is on the circle.
$h_3 = x^2 + y^2 + z^2 - 1 = 0$

$IP_5 = \{d_1 = \langle N \times o, N \times o\rangle \neq 0\}$

This case can be treated similarly as construction 4.

Construction 6. Taking the intersection P of two circles o_1 and o_2. Let $o_1 = (N, QR)$, $o_2 = (M, ST)$, and $P = \pi(x, y, z)$, $N = \pi(n_1, n_2, n_3)$, $M = \pi(m_1, m_2, m_3)$, $Q = \pi(x_1, y_1, z_1)$, $R = \pi(x_2, y_2, z_2)$, $S = \pi(x_3, y_3, z_3)$, $T = \pi(x_4, y_4, z_4)$. We have:

$EP_6 = \{h_1, h_2, h_3\}$ where
$h_1 = n_1x + n_2y + n_3z - x_1y_1 - x_2y_2 - z_1z_2 = 0$
$h_2 = m_1x + m_2y + m_3z - x_3x_4 - y_3y_4 - z_3z_4 = 0$
$h_3 = x^2 + y^2 + z^2 - 1 = 0$

$IP_6 = \{d_1 = \langle n \times m, n \times m\rangle \neq 0\}$

This case can be treated similarly as construction 4. ■

Lemma 4.9. Let $S = (ES, IS, C)$ be the algebraic version of a statement of constructive type and $\{u_1, ..., u_q\}$ be a parameter set for the statement, then either S is trivially true or we can furnish a decomposition of the following form:

$$Zero(ES/IS) = Zero(PD(ASC)/IS) \tag{4.10}$$

where (a). ASC is a (weak) ascending chain with the u as its parameter set. (b). $ASC \subset Ideal(ES)$. (c). No pseudo remainders of the polynomials in IS wrpt ASC are zero.

Proof. We prove the statement by induction on the number of constructions. We actually only need to prove the induction step. The base case, when there is only one construction, is almost the same. Now suppose we have Lemma 4.9 for a construction sequence CS whose equation part and inequation part are ES and IS respectively. We need to prove that for each construction CO belongs to Constructions 1-6, Lemma 4.9 is still true for the new construction sequence obtained by adding CO to CS.

Let the equation part and inequation part of the construction CO be EP and IP respectively. By Lemma 4.5, we have

$$Zero(EP/IP) = \cup_{i=1}^{l} Zero(ASC_i/IP \cup J_i)$$

Hence

$$Zero(ES \cup EP/IS \cup IP) = \cup_{i=1}^{l} Zero(PD(ASC) \cup ASC_i/IS \cup IP \cup J_i)$$

Note that the union of ASC and ASC_i is still a triangular form, then by Lemma A.6, we have

$$Zero(ES \cup EP/IS \cup IP) = \cup_{i=1}^{l} Zero(PD(ASC, ASC_i)/IS \cup IP \cup J_i) \tag{4.11}$$

As the coordinates of the points are all independent variables, then we have (i). if $g \in J_i \cup IP$ vanishes on one of the irreducible component of $Zero(ES/IS)$ it will vanish on $Zero(ES/IS)$; (ii). if for some $i \leq l, \exists g \in J_i \cup IP$ such that g vanishes on $Zero(ES/IS)$ then for $\forall i \leq l, \exists h \in J_i \cup IP$ such that h vanishes on $Zero(ES/IS)$. Thus we have either the statement is trivially true or for $\forall i \leq l, \forall h \in J_i \cup IP$, h do not vanish on any of the irreducible components of $Zero(ES/IS) = Zero(PD(ASC)/IS)$. At the later case, by Lemma A.10 and Lemma 5 (c), we have $Zero(PD(ASC, ASC_i)/IS) = Zero(PD(ASC, ASC_j)/IS)$ for all $i, j \leq l$. Hence, by repeated use of Lemma A.8, we can eliminate the J_i in (4.11) and have

$$Zero(ES \cup EP/IS \cup IP) = Zero(PD(ASC, ASC_i)/IS \cup IP)$$

We need to select ASC_i such that the parameter set of ASC_i is the one given in the lemma. This can be done, because, by the proof of Lemma 5, for each possible parameter set U of the construction CO, there exists an ASC_i with U as its parameter set. We have got the decomposition (4.10). (a) and (c) are true obviously. (b) comes from (b) of Lemma 4.5. ▮

Proof of Theorem 4.3. By Theorem 4.9, if the statement is not trivially true we get a decomposition like (4.10). Now the theorem comes Theorem A.13, since (4.10) is still true when $PD(ASC)$ is replaced by $QD(ASC)$. ▮

Remark. To confirm a statement of constructive type (ES, IS, C), we can use lemma 4.9 to get a decomposition (4.10). If $prem(C, ASC) = 0$ the statement is universally true. To do this we do not need any polynomial factorization.

4.2. The Irreducible Case

Definition 4.12. An algebraic statement (ES, IS, C) is called irreducible if

$$Zero(ES/IS) = Zero(PD/IS)$$

where PD is a prime ideal and no polynomials in IS belong to PD.

The non-degenerate conditions IS of an irreducible statement (ES, IS, C) is sufficient in the sense that if the statement is not universally true it cannot be universally true by adding more non-degenerate conditions unless the statement is trivially true under these non-degenerate conditions. Precisely, we have

Theorem. 4.13. If an irreducible algebraic statement (ES, IS, C) is not universally true, then for any polynomial P we have either $(ES, IS \cup \{P\}, C)$ is trivially true or $(ES, IS \cup \{P\}, C)$ is still not universally true.

Proof. Let $Zero(ES/IS) = Zero(PD/IS)$ where PD is a prime ideal. If $(ES, IS \cup \{P\}, C)$ is not trivially true then $Zero(PD/IS \cup \{P\})$ is not empty, i.e., $P \notin PD$. Thus by Lemma A.5, $(ES, IS \cup \{P\}, C)$ is still not universally true as $C \notin PD$. ▮

For a geometry statement of constructive type, we have

Theorem 4.14. Let (ES, IS, C) be the algebraic version of a constructive statement. If ASC in (4.10) is irreducible, then (ES, IS, C) is an irreducible algebraic statement.

Proof. It is obviously true, as $PD(ASC)$ is a prime ideal by Theorem A.1. ▮

If the algebraic version of a geometry statement of constructive type satisfies the condition of Theorem 4.14, this statement is called an *irreducible geometry statement*. More specifically, we have.

Theorem 4.15. Let $S = (ES, IS, C)$ be the algebraic version of a constructive statement whose construction sequence consists of only constructions 1-3, then either S is trivially true or S is an irreducible statement.

Proof. By Lemma 4.7, if S is not trivially true we have a decomposition like (4.10). We need to prove ASC is irreducible. Let $ASC = ASC' \cup ASC''$ where ASC'' be the polynomials provided by the last construction in the construction sequence. It is enough if we can prove that ASC is irreducible under the condition that ASC' is irreducible. In the following we shall prove the result assuming the last construction is each of the constructions 1-3 separately. Let $K = Q(U)[X]/(ASC')$ be the associate field of ASC' (see Appendix A.).

Construction 1. By the proof of lemma 4.7, $ASC'' = \{x^2 + y^2 + z^2 - 1\}$. By lemma A.3 in the Appendix A, ASC is irreducible if and only if the discriminant $D = 4(1 - y^2 + z^2)$ of $x^2+y^2+z^2-1$ as a polynomial of x is not a perfect square in K. Considering D as a polynomial of y, by Lemma A.4 this implies $1 + z^2 = 0$ in K which is impossible as z is an independent variable.

Construction 2. ASC'' has six possible cases. Let us consider one of them, say

$$ASC'' =$$
$$n_1x + n_3z + n_2y$$
$$(n_2^2 + n_1^2)y^2 + (n_3^2 + n_1^2)z^2 + 2n_2n_3yz - n_1^2$$

ASC is reducible if and only if the discriminant $D = 4n_1^2(n_1^2+n_2^2-(n_1^2+n_2^2+n_3^2)x^2)$ of the second polynomial in ASC'' as a polynomial of y is a perfect square in K. By Lemma 4.5, if $R_1 = prem(n_1, ASC') = 0$, or $R_2 = prem(n_1^2+n_2^2, ASC') = 0$, or $R_3 = prem(n_1^2+n_2^2+n_3^2, ASC') = 0$ then the statement is trivially true. Otherwise, we prove D can not be a perfect square in K. As $4n_1^2$ is already a perfect square and can not be zero, then we need only to consider $D' = n_1^2+n_2^2-(n_1^2+n_2^2+n_3^2)x^2$. By lemma A.4, D' is a perfect square implies either $n_1^2+n_2^2+n_3^2$ or $n_1^2 + n_2^2$ is zero in K, i.e., either $R_3 = 0$ or $R_2 = 0$ by lemma A.2. We get a contradiction.

The proof for Construction 3 is the same as construction 2. ∎

4.3. Generally True for Constructive Geometry Statements

In this section, we shall prove that for geometry statements of constructive type, the two approaches to dealing with non-degenerate conditions have connections.

Theorem 4.16. Let (ES, IS, C) be an unmixed algebraic statement with parameter set $u_1, ..., u_q$. If (ES, C) is generally true wrpt the u, then the (ES, IS, C) is universally true.

Proof. Let

$$Zero(ES/IS) = \cup_{i=1}^{t} Zero(PD(ASC_i)/IS)$$

be the irredundant decomposition of $Zero(ES/IS)$. The ASC_i are irreducible ascending chains with $u_1, ..., u_q$ as their parameter set. Since (ES, C) is generally true wrpt $u_1, ..., u_q$, then there is a polynomial D of the u such that $Zero(ES) \subset Zero(DC)$. Thus for each $i \leq t$ $Zero(PD(ASC_i)/IS) \subset Zero(ES/IS) \subset Zero(DC)$. By Lemma A.5, $prem(DC, ASC_i) = 0$. Then $prem(C, ASC_i) = 0$ as D is a polynomial of the u. This means (ES, IS, C) is universally true. ∎

Corollary. Let (ES, IS, C) be the algebraic version for a geometry statement of constructive type. If (ES, C) is generally true wrpt a parameter set of the statement, then the statement (ES, IS, C) is universally true.

Proof. The result comes from Theorem 4.16 and Theorem 4.3. ▮

Theorem 4.17. Let $S = (ES, IS, C)$ be the algebraic version for an irreducible geometry statement of constructive type, then S is universally true iff (ES, C) is generally true wrpt a parameter set of the statement.

Proof. By Theorem 4.16, we need only prove on direction. Let $u_1, ..., u_q$ be a parameter set of the statement, then by Theorem 4.14, we have

$$Zero(ES/IS) = Zero(PD(ASC)/IS)$$

where ASC is an irreducible ascending chain with the u as parameter set and no pseudo remainders of the polynomials in IS wrpt ASC are zero. As (ES, IS, C) is universally true, we have $prem(C, ASC) = 0$. By Lemma A.2, this implies that $C = 0$ in the associate field of ASC, or there is a polynomial D of the u such that DC belongs to the ideal generated by ASC. By Theorem 4.9 (b), $Zero(ES) \subset Zero(ASC)$. Now we have $Zero(ES) \subset Zero(DC)$. ▮

We can benefit from Theorems 4.16 and 4.17 by the following facts: there are lots of methods of proving a statement to be generally true and it is generally faster proving a statement to be generally true than proving the same statement to be true under certain non-degenerate conditions. So if we know a statement is irreducible, we only need to prove the statement is generally true. If it is generally true, then it is also universally true under the non-degenerate conditions generated by our method. If it is not generally true, then the algebraic statement can not be universally true by adding more non-degenerate conditions to the inequation part unless these conditions make the statement trivially true.

Remark. In this section, we assume the variables in the coordinates of the points in the statement cannot be zero. If this condition is not satisfied, some of the results in this section need modifications. For the irreducible case, see [CG2].

5. Experiment Results

With the results presented in this paper, we propose the following paradigm for mechanical theorem proving in Riemann geometry.

(i). At first, try to find if the given geometry statement is constructive. If it is, generating the algebraic version of the statement and do (iii). Otherwise do (ii).

(ii). Try to find whether the statement may become constructive if some of the geometry conditions are deleted. If so, generating the algebraic version of the constructive statement, adding the deleted conditions and going to (iii). Otherwise, find some non-degenerate conditions by yourself; translate the geometric conditions into algebraic equations; go to (iii).

(iii). Using Theorem 2.7 or 2.10, we can reduce the proof of the statement to the proofs of some substatements.

(iv). Prove the substatements using Ritt-Wu's zero decomposition method or the Gröbner basis method. If the answer is affirmative, then the statement is universally true under the given non-degenerate conditions. Otherwise, if the statement is constructive, then the statement can not be universally true without deleting some of its "normal" components, and if the statement is irreducible, then the statement can only be trivially true by adding more non-degenerate conditions.

We use a prover based on Ritt-Wu's decomposition theorem to prove geometry theorems according to the above paradigm. As books about Riemann geometry generally talk about the axiom system for Riemann geometry and very few geometry statements of equation type are given. So what we do is to try to find whether the similar statements of certain theorems in Euclidean geometry are true in Riemann geometry. Some theorems in Euclidean are obviously true in Riemann geometry. For example, if a statement only involves the geometry relations: collinear and a point on a circle is a statement in projective geometry. Hence such a statement is true in Euclidean geometry iff it is true in Riemann geometry. For example, the Pascal theorem for a circle (p8 of [CH2]) is true in Riemann geometry. We have proved this using our prover. We have also proved about twenty theorems which are not statements in projective geometry including the Butterfly theorem, Ceva theorem, and Menulus theorem etc. Here are two examples which are used to illustrate our method.

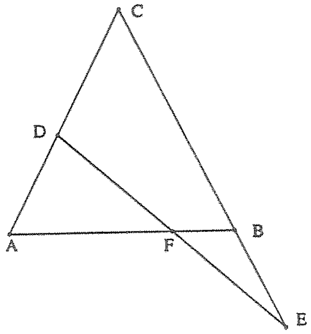

Figure 4

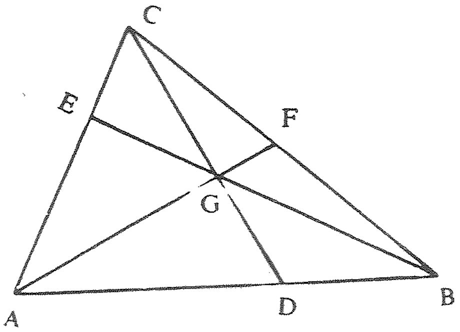

Figure 5

Example 1. Let ABC be a triangle such that $AC \equiv BC$. D is a point on AC; E is a point on BC such that $AD \equiv BE$. F is the intersection of DE and AB. Show $DF \equiv EF$.

This statement is of constructive type, and a construction sequence of the statement is:

Taking an arbitrary point A.	Construction 1.
Taking an arbitrary point B.	Construction 1.
C is on $B(AB)$.	Construction 2.
D is on $L(AC)$.	Construction 2.
$E = L(BC) \cap (B, AD)$.	Construction 5.
$F = L(AB) \cap L(DE)$.	Construction 4.

and the conclusion is:
cong(D, F, F, E).

Thus by section 3.1, in the real number case the example is equivalent to the geometry statement (HS,DS,cong(D, F, F, E)), where

$$HS = \{\ \text{cong}(A,C,C,B), \text{coll}(D,A,C,), \text{cong}(B,E,A,D),$$
$$\text{coll}(E,B,C,), \text{coll}(F,D,E), \text{coll}(F,A,B)\ \}.$$
$$DS = \{A = B, A = C, \text{pole}(B,B,C), \text{para}(A,B,D,E)\}$$

Let $A = (0,0,1), B = (0,x_1,x_2), C = (x_3,x_4,x_5), D = (x_6,x_7,x_8), E = (x_9,x_{10},x_{11}), F =$

$(0, x_{12}, x_{13})$*. By section 3.1, the algebraic version of the statement is: (ES, IS, g) where

$$
\begin{array}{ll}
ES = \{\|B\|-1, \|C\|-1, \|D\|-1, \|E\|-1, \|F\|-1, h_1, h_2, h_3, h_4, h_5\} & \\
h_1 = x_5^2 - (x_1x_4 + x_2x_5)^2 = 0 & \mathrm{cong}(A, C, C, B). \\
h_2 = x_3x_7 - x_4x_6 = 0 & \mathrm{coll}(D, A, C,). \\
h_3 = (x_1x_{10} + x_2x_{11})^2 - x_8^2 = 0 & \mathrm{cong}(B, E, A, D). \\
h_4 = x_1x_3x_{11} - x_2x_3x_{10} + (-x_1x_5 + x_2x_4)x_9 = 0 & \mathrm{coll}(E, B, C,). \\
h_5 = (x_6x_{10} - x_7x_9)x_{13} + (-x_6x_{11} + x_8x_9)x_{12} = 0 & \mathrm{coll}(F, D, E).
\end{array}
$$

$$
\begin{array}{ll}
IS = \{d_1, d_2, d_3, d_4\}. & \\
d_1 = \|A - B\|\|A + B\| \neq 0 & A \neq B. \\
d_2 = \|A \times C\| \neq 0 & A \neq C. \\
d_3 = \|(B \times C) \times B\| \neq 0 & \neg\mathrm{pole}(B, B, C). \\
d_4 = \|(A \times B) \times (D \times E)\| \neq 0 & \neg\mathrm{para}(A, B, D, E). \\
g = (x_{11}^2 - x_8^2)x_{13}^2 + ((2x_{10}x_{11} - 2x_7x_8)x_{12})x_{13} + (x_{10}^2 - x_7^2)x_{12}^2 = 0 & \mathrm{cong}(D, F, F, E).
\end{array}
$$

Bye Theorem 2.7, the equation part of the statement can be reduced to one substatement:

$$
\begin{array}{ll}
h'_1 = x_5 - (x_1x_4 + x_2x_5) = 0 & \mathrm{cong1}(A, C, C, B). \\
h'_2 = x_3x_7 - x_4x_6 = 0 & \mathrm{coll}(D, A, C,). \\
h'_3 = (x_1x_{10} + x_2x_{11}) - x_8 = 0 & \mathrm{cong1}(B, E, A, D). \\
h'_4 = x_1x_3x_{11} - x_2x_3x_{10} + (-x_1x_5 + x_2x_4)x_9 = 0 & \mathrm{coll}(E, B, C,). \\
h'_5 = (x_6x_{10} - x_7x_9)x_{13} + (-x_6x_{11} + x_8x_9)x_{12} = 0 & \mathrm{coll}(F, D, E).
\end{array}
$$

Let $ES' = \{\|B\|-1, \|C\|-1, \|D\|-1, \|E\|-1, \|F\|-1, h'_1, h'_2, h'_3, h'_4, h'_5\}$ To prove the statement using Ritt-Wu's decomposition algorithm, we first have the following decomposition:

$$Zero(ES'/IS) = Zero(PD(ASC_1)/IS) \cup Zero(PD(ASC_2)/IS)$$

where

$$
\begin{array}{l}
ASC_1 = \\
x_2^2 + x_1^2 - 1 \\
(x_2^2 - 2x_2 + x_1^2 + 1)x_4^2 + (x_2^2 - 2x_2 + 1)x_3^2 - x_2^2 + 2x_2 - 1 \\
(x_2 - 1)x_5 + x_1x_4 \\
x_3x_7 - x_4x_6 \\
x_8^2 + x_7^2 + x_6^2 - 1 \\
x_9 - x_6 \\
((x_2^2 + x_1^2)x_3)x_{10} + (x_1x_2x_5 - x_2^2x_4)x_9 - x_1x_3x_8 \\
x_2x_{11} + x_1x_{10} - x_8 \\
(x_6^2x_{11}^2 - 2x_6x_8x_9x_{11} + x_6^2x_{10}^2 - 2x_6x_7x_9x_{10} + (x_8^2 + x_7^2)x_9^2)x_{12}^2 - x_6^2x_{10}^2 + 2x_6x_7x_9x_{10} - x_7^2x_9^2 \\
(x_6x_{10} - x_7x_9)x_{13} + (-x_6x_11 + x_8x_9)x_{12}
\end{array}
$$

$$
\begin{array}{l}
ASC_2 = \\
x_2^2 + x_1^2 - 1 \\
(x_2^2 - 2x_2 + x_1^2 + 1)x_4^2 + (x_2^2 - 2x_2 + 1)x_3^2 - x_2^2 + 2x_2 - 1 \\
(x_2 - 1)x_5 + x_1x_4 \\
x_3x_7 - x_4x_6 \\
x_8^2 + x_7^2 + x_6^2 - 1
\end{array}
$$

* Here the coordinates of a point, say $C = (x_3, x_4, x_5)$ actually means $C = \pi(x_3, x_4, x_5)$. The same for Example 2.

$$
\begin{array}{l}
x_9 + x_6 \\
((x_2^2 + x_1^2)x_3)x_{10} + (x_1x_2x_5 - x_2^2x_4)x_9 - x_1x_3x_8 \\
x_2x_{11} + x_1x_{10} - x_8 \\
(x_6^2x_{11}^2 - 2x_6x_8x_9x_{11} + x_6^2x_{10}^2 - 2x_6x_7x_9x_{10} + (x_8^2 + x_7^2)x_9^2)x_{12}^2 - x_6^2x_{10}^2 + 2x_6x_7x_9x_{10} - x_7^2x_9^2 \\
(x_6x_{10} - x_7x_9)x_{13} + (-x_6x_11 + x_8x_9)x_{12}
\end{array}
$$

We have $prem(g, ASC_1) = prem(g, ASC_2) = 0$ which means the statement (ES, IS, g) is universally true.

Example 2. (Ceva Theorem) As in figure 2, let AG, BG, CG intersect BC, AC, AB in F, E, D respectively. Show that:

$$\frac{\sin(AD)\sin(BF)\sin(CE)}{\sin(DB)\sin(FC)\sin(EA)} = 1$$

Strictly speaking, this example is not a geometry statement according to Definition 2.1. To describe the statement, we need the following new predicates:

(a). cos-dis(A, B, x) means: $x = \langle A, B\rangle^2$,

(b). sin-dis(A, B, x) means: $x + \langle A, B\rangle^2 = 1$,

and we need to assume the conclusion of a geometry statement can be any polynomial equation.

The construction sequence of the statement is

$$
\begin{array}{ll}
\text{Taking arbitrary points } G, A, B, \text{ and } C \text{ in } \mathbf{P2}. & \text{Construction 1.} \\
D = L(GC) \cap L(AB). & \text{Construction 4.} \\
E = L(GB) \cap L(AC). & \text{Construction 4.} \\
F = L(GA) \cap L(BC). & \text{Construction 4.}
\end{array}
$$

Let $G = (0, 0, 0), C = (0, x_1, x_2)$, $A = (x_3, x_4, x_5)$, $B = (x_6, x_7, x_8)$, $D = (0, x_9, x_{10})$, $E = (x_{11}, x_{12}, x_{13})$, $F = (x_{14}, x_{15}, x_{16})$. The algebraic version of the statement is (ES, IS, g), where

$$
\begin{array}{ll}
ES = \{\|A\| - 1, \|B\| - 1, \|C\| - 1, \|D\| - 1, \|E\| - 1, \|F\| - 1, h_1, ...h_{11}\} & \\
\quad h_1 = x_5x_6x_9 + x_3x_7x_{10} - x_4x_6x_{10} - x_3x_8x_9 = 0 & \text{coll}(A, B, D). \\
\quad h_2 = x_6x_{12} - x_7x_{11} = 0 & \text{coll}(B, E, G). \\
\quad h_3 = x_1x_5x_{11} + x_2x_3x_{12} - x_2x_4x_{11} - x_1x_3x_{13} = 0 & \text{coll}(A, E, C). \\
\quad h_4 = x_3x_{15} - x_4x_{14} = 0 & \text{coll}(A, G, F). \\
\quad h_5 = x_1x_8x_{14} + x_2x_6x_{15} - x_2x_7x_{14} - x_1x_6x_{16} = 0 & \text{coll}(B, C, F). \\
\quad h_6 = x_{17} + 1 - (x_4x_9 - x_5x_{10})^2 = 0 & x_{17} = \sin(AD)^2. \\
\quad h_7 = x_{18} + 1 - (x_6x_{14} + x_7x_{15} - x_8x_{16})^2 = 0 & x_{18} = \sin(BF)^2. \\
\quad h_8 = x_{19} + 1 - (x_1x_{12} - x_2x_{13})^2 = 0 & x_{19} = \sin(CE)^2. \\
\quad h_9 = x_{20} + 1 - (x_9x_7 - x_{10}x_8)^2 = 0 & x_{20} = \sin(DB)^2. \\
\quad h_{10} = x_{21} + 1 - (x_1x_{15} + x_2 - x_{16})^2 = 0 & x_{21} = \sin(FC)^2. \\
\quad h_{11} = x_{22} + 1 - (x_2x_{11} + x_4x_{12} - x_5x_{13})^2 = 0 & x_{22} = \sin(EA)^2. \\
IS = \{d_1, d_2, d_3\} & \\
\quad d_1 = \|(G \times C) \times (A \times B)\| \neq 0 & \neg\text{para}(G, C, A, B). \\
\quad d_2 = \|(G \times B) \times (A \times C)\| \neq 0 & \neg\text{para}(G, B, A, C). \\
\quad d_3 = \|(G \times A) \times (B \times C)\| \neq 0 & \neg\text{para}(G, A, B, C). \\
g = x_{17}x_{18}x_{19} - x_{20}x_{21}x_{22} = 0 &
\end{array}
$$

To prove the statement using Ritt-Wu's decomposition method, we first get the following decomposition:

$$Zero(ES/IS) = Zero(PD(ASC_1)/IS)$$

where

$ASC_1 =$
$x_2^2 + x_1^2 - 1$
$x_5^2 + x_4^2 + x_3^2 - 1$
$x_8^2 + x_7^2 + x_6^2 - 1$
$(x_3^2x_8^2 - 2x_3x_5x_6x_8 + x_3^2x_7^2 - 2x_3x_4x_6x_7 + (x_5^2 + x_4^2)x_6^2)x_9^2 - x_3^2x_7^2 + 2x_3x_4x_6x_7 - x_4^2x_6^2$
$(x_3x_7 - x_4x_6)x_{10} + (-x_3x_8 + x_5x_6)x_9$
$(((x_2^2+x_1^2)x_3^2)x_7^2+((2x_1x_2x_3x_5-2x_2^2x_3x_4)x_6)x_7+(x_1^2x_5^2-2x_1x_2x_4x_5+x_2^2x_4^2+x_1^2x_3^2)x_6^2)x_{11}^2 - x_1^2x_3^2x_6^2$
$x_6x_{12} - x_7x_{11}$
$x_1x_3x_{13} - x_2x_3x_{12} + (-x_1x_5 + x_2x_4)x_{11}$
$(x_1^2x_3^2x_8^2 + (-2x_1x_2x_3^2x_7 + 2x_1x_2x_3x_4x_6)x_8 + x_2^2x_3^2x_7^2 - 2x_2^2x_3x_4x_6x_7 + ((x_2^2 + x_1^2)x_4^2 + x_1^2x_3^2)x_6^2)x_{14}^2 - x_1^2x_3^2x_6^2$
$x_3x_{15} - x_4x_{14}$
$x_1x_6x_{16} - x_2x_6x_{15} + (-x_1x_8 + x_2x_7)x_{14}$
$x_{17} + x_5^2x_{10}^2 + 2x_4x_5x_9x_{10} + x_4^2x_9^2 - 1$
$x_{18} + x_8^2x_{16}^2 + (2x_7x_8x_{15} + 2x_6x_8x_{14})x_{16} + x_7^2x_{15}^2 + 2x_6x_7x_{14}x_{15} + x_6^2x_{14}^2 - 1$
$x_{19} + x_2^2x_{13}^2 + 2x_1x_2x_{12}x_{13} + x_1^2x_{12}^2 - 1$
$x_{20} + x_8^2x_{10}^2 + 2x_7x_8x_9x_{10} + x_7^2x_9^2 - 1$
$x_{21} + x_2^2x_{16}^2 + 2x_1x_2x_{15}x_{16} + x_1^2x_{15}^2 - 1$
$x_{22} + x_5^2x_{13}^2 + (2x_4x_5x_{12} + 2x_3x_5x_{11})x_{13} + x_4^2x_{12}^2 + 2x_3x_4x_{11}x_{12} + x_3^2x_{11}^2 - 1$

We have $prem(g, ASC_1) = 0$ which means that the statement (ES, IS, g) is universally true.

Reference

[CH1] S.C. Chou, Proving and Discovering Geometry Theorems Using Wu's Method, PhD Thesis, Dept. of Math., University of Texas at Austin, 1985.

[CH2] S.C. Chou, *Mechanical Geometry Theorem Proving,* D.Reidel Publishing Company, 1988.

[CG1] S.C. Chou and X.S. Gao, Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving, TR-89-09, Computer Sciences Department, The University of Texas at Austin, March 1989.

[CG2] S.C. Chou and X.S. Gao, A Class of Geometry Statements of Constructive Type and Geometry Theorem Proving, TR-89-37, Computer Sciences Department, The University of Texas at Austin, November 1989.

[CK1] S.C. Chou and H.P. Ko, On the Mechanical Theorem Proving in Minkowskian Plane Geometry, *Proc. of Symp. of Logic in Computer Science*, pp187-192, 1986.

[CS2] S.C. Chou and W.F. Schelter, Proving Geometry Theorem with Rewrite Rules, *J. of Automated Reasoning* 2(4), 253-273.

[CY1] S.C. Chou and Yang Jingen, On the Algebraic Formulation of Certain Geometry Statements and Mechanical Geometry Theorem Proving, *Algorithmica*, Vol. 4, 1989, 237-262.

[GA1] X.S. Gao, Transcendental Functions and Mechanical Theorem Proving in Elementary Geometries, To appear at *J. of Automated Reasoning.*

[GW1] X.S. Gao and D.M. Wang, Geometry Theorems Proved Mechanically Using Wu's Method, Part on Elementary Geometries, MM preprint No2 1987.

[KA1] D. Kapur, Geometry Theorem Proving Using Hilbert's Nullstellensatz, *Proc. of SYMSAC'86*, Waterloo, 1986, 202–208.

[KU1] B.A. Kutzler, Algebraic Approaches to Automated Geometry Theorem Proving, Phd Thesis, Johnnes Kepler University, 1988.

[RI1] Ritt, J.F., *Differential Algebra*, Amer. Math. Soc., 1954.

[RY1] P. Ryan, *Euclidean and Non-Euclidean Geometries*, Cambridge, 1986.

[WU1] Wu Wen-tsün, On the Decision Problem and the Mechanization of Theorem in Elementary Geometry, *Scientia Sinica 21(1978)*, 159–172; Re-published in *Automated Theorem Proving: After 25 years*, A.M.S, Contemporary Mathematics, 29(1984), 213–234.

[WU2] Wu Wen-tsün, Basic Principles of Mechanical Theorem Proving in Geometries, Volume I: Part of Elementary Geometries, Science Press, Beijing (in Chinese), 1984.

[WU3] Wu Wen-tsün, Toward Mechanization of Geometry — Some Comments on Hilbert's "Grundlagen der Geometrie", *Acta Math. Scientia*, 2(1982), 125–138.

[YA1] I.M. Yaglom, *A Simple Non-Euclidean Geometry and Its Physical Basis*, Springer-Verlag, 1979.

Appendix A. Some Results about Ascending Chains

Let

$ASC =$
$A_1(U, x_1)$
$A_2(U, x_1, x_2)$
$\ldots$
$A_p(U, x_1, ..., x_p)$

be an ascending chain with the U as parameters and with the x as dependent variables. ASC is said to be an irreducible ascending chain if A_1 is irreducible, and for each k A_k is irreducible in $K(U)[x_1, ..., x_{k-1}]/(A_1, ..., A_{k-1})[x_k]$, where $(A_1, ..., A_{k-1})$ is the ideal generated by $\{A_1, ..., A_{k-1}\}$ in $K(U)[x_1, ..., x_{k-1}]$. If ASC is irreducible, we call $K = K(U)[X]/(ASC)$ the associate field of ASC.

We need the following results.

Theorem A.1. ASC is an irreducible ascending chain if and only if $PD(ASC)$ is a prime ideal.

Proof. See [RI1]. ∎

Lemma A.2. Let ASC be an irreducible ascending chain, then the pseudo remainder of a polynomial P w.r.t ASC is zero if and only if P is zero in the associate field of ASC.

Proof. P is zero in the associate field of ASC if and only if the product of P and a polynomial of the U is linear combination of the polynomials in ASC. This is true if and only if the P is in $PD(ASC)$ as the polynomial involving only the U is not in $PD(ASC)$ and $PD(ASC)$ is a prime ideal. ∎

Lemma A.3. Let ASC as above is irreducible, and $P = ay^2 + by + c$ be a polynomial where y is a new variable and a, b, and c are polynomials of the U and the X. Then $ASC \cup \{P\}$ is an irreducible ascending chain if and only if the pseudo remainder of a w.r.t ASC is not zero and $b^2 - 4ac$ is not a perfect square in the associate field of ASC.

Proof. See [CH1]. ∎

Lemma A.4. Polynomial $P = ax^2 + b$ in $K[x]$ is a perfect square in field $K(x)$ if and only if $a = 0$ and b is a perfect square in K or $b = 0$ and a is a perfect square in K.

Proof. At first note that if $P = Q^2$, then Q must be in $K[x]$ as the square of a proper rational function of x is still rational function. Let $Q = a_n x^n + ... + a_0$. Then $P = (a_n x_n^n + ... + a_0)^2$. Comparing coefficients for x we have $a_2 = a_3 = ..., a_n = 0$, $a_1^2 = a$, $2a_1 a_0 = 0$, and $a_0^2 = b$. From $2ab = 0$, we know that either $a = 0$ or $b = 0$. If $a = 0$, then $b = a_0^2$ must be a perfect square in K. If $b = 0$, then $a = a_1^2$ must be a perfect square in K. Q.E.D

The following result is for the completeness theorems proved in section 4.

Lemma A.5. Let ASC be an irreducible ascending chain and R be a polynomial with nonzero pseudo remainder wrpt ASC. Then a nonzero polynomial G vanishes on Zero$(PD(ASC)/R)$ for the complex field C iff prem$(G, ASC) = 0$.

Proof. The if part is obvious. As ASC is irreducible, $PD(ASC)$ is a prime ideal by theorem A.1. Since G vanishes on Zero($PD(ASC)/R$), GR vanishes on Zero($PD(ASC)$). Then $GR \in PD(ASC)$ by Hilbert's Zero Theorem. Since R is not in $PD(ASC)$, we have $G \in PD(ASC)$, i.e., prem$(G, ASC) = 0$. ∎

Lemma A.6. Let $ASC = f_1, \cdots f_p$ be a triangular form, I_p be the initial of f_p. Then we have

$$Zero(PD(ASC)/\{I_p\}) = Zero(PD(f_1 \cdots f_{p-1}) \cup \{f_p\}/\{I_k\})$$

Proof. Since $PD(f_1 \cdots f_{p-1}) \cup \{f_p\} \subset PD(ASC)$, then one direction is obviously true. To prove another direction, let $h \in PD(ASC)$, then $I_p^s h = Qf_p + R$ for some integer $s \geq 0$, and polynomials Q and $R \in PD(f_1, ..., f_{p-1})$. Thus a zero of $PD(f_1, ..., f_{p-1})$ and f_p which is not a zero of I_p is a zero of $PD(ASC)$. ∎

The following is another form of lemma 4.5 in [CG1].

Lemma A.7. Let $ASC = \{f_1, ..., f_r\}$ be a non-trivial ascending chain, $J = \{I_1, ..., I_r\}$ where I_i are the initials of f_i. Then

$$Zero(ASC/J) = \cup_{1 \leq i \leq l} Zero(PD(ASC_i)/J)$$

where each ASC_i is irreducible and with the same parameters as ASC.

Proof. Lemma 4.5 of [CG1] actually gives the following decomposition:

$$Zero(ASC/J) = \cup_{1 \leq i \leq k} Zero(ASC_i/J \cup J_i)$$

where the ASC_i are irreducible ascending chains with dimension $\leq n - r$ and J_i are the sets of initials for ASC_i. Then we have:

$$Zero(ASC/J) = \cup_{1 \leq i \leq k} Zero(PD(ASC_i)/J)$$

By dimension theorem, the components in the above decomposition with dimension lower than $d = n - r$ must be contained in a component with dimension d. From the proof of lemma 4.5, we know that the ascending chains ASC_i of dimension d in the decomposition are with the same parameters as ASC. This proves the lemma. ∎

Lemma A.8. For polynomial set PS, polynomials P_i $(i = 1, ..., k)$ and D, if $Zero(\{P_1, ..., P_k\})$ is contained in $Zero(D)$ we have:

$$Zero(PS/\{D\}) = \cup_{i=1}^{k} Zero(PS/\{D, P_i\}).$$

Proof. We have

$$Zero(PS/\{D\}) = Zero(PS \cup \{P_1, ..., P_k\}/\{D\}) \bigcup \cup_{i=1}^{k} Zero(PS/\{D, P_i\}).$$

Note the first component is empty as $Zero(\{P_1, ..., P_k\}) \subset Zero(D)$. Then we have proved the result. ∎

Lemma A.9. Let ASC_1 and ASC_2 be two ascending chains of which the later is irreducible. If the pseudo remainders of the polynomials in ASC_1 wrpt ASC_2 are zero and none of the pseudo remainders of the initials of ASC_1 wrpt ASC_2 is zero, then $PD(ASC_1) \subset PD(ASC_2)$.

Proof. See [CG1]. ▮

We have the following generalization for Lemma A.9.

Lemma A.10. Let ASC_1 and ASC_2 be two ascending chains, and

$$Zero(PD(ASC_2)) = \cup_{i=1}^{m} Zero(PD(ASC_i'))$$

be the irreducible decomposition of $PD(ASC_2)$. If the pseudo remainders of the polynomials in ASC_1 w.r.t ASC_2 are zero and none of the pseudo remainders of the initials of ASC_1 w.r.t ASC_i' for $(i = 1, ...m)$ is zero, then $Zero(PD(ASC_2)) \subset Zero(PD(ASC_1))$.

Proof. Let $h \in PD(ASC_1)$, then $Jh \in Ideal(ASC_1)$ where J is a product of the powers of some initials of the polynomials in ASC_1. As the pseudo remainders of the polynomials in ASC_1 w.r.t ASC_2 are zero, then $Jh \in Ideal(PD(ASC_2))$, hence $Jh \in PD(ASC_i')$ for $i = 1, ...m$. As none of the pseudo remainders of the initials of ASC_1 w.r.t ASC_i' is zero for $i = 1, ..., m$, then $prem(J, ASC_i') \neq 0$ for $i = 1, ..., m$. Thus $h \in PD(ASC_i')$ as $PD(ASC_i')$ are prime ideals. Hence a zero of $PD(ASC_2)$ is a zero of h. This proves the Theorem. ▮

For an ascending chain ASC, let

$$QD(ASC) = \{g \mid \exists J, Jg \in Ideal(ASC)\}$$

where J is a product of powers of the initials of the polynomials in ASC. By using $QD(ASC)$, the algorithm to compute the Grönber basis of $PD(ASC)$ when ASC is irreducible ([CH2]) can be generalized to the following form.

Theorem A.11. For an ascending chain ASC in $K[y]$, let $ID = Ideal(ASC, I_1 z_1 - 1, \cdots, I_p z_p - 1)$ where I_i are the initials of the polynomials in ASC and z_i are new variables. Then $QD(ASC) = ID \cap K[y]$.

Proof. Let $ASC = \{f_1, ..., f_p\}$. $QD(ASC) \subset ID \cap K[y]$ can be proved similarly as [CH2]. Let $P \in ID \cap K[y]$, then $P = \sum B_i f_i + \sum C_i(z_i I_i - 1)$ for some polynomials B_i and C_i in $K[y, z]$. Set $z_i = 1/I_i$ and clear the denominators. We have $JP = \sum B_i' f_i$ where J is a product of powers of the initials of the polynomials in ASC, i.e., $P \in QD(ASC)$. ▮

Theorem A.12. For polynomial sets PS and $DS = \{d_1, ..., d_p\}$ in $K[y]$, let $DP = Ideal(PS,$ $d_1 z_1 - 1,$ ... $, d_p z_p - 1)$ where z_i are new variables. If

$$Zero(PS/DS) = \cup_{i=1}^{m} Zero(PD(ASC_i)/DS) \tag{A.1}$$

is an irredundant decomposition for $Zero(PS/DS)$, then we have an irredundant decomposition for PD

$$Zero(DP) = \cup_{i=1}^{m} Zero(PD(ASC_i')) \tag{A.2}$$

where $ASC_i' = ASC_i, d_1 z_1 - 1, \cdots, d_p z_p - 1$, and vice versa.

Proof. Suppose we have (A.1). Since the pseudo remainders of the polynomials in DS wrpt ASC_i are not zero, then ASC_i' are weak irreducible ascending chains. Thus $PD \subset PD(ASC_i')$.

The one direction of (A.2) is proved. For the other direction, let (x_0, z_0) be a zero of $Zero(DP)$, then by the definition of DP we have $x_0 \in Zero(PS/DS)$. Thus $x_0 \in Zero(PD(ASC_i)/DS)$ for some i, say $i = 1$. We will prove $(x_0, z_0) \in Zero(PD(ASC_1'))$. Let $h \in PD(ASC_1')$, then $Jh = P + \sum C_i(z_i d_i - 1)$, where $P \in PD(ASC_1)$ and J is a product of the the powers of some d_i. As the d_i do not vanish on x_0, then (x_0, z_0) is a zero of h. Hence (A.2) is true. It is similar to derive (A.1) from (A.2) ▮

Theorem A.13. For an ascending chain ASC in $K[y]$, we have

$$Zero(QD(ASC)) = \cup_{i=1}^{m} Zero(PD(ASC_i))$$

where each ASC_i is irreducible and has the same parameter set as ASC.

Proof. Let J be the set of initials for ASC, then by Lemma A.7

$$Zero(ASC/J) = \cup_{1 \leq i \leq l} Zero(PD(ASC_i)/J)$$

where each ASC_i is irreducible and has the same parameter set as ASC. Then by Theorem A.12 and Theorem A.11,

$$Zero(PD(ASC)) = \cup_{1 \leq i \leq l} Zero(PD(ASC_i))$$

which proves the theorem. ▮

Appendix B. Some Basic Properties of P2

In this appendix, we shall prove some basic properties of **P2** using our prover based on Ritt-Wu's method. The results given in this section provide proofs for the equivalence of the DS in section 3.1 to certain combination of predicates in the real number case. For example, in case 4.3 $DS = \{\|p_1 \times (p_2 \times (p_3 \times p_4))\| \neq 0\}$ which is equivalent to $p_1 \times (p_2 \times (p_3 \times p_4)) \neq 0$ in the real number case. Now by $B12$, we get the result in section 3.1.

Let p_i be points on **S2** such that $\pi(p_i) = P_i \in \mathbf{P2}$ for $i = 1, ..., 6$.

B1. $P_1 = P_2$ iff $(p_1 \times p_2) = 0$.

Proof. If $P_1 = P_2$, we have $p_1 = p_2$ or $p_1 = -p_2$. Thus $(p_1 \times p_2) = 0$. If $(p_1 \times p_2) = 0$, there is a number r such that $p_1 = rp_2$. Then $\|p_1\| = r^2\|p_2\| = r^2 = 1$. We have $p_1 = p_2$ or $p_1 = -p_2$, i.e., $P_1 = P_2$. ▮

B2. Para(P_1, P_2, P_3, P_4) iff $P_1 = P_2$ or $P_3 = P_4$ or (coll(P_3, P_1, P_2) and coll(P_4, P_1, P_2) and coll(P_1, P_3, P_4) and coll(P_2, P_3, P_4)).

Proof. Using the following formulas

$$\begin{aligned}
(a \Rightarrow (b \text{ or } c)) &\longleftrightarrow ((a \text{ and } \neg b) \Rightarrow c)\\
((a \text{ or } b) \Rightarrow c) &\longleftrightarrow ((a \Rightarrow c) \text{ and } (b \Rightarrow c))\\
((a \Rightarrow b) \text{ and } (a \Rightarrow c)) &\longleftrightarrow (a \Rightarrow (b \text{ and } c))
\end{aligned}$$

B2 can be reduced to the following geometry statements

$$\begin{aligned}
&(\text{para}(P_1, P_2, P_3, P_4) \wedge P_1 \neq P_2 \wedge P_3 \neq P_4) \Rightarrow \text{coll}(P_3, P_1, P_2)\\
&(\text{para}(P_1, P_2, P_3, P_4) \wedge P_1 \neq P_2 \wedge P_3 \neq P_4) \Rightarrow \text{coll}(P_4, P_1, P_2)\\
&(\text{para}(P_1, P_2, P_3, P_4) \wedge P_1 \neq P_2 \wedge P_3 \neq P_4) \Rightarrow \text{coll}(P_1, P_3, P_4)\\
&(\text{para}(P_1, P_2, P_3, P_4) \wedge P_1 \neq P_2 \wedge P_3 \neq P_4) \Rightarrow \text{coll}(P_2, P_3, P_4)\\
&(P_1 = P_2) \Rightarrow \text{para}(P_1, P_2, P_3, P_4)\\
&(P_3 = P_4) \Rightarrow \text{para}(P_1, P_2, P_3, P_4)\\
&(\text{coll}(P_3, P_1, P_2) \wedge \text{coll}(P_4, P_1, P_2) \wedge \text{coll}(P_1, P_3, P_4) \wedge \text{coll}(P_2, P_3, P_4)\\
&\wedge P_1 \neq P_2 \wedge P_3 \neq P_4) \Rightarrow \text{para}(P_1, P_2, P_3, P_4)
\end{aligned}$$

which can be proved by our prover (Theorem 2.3). ▮

We have proved the following statements using the same method.

B3. Pole(P_1, P_2, P_3) iff perp(P_1, P_2, P_2, P_3) and perp(P_1, P_3, P_2, P_3).

B4. Pole(P_1, P_1, P_2) iff $P_1 = P_2$.

B5. Para(P_1, P_2, P_1, P_3) iff coll(P_1, P_2, P_3).

B6. We have $(p_1 \times p_2) \times (p_3 \times (p_4 \times p_5)) = 0$ iff pole(P_3, P_4, P_5) or (perp(P_1, P_2, P_4, P_5) and coll(P_1, P_2, P_3)).

B7. We have $(p_1 \times p_2) \times (p_3 - p_4) = 0$ or $(p_1 \times p_2) \times (p_3 + p_4) = 0$ iff $P_1 = P_2$ or (cong(P_1, P_3, P_1, P_4) and perp(P_1, P_2, P_3, P_4)).

B8. We have $(p_1 \times p_2) \times (p_1 - p_2) = 0$ or $(p_1 \times p_2) \times (p_1 + p_2) = 0$ iff $P_1 = P_2$.

B9. We have $(p_1 \times (p_2 \times p_3)) \times (p_4 \times (p_5 \times p_6)) = 0$ iff pole(P_1, P_2, P_3) or pole(P_4, P_5, P_6) or ($P_1 = P_2$ and cperp$(P_1, P_2, P_3, P_5, P_6)$) or (perp$(P_1, P_4, P_2, P_3)$ and perp(P_1, P_4, P_5, P_6)).

B10. We have $(p_1 \times (p_2 \times p_3)) \times (p_4 \pm p_5) = 0$ iff pole(P_1, P_2, P_3) or (cong(P_1, P_4, P_1, P_5) and cperp$(P_1, P_2, P_3, P_4, P_5)$).

B11. We have $(p_1 \pm p_2) \times (p_3 \pm p_4) = 0$ iff $P_1 = P_2$ or $P_3 = P_4$ or (cong(P_1, P_3, P_2, P_4) and cong(P_1, P_4, P_3, P_2)).

B12. We have $o \times (p_1 \times (p_2 \times p_3) = 0$ iff pole(P_1, P_2, P_3) or (coll(O, P_2, P_3) and polar(O, P_1)).

B13. We have $o \times (p_1 \pm p_2) = 0$ iff (coll(O, P_1, P_2) and cong(O, P_1, O, P_2)).