

---

Konrad-Zuse-Zentrum für Informationstechnik Berlin  
Heilbronner Str. 10, D-1000 Berlin 31



Jürgen Richter-Gebert \*)

## Mechanical Theorem Proving in Projective Geometry

\*) The author acknowledges partial support by the Konrad-Zuse-Zentrum Berlin  
Home Address: Auf dem Wingert 3, W-6101 Roßdorf

# Mechanical Theorem Proving in Projective Geometry

*Jürgen Richter-Gebert*

**Abstract:** We present an algorithm that is able to confirm projective incidence statements by carrying out calculations in the ring of all formal determinants (brackets) of a configuration. We will describe an implementation of this prover and present a series of examples treated by the prover, including *Pappos' and Desargues' Theorems*, the *Sixteen Point Theorem*, *Saam's Theorem*, the *Bundle Condition*, the *uniqueness of a harmonic Point* and *Pascal's Theorem*.

## 0. Introduction

*Mechanical theorem proving* deals with the question of developing algorithms which automatically produce proofs for given theorems. Mechanical theorem proving is on the one hand an interesting research goal for itself. On the other hand it is of great influence for topics like *computer aided geometric reasoning* [11], *robotics* and *robot motion planning* [10], *computer vision* and *scene analysis* [15], *rigidity of frameworks* [39], [40], *molecular conformation* [18], [16], *computer aided design* and *computer aided manufacturing* [23], and a lot of other related topics. In this paper we want to sketch an approach to mechanical theorem proving, based on the method of bi-quadratic final polynomials as introduced by J. Bokowski and J. Richter-Gebert in [2]. This method is of special interest for the case of projective incidence theorems since it makes use of the underlying geometric structure of the problem. Furthermore it provides a polynomial-time algorithm for confirming a large class of projective incidence theorems. Later on we will apply the prover to various problems.

One possible general outline for *mechanical geometric theorem proving* by algebraic methods can be described as follows

1. Choose a coordinate system
2. Translate the geometric theorem into an algebraic statement
3. Carry out the required algebraic manipulations
4. Retranslate the algebraic conclusions into geometric statements

## 0. Introduction

In 1951 A. Tarski gave a first decision method for what he called "elementary (real) geometry", which was based on an algebraic method [36]. This decision method was far from being of any practical use, but a first theoretical breakthrough was made. Later improvements like G. Collins' *cylindric algebraic decomposition* method [13] led also to practical algorithms which can be used to prove elementary geometric theorems, by algebraical methods.

When talking about algebraization of a geometric statement one has the choice between different levels of the algebraic translation. In particular, for the case of projective geometry we obtain the following hierarchy of algebraization levels (compare [38]).

1. Grassmann algebra
2. Bracket algebra
3. Coordinate algebra.

An introduction to Grassmann algebra (also called Cayley algebra) can be found in [38], [17]. Roughly speaking, Grassmann algebra is a multilinear algebra where projective subspaces are represented by their Plücker-coordinates. Operations like joins ( $\vee$ ) and meets ( $\wedge$ ) of projective subspaces can be carried out directly. There is a one-to-one correspondence between projective incidence properties and the terms in Grassmann algebra. Unfortunately it is difficult to check directly whether two terms of the Grassmann algebra are identical.

The next lower level of algebraization of a projective property is the bracket algebra. A bracket can be regarded as a formal variable representing the value of a determinant. The *bracket ring* as introduced by N. White [37] is the ring all bracket polynomials modulo the ideal generated by the Grassmann-Plücker polynomials. Up to a common scalar multiple, brackets are the fundamental invariants under projective transformations. Therefore the first theorem of invariant theorem states that any projective invariant, geometric property can be expressed as a homogeneous bracket equation. The bracket ring forms a suitable algebraic setting to deal with projective configurations in an invariant theoretic point of view. The bracket algebra is the most general structure where projective properties can be expressed in a coordinate free way. Any Grassmann algebra term can be easily expanded into a bracket algebra term. Using this fact one has a simple procedure for translating projective incidence properties into bracket algebra terms. The converse problem, "Cayley Factorization", is up to now not solved satisfactory. There is a theoretical result proved by B. Sturmfels and W. Whiteley [35] stating that every bracket algebra term can, after multiplication with a suitable bracket monomial, be factorized into a Grassmann algebra term. The algorithmic part of "Cayley Factorization" is up to now only solved for special cases (compare [38], [14]).

## 0. Introduction

After introducing coordinates every bracket algebra term can be expanded into a term of the usual coordinate algebra. In the coordinate algebra the geometric objects are directly represented by a suitable parameterization (vectors for points, center and radius for spheres etc.). The calculations are carried out directly, and arbitrary geometric objects (not only projective ones) can be expressed. Relations between geometric objects are expressed by suitable polynomials in the parameters. In general not all coordinate algebra terms factor into a bracket expression. Only those ones which are invariant under projective transformations can be so translated. In general it is difficult to recover the geometric meaning from the algebraic equations on the coordinate level.

Automated proving of theorems of projective geometry can be carried out on all different algebraic levels. An attempt on the level of coordinate algebra, lead to the well known approaches by *Ritt's characteristic set method* of W.T. Wu [41], [42], [43], [11], [12] and to the *Buchberger's Gröbner bases algorithm* of B. Buchberger [9], [10], [23], [24]. In both cases the main idea is to translate the hypotheses of the theorem as well as the conclusion into polynomials in the object parameters. After this is done a certain normal form algorithm is applied, which either proves that the polynomial representing the conclusion lies in the ideal generated by the hypotheses polynomials or generates certain *non-degeneracy* conditions under which the theorem becomes true (usually a complete collapse of the geometric configuration is induced by the non-degeneracy conditions if the theorem is false). In general both methods have the disadvantage that the success of the prover is heavily dependent on the choice of the "right" coordinate system and that the CPU-time grows over-exponential in the number of objects involved.

On the level of bracket algebra a geometric theorem prover can be implemented, using the so called *straightening algorithm* [17], [44]. The main idea behind this approach is to rewrite the projective incidence statement as a term in Grassmann algebra which vanishes if and only if the statement is true. After this the Grassmann algebra term is expanded into a bracket term. If this term vanishes modulo the ideal generated by the Grassmann-Plücker polynomials then the theorem is proved. There exist various implementations of the straightening algorithm which can solve this ideal-membership problem for special cases. The algorithm produces for a given bracket term an equivalent unique normalized term in *standard tableaux form*. This normalized term is zero if and only if the original bracket expression vanishes modulo the Grassmann-Plücker ideal. It was proved by N. White and B. Sturmfels [35] that the straightening algorithm can be considered as a special kind of Gröbner bases algorithm for bracket polynomials. The straightening algorithm works in full generality but requires over-exponential CPU-time as well.

The prover we want to present in this chapter works also on the bracket algebra level and makes use of the bi-quadratic final polynomial method introduced

in [2], [26]. Here any incidence relation is represented by a whole class of *bi-quadratic equations*. The main idea is to linearize the problem in a suitable way and to check whether a certain bi-quadratic equation can be deduced from a set of others. This can be done in principle by solving a system of linear equations. The necessary calculations can be carried out in polynomial time. Since only a restricted type of conclusions is allowed the algorithm will not work in general and will only be able to *confirm* theorems, not to *disprove* them (except of special cases as we will see in section 2). None the less, up to now the prover could manage all projective incidence theorems we tried to confirm with it. Section 2 will give an overview over a large class of examples. Using the automated prover based on bi-quadratic final polynomials, projective incidence theorems up to 25 points in the plane could be proved completely automatically.

## 1. Bi-quadratic expressions

Bi-quadratic final polynomials as introduced by J. Bokowski and J. Richter-Gebert [2], [26] are a method to prove non-realizability for *oriented matroids* [1]. bi-quadratic final polynomials can be considered as a specialization of the more general structure of *final polynomials* as introduced by J. Bokowski and B. Sturmfels [7]. The existence of a final polynomial forms a general criterion to prove the non-realizability of (oriented) matroids over a given field. In contrast to ordinary final polynomials, the bi-quadratic final polynomials are not generally applicable, but therefore very effectively to compute.

In this section we will adapt the bi-quadratic final polynomial method to the case of projective incidence theorems. In principle we will give a version of the bi-quadratic final polynomial method for the case of (ordinary) matroids. We prove an incidence statement by proving the non-realizability of a counterexample. This in turn can be done by finding a suitable bi-quadratic final polynomial. However we will present our results in a way that they are directly applicable to the case of projective incidence theorems.

A problem when proving geometric theorems automatically, is that a statement which is true for generic situations can become false when certain degenerations occur. Our first example will demonstrate this.

1. Bi-quadratic expressions

EXAMPLE 1.1.

Consider Desargues' Theorem: as pure incidence theorem it is often stated as follows (compare Figure 1.1.(a)):

Given ten points in the projective plane  $0, \dots, 9$ . Whenever the following triples of points are collinear:

$$(1, 2, 3); (1, 4, 8); (2, 4, 0); (2, 5, 9); (3, 5, 6); (3, 0, 8); (5, 0, 7); (9, 4, 7); (7, 6, 8)$$

then the triple  $(1, 6, 9)$  is also collinear.

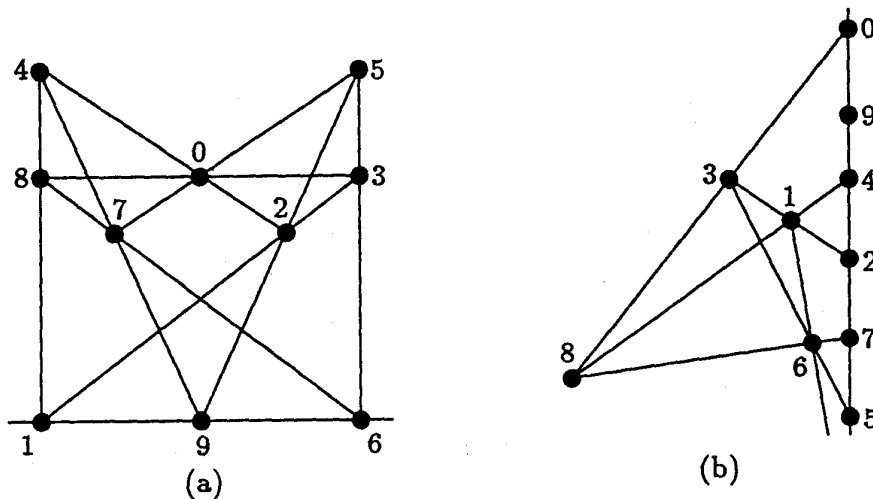


Figure 1.1 Desargues' Theorem.

This version of Desargues' Theorem is only true whenever the points are in suitably generic position. If one allows too many degenerations in the configuration the theorem becomes false. In Figure 1.1.(b). all the hypotheses of the above statement are fulfilled but the conclusion is obviously false.

To avoid such difficulties we will assume that the configurations under consideration are always suitable non-degenerate. To make this precise we define, how we want to express incidences in the real projective space  $\mathbb{RP}^{d-1} := (\mathbb{R}^d/\mathbb{R}) - \{0\}$ . Points are as usual represented by non-zero vectors in  $\mathbb{R}^d$  and vectors differing only by a non-zero scalar multiple represent the same point. Given  $d$  points  $x_1, \dots, x_d \in \mathbb{R}^d$  lie in a common hyperplane of  $P^{d-1}$  if and only if  $\det(x_1, \dots, x_d) = 0$ .

1. Bi-quadratic expressions

We now assume that a configuration  $X := (x_1, \dots, x_n)$  of  $n$  points in  $P^{d-1}$  is given. We set  $E := \{1, \dots, n\}$ . For a subset  $A := \{a_1, \dots, a_k\} \subset E$ ;  $d \leq k \leq n$  we define a logical predicate  $h_d(a_1, \dots, a_k)_X$  to be equivalent to the statement:

*All points in  $x_a$ ;  $a \in A$  are incident to a common hyperplane  $H$   
and none of the remaining points  $x_e$ ;  $e \in E - A$  is incident to  $H$ .*

Furthermore we define a weaker predicate  $h_d^*(A)_X$  indicating:

*All points in  $x_a$ ;  $a \in A$  are incident to a common hyperplane  $H$ .*

Using the predicates  $h_d(A)_X$  and  $h_d^*(A)_X$  we can now restate Desargues' Theorem as

*For any ten points  $X := (x_0, \dots, x_9)$  in  $P^2$  we have*

$$h_3(1, 2, 3)_X; h_3(1, 4, 8)_X; h_3(2, 4, 0)_X; h_3(2, 5, 9)_X; h_3(3, 5, 6)_X;$$

$$h_3(3, 0, 8)_X; h_3(5, 0, 7)_X; h_3(9, 4, 7)_X; h_3(7, 6, 8)_X$$

*implies  $h_3^*(1, 6, 9)_X$ .*

Desargues' Theorem stated this way is true, as we will see later.

Whenever no confusion can occur, we will drop the "For all configurations  $X \dots$ " part of the statement and the subscript  $X$  in the logical predicates  $h(A)_X$  and  $h^*(A)_X$ . We will also drop the subscript  $d$  whenever the dimension of the projective space is clear. Using this convention Desargues' Theorem can be simply stated as:

$$\left( h(1, 2, 3); h(1, 4, 8); h(2, 4, 0); h(2, 5, 9); h(3, 5, 6) \right.$$

$$\left. h(3, 0, 8); h(5, 0, 7); h(9, 4, 7); h(7, 6, 8) \right) \Rightarrow h^*(1, 6, 9).$$

Sometimes it will be necessary to state a certain non-degenerate situation explicitly. Therefore we define a third logical predicate  $g_d(A)_X$  equivalent to the statement that the points of  $X$  indexed by the elements of  $A$  lie in general position (i.e. no  $d$  points of  $A$  lie in a common hyperplane). In terms of the underlying matroid  $M_X$  of the configuration  $X$  the predicate  $g_d(A)_X$  is equivalent to the fact that the restriction of  $M_X$  to the elements in  $A$  is uniform. Notice that we have the following logical implications:

$$h_d(A)_X \Rightarrow h_d^*(A)_X \text{ and}$$

$$h_d(A)_X \Rightarrow g_d(\{a_1, \dots, a_{d-1}, e\}) \text{ for } (a_1, \dots, a_{d-1}) \in \Lambda(A, d-1) \text{ and } e \in E - A.$$

With the above predicates  $h$ ,  $h^*$  and  $g$  any projective incidence theorem containing only points and hyperplanes as objects can be expressed. Hyperplanes must be encoded implicitly as dependencies of points.

1. Bi-quadratic expressions

**DEFINITION 1.2.** For given rank  $d$  and a given set  $E := \{1, \dots, n\}$  and given subsets  $A_1, \dots, A_k, G_1, \dots, G_l \in E$  and a  $d$ -element subset  $C \subset E$  we call the statement

$$(h_d(A_1), \dots, h_d(A_k), g_d(G_1), \dots, g_d(G_l)) \Rightarrow h_d^*(C)$$

a projective incidence statement.

The predicates  $h_d(A_i), g_d(G_i)$  are the hypotheses of the statement and the predicate  $h_d^*(C)$  is called the conclusion of the statement. A projective incidence statement is called open if there is a configuration  $X$  in  $P^{d-1}$  fulfilling its hypotheses.

The task of our theorem prover is to check whether a given open projective incidence statement is true or not.

We now introduce *brackets* as formal expressions representing the  $d \times d$  sub-determinants of our configuration matrix  $X$ . For a  $d$ -tuple  $(a_1, a_2, \dots, a_d) \in E^d$  we abbreviate:

$$[a_1, a_2, \dots, a_d]_X := \det(x_{a_1}, x_{a_2}, \dots, x_{a_d}).$$

The values of the brackets of a given configuration  $X$  are not independent from each other. For instance they satisfy the alternating determinant rules

$$[a_{\pi(1)}, \dots, a_{\pi(d)}]_X = \text{sign}(\pi)[a_1, \dots, a_d]_X \quad (*)$$

for every permutation  $\pi \in S_d$ . Another special dependence among the brackets, which will play a crucial role for our considerations, is expressed in the next lemma.

**LEMMA 1.3.** For every configuration  $X = \{x_1, \dots, x_n\} \in (\mathbb{R}^n)^d$  and every  $(d+2)$  elements  $a_1, \dots, a_{d-2}, b, c, e, f \in \{1, \dots, n\}$  we have.

$$\begin{aligned} & [a_1, \dots, a_{d-2}, b, c]_X [a_1, \dots, a_{d-2}, e, f]_X \\ & + [a_1, \dots, a_{d-2}, b, e]_X [a_1, \dots, a_{d-2}, c, f]_X \\ & - [a_1, \dots, a_{d-2}, b, f]_X [a_1, \dots, a_{d-2}, c, e]_X = 0 \end{aligned}$$

**PROOF:** The lemma is simply a special case of the general Grassmann-Plücker-relations as described in [37].  $\square$

The next lemma will associate to any predicate  $h(A)$  or  $h^*(A)$  a set of expressions of the form:

$$[\dots]_X [\dots]_X = [\dots]_X [\dots]_X.$$

Such an expression will be called a *bi-quadratic equation* within the set of brackets.



1. Bi-quadratic expressions

**LEMMA 1.4.** *If for a configuration  $X := (x_1, \dots, x_n) \in (\mathbb{R}^d)^n$  the statement  $h_d^*(A)_X$  holds then we have:*

$$[a_1, \dots, a_{d-2}, b, e]_X [a_1, \dots, a_{d-2}, c, f]_X = [a_1, \dots, a_{d-2}, b, f]_X [a_1, \dots, a_{d-2}, c, e]_X$$

for any  $(a_1, \dots, a_{d-2}) \in \Lambda(A, d-2)$ ,  $b, c \in A - \{a_1, \dots, a_{d-2}\}$  and  $e, f \in E - A$ . Furthermore if  $h_d(A)$  holds then all brackets in the above expression are non-zero.

**PROOF:** The first part of the statement is simply a consequence of Lemma 1.3 and the fact that the bracket  $[a_1, \dots, a_{d-2}, b, c]_X$  vanishes whenever  $h_d^*(A)_X$  is true.

The second part of the lemma is simply a reformulation of the fact that whenever  $h_d(A)_X$  is true the points indexed by elements of  $E - A$  do not lie in the hyperplane spanned by the points indexed by elements of  $A$ .  $\square$

Conversely we have:

**LEMMA 1.5.** *If for a configuration  $X := (x_1, \dots, x_n) \in (\mathbb{R}^d)^n$  we have*

$$[a_1, \dots, a_{d-2}, b, e]_X [a_1, \dots, a_{d-2}, c, f]_X = [a_1, \dots, a_{d-2}, b, f]_X [a_1, \dots, a_{d-2}, c, e]_X$$

for  $(a_1, \dots, a_{d-2}) \in \Lambda(E, d-2)$  and  $b, c, e, f \in E - \{a_1, \dots, a_{d-2}\}$  then we have either  $h_d^*(\{a_1, \dots, a_{d-2}, b, c\})$  or  $h_d^*(\{a_1, \dots, a_{d-2}, e, f\})$ .

**PROOF:** Again, the lemma is simply a consequence of Lemma 1.3. If the sum of the last two summands in Lemma 1.3. is zero then also the first summand has to be zero as well. In this case at least one of the two statements  $h_d^*(\{a_1, \dots, a_{d-2}, b, c\})$  or  $h_d^*(\{a_1, \dots, a_{d-2}, e, f\})$  is true.  $\square$

A pair of brackets  $([a_1, \dots, a_d]_X, [b_1, \dots, b_d]_X)$  is called *comparable* if

$$|\{a_1, \dots, a_d\} \cap \{b_1, \dots, b_d\}| = d - 2.$$

Notice that the set of points in the two alternative conclusions in Lemma 1.5 form a pair of comparable brackets.

1. Bi-quadratic expressions

Using Lemma 1.4 and Lemma 1.5 we can now sketch how the mechanical prover will work in principle:

Finding a prove for the projective incidence statement:

$$\left( h_d(A_1), \dots, h_d(A_k), g_d(G_1), \dots, g_d(G_l) \right) \Rightarrow h_d^*(C)$$

can be subdivided into three steps:

1. Translate the hypotheses  $h_d(A_1), \dots, h_d(A_k)$  into a set  $\mathcal{A}$  of bi-quadratic equations using Lemma 1.4.
2. Translate any comparable pair of brackets  $([G], [C])$ , where  $g_d(G)$  is a known non-degeneracy, into the bi-quadratic equation suggested by Lemma 1.5. Collect these bi-quadratic equations in a set  $\mathcal{G}$ .
3. Check whether one of the equations in  $\mathcal{G}$  can be concluded algebraically from the equations in  $\mathcal{A}$ . If so, the projective incidence theorem is proved.

Now we are going to explain how to carry out step three of the above procedure. For this we linearize the problem in the same spirit as it was done in [2], where the oriented matroid case was considered. To make the algorithmic and algebraic background more transparent, we are going to study the structure detached from the concrete application to our bracket calculations. We therefore replace our brackets by variables  $x_1, \dots, x_m$  and think of bi-quadratic equations  $x_a x_b = x_c x_d$  in terms of rational functions  $\frac{x_a x_b}{x_c x_d} = 1$ . Let us start with some definitions.

**DEFINITION 1.6.** For given formal variables  $x_1, \dots, x_m$  the  $\mathbb{Z}$ -module of rational monomials  $M(x_1, \dots, x_m)$  is defined by:

$$M(x_1, \dots, x_m) := \left\{ x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_m^{\alpha_m} \mid (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}^m \right\}.$$

The module addition corresponds to the multiplication of two monomials, and the module multiplication by an integral scalar  $\lambda$  corresponds to taking the  $\lambda$ -th power of a monomial.

Notice that every bi-quadratic equation can be written in the form  $a = \pm 1$  where  $a \in M(x_1, \dots, x_m)$  is a suitable rational monomial in the brackets. The next lemma states explicitly the isomorphism between  $M(x_1, \dots, x_m)$  and the  $\mathbb{Z}$ -module  $\mathbb{Z}^m$ . The proof is trivial.

1. Bi-quadratic expressions

**LEMMA 1.7.** A module homomorphism  $f$  between  $M(x_1, \dots, x_m)$  and the  $\mathbb{Z}$ -module  $\mathbb{Z}^m$  is given by:

$$\begin{aligned} f : M(x_1, \dots, x_m) &\rightarrow \mathbb{Z}^m \\ x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_m^{\alpha_m} &\mapsto (\alpha_1, \alpha_2, \dots, \alpha_m). \end{aligned}$$

Now assume that a set of  $k$  equations of the form  $a_i = \sigma_i$  for  $0 \leq i \leq k$  is given, where  $a_i \in M(x_1, \dots, x_m)$  and  $\sigma_i \in \{-1, +1\}$ . The fact that  $a_0 = \sigma_0$  can be deduced from the rest of the equalities, corresponds to the existence of a suitable linear combination of the lattice points  $f(a_i)$ , as the next theorem shows:

**THEOREM 1.8.** Assume that  $a_i \in M(x_1, \dots, x_m)$  and  $\sigma_i \in \{-1, +1\}$  for  $0 \leq i \leq k$  are given and we have a linear combination of the form

$$\alpha_0 f(a_0) = \sum_{i=1}^k \alpha_i f(a_i); \quad \alpha_i \in \mathbb{Z}$$

where  $\alpha_0$  is an odd number. In this case for any  $(x_1, \dots, x_m) \in \mathbb{R}^m$  fulfilling  $x_i \neq 0$  for all  $1 \leq i \leq m$  and fulfilling  $a_i = \sigma_i$  for all  $1 \leq i \leq k$  we have:

$$a_0 = (-1)^\beta \text{ with } \beta := \sum_{\substack{i \in \{1, \dots, k\} \\ \sigma_i = -1}} \alpha_i.$$

Notice that if we have a linear combination as in the Theorem above we can conclude the sign of  $a_0$  using our information about the remaining monomials  $a_1, \dots, a_k$ .

**PROOF:** Assume that the requirements of the theorem are fulfilled. In this case we have:

$$a_0^{\alpha_0} := \prod_{i=1}^k a_i^{\alpha_i}.$$

In the case that we have values  $x_1, \dots, x_m \in \mathbb{R}$  fulfilling:

$$a_i = \sigma_i \text{ for } 1 \leq i \leq k,$$

we obtain:

$$a_0^{\alpha_0} := \prod_{i=1}^k \sigma_i^{\alpha_i}.$$

1. Bi-quadratic expressions

Since we had  $\sigma_i \in \{-1, +1\}$  for  $1 \leq i \leq k$  and  $\alpha_0$  was an odd integer we obtain:

$$a_0 = (-1)^\beta; \quad \beta := \sum_{\substack{i \in \{1, \dots, k\} \\ \sigma_i = -1}} \alpha_i.$$

This proves the theorem. □

Theorem 1.8 gives us the main key how to conclude a certain bi-quadratic equation  $a_0 = \sigma_0$  from others. One only has to be sure that there is a linear combination of the required form where  $\alpha_0$  is odd. After such a suitable linear combination is given it must be explicitly checked whether  $a_0 := (-1)^\beta = \sigma_0$ . If so the equation  $a_0 = \sigma_0$  can be concluded. Notice that it is essential to have  $\alpha_0$  an odd number. If  $\alpha_0$  was even one would still obtain  $\alpha_0 = \pm 1$ , but there would be no control over the sign.

It remains to develop a procedure that explicitly produces a suitable linear dependency if one exists. In principle this can be done by calculating an explicit lattice basis for the lattice spanned by the points  $f(a_1), \dots, f(a_k)$  (compare [21]). Here we prefer a way that turns out to be of less algorithmic effort.

In general the vector space  $V$  spanned by  $f(a_1), \dots, f(a_k)$  does not have the full rank  $k$ . There may be many ways to express  $\alpha_0 f(a_0)$  as a linear combination of the rest of the terms. In some of them  $\alpha_0$  may be odd, in some of them  $\alpha_0$  may be even. In order to get a procedure that decides whether there is a linear combination with odd  $\alpha_0$  we introduce a special basis of  $\text{span}(f(a_1), \dots, f(a_k))$ . We construct a basis  $\{b_1, \dots, b_l\} \subset \{f(a_1), \dots, f(a_k)\}$  with the following property:  
Whenever there exist  $\alpha_0, \dots, \alpha_k \in \mathbb{Z}$  where  $\alpha_0$  is odd and

$$\alpha_0 f(a_0) = \sum_{i=1}^k \alpha_i f(a_i)$$

Then there also exist  $\beta_0, \dots, \beta_l \in \mathbb{Z}$  where  $\beta_0$  is odd and

$$\beta_0 f(a_0) = \sum_{i=1}^l \beta_i b_i$$

Such a basis  $b_1, \dots, b_l$  will be called *rooted* for  $f(a_1), \dots, f(a_k)$ . It should be mentioned that  $b_1, \dots, b_l$  is not yet a lattice basis for the lattice spanned by the points  $f(a_1), \dots, f(a_k)$ . The following algorithm will produce a rooted basis for any given set of vectors  $v_1, \dots, v_k \in \mathbb{Z}^m$ .

ALGORITHM 1.9.INPUT: Vectors  $v_1, \dots, v_k \in \mathbb{Z}^m$ .OUTPUT: Rooted basis  $b_1, \dots, b_l \in \{v_1, \dots, v_k\}$  of  $v_1, \dots, v_k$ .

---

```

1.  $\mathcal{B} := \emptyset; \mathcal{V} := \{v_1, \dots, v_k\};$ 
2. FOR  $i := 1$  TO  $k$  DO
3.   IF  $v_i \in \text{span}(\mathcal{B})$  THEN
4.     BEGIN
5.       Pick linear combination  $\beta v_i = \sum_{j=1}^{|\mathcal{B}|} \beta_j v_j$ 
6.       such that  $\beta, \beta_j$  are integral and  $\text{gcd}(\beta, \beta_1, \dots, \beta_{|\mathcal{B}|}) = 1$ ;
7.       IF  $\beta$  is even THEN
8.         BEGIN
9.           Pick  $j$  such that  $\beta_j$  is odd;
10.           $\mathcal{B} := (\mathcal{B} - \{b_j\}) \cup v_i$ ;
11.        END
12.      ELSE
13.         $\mathcal{B} := \mathcal{B} \cup v_i$ ;
14.    END
15. OUTPUT( $\mathcal{B}$ );

```

---

THEOREM 1.10. Algorithm 1.9 is correct and produces a rooted basis for the vectors  $v_1, \dots, v_k$ .

PROOF: First we want to state the correctness of the algorithm. The only critical steps are step 4 and step 6. Step 4 is correct since whenever  $v_i$  is contained in  $\text{span}(\mathcal{B})$  then there exists a linear combination as required. Moreover, the linear combination is unique since  $v_1, \dots, v_{|\mathcal{B}|}$  are linearly independent and the greatest common divisor of  $\beta, \beta_1, \dots, \beta_{|\mathcal{B}|}$  was chosen to be 1. It can be computed easily, using any algorithm that is able to solve a system of linear equations. In Step 6, there is always at least one odd  $\beta_j$  since the greatest common divisor of  $\beta, \beta_1, \dots, \beta_{|\mathcal{B}|}$  was chosen to be 1.

It remains to show that  $\mathcal{B} := \{b_1, \dots, b_l\}$  is indeed a rooted basis for  $v_1, \dots, v_k$ . Assume that for  $v \in \mathbb{Z}^m$  there is an integral linear combination

$$\alpha v = \sum_{i=1}^k \alpha_i v_i, \quad (*)$$

Where  $\alpha$  is odd. We have to prove that there is also an integral linear combination

$$\beta v = \sum_{i=1}^l \beta_i b_i,$$

1. Bi-quadratic expressions

where  $\beta$  is odd. According to the choice made by our algorithm we can express any  $v_i$  as a linear combination

$$\gamma_i v_i = \sum_{j=1}^l \gamma_{(i,j)} b_j, \quad (**)$$

where the  $\gamma_i$  are odd integers. Multiplying the linear combination (\*) by  $\prod_{r=1}^k \gamma_r$  and applying (\*\*) we obtain:

$$\begin{aligned} & \left( \prod_{r=1}^k \gamma_r \right) \alpha v \\ &= \sum_{i=1}^k \left( \alpha_i \cdot \prod_{r=1}^k \gamma_r \cdot v_i \right) \\ &= \sum_{i=1}^k \left( \alpha_i \cdot \prod_{\substack{r \in \{1, \dots, k\} \\ r \neq i}} \gamma_r \cdot \sum_{j=1}^l \gamma_{(i,j)} b_j \right) \end{aligned}$$

Since  $\alpha, \gamma_1, \dots, \gamma_k$  are odd, the product of them is odd as well. This implies that the above equation is the desired linear combination.  $\square$

Using the concept of rooted bases it is now easy to decide whether a linear combination as required for Theorem 1.8 exists. The following algorithm is a more detailed version of step three of the our general outline of the prover given before.

1. Bi-quadratic expressions

**ALGORITHM 1.11.**

**INPUT:** Equations  $a_0 = \sigma_0, \dots, a_k = \sigma_k$  with  $a_i \in M(x_1, \dots, x_m)$   
and  $\sigma_i \in \{-1, +1\}$ .

**OUTPUT:** If "CONFIRMED" is returned then for non-zero  $x_1, \dots, x_m \in \mathbb{R}$   
the validity of  $a_1 = \sigma_1$  upto  $a_k = \sigma_k$  implies the  
validity of  $a_0 = \sigma_0$ .

- 
1. Compute a rooted basis  $b_1, \dots, b_l$  for  $f(a_1), \dots, f(a_k)$   
using Algorithm 9.11;
  2. IF  $f(a_0) \in \text{span}(b_1, \dots, b_l)$  THEN  
BEGIN
  3. Pick a linear combination  $\beta f(a_0) = \sum_{j=1}^l \beta_j b_j$   
such that  $\beta, \beta_j$  are integral and  $\text{gcd}(\beta, \beta_1, \dots, \beta_l) = 1$ ;
  4.  $s := \sum_{\substack{i \in \{1, \dots, l\} \\ \sigma_i = -1}} \beta_i$
  5. IF  $(-1)^s := \sigma_0$  and  $\beta$  is odd THEN
  6. OUTPUT("CONFIRMED");
- END;
- 

**PROOF OF THE CORRECTNESS OF ALGORITHM 1.11:** Similar to Algorithm 1.9 the only critical step is Step three. This step is correct since whenever  $f(a_0)$  is contained in  $\text{span}(b_1, \dots, b_l)$  then there exists a unique linear combination where  $\text{gcd}(\beta, \beta_1, \dots, \beta_l) = 1$  as required. It can be computed easily, using any algorithm that is able to solve a system of linear equations. If "CONFIRMED" is returned by the algorithm then by Theorem 9.10 for any  $x_1, \dots, x_m \in \mathbb{R}$  where  $x_i \neq 0$  for all  $1 \leq i \leq m$  and  $a_i = \sigma_i$  for all  $1 \leq i \leq k$  is fulfilled, also the equation  $a_0 = \sigma_0$  is fulfilled.  $\square$

Algorithm 1.11 can be used as an explicit procedure to carry out the check mentioned in step three of the general outline of the prover as sketched before. To finish the details of this algorithm we will finally explicitly describe the content of the sets  $\mathcal{A}$  and  $\mathcal{G}$  mentioned in step one and step two.

If

$$\left( h_d(A_1), \dots, h_d(A_k), g_d(G_1), \dots, g_d(G_l) \right) \Rightarrow h_d^*(C)$$

is the statement that should be proved we obtain the following assignments. The set  $\mathcal{A}$  should collect all bi-quadratic equations corresponding to the hypotheses  $h_d(A_1), \dots, h_d(A_k)$  of the projective incidence statement. Assume that the statement works on the set of points  $E$  in rank  $d$ . We can express the bi-quadratic

1. Bi-quadratic expressions

equations as rational monomials over  $M(\Lambda(E, d))$ . Therefore let  $\sigma[a_1, \dots, a_d]$  be the sign of the permutation of  $(a_1, \dots, a_d)$  and define:

$$\mathcal{A}_i := \left\{ \frac{[a, b, e][a, c, f]}{[a, b, f][a, c, e]} = \sigma[a, b, e]\sigma[a, c, f]\sigma[a, b, f]\sigma[a, c, e] \mid \right. \\ \left. a \in \Lambda(A_i, d-2); b, c \in A_i - \{a_1, \dots, a_{d-2}\}; e, f \in E - A_i \right\}$$

and

$$\mathcal{A} := \mathcal{A}_1 \cup \dots \cup \mathcal{A}_k.$$

Notice that all variables (i.e. brackets) occurring in the monomials are by definition non-zero, as required for Algorithm 1.11.

The set  $\mathcal{G}$  of bi-quadratic equations corresponding to the conclusion  $h_d^*(A)$  can be defined as follows. First define the set of brackets  $\bar{\mathcal{G}}$  that are known to be non-degenerate by:

$$\bar{\mathcal{G}} := \{G_1\} \cup \dots \cup \{G_l\} \cup \bigcup_{i=1}^k \left\{ [a, e] \mid a \in \Lambda(A_i, d-1); e \in E - A_i \right\}.$$

Then define the set  $\mathcal{G}$  of bi-quadratic equations corresponding to the conclusion by:

$$\mathcal{G} := \left\{ \frac{[a, b, e][a, c, f]}{[a, b, f][a, c, e]} = \sigma[a, b, e]\sigma[a, c, f]\sigma[a, b, f]\sigma[a, c, e] \mid \right. \\ \left. [G] \in \bar{\mathcal{G}}; ([C], [G]) \text{ are comparable and} \right. \\ \left. [C] := [a_1, \dots, a_{d-2}, c, b]; [G] := [a_1, \dots, a_{d-2}, e, f] \right\}.$$

The description of the geometric prover was given in a way that the main ideas become transparent. No attention was paid on the algorithmic efficiency of the developed algorithms. Indeed many of the computational steps can be speeded up in concrete implementations. For example, the set  $\mathcal{A}$  where all the bi-quadratic equations corresponding to the hypotheses were collected is much too large. Reduction methods as introduced in Corollary 5.10. can be applied reducing the number of bi-quadratic equations involved. Also the rooted basis has to be computed only once when proving a theorem. None the less, even for the version of the algorithm described above it is clear that for fixed rank the number of arithmetic steps necessary to carry out the calculations is bounded by a polynomial in the number of points involved.



## 2. A catalogue of examples

In this chapter we want to give a collection of examples of bi-quadratic final polynomial-proves for projective incidence statements. The first part of this chapter is dedicated to results found by a PASCAL implementation of the mechanical theorem prover as described in the last chapter. The implementation is able to handle incidence statements in the real projective plane. Besides the elementary incidences of the form *three points are collinear*, the program is also able to handle more complicated incidence properties like *line(a, b), line(c, d), line(e, f) meet in a common point*, or like *six points lie on a common conic*. It will be described below how this incidence statements can be managed. Among the results there will be proves for theorems like *Pappos' Theorem*, *Desargues' Theorem*, *Saam's Theorem* and lot of others.

After this we will give some bi-quadratic final polynomials for incidence theorems in higher dimensions. Most of these results were found by hand. Among the results there will be proves for the *bundle condition*, the *sixteen point theorem* and certain non-embedability proofs for some tori.

In the third part of this chapter, we will describe some infinite classes of projective incidence theorems that can be proved completely using bi-quadratic final polynomials. Among these results there will be a non-realizability proof for the minor minimal non-realizability class of oriented matroids given by J. Bokowski and B. Sturmfels.

We now start with a description of the implementation of the prover. The prover was developed especially for the planar case. The input consists of a certain set of hypotheses describing the geometric situation of the configuration, together with one conclusion. After the hypotheses are read and translated into a suitable set of rational monomial equations, a rooted basis is calculated as described in the last chapter. Then it is checked whether there exists a bi-quadratic final polynomial that proves that the conclusion is a consequence of the hypotheses.

It is assumed that the configuration consists of points belonging to a set  $E$ . The basic predicates used to describe the hypotheses of a geometric situation are the following four:

$h(A)$ :

*The points in  $A$  are collinear and  
the points in  $E - A$  do not lie on the line corresponding to  $A$ .*

$g(A)$ :

*The points in  $A$  are in general position.*

$m((a, b), (c, d), (e, f))$ :

*The three lines  $(a, b)$ ,  $(c, d)$ ,  $(e, f)$  are concurrent and distinct.*

$c(a, b, c, d, e, f)$ :

*the six points  $a, b, c, d, e, f$  lie on a common conic  
and no three of the points are collinear.*

The conclusions are described by the predicates:

$h^*(A)$ :

*The points in  $A$  are collinear.*

$m^*((a, b), (c, d), (e, f))$ :

*The three lines  $(a, b)$ ,  $(c, d)$ ,  $(e, f)$  have one point in common.*

$c^*(a, b, c, d, e, f)$ :

*the six points  $a, b, c, d, e, f$  lie on a common conic.*

We now explain how the predicates  $m((a, b), (c, d), (e, f))$ ,  $m^*((a, b), (c, d), (e, f))$ ,  $c(a, b, c, d, e, f)$  and  $c^*(a, b, c, d, e, f)$  can be expressed as rational monomial equations in the brackets. In correspondence to Lemma 1.4 we have:

**LEMMA 2.1.** *If for a configuration  $X := (x_1, \dots, x_n) \in (\mathbb{R}^d)^n$  the statement  $m((a_1, b_1), (a_2, b_2), (a_3, b_3))_X$  holds then we have*

$$[a_i, b_i, a_k]_X [a_j, b_j, b_k]_X = [a_i, b_i, b_k]_X [a_j, b_j, a_k]_X$$

and

$$[a_1, b_1, r_2]_X [a_2, b_2, s_3]_X [a_3, b_3, t_1]_X = -[a_1, b_1, r_3]_X [a_2, b_2, s_1]_X [a_3, b_3, t_2]_X$$

for any  $\{i, j, k\} = \{1, 2, 3\}$  and  $r, s, t \in \{a, b\}$ . Furthermore all brackets in the above expressions are non-zero.

2. A catalogue of examples

PROOF: Since any bracket of the above expressions is of the form  $[a_i, b_i, p]$ , where  $i \in \{1, 2, 3\}$  and  $p \in \{a_1, a_2, a_3, b_1, b_2, b_3\} - \{a_i, b_i\}$ , and the three lines  $(a_1, b_1)$ ,  $(a_2, b_2)$ ,  $(a_3, b_3)$  are assumed to be distinct, it is clear that none of the brackets is zero.

We now may assume that a configuration  $X$  is given such that the three lines  $(a_1, b_2)$ ,  $(a_2, b_2)$ ,  $(a_3, b_3)$  meet in a common point  $x_0$ . We first prove the validity of the second equation of the lemma. Therefore we assume w.l.o.g  $r = s = t := a$ . We have to prove:

$$[a_1, b_1, a_2]_X [a_2, b_2, a_3]_X [a_3, b_3, a_1]_X = -[a_1, b_1, a_3]_X [a_2, b_2, a_1]_X [a_3, b_3, a_2]_X.$$

Since  $(a_i, b_i, 0)$  is collinear for  $i = 1, \dots, 3$  we have  $[a_1, b_1, 0]_X = [a_2, b_2, 0]_X = [a_3, b_3, 0]_X = 0$  this implies the following three bi-quadratic equations:

$$\begin{aligned} [a_1, b_1, a_2]_X [a_1, 0, a_3]_X &= [a_1, b_1, a_3]_X [a_1, 0, a_2]_X \\ [a_2, b_2, a_3]_X [a_2, 0, a_1]_X &= [a_2, b_2, a_1]_X [a_2, 0, a_3]_X \\ [a_3, b_3, a_1]_X [a_3, 0, a_2]_X &= [a_3, b_3, a_2]_X [a_3, 0, a_1]_X. \end{aligned}$$

Multiplying all left and right sides and canceling pairs that occur on both sides gives the desired result.

To prove the first equation we may assume w.l.o.g that  $i := 1, j := 2, k := 3$ . We have to prove:

$$[a_1, b_1, a_3]_X [a_2, b_2, b_3]_X = [a_1, b_1, b_3]_X [a_2, b_2, a_3]_X.$$

Using the second equation of the lemma, we obtain:

$$\begin{aligned} [a_1, b_1, a_2]_X [a_2, b_2, a_3]_X [a_3, b_3, a_1]_X &= -[a_1, b_1, a_3]_X [a_2, b_2, a_1]_X [a_3, b_3, a_2]_X \text{ and} \\ [a_1, b_1, b_3]_X [a_2, b_2, a_1]_X [a_3, b_3, a_2]_X &= -[a_1, b_1, a_2]_X [a_2, b_2, b_3]_X [a_3, b_3, a_1]_X. \end{aligned}$$

Multiplying all left and right sides and canceling out pairs that occur on both sides gives the desired result.  $\square$

Indeed, there are more direct ways to prove the above lemma. We used this approach since it implies that all calculations could be carried out on the bi-quadratic equation level after a suitable point  $x_0$  had been added.

Conversely to Lemma 2.1 we have

**LEMMA 2.2.** *If for a configuration  $X := (x_1, \dots, x_6) \in (\mathbb{R}^d)^6$  we have*

$$[1, 2, 5]_X [3, 4, 6]_X = [1, 2, 6]_X [3, 4, 5]_X$$

where  $x_1 \neq x_2, x_3 \neq x_4$  and  $x_5 \neq x_6$  then the lines  $(1, 2), (3, 4), (5, 6)$  have one point in common (i.e. we have  $m^*((1, 2), (3, 4), (5, 6))$ ).

## 2. A catalogue of examples

PROOF: Again the proof can be done purely on the bi-quadratic equation level. Here we give an alternative proof based on the Grassmann algebra representation of the configuration (compare [38]). The Grassmann algebra expression  $(1 \vee 2) \wedge (3 \vee 4) \wedge (5 \vee 6)$  vanishes if and only if the three lines are not in general position (i.e. if they either meet in a point or at least two of the lines agree). Expanding this term into a bracket expression we get:

$$(1 \vee 2) \wedge (3 \vee 4) \wedge (5 \vee 6) = [1, 2, 5][3, 4, 6] - [1, 2, 6][3, 4, 5].$$

This proves the theorem. □

Finally, we want to give a bracket expression to express the fact that six lines lie on a common conic. This condition can be found in [40]:

**LEMMA 2.3.** *If for a configuration  $X := (x_1, \dots, x_6) \in (\mathbb{R}^d)^6$  the six points  $x_1, x_2, \dots, x_6$  lie on a common conic (i.e.  $c^*(1, 2, 3, 4, 5, 6)$  is true) then:*

$$[1, 2, 3]_X [1, 5, 6]_X [4, 2, 6]_X [4, 5, 3]_X = [4, 5, 6]_X [4, 2, 3]_X [1, 5, 3]_X [1, 2, 6]_X.$$

*If no three of the points are collinear all of the above brackets are non-zero.*

We now start with the descriptions of the examples.

**EXAMPLE 1.: PAPPUS' THEOREM**

For all points 1, 2, 3, 4, 5, 6, 7 in  $P^2$  we have:

$$\left[ h(236), h(137), m((12)(46)(57)), m((14)(67)(25)) \right] \Rightarrow h^*(345)$$

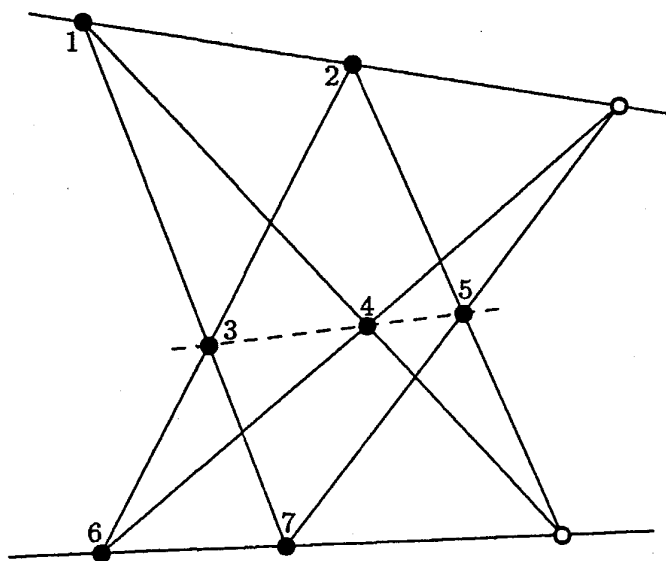


Figure 1.

The following bi-quadratic final polynomial was produced by the prover:

$$\begin{array}{ll} [124][567] = -[126][457] & \Leftarrow m([12], [46], [57]) \\ [145][267] = -[124][567] & \Leftarrow m([14], [67], [25]) \\ [123][347] = [134][237] & \Leftarrow h(137) \\ [126][237] = [123][267] & \Leftarrow h(236) \end{array}$$

$$[145][347] = [134][457] \quad \Rightarrow h^*(345)$$

Multiplying left and right sides of the first 4 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 2.: DESARGUES' THEOREM**

For all points 1, 2, 3, 4, 5, 6, 7, 8 in  $P^2$  we have:

$$\left[ h(123), h(148), h(356), m((16)(47)(25)), m((42)(57)(38)) \right] \Rightarrow h^*(678)$$

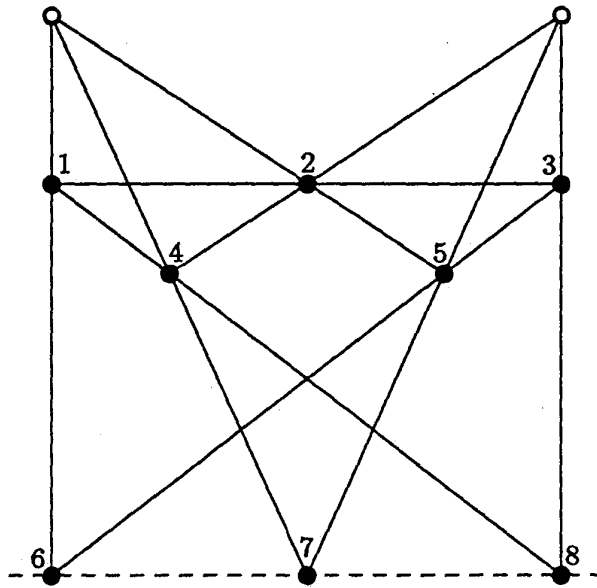


Figure 2.

The following bi-quadratic final polynomial was produced by the prover:

$[125][467] = -[147][256]$	$\Leftrightarrow m([16], [47], [25])$
$[234][578] = -[248][357]$	$\Leftrightarrow m([42], [57], [38])$
$[124][235] = [125][234]$	$\Leftrightarrow h(123)$
$[147][248] = [124][478]$	$\Leftrightarrow h(148)$
$[256][357] = [235][567]$	$\Leftrightarrow h(356)$
-----	
$[467][578] = [478][567]$	$\Rightarrow h^*(678)$

Multiplying left and right sides of the first 5 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 3.: PERMUTATION THEOREM**

The following incidence theorem is consequence of the so called *permutation theorem* (compare [19]):

If  $a, b, c, d$  are four points on a line  $L$ , then there exists a projectivity:

$$L(a, b, c, d) \sim L(d, c, b, a)$$

The oriented version of the corresponding incidence theorem occurred as one underlying non-realizable structure in the classification of arrangements with 10 points in the plane [5].

For all points 1, 2, 3, 4, 5, 6 in  $P^2$  we have:

$$\left[ m((16)(34)(25)), m((26)(34)(15)), m((12)(46)(35)) \right] \Rightarrow m^*((12)(36)(45))$$

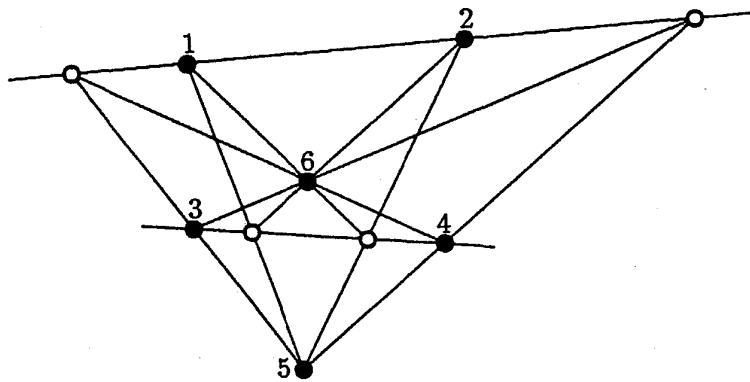


Figure 3.

The following bi-quadratic final polynomial was produced by the prover:

$$\begin{array}{lll} [125][346] = [134][256] & \Leftrightarrow & m([16], [34], [25]) \\ [134][256] = -[126][345] & \Leftrightarrow & m([26], [34], [15]) \\ [123][456] = -[125][346] & \Leftrightarrow & m([12], [46], [35]) \end{array}$$

$$[123][456] = [126][345] \quad \Rightarrow \quad m^*([12], [36], [45])$$

Multiplying left and right sides of the first 3 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 4.: ANOTHER 10-POINT INCIDENCE THEOREM**

This is another example of an incidence theorem that occurred as one underlying non-realizable structure in the classification of arrangements with 10 points in the plane [5].

For all points 1, 2, 3, 4, 5, 6, 7, 8 in  $P^2$  we have:

$$\left[ \begin{array}{l} h(147), h(257), h(654), h(348), h(678) \\ m((24)(18)(36)), m((26)(37)(58)) \end{array} \right] \Rightarrow h^*(123)$$

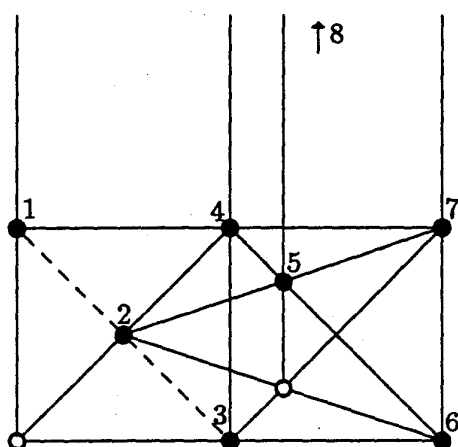


Figure 4.

The following bi-quadratic final polynomial was produced by the prover:

[148] [236] = -[128] [346]	<== m([24], [18], [36])
[267] [358] = [236] [578]	<== m([26], [37], [58])
[146] [157] = [167] [145]	<== h(147)
[124] [178] = [127] [148]	<== h(147)
[127] [578] = [157] [278]	<== h(257)
[138] [345] = -[134] [358]	<== h(348)
[145] [346] = [146] [345]	<== h(654)
[167] [278] = [178] [267]	<== h(678)
-----	
[124] [138] = [128] [134]	==> h*(123)

Multiplying left and right sides of the first 8 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.



**EXAMPLE 5.: HARMONIC POINTS**

The well known statement that if  $a, b, c, d$  is a harmonic quadruple of points on a line, the point  $d$  is uniquely determined by the other three, translates into the following incidence theorem.

For all points 1, 2, 3, 4, 5, 6, 7, 8, 9 in  $P^2$  we have:

$$\left[ h(136), h(234), h(456), h(479), h(678) \right. \\ \left. m((14)(35)(26)), m((48)(57)(69)) \right] \Rightarrow m^*((46)(12)(89))$$

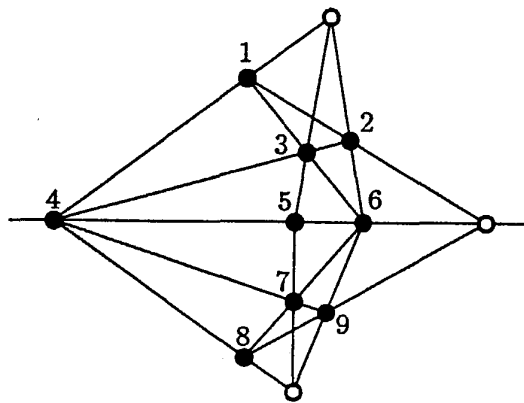


Figure 5.

The following bi-quadratic final polynomial was produced by the prover:

$[145][236] = -[134][256]$	$\Leftarrow m([14], [35], [26])$
$[469][578] = -[457][689]$	$\Leftarrow m([48], [57], [69])$
$[126][134] = -[123][146]$	$\Leftarrow h(136)$
$[123][246] = [124][236]$	$\Leftarrow h(234)$
$[146][256] = [156][246]$	$\Leftarrow h(456)$
$[156][457] = [145][567]$	$\Leftarrow h(456)$
$[467][489] = -[469][478]$	$\Leftarrow h(479)$
$[478][567] = [467][578]$	$\Leftarrow h(678)$

$$[126][489] = [124][689] \quad \Rightarrow m^*([46], [12], [89])$$

Multiplying left and right sides of the first 8 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 6.: COMPLETE QUADRILATERAL**

The last example can be considered as a special case of the following fact:  
*If  $a, b, c, d, e$  and  $f$  are the points of intersection of the sides of a complete quadrilateral with a line, then  $f$  is uniquely determined by  $a, b, c, d$  and  $e$ .*

Here is the corresponding incidence theorem:  
 For all points 1, 2, 3, 4, 5, 6, 7, 8, 9 in  $P^2$  we have:

$$\left[ \begin{array}{l} h(456), m((14)(25)(36)), m((74)(85)(96)) \\ m((45)(12)(78)), m((46)(12)(78)), m((45)(23)(89)) \\ m((46)(23)(89)) \end{array} \right] \Rightarrow m^*((46)(13)(79))$$

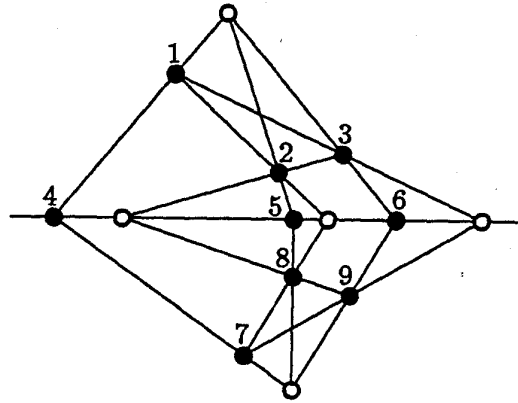


Figure 6.

The following bi-quadratic final polynomial was produced by the prover:

$$\begin{array}{lll} [125] [134] [236] = [124] [136] [235] & \Leftarrow m([14], [25], [36]) \\ [478] [589] [679] = [479] [578] [689] & \Leftarrow m([74], [85], [96]) \\ [124] [578] = [125] [478] & \Leftarrow m([45], [12], [78]) \\ [235] [489] = [234] [589] & \Leftarrow m([45], [23], [89]) \\ [234] [689] = [236] [489] & \Leftarrow m([46], [23], [89]) \\ \hline [134] [679] = [136] [479] & \Rightarrow m^*([46], [13], [79]) \end{array}$$

Multiplying left and right sides of the first 5 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

### EXAMPLE 7.: SAAM'S THEOREM

The following projective incidence theorem is due to Saam [29], [30]. It is the smallest representative of an infinite class of projective incidence theorems. A proof for the next larger representative was also found by the prover. It is still an open questions whether all representatives admit a bi-quadratic final polynomial-proof. An alternative algebraic proof of this representative can be found in [32]. For all points 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B in  $P^3$  we have:

$$\left[ \begin{array}{l} m((17)(26)(B4)), m((28)(37)(B5)) \\ m((39)(48)(B1)), m((4A)(59)(B2)) \\ h(16B), h(27B), h(38B), h(49B), h(5AB) \end{array} \right] \Rightarrow m^*((56)(1A)(B3))$$

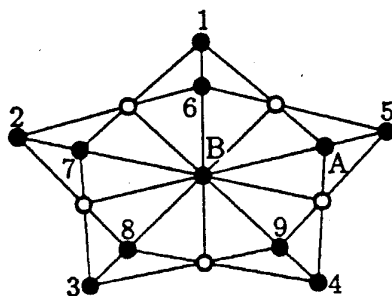


Figure 7.

The following bi-quadratic final polynomial was produced by the prover:

[127] [14B] [26B] = [126] [17B] [24B]	<== m([17], [26], [B4])
[237] [28B] [35B] = [238] [25B] [37B]	<== m([28], [37], [B5])
[14B] [348] [39B] = [13B] [349] [48B]	<== m([39], [48], [B1])
[25B] [459] [4AB] = [24B] [45A] [59B]	<== m([4A], [59], [B2])
[156] [26B] = [126] [56B]	<== h(16B)
[127] [37B] = -[17B] [237]	<== h(27B)
[48B] [238] = -[348] [28B]	<== h(38B)
[59B] [349] = -[459] [39B]	<== h(49B)
[45A] [3AB] = [3AB] [35A]	<== h(5AB)
[35A] [56B] = [35B] [56A]	<== h(5AB)

---


$$[156] [3AB] = -[13B] [56A] \quad \implies m^*((56), [1A], [B3])$$

Multiplying left and right sides of the first 10 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 8.: A SEQUENCE OF PERSPECTIVITIES**

The following example is one representative of an infinite sequence of incidence theorems given by A. Saam in [30]. The theorems state that the composition of a certain sequence of perspectivities is the identity. A proof for the whole class of theorems is given in Example 20. The proof for this incidence theorem was produced automatically; the CPU-time was about 10 minutes on an ATARI Computer. The final polynomial is given on the next page.

For all points 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H in  $P^2$  we have:

$$\left[ \begin{aligned} &h(123), h(345), h(567), h(789), h(9AB), h(BCD), h(DEF), h(FG1) \\ &m((24)(EG)(H1)), m((2G)(46)(3H)), m((24)(68)(5H)) \\ &m((46)(8A)(7H)), m((68)(AC)(9H)), m((A8)(CE)(BH)) \\ &m((AC)(EG)(DH)) \end{aligned} \right] \Rightarrow m^*((2G)(EC)(FH))$$

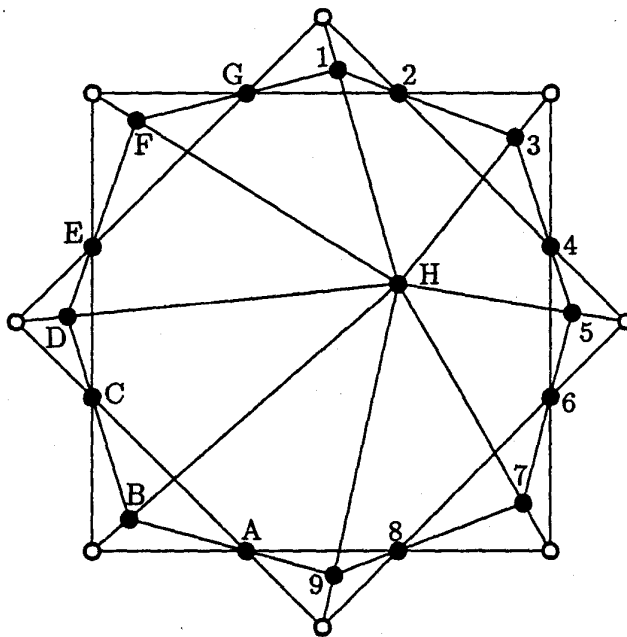


Figure 8.

The following bi-quadratic final polynomial was produced by the prover:

$$\begin{array}{l}
 [124] [EGH] = [1EG] [24H] \\
 [23G] [46H] = -[2GH] [346] \\
 [24H] [568] = [245] [68H] \\
 [467] [8AH] = [46H] [78A] \\
 [68H] [9AC] = [689] [ACH] \\
 [8AB] [CEH] = [8AH] [BCE] \\
 [ACH] [DEG] = [ACD] [EGH] \\
 [12G] [234] = [124] [23G] \\
 [1DF] [2FG] = [12F] [DFG] \\
 [12F] [1EG] = [12G] [1EF] \\
 [347] [245] = [457] [234] \\
 [357] [346] = [347] [356] \\
 [457] [356] = [456] [357] \\
 [678] [456] = [568] [467] \\
 [78B] [689] = [89B] [678] \\
 [79B] [78A] = [78B] [79A] \\
 [89B] [79A] = [89A] [79B] \\
 [ABC] [89A] = [9AC] [8AB] \\
 [BCE] [ACD] = [CDE] [ABC] \\
 [1EF] [CDE] = [1DE] [CEF] \\
 [1DE] [DFG] = [1DF] [DEG] \\
 [2FG] [CEH] = -[2GH] [CEF] \\
 \implies m^*([2G], [EC], [FH])
 \end{array}$$

Multiplying left and right sides of the first 21 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 9.: PASCAL'S THEOREM**

Pascal's Theorem is a well known generalization of Pappos' Theorem. It can be formulated as follows:

*If  $(a, b, c, d, e, f)$  is a hexagon where the six vertices lie on a conic, then the intersections of opposite sides lie on a common line.*

The following theorem is a slightly more special version, since the conic is assumed not to degenerate into two straight lines.

For all points 1, 2, 3, 4, 5, 6, 7, 8, 9 in  $P^2$  we have:

$$\left[ h(175), h(186), h(274), h(296), h(384), h(395), c(123456) \right] \Rightarrow h^*(789)$$

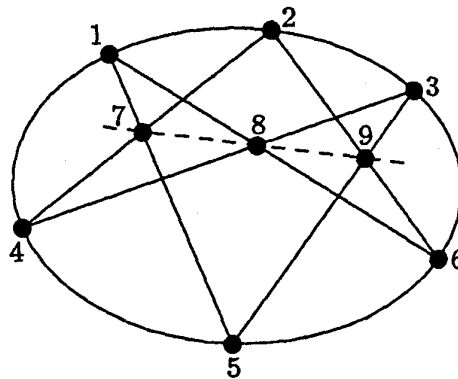


Figure 9.

The following bi-quadratic final polynomial was produced by the prover:

$$\begin{array}{lll}
 [125] [136] [246] [345] = [126] [135] [245] [346] & \Leftarrow & C(123456) \\
 [159] [257] = -[125] [579] & \Leftarrow & h(175) \\
 [126] [368] = [136] [268] & \Leftarrow & h(186) \\
 [245] [279] = -[249] [257] & \Leftarrow & h(274) \\
 [249] [268] = -[246] [289] & \Leftarrow & h(296) \\
 [346] [358] = [345] [368] & \Leftarrow & h(384) \\
 [135] [589] = -[159] [358] & \Leftarrow & h(395) \\
 \hline
 [279] [589] = [289] [579] & \Rightarrow & h^*(789)
 \end{array}$$

Multiplying left and right sides of the first 7 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 10.: A NON-REALIZABLE  $10_3$ -CONFIGURATION**

Among the 11 combinatorial types of  $10_3$  configurations there is one non-realizable one, namely the one with the following triples of points collinear (compare [25]):

$$[136], [148], [235], [247], [129], [689], [579], [34A], [56A], [78A]$$

The nonrealizability can be stated as follows (here the conclusion forces a complete collapse of the configuration):

For all points  $1, 2, 3, 4, 5, 6, 7, 8, 9, A$  in  $P^2$  we have:

$$\left[ \begin{array}{l} h(129), h(136), h(148), h(235), h(247), h(34A) \\ h(579), h(56A), h(689), h(78A) \end{array} \right] \Rightarrow h^*(512)$$

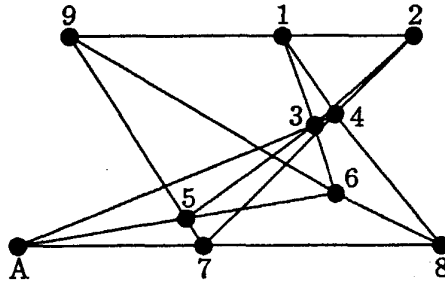


Figure 10.

The following bi-quadratic final polynomial was produced by the prover:

$[128] [179] = [127] [189]$	$\Leftarrow h(129)$
$[146] [13A] = -[134] [16A]$	$\Leftarrow h(136)$
$[124] [168] = -[128] [146]$	$\Leftarrow h(148)$
$[234] [25A] = -[245] [23A]$	$\Leftarrow h(235)$
$[127] [245] = -[124] [257]$	$\Leftarrow h(247)$
$[134] [23A] = [13A] [234]$	$\Leftarrow h(34A)$
$[16A] [57A] = [15A] [67A]$	$\Leftarrow h(34A)$
$[157] [789] = -[179] [578]$	$\Leftarrow h(579)$
$[189] [678] = -[168] [789]$	$\Leftarrow h(689)$
$[578] [67A] = [57A] [678]$	$\Leftarrow h(78A)$

$$[157] [25A] = [15A] [257] \quad \Rightarrow h^*(512)$$

Multiplying left and right sides of the first 10 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 11.: BUNDLE CONDITION**

The following Examples all take place in projective 3-space. The most easy incidence theorem is the so called *bundle condition* (also known as *Veblen-Young axiom*):

Let  $l_1, l_2, l_3, l_4$  be four lines in  $P^3$ . If five pairs of lines are coplanar then the sixth pair is also coplanar.

Assuming that the lines are spanned by pairs of points  $(1, 5), (2, 6), (3, 7), (4, 8)$  the theorem can be stated as follows:

For all points  $1, 2, 3, 4, 5, 6, 7, 8$  in  $P^3$  we have:

$$\left[ h(1256), h(1357), h(1458), h(2367), h(2468) \right] \Rightarrow h^*(3478)$$

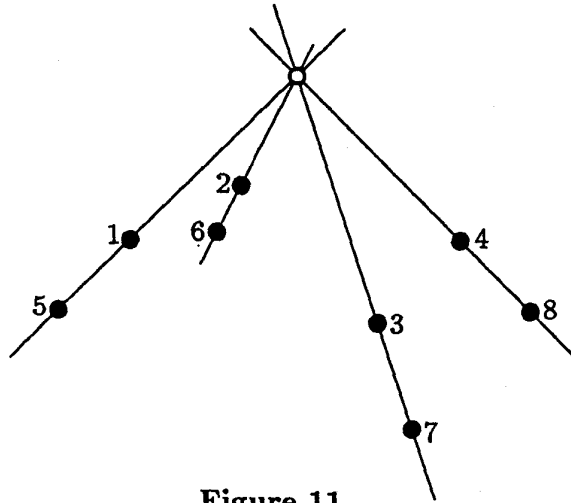


Figure 11.

The following bi-quadratic final polynomial implies the statement:

$[1235][1246]$	$=$	$[1236][1245]$	$\Leftrightarrow$	$h(1256)$
$[1327][1345]$	$=$	$[1325][1347]$	$\Leftrightarrow$	$h(1357)$
$[1425][1438]$	$=$	$[1428][1435]$	$\Leftrightarrow$	$h(1458)$
$[2316][2347]$	$=$	$[2317][2346]$	$\Leftrightarrow$	$h(2367)$
$[2418][2436]$	$=$	$[2416][2438]$	$\Leftrightarrow$	$h(2468)$
$[3418][3427]$	$=$	$[3417][3428]$	$\Rightarrow$	$h^*(3478)$

Multiplying left and right sides of the first 5 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.



**EXAMPLE 12.: SIXTEEN-POINT THEOREM I**

The following theorem is known as the sixteen-point theorem (compare [22]):  
*Given 8 lines  $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$  in  $P^3$ . If fifteen of the pairs  $(a_i, b_j)$  are coplanar the sixteenth pair is also coplanar.*

Using the assumed incidences among the lines one can parameterize the lines using only 8 points. Up to isomorphism there are two ways to do this. Here is the first one that can also be interpreted as a non-realizability statement for a certain torus with 8 vertices (compare [3], [4]):

For all points 1, 2, 3, 4, 5, 6, 7, 8 in  $P^3$  we have:

$$\left[ h(1256), h(2367), h(3456), h(4167), h(3478), h(4185), h(1278) \right] \Rightarrow h^*(2385)$$

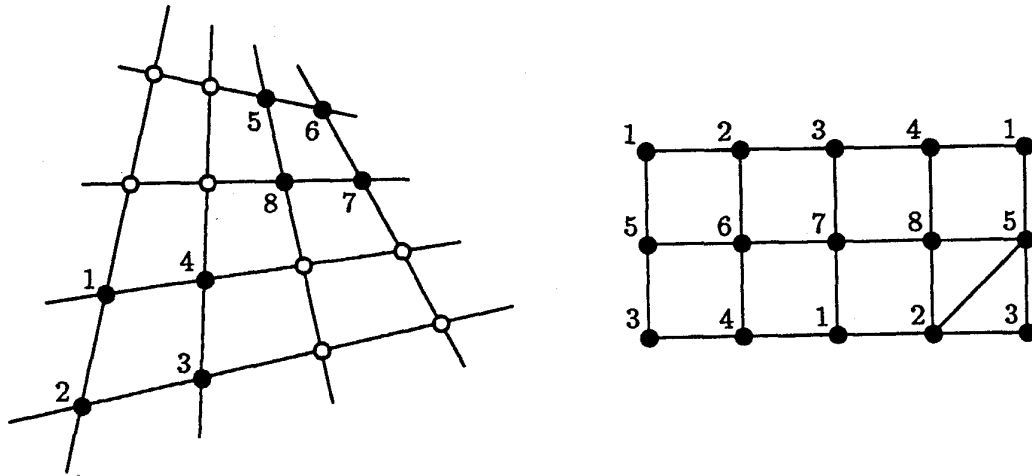


Figure 12.

The following bi-quadratic final polynomial implies the statement:

$$\begin{aligned} [1253] [1264] &= [1254] [1263] &<== h(1526) \\ [2361] [2374] &= [2364] [2371] &<== h(2637) \\ [3451] [3462] &= [3452] [3461] &<== h(6453) \\ [1463] [1472] &= [1462] [1473] &<== h(6471) \\ [3471] [3482] &= [3472] [3481] &<== h(4837) \\ [1452] [1483] &= [1453] [1482] &<== h(4815) \\ [1273] [1284] &= [1274] [1283] &<== h(8271) \end{aligned}$$

$$[2351] [2384] = [2354] [2381] \quad ==> h^*(8253)$$

Multiplying left and right sides of the first 7 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 13.: SIXTEEN-POINT THEOREM II**

This is the second combinatorial way to express the sixteen-point theorem as an incidence theorem on 8 points in projective 3-space. Again, the structure can be interpreted as the nonrealizability of a suitable torus. It should be mentioned that the oriented versions of the last three examples as non-realizable oriented matroids are the only non-realizable structures for uniform rank 4 oriented matroids with 8 points [3], [4].

For all points 1, 2, 3, 4, 5, 6, 7, 8 in  $P^3$  we have:

$$\left[ h(1245), h(2356), h(3467), h(4578), h(5681), h(6712), h(7823) \right] \Rightarrow h^*(8134)$$

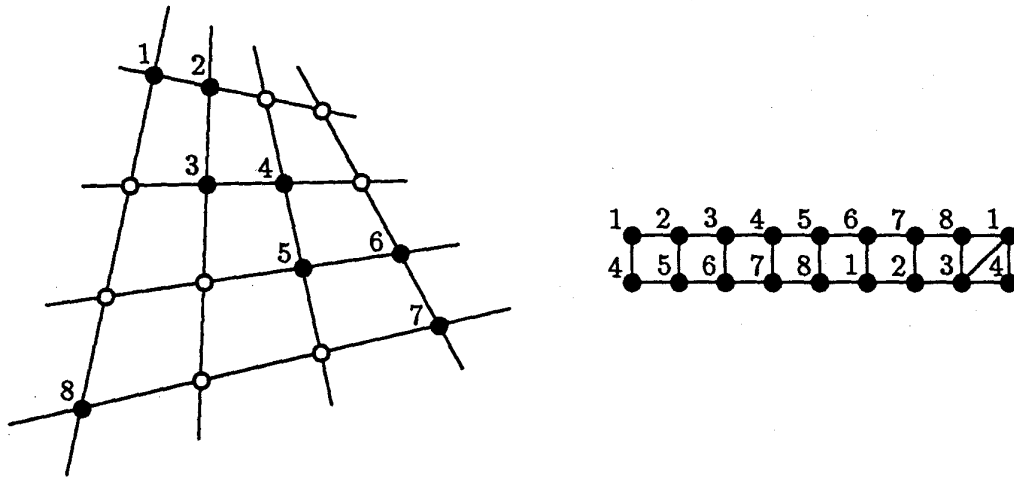


Figure 13.

The following bi-quadratic final polynomial implies the statement:

[4218] [4256] = [4216] [4258]	<== h(1245)
[2658] [2634] = [2654] [2638]	<== h(2356)
[6438] [6472] = [6432] [6478]	<== h(3467)
[4876] [4852] = [4872] [4856]	<== h(4578)
[8654] [8612] = [8652] [8614]	<== h(5681)
[6214] [6278] = [6218] [6274]	<== h(6712)
[2874] [2836] = [2876] [2834]	<== h(7823)

---


$$[8436] [8412] = [8432] [8416] \quad ==> \quad h^*(8134)$$

Multiplying left and right sides of the first 7 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 14.: A NON-REALIZABLE TORUS**

As a last example in projective 3-space, we give an incidence theorem that also can be expressed as the non-realizability of a suitable torus (compare [7]). An alternative geometric proof is due to D. Ljubić:

For all points 1, 2, 3, 4, 5, 6, 7, 8, 9 in  $P^3$  we have:

$$\left[ \begin{array}{l} h(1245), h(2356), h(3164), h(4578) \\ h(5689), h(6497), h(7812), h(8923) \end{array} \right] \Rightarrow h^*(9741)$$

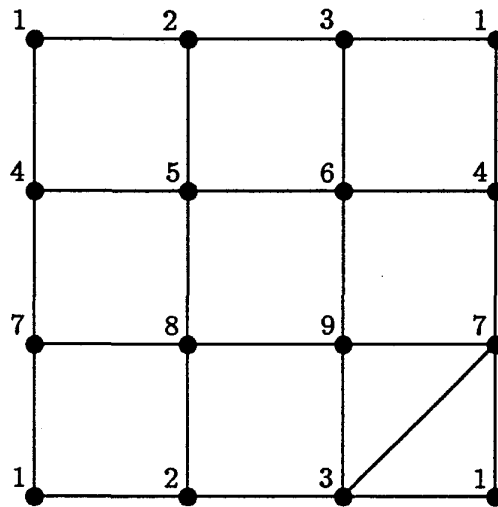


Figure 14.

The following bi-quadratic final polynomial implies the statement:

[1427] [1458] = [1428] [1457]	<== h(1245)
[2538] [2569] = [2539] [2568]	<== h(2356)
[3619] [3647] = [3617] [3649]	<== h(3164)
[4571] [4586] = [4576] [4581]	<== h(4578)
[5682] [5694] = [5684] [5692]	<== h(5689)
[6493] [6475] = [6495] [6473]	<== h(6497)
[1273] [1284] = [1274] [1283]	<== h(7812)
[2381] [2395] = [2385] [2391]	<== h(8923)

[3196] [3172] = [3192] [3176]	==> h*(9741)
-------------------------------	--------------

Multiplying left and right sides of the first 8 bi-quadratic equations, and canceling brackets that occur on both sides, implies the last equation.

**EXAMPLE 15.: THE GOODMAN/POLLACK N-STAR**

Let us close this chapter with two examples of infinite classes of projective incidence theorems. The first one is the  $n$ -star which is due to E. Goodman and R. Pollack [20]. An oriented version of this class was used by J. Bokowski and B. Sturmfels [8] as a minor minimal class of non-realizable oriented matroids. It was a longstanding question whether a bi-quadratic final polynomial for the whole class exists.

For any  $n \geq 5$  and all points  $A_1, \dots, A_n, C, B$  in  $P^2$  we have:

$$\left[ \begin{aligned} &h(A_{n-2}A_1B), h(A_{n-1}A_nB), h(A_{n-1}A_2C), h(A_nA_1C), \\ &m((A_1A_4)(A_2A_3)(BC)), m((A_2A_5)(A_3A_4)(BC)), \dots, \\ &m((A_{n-3}A_n)(A_{n-2}A_{n-1})(BC)) \end{aligned} \right] \Rightarrow m^*((A_nA_3)(A_1A_2)(BC))$$

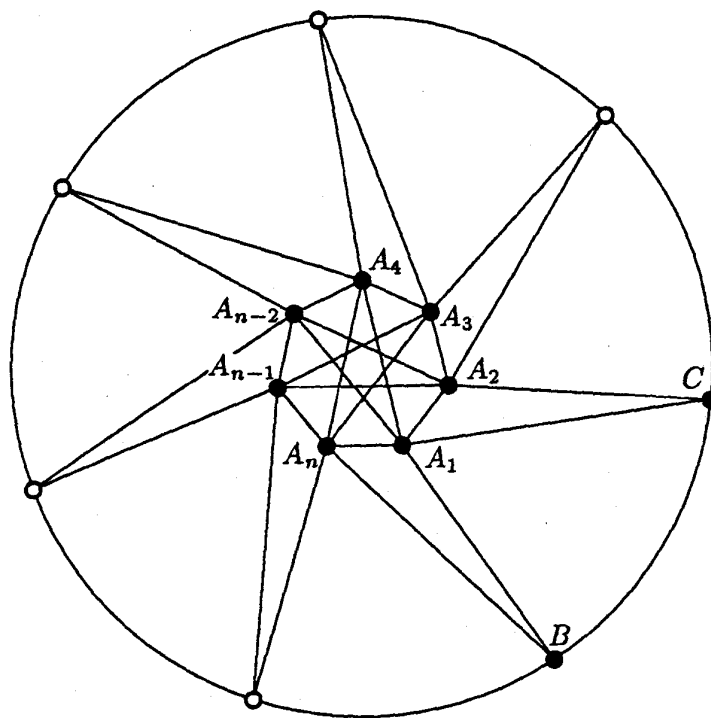


Figure 15.

The following sequence of bi-quadratic equations is in one-to-one correspondence to the sequence of hypotheses:

$$\begin{aligned}
[BA_{n-2}C][BA_1A_{n-1}] &= [BA_{n-2}A_{n-1}][BA_1C] \\
[A_{n-1}A_nA_1][A_{n-1}BA_{n-2}] &= [A_{n-1}BA_1][A_{n-1}A_nA_{n-2}] \\
[CA_{n-1}B][CA_2A_n] &= [CA_{n-1}A_n][CA_2B] \\
[A_nA_1A_2][A_nCA_{n-1}] &= [A_nCA_2][A_nA_1A_{n-1}] \\
[A_2A_3A_4][BCA_1] &= [A_2A_3A_1][BCA_4] \\
[A_3A_4A_5][BCA_2] &= [A_3A_4A_2][BCA_5] \\
&\vdots \\
&\vdots \\
[A_{n-2}A_{n-1}A_n][BCA_{n-3}] &= [A_{n-2}A_{n-1}A_{n-3}][BCA_n]
\end{aligned}$$


---

$$[A_1A_2A_3][BCA_n] = [A_1A_2A_n][BCA_3]$$

Multiplying left and right sides of the first  $n + 3$  bi-quadratic equations and canceling out brackets that occur on both sides implies the last equation.

**EXAMPLE 16.: A SEQUENCE OF PERSPECTIVITIES**

The following example is the infinite class of incidence theorems corresponding to Example 7. This class was mentioned in [30]. In the sequel the indices are counted modulo  $n$ .

For any even  $n \geq 4$  and all points  $A_1, \dots, A_n, B_1, \dots, B_n, O$  in  $P^2$  we have:

$$\left[ \begin{aligned} & m((B_1 B_2)(B_3 B_4)(A_3 O)), m((B_2 B_3)(B_4 B_5)(A_4 O)), \dots, \\ & m((B_{n-1} B_n)(B_1 B_2)(A_1 O)), m((B_n B_1)(B_2 B_3)(A_2 O)), \\ & h(A_1 B_1 A_2), h(A_2 B_2 A_3), \dots, h(A_{n-1} B_{n-1} A_n) \end{aligned} \right] \Rightarrow h^*(A_n B_n A_1)$$

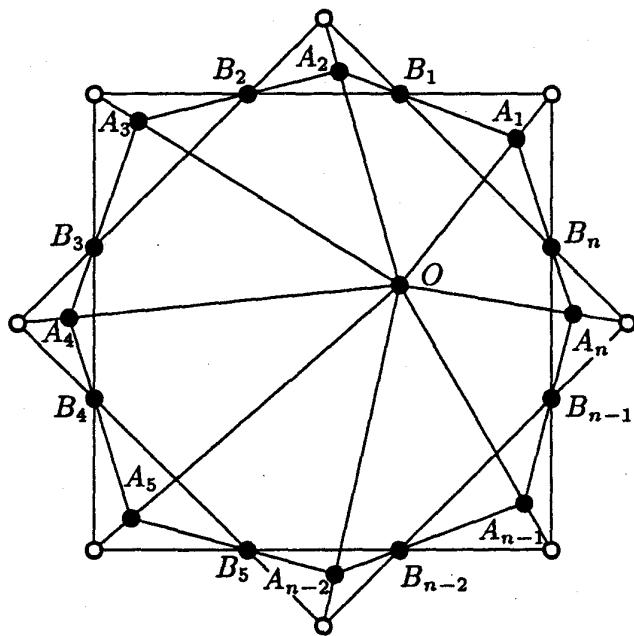


Figure 16.

The following sequence of four hypotheses:

$$m((B_i B_{i+1})(B_{i+2} B_{i+3})(A_{i+2} O)), m((B_{i+1} B_{i+2})(B_{i+3} B_{i+4})(A_{i+3} O)), \\ h(B_{i+1} A_{i+1} A_{i+2}), h(B_{i+2} A_{i+2} A_{i+3})$$

corresponds to the sequence of bi-quadratic equations given below:

$$[B_i B_{i+1} A_{i+2}][B_{i+2} B_{i+3} O] = [B_i B_{i+1} O][B_{i+2} B_{i+3} A_{i+2}] \\ [B_{i+3} B_{i+4} A_{i+3}][B_{i+1} B_{i+2} O] = [B_{i+3} B_{i+4} O][B_{i+1} B_{i+2} A_{i+3}] \\ [B_{i+1} A_{i+1} B_i][B_{i+1} A_{i+2} B_{i+2}] = [B_{i+1} A_{i+1} B_{i+2}][B_{i+1} A_{i+2} B_i] \\ [B_{i+2} A_{i+2} B_{i+3}][B_{i+2} A_{i+3} B_{i+1}] = [B_{i+2} A_{i+2} B_{i+1}][B_{i+2} A_{i+3} B_{i+3}]$$

Taking this collection for  $i = 1, 3, 5, \dots, n-1$  forms a bi-quadratic final polynomial for the incidence theorem. Any equation can be deduced from the remaining equations.

## 13. References

- [1] A. BJÖRNER, M. LAS VERGNAS, B. STURMFELS, N. WHITE & G.M. ZIEGLER: "Oriented Matroids". Cambridge University Press, 1992.
- [2] J. BOKOWSKI & J. RICHTER: "On the finding of final polynomials". *Eur. J. Comb.*, 11 (1990) 21-34.
- [3] J. BOKOWSKI & J. RICHTER-GEBERT: "Reduction theorems for oriented matroids". Preprint, TH-Darmstadt, (1990) 16 p.
- [4] J. BOKOWSKI & J. RICHTER-GEBERT: "On the classification of non-realizable oriented matroids, Part II: properties". Preprint, TH-Darmstadt, (1990) 16 p.
- [5] J. BOKOWSKI, G. LAFFAILLE & J. RICHTER-GEBERT: "10 point oriented matroids and projective incidence theorems". (In preparation), TH-Darmstadt 1992.
- [6] J. BOKOWSKI, J. RICHTER & B. STURMFELS: "Nonrealizability proofs in computational geometry". *Discrete Comput. Geom.*, 5 (1990) 333-350.
- [7] J. BOKOWSKI & B. STURMFELS: "Computational Synthetic Geometry". Lecture Notes in Mathematics 1355 Springer, Heidelberg, 1989.
- [8] J. BOKOWSKI & B. STURMFELS: "An infinite family of minor-minimal non-realizable 3-chirotopes". *Math. Z.*, 200 (1989) 583-589.
- [9] B. BUCHBERGER: "Gröbner Bases - an algorithmic method in polynomial ideal theory". Chapter 6 in N.K. Bose 8ed.9: "Multidimensional Systems Theory", D. Reidel Publ., 1985.
- [10] B. BUCHBERGER: "Applications of Gröbner Bases in non-linear computational geometry". in J.R. Rice (ed.): "Scientific Software", I.M.A. Volumes in Mathematics and its Applications, 444, Springer. New York, 1988.
- [11] S. C. CHOU: "Characteristic sets and Gröbner Bases in Geometry Theorem Proving". Proceedings of Computer-aided Geometric Reasoning, INRIA, Antibes (France), (1987) 29-56.
- [12] S.C. CHOU: "Mechanical Geometry Theorem Proving". D. Reidel Publishing Company, Dodrecht, Holland, 1988.