J. Symbolic Computation (1991) **11**, 549-578

Invariant Computations for Analytic Projective Geometry*

WALTER WHITELEY

Department of Mathematics, Champlain Regional College and Centre de récherches mathmatiques, Université de Montréal

(Received February 17, 1989)

This paper focuses on two underlying questions for symbolic computations in projective geometry:

I How should a projective geometric property be written analytically? A first order formula in the language of fields which expresses a "projective geometric property" is translated, by an algorithm, into a restricted class of formulas in the analytic geometric language of brackets (or invariants). This special form corresponds to statements in synthetic projective geometry and the algorithm is a basic step towards translation back into synthetic geometry.

II How are theorems of analytic geometry proven? Axioms for the theorems of analytic projective geometry are given in the invariant language. Identities derived form Hilbert's Nullstellensatz then play a central role in the proof. From a proof of an open theorem about "geometric properties", over all fields, or over ordered fields, an algorithm derives Nullstellensatz identities - giving maximal algebraic simplicity, and maximal information in the proof.

The results support the proposal that computational analytic projective geometry should be carried out directly with identities in the invariant language.

1. Introduction.

In traditional "analytic projective geometry", we write the points with homogeneous coordinates over a field and prove theorems with polynomial (maybe rational) equations in these coordinates.

Why was this language chosen? First order synthetic geometric properties can be translated into algebraic formulas in this language of fields. Recall that the basic synthetic projective geometric statements are traditionally expressed by synthetic constructions which use the operations of join and intersect for points, lines etc., and conclude with a special incidence of the defined points, lines etc.. The classical coordinatization theorem of projective geometry (see, for example, Baer (1956)) guarantees that, if Desargues' Theorem and Pappus' Theorem hold in the geometry, then the points, lines, planes etc. can be assigned coordinates in a field. The synthetic statements immediately translate into first-order algebraic formulas over commutative fields, built on equations of polynomial terms in the coordinates. Finally, all geometric theorems expressed in this language can, in principle, be proven in the theory of fields.

However, working with these translated formula creates several basic problems.

a) Not all algebraic formulas in this language for fields express "geometric properties" (see Sections 3, 4 and 5 for examples). An algebraic formula in the coordinates represents a "geometric property" only if it's truth is "invariant" for the underlying geometric transformations of the space.

*Work supported, in part, by grants from NSERC (Canada) and FCAR (Québec).

0747-7171/91/050549+30 $03.00/0

b) Certain algebraic and computer algorithms in the theory of fields generate algebraic side conditions which are not, in any obvious way "geometric" (Kutzler (1988)).

c) Even if the property is "geometric", it is a difficult task, not covered by current algorithms, to translate the algebraic formulas into synthetic geometric conditions.

d) The algebraic methods of proof leave few traces of "geometric reasoning" - with the result that simple geometric results may have only complex algebraic proofs. Conversely, simple algebraic proofs may have no reasonable synthetic derivation.

Drawing on modern developments of classical invariant theory, and our experiences working in applied projective geometry, we address the first three problems. We propose a more appropriate language for computational work on analytic projective geometry: the coordinate free language of brackets (determinants of n vectors), and its extensions as Cayley algebra (see Doubilet *et al.* (1974), White (1991)). We explicitly select a class of these formulas as "the language of analytic projective geometry". We summarize some arguments for this choice.

a) All the selected formulas express "geometric properties" (see Sections 3-6).

b) All "synthetic geometric properties" translate into the selected class (see, for example, White (1991)).

c) All the selected formulas translate, after multiplication by simple non-degeneracy conditions, into synthetic geometric conditions (Sturmfels & Whiteley (1991)).

d) Every "geometric property" expressed by a general formula using polynomial equations with integer coefficients translates, algorithmically, into the selected class (Sections 3-6).

e) All theorems about these properties can be proven within this invariant language and some mild extensions (Sections 7-10). The proofs use standard algebraic methods, and classical syzygies of invariant theory. Any side conditions generated are automatically "geometric".

f) The methods of proof remain suitable to automatic theorem proving. The algebraic methods emphasize the role of Nullstellensatz identities (Sections 7-10), with the straightening algorithm of invariant theory as an added computational tool.

g) Current applications of projective geometry to areas such as the rigidity of frameworks, the realizability of configurations and multivariate splines yield a rich variety of properties, proofs and unsolved problems expressed in this language (see, for example, Crapo & Whiteley (1982), White & Whiteley (1983),(1987), Whiteley (1982),(1983),(1984),(1987a),(1989), (1991)). Such applications have raised the need for appropriate computer programs for work in these invariant languages, and for computer programs for the translation back into synthetic geometry.

Other papers in this volume address points b and c. Along the way, we present some new results on Hilbert's Nullstellensatz and its place in all proofs over algebraically closed fields and real closed fields.

What do we mean by a "geometric property" and "invariance for geometric transformations"? Klein's Erlanger program for geometry defined a "geometric property" as a property whose truth is "invariant" under some group of "geometric transformations" (Klein (1939), Weyl (1946)). In the hands of generations of algebraists, this examination was transformed into two algebraic tasks. The first task was:

Given a group of transformations on a vector space, find a finite set of algebraic generators for the set of all polynomials in the elements of the field which are *relative*

invariants: for all transformations T:

$$p(T(\mathbf{a}_1),\ldots,T(\mathbf{a}_m)) = g(T)p(\mathbf{a}_1,\ldots,\mathbf{a}_m) \qquad \text{for all} \quad \mathbf{a}_1,\ldots,\mathbf{a}_m$$

for a scalar function $g(T)$.

For example, the First Fundamental Theorem of Invariant Theory shows that all relative invariants for the general linear group (the non-singular linear transformations) are homogeneous polynomials in the bracket, or determinant of n vectors (see, for example, Weyl (1946), Dieudonné & Carrell (1970), Rota & Sturmfels (1988)). In this case, the function $g(T)$ is $(det[T])^k$, for polynomials of degree k in the brackets.

The second task became:

Find a finite set of generators for all identities in the relative invariants.

For example, the Second Fundamental Theorem of Invariant Theory shows that the classic Grassmann-Plücker syzygies generate the identities for polynomials in the brackets (see Weyl (1946), Dieudonné & Carrell (1970), and Section 7). This is also translated into the straightening algorithm, which gives standard forms for the invariants (Doubilet *et al.* (1974), Sturmfels & White (1989), White (1988))

Because we wish to study actual analytic geometry, we reformulated this program as follows (Whiteley (1973),(1977),(1978),(1979)):

Select a set of algebraic models (e.g. non-zero vectors of dimension n over the complex numbers) and a category of transformations either within a particular model, or between these models (e.g. non-singular linear transformations). A first-order formula F in the corresponding algebraic language (e.g. the language of rings) expresses a *geometric property* for this geometry if the truth of the formula in a model is unchanged by applying these transformations to any free variables in the formula.

With this definition of a geometric property, the initial problem is:

Give a precise language for analytic geometry such that all first order formulas in this language express geometric properties (are invariant under the appropriate morphisms) and an algorithm which translates any invariant formula in the broader algebraic language into an equivalent to a formula in this restricted language.

In Part I we discuss algorithms for translating invariant formulas under four basic settings for "projective transformations" on the vector spaces of homogeneous coordinates:

i non-singular linear transformations on the underlying vector space(s) of homogeneous coordinates (Section 3);
ii homogeneous multiplication of the vector coordinates of a point (section 4);
iii automorphisms of the underlying field (Section 5);
iv formulas for ordered fields with inequalities (Section 6).

A "projective property" for complex analytic geometry is defined as a property invariant under the first three three types of transformations, and is shown to correspond, in general, to a totally homogeneous formula in the language of brackets. A "projective property" for real analytic geometry is defined as a property invariant in all four settings, and is shown to correspond, in general, to a totally homogeneous, even formula in the language of brackets. These results, refining and extending the results in Whiteley (1973),(1978), form a geometric context for much of the work presented in this volume.

Given a language for geometric invariants, the second problem is becomes:

Give axioms and rules in the invariant language to prove all formulas in the invariant language which are true in the models of the geometric category.

In Part II presents the necessary axioms and rules for theorems true over all fields, or fields of a fixed characteristic. These axioms are based on the "syzygies" of classical invariant theory and on the theory of integral domains (Section 7) and ordered integral domains (Section 10).

For open theorems over the theory of fields, Hilbert's Nullstellensatz plays a fundamental role. In Sections 7-10 we investigate the role of such Nullstellensatz identities for proofs. Using a Gentzen style system of logical rules which derives theorems through a proof tree, we demonstrate a metatheorem that any first order proof of such an open theorem leads, algorithmically, to a corresponding conjunction of identities which yields the entire algebraic proof of the theorem. The metatheorem can be paraphrased:

Unlike money, Nullstellensatz identities do grow on trees!

The results of Sections 8-9 present a constructive approach to Hilbert's Nullstellensatz for algebraically closed fields - and emphasize the central role of such identities, which reappear in current work on automated geometric theorem proving. This approach was developed in Whiteley (1971), but was previously unpublished. Such identities, even for the invariant language, can be easily checked by existing computer algorithms. The conclusion is that any automated theorem prover should output these identities, whenever they exist (see Example 8.7).

In Section 10, we present new analogues of these results for projective geometry over the reals (i.e. ordered fields and real-closed fields). The results include a constructive technique for growing real Nullstellensatz identities on proof trees of open theorems.

For other geometries, such as Euclidean geometry, similar questions can be raised about the choice of language. For congruences on points in Euclidean space, it appears that "distance" forms the basic invariant (see, for example, Havel (1991)). While we have not seen the details worked out, it is anticipated that all the methods use here will extend to the other geometries.

In summary, we propose that symbolic calculations for projective geometry should be carried out directly in this invariant language, and its extensions. While we present algorithms for translating projective properties from the language of coordinates over a field into this language, some portions have high complexity, and therefore cannot be reasonably implemented. It is better to remain inside this language and not struggle to to recover the invariants, after the fact. The algebraic proofs should be carried out within the invariant language, using identities which are open to synthetic interpretation. Why not develop symbolic programs which will be used by actual geometers?

PART I Geometric Properties in Algebraic Formulas.

2. A Language for Analytic Projective Geometry.

Throughout this paper we will work with first-order formulas in an algebraic language for fields and integral domains. In particular, we work with coordinates of vectors over a field. This language begins with:

variables $\{x_1, \ldots, x_n, y_1, \ldots, y_n, \ldots\}$ for elements of the field,

constants 0 and 1 in the field, and operations $+, -, \times$.

Combinations of these variables, constants and operations produce polynomial *terms* s, $t, \ldots$. The *atomic* formulas of the language are polynomial equations among these terms:

$s = t$. These equations form the basis for our algebraic language which we abbreviate as $LALG_n$.

We have omitted division, since any equation with non-zero divisors can be simplified to an equivalent polynomial equation. Notice also that the terms of the language are polynomials in the variables, with coefficients $\pm 1, 0$. Of course we use 2 as the shorthand for $(1+1)$, etc., leading to polynomials with integer coefficients.

These atomic equations are combined by the propositional operations: $\neg$ (negation of a formula), $\vee$ (or, placed between two formulas), & (and, placed between two formulas); as well as the quantifier operations: $(\exists x)$ (there exists) and $(\forall x)$ (for all). The formula $F \Rightarrow G$ is treated as a shorthand for the formula $(\neg F) \vee G$, and the formula $F \Leftrightarrow G$ is defined as $((\neg F) \vee G)\&((\neg G) \vee F)$.

This restriction to a *first order language* excludes statements such as: "there exists a non-algebraic number"; "there exists a polynomial such that ...". Such second order statements would require either quantifiers for higher order objects (such as general polynomials, sequences etc.), or an infinite number of the simpler polynomial equations.

We recall a standard form for any quantifier free, or *open*, formula in a first order language. We can distribute $\neg$ over & and $\vee$, and distribute $\vee$ over &:

$$\neg(F\&G) \leftrightarrow (\neg F \vee \neg G) \quad \text{and} \quad \neg(F \vee G) \leftrightarrow (\neg F \& \neg G)$$
$$F \vee (G\&H) \leftrightarrow (F \vee G)\&(F \vee H).$$

After repeated applications of these rules, an open formula assumes an equivalent *conjunctive normal form*:

$$(\neg F_1 \vee \ldots \vee \neg F_m \vee G_1 \vee \ldots \vee G_n)\& \ldots \&(\neg F_p \vee \ldots \vee \neg F_q \vee G_r \vee \ldots \vee G_t)$$

and any formula in LALG_n can be put in the form:

$$(f_1 \neq 0 \vee \ldots \vee f_m \neq 0 \vee g_1 = 0 \vee \ldots \vee g_n = 0)\& \ldots \&(f_p \neq 0 \vee \ldots \vee g_s = 0).$$

As a convenient short hand, we sometimes write repeated conjunctions as $\bigwedge_i F_i$, and repeated disjunctions as $\bigvee_i F_i$.

We can also place any quantified formula into an equivalent *prenex form*:

$$(\forall x_1 \ldots x_m)(\exists y_1 \ldots y_m) \ldots (\forall x_r \ldots x_s)(\exists y_t \ldots y_u)M \ ,$$

where M is an open formula. We pull all quantifiers to the front of the formula, changing the name of the quantified variable if it appears as a free variable or as a quantified variable in another part of the formula. For this translation we use the simple rules:

$\neg(\forall x)F \leftrightarrow (\exists x)\neg F$;	$\neg(\exists x)F \leftrightarrow (\forall x)\neg F$;
$((\forall x)F)\&G \leftrightarrow (\forall x)(F\&G)$	provided x does not occur in G;
$((\forall x)F) \vee G \leftrightarrow (\forall x)(F \vee G)$	provided x does not occur in G;
$((\exists x)F)\&G \leftrightarrow (\exists x)(F\&G)$	provided x does not occur in G;
$((\exists x)F) \vee G \leftrightarrow (\exists x)(F \vee G)$	provided x does not occur in G.

As we mentioned in the introduction, we are interested in the properties and theorems of the projective geometry of points. For this purpose, we use a language built on the n-bracket $[\mathbf{v}_1 \dots \mathbf{v}_n]$ (thought of as the determinant of an $n \times n$ matrix with the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ as the columns).

We work with a two sorted language for vectors of dimension n and for field elements. The variables of this language will be a set $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{u}_1, \mathbf{u}_2, \dots\}$ of sort *vector*. The constants will be 0, 1 of sort *field*. The basic operation on variables of sort vector is the *bracket operator* $[\ \dots\ ]$ which takes n terms of sort vector and produces a term of sort field. The remaining operations are the usual algebraic operations for terms of sort field: $+, -, \times$. Thus the general terms of sort field are polynomials in the basic monomials $[\mathbf{v}_1 \dots \mathbf{v}_n], [\mathbf{u}_{k+1} \dots \mathbf{u}_{k+n}], \dots$, with integer coefficients. Once more the atomic formulas are polynomial equations between terms of sort field: $s = t$. These formulas, combined by the standard first order logical operations, are our basic language for n-dimensional analytic geometry $LANGE_n$.

3. Invariants for Linear Transformations.

In the introduction, a geometry was specified by a set of models and geometric morphisms among these models. In projective geometry, points are written with homogeneous coordinates, so a point in projective d-space is recorded by a $(d+1)$-tuple $(x_1, \dots, x_d, x_{d+1})$, and the zero vector does not represent a point. Therefore, the final models in our geometric categories will be vector spaces of a set dimension $n = d+1$ over a field, with the zero vector deleted.

We will work with several types of transformations through the next three sections. We begin with the non-singular linear transformations within the models as morphisms.

EXAMPLE 3.1. Consider the category with a single model: the vector space of dimension 3 over the real numbers, minus the zero vector - the model for the real projective plane.

An atomic formula is a polynomial equation involving variables for the coordinates:

$$p(v_{11}, v_{12}, v_{13}, \dots, v_{m1}, v_{m2}, v_{m3}) = 0.$$

This equation is *invariant* for the non-singular linear transformations if, for each T, and each selection $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ of non-zero real vectors for the variable vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$:

$$p\left((T(\mathbf{a}_1))_1, (T(\mathbf{a}_1))_2, (T(\mathbf{a}_1))_3, \dots, (T(\mathbf{a}_m))_1, (T(\mathbf{a}_m))_2, (T(\mathbf{a}_m))_3\right) = 0$$

if and only if

$$p(a_{11}, a_{12}, a_{13}, \dots, a_{m1}, a_{m2}, a_{m3}) = 0.$$

For example $[\mathbf{uvw}] = 0$ is an invariant equation, where $[\mathbf{uvw}]$ is interpreted as the determinant of a 3×3 matrix. Writing $\det(T)$ for the (non-zero) determinant of a matrix for the non-singular linear transformation T, we have, for all vectors $\mathbf{a}, \mathbf{b}, \mathbf{c}$:

$$[T(\mathbf{a})T(\mathbf{b})T(\mathbf{c})] = 0 \leftrightarrow det(T)[\mathbf{abc}] = 0 \leftrightarrow [\mathbf{abc}] = 0.$$

Similarly for a product of k of brackets (a *monomial of degree k in the brackets*):

$$[T(\mathbf{a}_1)T(\mathbf{a}_2)T(\mathbf{a}_3)] \dots [T(\mathbf{c}_1)T(\mathbf{c}_2)T(\mathbf{c}_3)] = det(T)^k [\mathbf{a}_1\mathbf{a}_2\mathbf{a}_3] \dots [\mathbf{c}_1\mathbf{c}_2\mathbf{c}_3] = 0$$

if and only if

$$[\mathbf{a}_1\mathbf{a}_2\mathbf{a}_3][\mathbf{b}_1\mathbf{b}_2\mathbf{b}_3] \dots [\mathbf{c}_1\mathbf{c}_2\mathbf{c}_3] = 0.$$

A *homogeneous bracket polynomial* is any sum of monomials, all of degree k in the brackets. The reader can check that any homogeneous bracket polynomial equation $p = 0$ is also invariant.

On the other hand, a simple equation without brackets, such as $v_1 - u_1 = 0$, is not invariant under the linear transformations. (Try vectors with different second coordinates, and apply a transformation with $T(v_1, v_2, v_3) = (v_1 + v_2, v_2, v_3)$.) However, a more complex equation of the form:

$$(v_1 - u_1)^2 + (v_2 - u_2)^2 + (v_3 - u_3)^2 = 0$$

which is equivalent, over the reals, to the conjunction:

$$(v_1 - u_1 = 0)\&(v_2 - u_2 = 0)\&(v_3 - u_3 = 0)$$

is invariant for the linear transformations on the reals, and has no brackets.

From this example, we see that any first order formula which is built from homogeneous bracket equations will be invariant for the non-singular linear transformations. In spite of the apparently bad equations given above, the converse is true.

Since all our chosen transformations take the zero vector to the zero vector, and its inclusion does not effect the invariance, we will, for convenience throughout Part I, consider the full vector spaces as our models.

THEOREM 3.2. Whiteley (1973) *A first-order formula F in $LALG_n$ is invariant for the category of vector spaces of dimension n over fields, with non-singular linear transformations as the morphisms, if and only if there is a formula G in the language of n-brackets $LANGE_n$, with each equation homogeneous in the brackets, such that F equivalent to G over each field.*

Proof. The transformations are isomorphisms of the models which leave each homogeneous bracket polynomial equation invariant. Clearly, the formula G and any equivalent formula F are invariant.

Conversely, assume that F is invariant. We will give an algorithm to create the formula G. We choose a set of n new vector variables, $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$. Each variable x_i, representing the ith coordinate of a vector $\mathbf{x}$, is replaced by:

$$\frac{[\mathbf{e}_1 \ldots \mathbf{e}_{i-1}\mathbf{x}\mathbf{e}_{i+1} \ldots \mathbf{e}_n]}{[\mathbf{e}_1 \ldots \mathbf{e}_{i-1}\mathbf{e}_i\mathbf{e}_{i+1} \ldots \mathbf{e}_n]}.$$

Applied to all variables of F , including variables which are bound by quantifiers, this creates a formula $G'(\mathbf{x}, \mathbf{y}, \ldots, \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$. We then multiply each equation by the smallest power of $[\mathbf{e}_1\mathbf{e}_2 \ldots \mathbf{e}_n]$, clearing the fractions in this equation. This creates a formula $G''(\mathbf{x}, \mathbf{y}, \ldots, \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ in LANGE_n, with each equation homogeneous in the brackets. We claim that $F(x_1, \ldots, x_n, y_1, \ldots, y_n, \ldots)$ is equivalent, over any vector space, to the formula

$$G(\mathbf{x}, \mathbf{y}, \ldots) = (\forall \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)\left(([\mathbf{e}_1 \ldots \mathbf{e}_n] = 0) \vee G''(\mathbf{x}, \mathbf{y}, \ldots, \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)\right)$$

(i) Assume that $F(a_1, \ldots, a_n, b_1, \ldots, b_n, \ldots)$ is true for a particular choice of coordinates for the vectors $\mathbf{a}, \mathbf{b}, \ldots$. For any choice of $[\mathbf{e}_1 \ldots \mathbf{e}_n] \neq 0$, the equations:

$$T(\mathbf{v}) = \left(\frac{[\mathbf{v}\mathbf{e}_2 \ldots\ldots \mathbf{e}_n]}{[\mathbf{e}_1 \ldots \mathbf{e}_n]}, \ldots, \frac{[\mathbf{e}_1 \ldots \mathbf{e}_{i-1}\mathbf{v}\mathbf{e}_{i+1} \ldots \mathbf{e}_n]}{[\mathbf{e}_1 \ldots \mathbf{e}_n]}, \ldots, \frac{[\mathbf{e}_1 \ldots \mathbf{e}_{n-1}\mathbf{v}]}{[\mathbf{e}_1 \ldots \mathbf{e}_n]}\right)$$

define a unique non-singular linear transformation, with $det(T) = [\mathbf{e}_1 \dots \mathbf{e}_n]^{-(n-1)} \neq 0$. Since F is invariant,

$$F(T(\mathbf{a})_1, \dots, (T(\mathbf{a})_n, T(\mathbf{b})_1, \dots, T(\mathbf{b})_n, \dots)$$

is also true. If a variable is inside a universal quantifier, then $(\forall \mathbf{v}_i)H$ is equivalent to $(\forall T(\mathbf{v})_i)H$, since T is an isomorphism in each model. Similarly, for a variable inside an existential quantifier, $(\exists \mathbf{u}_i)H$ is equivalent to $(\exists T(\mathbf{w})_i)H$, since we can choose $\mathbf{w} = T^{-1}(\mathbf{u})$. This chain of equivalences shows that $G'(\mathbf{x}, \mathbf{y}, \dots, \mathbf{e}_1, \dots, \mathbf{e}_n)$ is also true. The multiplication of the atomic equations by powers of $[\mathbf{e}_1 \dots \mathbf{e}_n]$ also preserves the truth of the statement. Since this equivalence holds for all $[\mathbf{e}_1 \dots \mathbf{e}_n] \neq 0$, we find that $G(\mathbf{x}, \mathbf{y}, \dots)$ is also true.

(ii) Conversely, assume that $G(\mathbf{a}, \mathbf{b}, \dots)$ is true. We choose the vectors $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\dots$, $\mathbf{e}_n = (0, \dots, 0, 1)$. This makes $[\mathbf{e}_1 \dots \mathbf{e}_n] = 1$, and makes $[\mathbf{e}_1 \dots \mathbf{e}_{i-1} \mathbf{x} \dots \mathbf{e}_n] = x_i$. Therefore,

$$G''(\mathbf{a}, \mathbf{b}, \dots, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n) = F(a_1, \dots, a_n, b_1, \dots, b_n, \dots)$$

and $F(a_1, \dots, a_n, b_1, \dots, b_n, \dots)$ is also true, as required.

REMARK 3.3. This proof offers an algorithm: for any invariant formula F:

(1) replace x_i by $\frac{[\mathbf{e}_1 \dots \mathbf{e}_{i-1} \mathbf{x} \mathbf{e}_{i+1} \dots \mathbf{e}_n]}{[\mathbf{e}_1 \dots \mathbf{e}_n]}$;
(2) multiply by $[\mathbf{e}_1 \dots \mathbf{e}_n]^k$ to clear fractions;
(3) add $(\forall \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)([\mathbf{e}_1 \dots \mathbf{e}_n] = 0 \vee \dots)$.

This gives the equivalent formula with an invariant appearance. If applied to a non-invariant (variant?) formula F, the algorithm produces an invariant formula G which implies F, but is not equivalent to F.

The algorithm introduces new variables with an additional quantifier. This is inevitable. As we saw in Example 3.1, the formula

$$(\mathbf{v}_1 - \mathbf{u}_1 = 0) \& (\mathbf{v}_2 - \mathbf{u}_2 = 0) \& (\mathbf{v}_3 - \mathbf{u}_3 = 0)$$

is invariant for linear transformations. The simplest equivalent expression with brackets is:

$$(\forall \mathbf{e}_1, \mathbf{e}_2)([\mathbf{e}_1 \mathbf{e}_2 \mathbf{v}] - [\mathbf{e}_1 \mathbf{e}_2 \mathbf{u}] = 0).$$

For some formulas, this introduction of the new variables is unnecessary. The *straightening algorithm* of invariant theory can be applied to any polynomial in the brackets to place it in "standard form" (see Sturmfels & White (1989), White (1988)). If applied with the vector variables $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n$ at the beginning of the linear order for the straightening, this algorithm will pull a maximal number of factors $[\mathbf{e}_1 \dots \mathbf{e}_n]$ to the front of all monomials. Any such common factor can be discarded, and if all occurrences of these variables disappear, we also discard $(\forall \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ and $([\mathbf{e}_1 \dots \mathbf{e}_n] = 0) \vee$. This is a classical method of turning any relatively invariant polynomial for the group of linear transformations into a bracket polynomial in the same variables (Rota & Sturmfels (1988)). This straightening algorithm adds enormously to the complexity, although removing the variables may simplify further stages of analysis.

REMARK 3.4. If the original formula has no quantifiers (or has only universal quantifiers in prenex form) then there is another, more elegant algorithm to make it homogeneous. Each polynomial term t in F is the sum $\sum_i t_i$ of terms t_i which are homogeneous polynomials of degree i. If we replace each equation $t = 0$ in F by the conjunction of equations: $t_1 = 0 \& \ldots \& t_k = 0$, (using all nonzero homogeneous pieces of t), we create a homogeneous formula F'. Whiteley (1978) shows that F' is equivalent to F, provided that F is an open formula and the models have infinite fields.

4. Invariants for Homogeneous Multiplication.

EXAMPLE 4.1. In projective geometry, $\mathbf{v}$ and $\lambda\mathbf{v}$, $\lambda \neq 0$, represent the same point (we use *homogeneous coordinates*). Thus, for projective geometry, we need homogeneous multipliers which multiply a vector with name $\mathbf{v}_j$ by a non-zero scalar λ_j. This is not a morphism of the vectors in the model, per se, or of the formulas in the language. This is a transformation between two *valuations*: assignments of vectors in a model to variables in the language. For example, the valuation $(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots)$ assigns each vector variable $\mathbf{v}_j$ the vector value $\mathbf{a}_j$ over the reals. For any set of non-zero real numbers $(\lambda_1, \ldots, \lambda_j, \ldots)$ we have a *homogeneous multiplication* which takes the valuation $(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots)$ to the valuation $(\lambda_1\mathbf{a}_1, \ldots, \lambda_j\mathbf{a}_j, \ldots)$. (Technically we are now working with a category of valuations, not of models.)

A single bracket $[\mathbf{uvw}] = 0$ remains invariant for homogeneous multiplication, as does a bracket polynomial equation which is homogeneous in each of the vector variables. However, an equation such as $[\mathbf{e}_1\mathbf{e}_2\mathbf{v}] - [\mathbf{e}_1\mathbf{e}_2\mathbf{u}] = 0$ is not invariant for these transformations - and therefore does not express a projective geometric property of the points. (That two points $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$ coincide in the projective plane is expressed by the formula $(\forall \mathbf{e})[\mathbf{xye}] = 0)$.

The formula: $(\exists \mathbf{w})([\mathbf{e}_1\mathbf{e}_2\mathbf{v}] - [\mathbf{we}_2\mathbf{e}_3] = 0)$ is invariant under the homogeneous multipliers, but it is not, as written, homogeneous in the variables $\mathbf{v}$ and $\mathbf{w}$. Since it is a valid theorem for every vector space, it is equivalent to the homogeneous equation $0 = 0$.

We have a partial result for invariants of homogeneous multiplication.

THEOREM 4.2. Whiteley (1978) *An open first-order formula F in $LALG_n$ is invariant for the category of homogeneous multiplication on valuations into vector spaces of dimension n over fields (or over a single infinite field), if and only if F is equivalent to a formula F' in $LALG_n$ with each equation homogeneous in each of the vectors.*

REMARK 4.3 We obtain F' by a simple algorithm. Each equation

$$g(x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{m}, \ldots, x_{mn}) = 0$$

is replaced by a conjunction of equations:

$$\bigwedge_i (g_i(x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{m1}, \ldots, x_{mn}) = 0),$$

where each g_i is homogeneous in each of the vectors. This creates the required formula F'. See Whiteley (1978) for the verification.

COROLLARY 4.4. Whiteley (1978) *An open first-order formula F in $LALG_n$ is invariant for the category of valuations into vector spaces of dimension n over fields (or over*

a single infinite field), with morphisms: homogeneous multiplication of variables and linear transformations within the models if and only if F is equivalent to a formula G in $LANGE_n$ with each equation homogeneous in each of the vectors.

For formulas with quantifiers, we recall a less complete result and a conjecture. For the theory of an algebraically closed field, we have the technique of quantifier elimination (Kreisel & Krivine (1967), Chapter 4, Robinson (1965)).

THEOREM 4.5. *Every first order formula F in $LALG_n$ is equivalent, in the theory of all algebraically closed fields, to a quantifier free formula G in $LALG_n$.*

COROLLARY 4.6. *A formula F in $LALG_n$ is invariant for the category of valuations into a vector space of dimension n over an algebraically closed field, with morphisms: homogeneous multiplication and linear transformations within the model, if and only if there is a formula G in $LANGE_n$, with each equation homogeneous in each of the vectors such that F is equivalent to G in every model with an infinite field.*

The algorithm used in Theorem 4.2 is very simple, with low complexity. On the other hand, the algorithm for quantifier elimination is very complex, and is not currently implemented for general formulas. It would be desirable to avoid this approach entirely. This is another reason to begin, and remain inside the invariant language.

5. Invariance for all Projective Automorphisms.

In synthetic projective geometry, all the "geometric properties" are preserved by general *projective automorphisms*: any map which takes points to points, lines to lines, planes to planes, etc., and preserves all incidences of such objects.

EXAMPLE 5.1. In the projective geometry of the complex plane, the conjugacy map: $(a + b\sqrt{-1}) \rightarrow (a - b\sqrt{-1})$, applied to all coordinates of points, induces a projective automorphism. This suggests a new map to be added to our category of "geometric maps".

Consider the formula:

$$[\mathbf{uxw}][\mathbf{vyw}] - \sqrt{-1}[\mathbf{uyw}][\mathbf{vyw}] = 0.$$

This totally homogeneous equation in the brackets is invariant under linear transformations and homogeneous multiplication. It is not, however, invariant under the conjugacy map. Thus it does not represent a projective geometric property. Of course the broader formula:

$$([\mathbf{uxw}][\mathbf{vyw}] + \sqrt{-1}[\mathbf{uyw}][\mathbf{vyw}] = 0)$$
$$\vee([\mathbf{uxw}][\mathbf{vyw}] - \sqrt{-1}[\mathbf{uyw}][\mathbf{vyw}] = 0)$$

is invariant for the conjugacy map and does represent a geometric property.

We get a basic understanding of projective collineations from the First Fundamental Theorem of Projective Geometry (Baer (1952), p.44), which we paraphrase as follows:

> For a projective space of dimension > 3 every projective transformation is induced by a semilinear transformation (a composition of a linear transformation and a field automorphism).

To complete our examination of projective geometric properties, we need to consider which formulas as invariant for automorphisms of the fields. Since the integers are fixed by all fields automorphisms, we have an obvious result.

THEOREM 5.2. *An open formula in $LALG_n$ is invariant for the category of vector spaces of dimension n, with the zero vector removed, and compositions of the non-singular linear transformations, the field automorphisms, and homogeneous multiplications if and only if there is a formula G in $LANGE_n$, homogeneous in all vector variables, such that G is equivalent to F for every model with an infinite field.*

REMARK 5.3. If we wish other field elements as coefficients, such as $\sqrt{2}$, or $\sqrt{-1}$, we must add these as additional constants. We may extend our language to include constants for elements of a field K, creating the languages $\mathrm{LALG}_n(K)$ and $\mathrm{LALGE}_n(K)$. The results of sections 3 and 4 extend immediately to these languages. There remains an unresolved problem for field automorphisms and formulas in $\mathrm{LALG}_n(K)$.

Consider the category of the complex numbers, with field automorphisms as the morphisms. Clearly any formula written using only rational coefficients will be invariant, since the rationals form the fixed field under such morphisms. We conjecture that the converse is true.

CONJECTURE 5.4. *A first order formula F in $LALG_n(K)$ is invariant for the automorphisms if and only if it is equivalent in this theory to a formula G in $LALG_n$.*

For formulas larger than a single polynomial equation (Whiteley 1978), we know of no proof that all invariant formulas for field automorphisms can be rewritten with integer coefficients.

All synthetic constructions can be written with the rational numbers (see Sturmfels & Whiteley (1991)) - and it would be nice to prove that these synthetic geometric formulas coincide with the invariant formulas for the category of all projective transformations. ∎

REMARK 5.4. We have concentrated on the geometry of points. General geometry works with points, lines, planes etc.. Similar results hold for any algebraic language which includes coordinates for these objects. There are no major changes except the inclusion of simple additional invariants such as $(\mathbf{Px}) = 0$ for $P^1x_1+P^2x_2+P^3x_3 = 0$, to represent the statement "the point $\mathbf{x}$ lies on the line $\mathbf{P}$" (Whiteley (1978)). ∎

6. Invariance for Ordered Fields.

To model geometry over the reals, we should include "separate" as a geometric concept (e.g. "$\mathbf{u}, \mathbf{v}$ separate $\mathbf{x}, \mathbf{y}$"). This concept is represented by an order relation on the field. For example, "$\mathbf{u}, \mathbf{v}$ separate $\mathbf{x}, \mathbf{y}$" becomes: "the cross ratio of u, v and x, y is negative" or

$$\frac{[\mathbf{uxw}][\mathbf{vyw}]}{[\mathbf{uyw}][\mathbf{vxw}]} < 0.$$

We therefore switch from the theory of fields, and algebraically closed fields, to the theory ordered fields, and real closed fields (Tarski (1951), Collins (1975), Dickmann (1983), Bochnak *et al.* (1987)). We extend the algebraic languages to include the atomic formulas of the form $s < t$, where s and t are terms of sort field. With these added formulas, the language LALG_n becomes $LRALG_n$ and the bracket language LANGE_n becomes $LRANGE_n$.

A formula G in LRANGE_n is *homogeneous* if each atomic equation and each atomic inequality is homogeneous in the brackets. A homogeneous formula G in LRANGE_n is

even if each atomic inequality is of even degree in the brackets. Our continued restriction to first order formulas excludes statements like: "the field is archimedian" or "the geometry is continuous".

To characterize "real geometric properties", we want to characterize the invariant formulas of the extended language for the three classes of geometric transformations in sections 3, 4 and 5.

EXAMPLE 6.1. Consider the vector space of dimension 3 over the reals (the real projective plane). For the category of non-singular linear transformations over ordered fields, the homogeneous even formula $[\mathbf{uvy}][\mathbf{wxy}] < [\mathbf{uxy}][\mathbf{wvy}]$ is invariant. However the formula $[\mathbf{uvw}] < 0$ is not invariant (try $\det[T] = -1$), since it is not even. The formula $([\mathbf{uvw}] < 0) \vee ([\mathbf{uvw}] > 0)$, or equivalently $[\mathbf{uvw}] \neq 0$, is invariant under linear transformations, as is $[\mathbf{uvw}]^4 + [\mathbf{uvx}]^2 > 0$. Finally $[\mathbf{uvw}]^4 - [\mathbf{uvx}]^2 > 0$ is not invariant. ∎

THEOREM 6.2. *A formula $F(x_1, \dots, x_n, y_1, \dots, y_n, \dots)$ in $LRALG_n$ is invariant for non-singular linear transformations of ordered fields if and only if there is a formula $G(\mathbf{x}, \mathbf{y}, \dots)$ in $LRANGE_n$, with the same free variables, plus at most n new, universally quantified vector variables and with only homogeneous equalities and homogeneous even inequalities, such that F equivalent to G in each vector space over an ordered field.*

Proof. It is clear that a formula G in LRANGE_n, with homogeneous equalities and homogeneous even inequalities, is invariant for non-singular linear transformations, as is any equivalent formula F.

Conversely, assume that F is invariant for non-singular linear transformations over one (or all) ordered fields. As in Theorem 3.3 we apply the replacement:

$$x_i \to \frac{[\mathbf{e}_1 \dots \mathbf{e}_{i-1} \mathbf{x} \mathbf{e}_{i+1} \dots \mathbf{e}_n]}{[\mathbf{e}_1 \dots \mathbf{e}_n]}.$$

to all variables of F, including variables which are bound by quantifiers, creating a formula $G'(\mathbf{x}, \mathbf{y}, \dots, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$. We multiply each inequality by the smallest even power of $[\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n]$ which clears the fractions. This transfers a formula

$$F(x_1, \dots, x_n, y_1, \dots, y_n, \dots)$$

in LALG_n into a formula $G''(\mathbf{x}, \mathbf{y}, \dots, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ in LANGE_n which is homogeneous and even. Finally we define the formula G by:

$$G(\mathbf{x}, \mathbf{y}, \dots) = (\forall \mathbf{e}_1, \dots, \mathbf{e}_n)(([\mathbf{e}_1 \dots \mathbf{e}_n] = 0) \vee G''(\mathbf{x}, \mathbf{y}, \dots, \mathbf{e}_1, \dots, \mathbf{e}_n)).$$

The proof that F is equivalent to G over each model runs as in Theorem 3.2, noting that an inequality is invariant under multiplication by an even power of a non-zero number. ∎

EXAMPLE 6.3. Which formulas are invariant for homogeneous multiplication of the vectors? Clearly $[\mathbf{uvw}][\mathbf{xyz}] < 0$, and $[\mathbf{uxw}][\mathbf{vyw}] < [\mathbf{uyw}][\mathbf{vxw}]$ are not invariant for multiplication of $\mathbf{x}$ by -1. However $[\mathbf{uyw}][\mathbf{vxw}][\mathbf{uxw}][\mathbf{vyw}] < 0$ (the cross ratio of u, v, x, y is less than zero) and $[\mathbf{uyw}][\mathbf{vxw}][\mathbf{uxw}][\mathbf{vyw}] < ([\mathbf{uyw}][\mathbf{vxw}])^2$ (the cross ratio of $\mathbf{u}, \mathbf{v}$ and $\mathbf{x}, \mathbf{y}$ is less than 1) are invariant for all homogeneous multiplications.

CONJECTURE 6.4. *An open formula $F(x_1, \dots, x_n, y_1, \dots, y_n, \dots)$ in $LRALG_n$ is invariant for homogeneous multiplications and for non-singular linear transformations over real closed fields if and only if there is a formula $G(\mathbf{x}, \mathbf{y}, \dots)$ in $LRANGE_n$, with the same free variables, plus at most n new, universally quantified vector variables and with all*

atomic equalities homogeneous in each vector and all inequalities homogeneous of even degree in each vector, such that F equivalent to a formula G in each vector space over a real-closed field.

Suggested proof. Clearly these G are invariant for homogeneous multiplication over all ordered fields.

Conversely, assume that $F(x_1, \dots, x_n, y_1, \dots, y_n, \dots)$ is invariant for homogeneous multiplication of the vector $\mathbf{x}$. Informally, this means that:

$$F(x_1, \dots, x_n, y_1, \dots, y_n, \dots) \leftrightarrow (\forall t)F(tx_1, \dots, tx_n, y_1, \dots, y_n, \dots).$$

Over a real closed field, there is a constructive process of quantifier elimination (see, for example, Kreisel & Krivine (1967), Collins (1975)). If this is applied to

$$(\forall t)F(tx_1, \dots, tx_n, y_1, \dots, y$$

this creates an equivalent open formula $G(x_1, \dots, x_n, y_1, \dots, y_n, \dots)$. We *claim* that this algorithm actually decomposes each inequality into inequalities which are homogeneous, of even degree, in the entries for $\mathbf{x} = (x_1, \dots, x_n)$. This formula is equivalent to F over any real-closed field.

If this claim is verified, repeated application of this process will prove the conjecture over any real-closed field. ∎

In Whiteley (1979), we suggested that a geometric property is *combinatorial* only if it is invariant under extensions of the models by field extensions. Informally, we claim that completion of a "combinatorial" construction is not changed by adding more points to the lines. Therefore such combinatorial properties are invariant under homogeneous multiplication in the extension. With this condition, Conjecture 6.4 could characterize combinatorial projective properties for other ordered fields.

If the conjecture is verified, we will still be left with a brutal algorithm. This is another argument for beginning and remaining, inside the class of invariant formulas for all the calculations.

What happens with constants for non-rational field elements?

EXAMPLE 6.5. The rational numbers, the real numbers and other archimedian ordered fields admit only the trivial automorphism. If we add constants for other elements of the fields - we may now have invariance under field automorphisms. Thus a formula such as: $[\mathbf{uxw}][\mathbf{vyw}] = \sqrt{2}[\mathbf{uyw}][\mathbf{vxw}]$ is invariant for all projective transformations over fields extending the algebraic real numbers.

No single synthetic construction, or single identity in our basic language, translates to this equation. However, two projective constructions do translate to:

$$([\mathbf{uxw}][\mathbf{vyw}])^2 = 2([\mathbf{uyw}][\mathbf{xvw}])^2 \;\&\; ([\mathbf{uxw}][\mathbf{vyw}])([\mathbf{uyw}][\mathbf{vxw}]) > 0.$$

Together, these are equivalent to the original equation. With similar difficulty, we can transform any equation or inequality with real algebraic coefficients into equations and inequalities in our language. Thus we have, in principle, covered all properties expressed by polynomials with algebraic coefficients.

Polynomials with transcendental coefficients, such as π will require second-order statements (conjunctions of an infinite number of inequalities defining the corresponding cut in the rationals) for translation into our language. Note that the translation for numbers like $\sqrt{2}$ depends on the order in the rationals, and did not exist over unordered fields such as the complex numbers. ∎

Finally we note that the results of Sturmfels & Whiteley (1991) can be extended to show that synthetic constructions in a real geometry of the reals correspond to the totally homogeneous even formulas in LRANGE_n. This really is an adequate language for representing synthetic projective geometry.

To summarize Part I, we propose that totally homogeneous formulas in LANGE_n, or totally homogeneous even formulas in LRANGE_n, should be used to express all projective geometric properties for analytic geometry. These are the languages which should be built into "automated geometry theorem provers". The evidence for this proposal includes:

a) All formulas of this type are invariant for the appropriate projective geometric transformations.
b) All projective properties represented by open formulas in the usual language for analytic geometry, without order, can be translated by a simple algorithm into an equivalent totally homogeneous formula in the brackets.
c) It is conjectured that all projective properties represented by open formulas in the usual language for real analytic geometry can be translated into an equivalent totally homogeneous formula in the brackets.
d) These formulas correspond directly to analytic translations of synthetic properties.
e) All formulas in these languages can, in principle, be translated into synthetic geometric properties.

In conclusion, we do not claim that our invariant language, as given, is the optimum language for translation from synthetic geometry. In practice, such translation is carried out with the Cayley algebra, or similar variants of Grassman's algebra (see White (1991) for examples). In this richer algebraic extension language, all totally homogeneous formulas are invariant for projective transformations. In part II we will make a small move in this direction, by including vector addition and multiplication of a vector by a scalar. (This extension is necessary to prove some quantified theorems.) For practical, automated theorem proving, we will also need implemented programs to translate synthetic statements into Cayley algebra and for the expansion from Cayley algebra into the brackets.

PART II. Theorems and Proofs.

7. Proofs for Open Theorems over Algebraically Closed Fields.

Having chosen an algebraic language for analytic projective geometry, we would like to carry out proofs for such properties within the language. Thus our goal is to prove all theorems in LANGE_n which are homogeneous in all vector variables using axioms, using first order logic and intermediate formulas in this language.

For any vector space of dimension n over fields, the classical Grassmann-Plücker syzygies become the essential axioms for the bracket operation:

$$[\mathbf{y}\mathbf{y}\ldots\ldots] = 0$$

$$[\mathbf{y}_1\mathbf{y}_2\ldots\mathbf{y}_i\mathbf{y}_{i+1}\ldots\mathbf{y}_n] = -[\mathbf{y}_1\mathbf{y}_2\ldots\mathbf{y}_{i+1}\mathbf{y}_i\ldots\mathbf{y}_n]$$

$$[\mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_n][\mathbf{y}_1\mathbf{y}_2\ldots\mathbf{y}_n] = \sum_i [\mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_{i-1}\mathbf{y}_1\mathbf{x}_{i+1}\ldots\mathbf{x}_n][\mathbf{x}_i\mathbf{y}_2\ldots\mathbf{y}_n].$$

(The first axiom is implied by the second, if we assume $2 \neq 0$.) We also add the usual axioms for equality, and for integral domains.

For all field terms s, t, u (polynomials with integer coefficients):

$$
\begin{array}{ll}
t = t & s = t \Rightarrow t = s \\
s = t \& t = u \;\Rightarrow\; s = u & s = t \& s' = t' \;\Rightarrow\; s + s' = t + t' \\
s = t \;\Rightarrow\; -s = -t & s = t \& s' = t' \;\Rightarrow\; s \cdot s' = t \cdot t' \\
s + (t + u) = (s + t) + u & t + s = s + t \\
t + (-t) = 0 & t + 0 = t \\
s \cdot (t \cdot u) = (s \cdot t) \cdot u & t \cdot s = s \cdot t \\
t \cdot 1 = t & s \cdot (t + u) = s \cdot t + s \cdot u \\
s(-t) = -st & s \cdot t = 0 \;\Rightarrow\; s = 0 \vee t = 0 \\
1 \neq 0. &
\end{array}
$$

We call this collection of axioms for open theorems of vector spaces AXOV_n.

Together with the usual axioms for propositional logic (see below), these give proofs in LANGE_n for all open invariant theorems which hold over all all fields. A simple proof is given in Whiteley (1977).

We saw in Section 2 that any open formula M in our languages can be placed in conjunctive normal form:

$$(f_1 \neq 0 \vee \ldots \vee f_k \neq 0 \vee g_1 = 0 \vee \ldots \vee g_n = 0) \& \ldots \& (\ldots \vee f_q \neq 0 \vee g_r = 0 \vee \ldots).$$

Equivalently, every such formula can be written:

$$(f_1 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \vee \ldots \vee g_n = 0) \;\& \ldots \&\; (\ldots f_m = 0 \Rightarrow g_r = 0 \ldots).$$

For algebraically closed fields, Hilbert's Nullstellensatz translates each of these implications into an algebraic identity.

THEOREM 7.1. Hilbert's Nullstellensatz *A formula of the form:*

$$f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \vee \ldots \vee g_m = 0$$

where f_i and g_j are polynomials with integer coefficients, is true over an algebraically closed field if and only if there are polynomials a_i, with coefficients in the integers, an integer $k \neq 0$ in the field, and integers n_j such that:

$$\sum_i a_i f_i = k \prod_j (g_j^{n_j})$$

as polynomials.

We call $\sum_i a_i f_i = k \prod_j (g_j^{n_j})$ a *Nullstellensatz identity*, $N(F)$, for the implication F. If there are no g_i, the theorem is written

$$f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow 1 = 0,$$

and the Nullstellensatz identity has the form $\sum_i a_i f_i = k$.

In general it is a simple task to check such an identity: expand the two sides, as polynomials in the variables, and compare coefficients on both sides. Within our language of brackets, this direct expansion is replaced by the straightening algorithm of classical invariant theory (Sturmfels & White (1989), White (1988)).

It is also a simple task to recover the original implication from the Nullstellensatz identity:

$$f_1 = 0 \& f_2 = 0 \& \dots \& f_k = 0 \;\Rightarrow\; \sum_i a_i 0 = \prod_j (g_j^{n_j})$$

$$f_1 = 0 \& f_2 = 0 \& \dots \& f_k = 0 \;\Rightarrow\; g_1 = 0 \vee \dots \vee g_m = 0$$

Thus a Nullstellensatz identity $N(F)$ gives an *algebraic proof* of the formula F. For an F in the language of brackets, it is a simple exercise to check that the polynomials a_i can also be found in this language (see Corollary 8.4). If the g_i and the f_i are homogeneous in any variable - or all variables, the polynomials a_i can be found with the same homogeneity. (Since $\prod_j (g_j^{n_j})$ is homogeneous, select the corresponding homogeneous part of $\sum_i a_i f_i$.)

Since every field has an algebraically closed extension, we note that an open theorem is true (provable) over an algebraically closed field if and only if it is true over all fields of the same characteristic. Thus Hilbert's Nullstellensatz can be paraphrased:

A logical proof guarantees an algebraic proof.

This algebraic proof is by far the simplest type to check, by hand or by computer.

EXAMPLE 7.2. Consider the problem of coordinatizing a matroid of rank n over the complex numbers. Such a configuration has certain n-tuples independent, and other n-tuples dependent. Thus a set of coordinates must satisfy a first order formula:

$$(\exists \mathbf{x_1} \dots \mathbf{x_k})([\mathbf{x_1} \dots \mathbf{x}_n] = 0 \& \dots \& [\mathbf{x_s} \dots \mathbf{x_t}] \neq 0 \& \dots).$$

A proof of non-coordinatizability over the complex numbers (or over any extension of the rationals) is therefore a theorem of the form:

$$\neg(\exists \mathbf{x_1} \dots \mathbf{x_k}) \neg([\mathbf{x_1} \dots \mathbf{x}_n] = 0 \& \dots \& [\mathbf{x_s} \dots \mathbf{x_t}] \neq 0 \& \dots)$$

or $$(\forall \mathbf{x_1} \dots \mathbf{x_k})([\mathbf{x_1} \dots \mathbf{x}_n] \neq 0 \vee \dots [\mathbf{x_j} \dots \mathbf{x_m}] \neq 0 \vee [\mathbf{x_s} \dots \mathbf{x_t}] = 0 \vee \dots).$$

This universal theorem is equivalent to a single Nullstellensatz identity:

$$a[\mathbf{x_1} \dots \mathbf{x}_n] + \dots + c[\mathbf{x_j} \dots \mathbf{x_m}] = [\mathbf{x_s} \dots \mathbf{x_t}]^p \dots [\mathbf{x_d} \dots \mathbf{x_r}]^q.$$

In their studies of coordinatizing matroids, Bokowski and Sturmfels have called such a Nullstellensatz identity the "final polynomial" of a proof of non-coordinatizability (Sturmfels (1991)). ∎

For a general open formula, the conjunction:

$$(f_1 = 0 \& \dots \& f_m = 0 \Rightarrow g_1 = 0 \vee \dots \vee g_n = 0) \& \dots \& (\dots f_1 = 0 \Rightarrow g_r = 0 \dots)$$

is equivalent to a conjunction of Nullstellensatz identities. Thus the Nullstellensatz identities form a preferred presentation of any open theorem.

Is it more difficult to find a Nullstellensatz identity than to find another first order proof of the same theorem? Our experience with such proofs, over twenty years, and some logical results we give below, have convinced us that a Nullstellensatz identity can be found, in a simple algorithmic way, from any first order proof of such a theorem. This observation was found independently by Scarpellini (1969) and Whiteley (1971) using two distinct approaches. It can be stated as a metatheorem.

META-THEOREM 7.3. *A first order proof of a formula of the form*

$$f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \& \ldots \& g_m = 0$$

from axioms for a field of fixed characteristic, gives an algorithmic construction for a corresponding Nullstellensatz identity:

$$\sum_i a_i f_i = k \prod_j (g_j^{n_j}).$$

A first order proof of a formula of the form

$$f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \& \ldots \& g_m = 0$$

from axioms for all fields, gives an algorithmic construction for a corresponding Nullstellensatz identity:

$$\sum_i a_i f_i = \prod_j (g_j^{n_j}).$$

In the next section, we outline the algorithm for a particular set of rules for first order logic. This approach is, logically weaker than the results of Seidenberg (1956) which derive the Nullstellensatz from the statement of the theorem - without inputting the proof. However it represents a practical approach to existing proofs of theorems. Our fundamental point is that an "automated theorem prover" can, and should, output the Nullstellensatz identities.

8. From a Proof to a Nullstellensatz Identity.

We now examine proofs using a system of "natural rules" for logical proofs - a Gentzen style system (see, for example, Feferman (1968), Takeuti (1975)). The pieces of this system are written as *sequents* composed of formulas: $F_1, \ldots, F_m \supset G_1, \ldots, G_n$. If m or $n = 0$, there are no formulas in this part, and we write $\emptyset$ in the corresponding spot. The sequent $F_1, \ldots, F_m \supset G_1, \ldots, G_n$ is equivalent, in any model, to the formula $F_1 \& \ldots \& F_m \Rightarrow G_1 \vee \ldots \vee G_n$. In this system, a proof or *derivation* D is a tree of formulas, with axioms at the top, and the final theorem at the bottom.

The reader can check that all of our axioms from Section 7 can be rewritten as *atomic sequents* - with single equations as the F_i and the G_j (see the proof of Theorem 8.2). The only logical axioms are:

$$s = t \supset s = t$$

and our desired theorem can also be written as a sequent:

$$f_1 = 0, \ldots, f_m = 0 \supset g_1 = 0, \ldots, g_n = 0.$$

There are four sets of logical rules in this system.

The propositional rules (M and N will be sets of formulas):

1. $$\frac{M \supset N, F}{M, \neg F \supset N}$$

2. $$\frac{M, F \supset N}{M \supset N, \neg F}$$

3. $\dfrac{M, F \supset N \quad M, G \supset N}{M, F \vee G \supset N}$ 4. $\dfrac{M \supset N, F \text{ or } M \supset N, G}{M \supset N, F \vee G}$

5. $\dfrac{M, F \supset N \text{ or } M, G \supset N}{M, F\&G \supset N}$ 6. $\dfrac{M \supset N, F \quad M \supset N, G}{M \supset N, F\&G}$.

The quantifier rules:

7.† $\dfrac{M, F(w) \supset N}{M, (\exists x)F(x) \supset N}$ 8.‡ $\dfrac{M \supset N, F(t)}{M \supset N, (\exists x)F}$

9.‡ $\dfrac{M, F(t) \supset N}{M, (\forall x)F(x) \supset N}$ 10† $\dfrac{M \supset N, F(w)}{M \supset N, (\forall x)F}$

† x is the same sort of variable as w, and w is not free in M or N;
‡ x is the same sort as t.

The structural rules

11. $\dfrac{M \supset N}{M, E \supset N}$ 12. $\dfrac{M \supset N}{M \supset N, E}$

13. $\dfrac{M' \supset N'}{M \supset N}$ $M' = M$ and $N' = N$, as sets of formulas.

The cut rule:

14. $\dfrac{M, E \supset N \quad M' \supset N', E.}{M, M' \supset N, N'}$

It is well known that these rules, with the logical axioms $F \supset F$, for any atomic formula, give all first order theorems (see Feferman (1968), Takeuti (1975)). It is also a classical result that for logical theorems, the cut rule can be eliminated.

With our added axioms, we still want to minimize the occurrences of the "cut" rule, so that the entire proof consists of formulas which are "pieces" of the final sequent, and does not involve hidden, more complex pieces. This is particularly easy for theories such as AXOV_n, which are *atomic theories*: theories for which all axioms are sequents with atomic formulas.

THEOREM 8.1. Whiteley (1971) *Given a proof tree D of a sequent $M \supset N$ from an atomic theory Ax, there is a proof tree D^* of the sequent $M \supset N$ from Ax with all cuts restricted to atomic formulas.*

The proof in Whiteley (1971) is a straightforward extension of the proofs of Feferman (1967) or Takeuti (1975) for cut reduction of the theory of equality. It will not be repeated here.

It is important to emphasize is that this *cut reduction* is a constructive algorithm transferring one proof tree to another proof tree with all cuts at the top, involving atomic formulas which arise in axioms. It is also important to realize that any first order proof can, in principle, be translated into this Gentzen system, and then pulled into cut reduced form. We will show that such a cut reduced proof leads naturally to a Nullstellensatz identity for the theorem.

THEOREM 8.2. *There is a constructive algorithm which takes any derivation D of an atomic sequent*

$$f_1 = 0, \ldots, f_m = 0 \supset g_1 = 0, \ldots, g_n = 0$$

from the theory of integral domains to a Nullstellensatz identity with integer polynomials a_i: $\sum_i a_i f_i = \prod_j (g_j^{n_j})$.

Proof. There is a constructive algorithm form any derivation D to a cut reduced derivation D^*. We proceed by induction down the tree of such a cut reduced proof.

The axioms for equality, integral domains, etc., all give immediate Nullstellensatz identities. For example:

$N(t = t)$:	$(t - t) = 0$
$N(s = t \supset t = s)$:	$(t - s) = -(s - t)$
$N(s = t, t = u \supset s = u)$:	$(s - t) + (t - u) = (s - u)$
$N(s = t, s' = t' \supset s + s' = t + t')$:	$(s - t) + (s' - t') = (s + s' - (t + t'))$
$N(s = t, s' = t' \supset s \oplus s' = t \oplus t')$:	$s'(s - t) + t(s' - t') = (s \oplus s' - t \oplus t')$
$N(1 = 0 \supset \emptyset)$:	$1 = 1$.

The logical axioms, $s = t \supset s = t$, also yield an immediate identity. This covers the top leaves of the derivation tree.

A cut reduced proof for an atomic sequent will include only atomic sequents at all stages of a derivation - with no occurrences of quantifiers, or of &, $\vee$ or $\neg$. This means that there are no occurrences of the propositional rules (rules 1-6) or the quantifier rules (rules 7-10).

We now assume that the initial stages of the cut reduced proof have been converted into Nullstellensatz identities, and show how to work through the structural rules and applications of cut to single equations.

11. $$\frac{F_1, \ldots, F_m \supset G_1, \ldots, G_p \qquad \sum_{i=1}^{i=m} a_i f_i = \prod_{j=1}^{j=p} g_j^{n_j}}{F_1, \ldots, F_m, F_0 \supset G_1, \ldots, G_p \qquad \sum_{i=1}^{i=m} a_i f_i + 0 f_0 = \prod_{j=1}^{j=p} g_j^{n_j}}$$

12. $$\frac{F_1, \ldots, F_m \supset G_1, \ldots, G_p \qquad \sum_{i=1}^{i=m} a_i f_i = \prod_{j=1}^{j=p} g_j^{n_j}}{F_1, \ldots, F_m \supset G_1, \ldots, G_p, G_0 \qquad \sum_{i=1}^{i=m} g_0 a_i f_i = g_0 \prod_{j=1}^{j=p} g_j^{n_j}}$$

13. $$\frac{M' \supset N'}{M \supset N}$$ $M' = M$ and $N' = N$, as sets of formulas.

If this rule collapses occurrences of an equation, we simply combine coefficients and powers. If the rule adds occurrences of an equation, we add zero coefficients or multiply by first powers of the term.

This leaves the cut rule:

$$14.\quad \frac{F_1,\dots,F_m,E \supset G_1,\dots,G_p \qquad F_{m+1},\dots,F_n \supset G_{p+1},\dots,G_q,E}{F_1,\dots,F_m,F_{m+1},\dots,F_n \supset G_1,\dots,G_p,G_{p+1},\dots,G_q}$$

with the following Nullstellensatz identities for the top pieces:

$$\sum_{i=1}^{i=m} a_i f_i + a_e e = \prod_{j=1}^{j=p} g_j^{n_j} \qquad \sum_{i=m+1}^{i=n} a_i f_i = e^{n_e}\left(\prod_{j=p+1}^{j=q} g_j^{n_j}\right).$$

We solve the first equation for $a_e e$, and multiply the second equation by $a_e^{n_e}$.

$$a_e e = \prod_{j=1}^{j=p} g_j^{n_j} - \sum_{i=1}^{i=m} a_i f_i \qquad \sum_{i=m+1}^{i=n} a_e^{n_e} a_i f_i = (a_e e)^{n_e}\left(\prod_{j=p+1}^{j=q} g_j^{n_j}\right).$$

We now substitute for $a_e e$ in the modified second equation to obtain the required Nullstellensatz identity, with a complex multiplier S formed from the pieces of the first equation:

$$\left(\prod_{j=p+1}^{j=q} g_j^{n_j}\right)(S)\left(\sum_{i=1}^{i=m} a_i f_i\right) + \sum_{i=m+1}^{i=n} a_e^{n_e} a_i f_i = \left(\prod_{j=1}^{j=p} g_j^{n_j}\right)^{n_e}\left(\prod_{j=p+1}^{j=q} g_j^{n_j}\right).$$

This completes the induction. ∎

REMARK 8.3. As mentioned above, this result is weaker than the results of Seidenberg (1956) which derive the Nullstellensatz from the statement of the theorem, without a proof as input. Our approach will extend to real-closed fields (see Section 10), while the constructive approach of Seidenberg has not been extended. In practical terms, we have found that the derivation of a Nullstellensatz identity from our proofs was an simple task.

In terms of symbolic computation, the metatheorem suggests that a little extra bookkeeping in any computer proof will give these Nullstellensatz identities - and more information than any other proof. The conclusion is that the computer algorithm to prove of an open theorem about vector spaces should output a conjunction of Nullstellensatz identities. To do less with an algorithm is to throw away information. ∎

How does this principle apply to proofs in the invariant language?

COROLLARY 8.4. *Given a derivation D of a sequent*

$$f_1 = 0, f_2 = 0, \dots, f_k = 0 \supset g_1 = 0, \dots, g_m = 0$$

in $LANGE_n$ from $AXOV_n$, there is a corresponding Nullstellensatz identity:

$$\sum_i a_i f_i = \prod_j (g_j^{n_j})$$

with all terms in $LANGE_n$.

Proof. The special axioms for brackets are equations (identities) thus they have immediate Nullstellensatz identities. For example:

$$N([\mathbf{y}_1\mathbf{y}_2\dots\mathbf{y}_i\mathbf{y}_{i+1}\dots\mathbf{y}_n] = -[\mathbf{y}_1\mathbf{y}_2\dots\mathbf{y}_{i+1}\mathbf{y}_i\dots\mathbf{y}_n]) :$$

$$[\mathbf{y}_1\mathbf{y}_2\dots\mathbf{y}_i\mathbf{y}_{i+1}\dots\mathbf{y}_n] + [\mathbf{y}_1\mathbf{y}_2\dots\mathbf{y}_{i+1}\mathbf{y}_i\dots\mathbf{y}_n] = 0.$$

In the cut reduced proof, all formulas are subformulas of the final theorem, so all terms in any cut reduced proof are in the language LANGE_n. The rest of the proof applies without change, producing homogeneous terms a_i in the language of brackets. ∎

EXAMPLE 8.5. Consider the example of the Fano plane (Figure 1), which exists only over fields of characteristic 2. Since this is a plane configuration, we use 3-brackets. We assume that $[\mathbf{xbc}] = 0$, $[\mathbf{ayc}] = 0$, $[\mathbf{abz}] = 0$, $[\mathbf{apx}] = 0$, $[\mathbf{pzc}] = 0$, $[\mathbf{pzc}] = 0$, and $[\mathbf{xyz}] = 0$. We also assume that all other brackets are non-zero (no other triples are collinear).

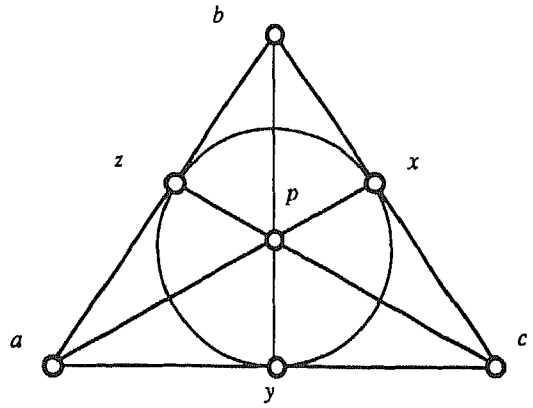

Figure 1. *The Fano plane.*

By a direct check with the identities for the brackets, we have the following identity. (As a convention, we underline all terms which are assumed =0:)

$$\begin{aligned}2[\mathbf{axc}][\mathbf{abp}][\mathbf{pbc}][\mathbf{ayp}][\mathbf{zbc}][\mathbf{apc}] &= [\mathbf{abc}][\mathbf{pbc}][\mathbf{apc}][\mathbf{abp}][\mathbf{ayz}]\underline{[\mathbf{xbc}]}\\ &\quad - [\mathbf{axc}][\mathbf{ybc}][\mathbf{pbc}][\mathbf{apc}][\mathbf{abp}]\underline{[\mathbf{abz}]} + [\mathbf{abc}][\mathbf{abp}][\mathbf{ybc}][\mathbf{pbc}][\mathbf{azc}]\underline{[\mathbf{apx}]}\\ &\quad + [\mathbf{abc}][\mathbf{pbc}][\mathbf{azc}][\mathbf{axc}][\mathbf{abp}]\underline{[\mathbf{ybp}]} + [\mathbf{abc}][\mathbf{pbc}][\mathbf{azc}][\mathbf{axc}][\mathbf{abp}]\underline{[\mathbf{ybp}]}\\ &\quad + [\mathbf{aby}][\mathbf{pbc}][\mathbf{aby}][\mathbf{axc}][\mathbf{abp}]\underline{[\mathbf{pzc}]} - [\mathbf{abc}]^2[\mathbf{pbc}][\mathbf{apc}][\mathbf{abp}]\underline{[\mathbf{xyz}]}.\end{aligned}$$

Since we assumed that $[\mathbf{axc}] \neq 0$, $[\mathbf{abp}] \neq 0$, $[\mathbf{pbc}] \neq 0$, $[\mathbf{apy}] \neq 0$, $[\mathbf{zbc}] \neq 0$, $[\mathbf{apc}] \neq 0$, the configuration can be coordinatized only if $2 = 0$. ∎

REMARK 8.6. If we work with a particular characteristic, then we would add the corresponding axioms. These also give initial Nullstellensatz identities:

$$N(n \neq 0) : n = n \qquad N(m = 0) : 0 = m.$$

While these non-zero numbers will accumulate on the right hand side, the net product will be a non-zero integer in the appropriate characteristic, as required. Our algorithm constructs a Nullstellensatz identity for any of these theories. ∎

To emphasize the role of identities in proofs, we have cheated. We quietly continued with full vector spaces rather than models of projective geometry to vector spaces.

EXAMPLE 8.7. In projective geometry, a variable for a point cannot be the zero vector. Thus the formula:

$$[\mathbf{e}_1 \dots \mathbf{e}_n] = 0 \vee [\mathbf{y}\mathbf{e}_2 \dots \mathbf{e}_n] \neq 0 \vee \dots \vee [\mathbf{e}_1 \dots \mathbf{e}_{n-1}\mathbf{y}] \neq 0$$

$$\text{or} \quad [\mathbf{y}\mathbf{e}_2 \dots \mathbf{e}_n] = 0, \dots, [\mathbf{e}_1 \dots \mathbf{e}_{n-1}\mathbf{y}] = 0 \supset [\mathbf{e}_1 \dots \mathbf{e}_n] = 0$$

is a theorem for the projective models. ∎

We will add this as an axiom. However, this axiom does not have a Nullstellensatz identity! The axiom is false for $\mathbf{x} = 0$ and any Nullstellensatz identity would be true for $\mathbf{x} = 0$.

THEOREM 8.8. *An open theorem for all models of projective space of dimension n is equivalent to a conjunction of Nullstellensatz identities if and only if it is also true when the zero vector is substituted for some or all variables.*

In the introduction to his book The Calculus of Extension (a variant of the invariant language), Forder (1960) summarized his experiences with identities for geometric theorems:

> In the method of this book, we use equations involving the geometric entities themselves, such as points, lines, circles, or quadrics, and not their coordinates; to prove a geometric theorem is to prove such an equation, and as in most cases the equation turns out to be an identity, we have an automatic method for proving geometric theorems.

We hope our results have extracted the essential content of this observation by a practicing geometer.

9. Quantified Theorems and their Proofs.

If we add quantifiers, we have an additional gap in our language.

EXAMPLE 9.1. Consider the simple result, true in projective spaces over all fields:

A line through two distinct points contains a third point.

This translates, in the brackets for the projective plane, to a statement:

$$(\exists \mathbf{e}_1)([\mathbf{x}\mathbf{y}\mathbf{e}_1] \neq 0 \supset (\exists \mathbf{z})([\mathbf{x}\mathbf{z}\mathbf{e}_1] \neq 0 \& [\mathbf{z}\mathbf{y}\mathbf{e}_1] \neq 0 \& [\mathbf{x}\mathbf{y}\mathbf{z}] = 0)).$$

Assume $[\mathbf{x}\mathbf{y}\mathbf{e}_1] \neq 0$. Therefore, since $[\mathbf{y}\mathbf{y}\mathbf{e}_1] = 0$:

$$[\mathbf{x}\mathbf{y}\mathbf{e}_1] + [\mathbf{y}\mathbf{y}\mathbf{e}_1] \neq 0 \quad \text{or} \quad [(\mathbf{x} \oplus \mathbf{y})\mathbf{y}\mathbf{e}_1] \neq 0.$$

Similarly: $[\mathbf{x}(\mathbf{x} \oplus \mathbf{y})\mathbf{e}_1] \neq 0$. Thus

$$[\mathbf{x}\mathbf{y}\mathbf{e}_1] \neq 0 \supset [(\mathbf{x} \oplus \mathbf{y})\mathbf{y}\mathbf{e}_1] \neq 0 \& [\mathbf{x}(\mathbf{x} \oplus \mathbf{y})\mathbf{e}_1] \neq 0.$$

Since $[\mathbf{xy}(\mathbf{x} \oplus \mathbf{y})] = 0$, this proves that :

$$[\mathbf{xye}_1] \neq 0 \supset ([\mathbf{x}(\mathbf{x} \oplus \mathbf{y})\mathbf{e}_1] \neq 0 \& [(\mathbf{x} \oplus \mathbf{y})\mathbf{ye}_1] \neq 0 \& [\mathbf{xy}(\mathbf{x} \oplus \mathbf{y})] = 0).$$

Using quantifier rules, we have:

$$(\exists \mathbf{e}_1)([\mathbf{xye}_1] \neq 0 \supset (\exists \mathbf{z})([\mathbf{xze}_1] \neq 0 \& [\mathbf{zye}_1] \neq 0 \& [\mathbf{xyz}] = 0)). \quad \blacksquare$$

As this example clearly indicates, we need to add a new operation *vector addition* $\mathbf{u} \oplus \mathbf{v}$. In fact we need to add a second operation: *scalar multiplication* $s * \mathbf{u}$, which produces a vector term. These operations satisfy two axioms with the bracket operation:

$$[\mathbf{t} \oplus \mathbf{t}' \ldots\ldots] = [\mathbf{t} \ldots\ldots] + [\mathbf{t}' \ldots\ldots]$$
$$[s * \mathbf{t} \ldots\ldots] = s[\mathbf{t} \ldots\ldots].$$

We want the variables to represent points (non-zero vectors), while these sums may be zero. We therefore switch to a three sorted language - with variables of sort *points*, with terms of sort *vector*, created by $\oplus$ and $*$, and terms of sort *field* created by $[\ldots]$ applied to n vectors or points, and by polynomials in these brackets and the constants. With polynomial equations for terms of sort field, this forms the extended language $LANGEE_n$.

Since the variables are to represent points, we have the axiom

$$[\mathbf{e}_1 \ldots \mathbf{e}_n] = 0 \vee [\mathbf{ye}_2 \ldots \mathbf{e}_n] \neq 0 \vee \ldots \vee [\mathbf{e}_1 \ldots \mathbf{e}_{n-1}\mathbf{y}] \neq 0.$$

For the projective space of dimension $(n-1)$, we assume:

$$(\exists \mathbf{e}_1, \ldots, \mathbf{e}_n)([\mathbf{e}_1 \ldots \mathbf{e}_n] \neq 0).$$

Since we have terms of sort vector, and variables of sort point, we must modify our rules for quantifiers:

$$8'.\ddagger \quad \frac{M \supset N,\ [\mathbf{te}_2 \ldots \mathbf{e}_n] \neq 0 \& F(\mathbf{t})}{M \supset N, (\exists \mathbf{x})F} \qquad 9'.\ddagger \quad \frac{M,\ [\mathbf{te}_2 \ldots \mathbf{e}_n] \neq 0 \& F(\mathbf{t}) \supset N}{M, (\forall \mathbf{x})F(\mathbf{x}) \supset N}$$

$\ddagger$ $\mathbf{t}$ is of sort vector, while $\mathbf{x}$ is of sort point.

With these axioms and modified rules, we call the theory AXPG_n.

Notice that we can use the added axioms to push any open formula in LANGEE_n back into LANGE_n, and apply the results from Sections 7 and 8. For more general theorems we have the following result.

THEOREM 9.2. Whiteley (1977) *A formula F in $LANGEE_n$ has a proof in $AXPG_n$ if and only if F is true for the models of all non-zero vectors in vector spaces of dimension n.*

Implicitly, this logical result guarantees that any automated symbolic computations for the invariant language can all be carried out within our invariant bracket language LANGEE_n. The theorems are totally homogeneous, and the axioms could be reduced to totally homogeneous pieces. However the stages of the proof for Example 9.1 were

not homogeneous in the variables $\mathbf{x}$ or $\mathbf{y}$. (If $\mathbf{x}$ is multiplied by a scalar $\neq 1$, the point $\mathbf{z} = \mathbf{x} \oplus \mathbf{y}$ moves along the line, and all of these moving points have the desired property.) The proofs lie in the invariant language but not inside the special subclass of totally homogeneous formulas.

We offer a simple example which emphasizes the role of the Nullstellensatz identities in proofs of even general theorems.

EXAMPLE 9.3. Consider the following simple geometric theorem.

If **ab** and *bc* are two non-skew lines in 3-space, and the line **de** intersects both **ab** and **cd**, then either **d** and **e** are coplanar with **a**, **b**, and **c**, or the point of intersection **b** lies on **de**.

We translate the theorem into brackets. The statement that line **de** intersects **ab** is written $[\mathbf{abde}] = 0$. Similarly for *bc* and *de* we have the assumption $[\mathbf{bcde}] = 0$. The conclusion that **d** and **e** are coplanar with **abc** is written as $[\mathbf{abcd}] = 0 \& [\mathbf{abce}] = 0$. The alternative that **b** is on line **de** is written $(\forall \mathbf{x})([\mathbf{debx}] = 0)$. Thus the entire theorem translates as:

$$[\mathbf{abde}] = 0, [\mathbf{bcde}] = 0 \ldots ([\mathbf{abcd}] = 0 \& [\mathbf{abce}] = 0),\ (\forall \mathbf{x})[\mathbf{debx}] = 0.$$

The proof comes in the following four stages:

I From the axioms of rings and the syzygies for the brackets, we have two Nullstellensatz identities:

$$([\mathbf{abcd}][\mathbf{debx}] = [\mathbf{abde}][\mathbf{bcdx}] + [\mathbf{abxd}][\mathbf{debc}])$$
$$([\mathbf{bcde}][\mathbf{debx}] = [\mathbf{abde}][\mathbf{bcex}] + [\mathbf{abxe}][\mathbf{bcde}]).$$

II Integral domain substitutions produce two sequents:

$$[\mathbf{abde}] = 0, [\mathbf{bcde}] = 0 \ \supset\ [\mathbf{abcd}] = 0, [\mathbf{debx}] = 0$$
$$[\mathbf{abde}] = 0, [\mathbf{bcde}] = 0 \ \supset\ [\mathbf{abce}] = 0, [\mathbf{debx}] = 0.$$

III By rule 5, we obtain the midsequent (a variant of the Herbrand formula):

$$([\mathbf{abde}] = 0, [\mathbf{bcde}] = 0 \ \supset\ ([\mathbf{abcd}] = 0)\ \&\ ([\mathbf{abce}] = 0), [\mathbf{debx}] = 0).$$

IV By quantifier rule 10, we obtain the theorem:

$$[\mathbf{abde}] = 0, [\mathbf{bcde}] = 0 \supset ([\mathbf{abcd}] = 0 \& [\mathbf{abce}] = 0), (\forall \mathbf{x})[\mathbf{debx}] = 0. \ \blacksquare$$

10. Proofs over Ordered Fields.

Clearly, the usual syzygies from Section 7, added to axioms for ordered integral domains, will prove all open theorems in the invariant language which are true over all ordered fields. Similarly, the extensions and the axioms of Section 9 can be added to the axioms for ordered integral domains or for real closed fields to prove all theorems within our languages.

What about a special form for open theorems? As before, we can restrict the proof of a totally homogeneous formula to work within this class of projective formulas, etc.. Basic differences in the pattern of a proof do arise from two sources: the presence of inequalities, and the modified form of the real Nullstellensatz. We begin with the second issue.

THEOREM 10.1. Krivine (1964) *A formula of the form:*

$$f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \& \ldots \& g_m = 0,$$

is true over a real closed field if and only if there are polynomials a_i, b_k, with integer coefficients, and positive integers n and m such that:

$$\sum_i a_i f_i = m \prod_j (g_j)^{2n} + \sum_k (b_k)^2.$$

EXAMPLE 10.2. A simple example illustrates this difference between algebraically closed fields and real closed fields.

$$x^2 + y^2 + 1 = 0 \;\Rightarrow\; 1 = 0$$

is true over the real numbers, but false over the complex numbers. Clearly there is *no* Nullstellensatz identity in the sense of Section 8: $a(x^2 + y^2 + 1) = 1$ is impossible. However,

$$(x^2 + y^2 + 1) = 1^2 + (x^2 + y^2)$$

is a correct decomposition. There is a basic technique over ordered fields, called the *squares principal*, which states:

$$\sum (a_i)^2 = 0 \;\Rightarrow\; a_1 = 0 \& \ldots \& a_m = 0$$

Applied to our example, this principle gives an immediate deduction:

$$x^2 + y^2 + 1 = 0 \;\Rightarrow\; 1 = 0$$

or

$$x^2 + y^2 + 1 \neq 0$$

∎

For formulas with equalities and their negations (no inequalities), the real Nullstellensatz guarantees that this squares principle is the only principle we need to add to the axioms of fields of characteristic zero to prove all open theorems. More generally, a field of characteristic zero can be ordered if and only if this squares principle holds. Such fields are called *formally real* (see, for example, van der Waerden (1953)).

For formally real fields, we take the axioms of integral domains of characteristic zero, plus a simplified squares principle:

$$(s_1)^2 + \ldots + (s_m)^2 = 0 \;\supset\; s_1 = 0.$$

With these axioms, and the Gentzen style system of Section 8, we have a constructive metatheorem for the real Nullstellensatz:

THEOREM 10.3. *Given a derivation D of a theorem:*

$$f_1 = 0, f_2 = 0, \ldots, f_k = 0 \;\supset\; g_1 = 0, \ldots, g_m = 0,$$

from the axioms for formally real fields, there is a constructive algorithm which reads, from this derivation, a real Nullstellensatz identity:

$$\sum_i a_i f_i = t \prod_j (g_j)^{2w} + \sum_k (b_k)^2$$

with the a_i, b_k polynomials with integer coefficients, and t, w positive integers.

Proof. Each of the axioms for integral domains gives a real Nullstellensatz identities: $RN(S)$, with no b_i. (Simply square the identities $N(S)$ used for Hilbert's Nullstellensatz.) The squares principle gives the simple identity:

$$RN((s_1)^2 + \ldots + (s_m)^2 = 0 \supset s_1 = 0) : (s_1)^2 + \ldots (s_m)^2 = (s_1)^2 + \ldots (s_m)^2$$

Once more this derivation can be cut reduced, so that only rules 11-14 are used, and all sequents are atomic. Again the only challenging rule is the cut rule:

$$14. \quad \frac{F_1, \ldots, F_m, E \supset G_1, \ldots, G_p \qquad F_{m+1}, \ldots, F_n \supset G_{p+1}, \ldots, G_q, E}{F_1, \ldots, F_m, F_{m+1}, \ldots, F_n \supset G_1, \ldots, G_p, G_{p+1}, \ldots, G_q}$$

with the following real Nullstellensatz identities for the top pieces:

$$\sum_{i=1}^{i=m} a_i f_i + a_e e = t \left(\prod_{j=1}^{j=n} g_j \right)^{2v} + \sum_{k=1}^{k=r} (b_k)^2$$

$$\sum_{i=m+1}^{i=p} a_i f_i = t' \left(\prod_{j=n+1}^{j=q} g_j \right)^{2w} e^{2w} + \sum_{k=r+1}^{k=s} (b_k)^2.$$

We solve the first equation for $a_e e$, and take to the power ^{2w}:

$$(a_e e)^{2w} = \left(t \left(\prod_{j=1}^{j=n} g_j \right)^{2v} + \sum_{k=1}^{k=r} (b_k)^2 - \sum_{i=1}^{i=m} a_i f_i \right)^{2w}$$

$$= t^{2w} \left(\left(\prod_{j=1}^{j=n} g_j \right)^{4vw} + \sum_{k=1}^{k=r} (c_k)^2 + \sum_{h=1}^{h=r} (z_h)^2 (f_i)^2 - \sum_{i=1}^{i=m} d_i f_i \right)^{2w}$$

We multiply by the term $t' \left(\prod_{j=n+1}^{j=q} g_j \right)^{4vw}$, and substitute from equation 2:

$$a_e^{2w} \left(\prod_{j=n+1}^{j=q} g_j \right)^{4vw-2w} \left(\sum_{i=m+1}^{i=p} a_i f_i - \sum_{k=1}^{k=r} (b_k)^2 \right)$$

$$= t''' \left(\prod_{j=1}^{j=q} g_j \right)^{2(2vw)} + \sum_{k=1}^{k=x+y} (c_k^*)^2 + \sum_{i=1}^{i=p} d_i^* f_i.$$

This simplifies to a real Nullstellensatz identity for the bottom sequent. Induction on the entire proof tree leads to the desired identity for the final sequent. ∎

PROBLEM 10.3. Does this logical "metatheorem" apply to other typical proofs of such an open theorem? That is, does any "natural" computer proof of such a formula generate

an explicit construction of a real Nullstellensatz identity, from which the theorem results by simple substitutions? It is clearly desirable that the algorithm should output the real Nullstellensatz identities for the theorem

EXAMPLE 10.4. An explicit case of this problem is presented by Sturm sequences (van der Waerden (1953), 220-222). Assume that a univariate polynomial $p(x)$, and its derivative $p'(x)$ are relatively prime. First establish a finite sequence of polynomials:

$$f_0(x) = p(x); f_1(x) = p'(x); \ldots ; f_{i-2}(x) = q_i(x) f_{i-1}(x) - f_i(x); \ldots$$

with degree $f_i <$ degree f_{i-1}, using the Euclidean algorithm. Next create two sequences of signs:

$$S(\infty) : \ldots , \text{sign(highest power in } f_i(x)), \ldots$$

and

$$S(-\infty) : \ldots , \text{sign(highest power in } f_i(-x)), \ldots .$$

From these sequences, we have two numbers:

$$w(\infty) = \sharp\text{sign changes in } S(\infty); \quad \text{and} \quad w(-\infty) = \sharp\text{sign changes in } S(-\infty).$$

Sturm's theorem says that the number of real roots of $p(x)$ is $w(-\infty) - w(\infty)$. In particular, if $w(-\infty) = w(\infty)$ there no real roots. This guarantees that:

$$a(x)p(x) = \sum_i [q_i(x)]^2 + 1$$

for some polynomials a and q_i.

How does this sequence (or the proof that the theorem holds) generate these polynomials? Since Sturm sequences are used in computer algorithms for real algebraic geometry, this is a practical example for symbolic computation. ∎

For ordered fields, with $<$, there are forms of a Positivstellensatz (see, for example, Bochnak *et al.* (1987)), which can be used to give a standard form for open theorems. We note that any open formula in LRALG_n can be written in the many different conjunctive normal forms:

$$\left(\bigvee_h (r_h > 0) \vee \bigvee_i (s_i \geq 0) \vee \bigvee_j (t_j = 0) \right) \& \ldots$$

or

$$\left(\bigvee_h (r_h > 0) \vee \bigvee_i (s_i \geq 0) \right) \& \ldots \& \left(\bigvee_k (u_k > 0) \vee \bigvee_m (v_m \geq 0) \right)$$

or

$$\left(\bigvee_h (r_h > 0) \vee \bigvee_j (t_j = 0) \right) \& \ldots \& \left(\bigvee_k (u_k > 0) \vee \bigvee_n (w_n = 0) \right).$$

It remains a subject for further research to select an optimal form, with a corresponding Positivstellensatz which grows on proof trees.

For a general survey of constructive approaches to these problems see (Lombardi (1990)).

In conclusion, appropriate identities are available to express almost all of the theorems. These identities carry more information than any other proof of the corresponding theorem. The identities are easily derived from typical first order proofs - and should be the output of future symbolic computer algorithms for analytic projective geometry.

ACKNOWLEDGEMENTS. This work originated, 20 years ago, as part of a general program of Gian-Carlo Rota to translate combinatorial properties and theorems of projective geometry into properties and theorems of a matroid using classical invariant theory. We thank Gian-Carlo for twenty years of conversations on these topics. We also thank Bernd Sturmfels for more recent discussions of the content, and the form, of this paper.

We thank Henry Crapo and Neil White for fifteen years of joint work on applied projective geometry. These shared experiences confirmed our sense that the language of brackets, and its companion Cayley algebra, are an excellent setting for analytic projective geometry.

References.

Baer, R. (1952). *Linear Algebra and Projective Geometry*, Academic.Press, New York.

Bochnak, J., Coste, M., Roy, M-F. (1987). *Géometrie algébraique réelle*, Springer-Verlag, New York.

Collins, G.E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition, in *Automata Theory and Formal Languages, 2nd G.I. Conf., Kaiserslautern*, Springer-Verlag, New York, 134-151.

Crapo, H., Whiteley, W. (1982). Statics of frameworks and motions of panel structures: a projective geometric introduction, *Structural Topology* **6**, 43-82.

Dickmann, M.A. (1983). Applications of model theory to real algebraic geometry, in *Methods in Mathematical Logic*, Lecture Notes in Math **1130**, Springer Verlag, New York, 76-150.

Dieudonné, J., Carrell, J.B. (1970). Invariant theory old and new, *Advances in Math.* **4**, 1-80.

Doubilet, P., Rota, G-C., Stein, J., (1974). On the foundations of combinatorial theory IX: Combinatorial methods in invariant theory, *Studies in Applied Math.* **57**, 185-216.

Feferman, S. (1968). Lectures in proof theory, in *Proceeding of the Summer School in Logic, Leeds 1967*, Springer-Verlag, New York, 1-107.

Forder, H. (1960). *The Calculus of Extensions*, Chelsea, New York.

Havel, T. (1991). A distance geometry proof of Simpson's theorem, *J. Symbolic Computation***11**, 579-593.

Klein, F. (1937). *Elementary Mathematics from an Advanced Standpoint: Geometry*. Dover, New York.

Krivine, J. (1964). Anneaux préordonnés, *J. Anal. Math.* **21**, 307-326.

Kreisel, G., Krivine, J. (1967). *Elements of Mathematical Logic*, North-Holland, Amsterdam.

Kutzler, B. (1988). Algebraic Approaches to Automated Theorem Proving, PhD Thesis, Research Institute for Symbolic Computation Linz, Johannes Kepler University, A-4040 Linz, Austria.

Lombardi, H. (1990). Une etude historique sur les problémes d'effectivé en algebre réalle, preprint, Mathematiques, UFR des Sciences et Techniques, Université de France-Comté, 15030 Besanon cedex France.

Robinson, A. (1965). *Introduction to Model Theory and the Metamathematics of Algebra* 2nd ed., North-Holland, Amsterdam.

Rota, G-C., and Sturmfels, B. (1988). Introduction to invariant theory in superalgebras, in *Invariant Theory and Tableaux*, D. Stanton (ed.) IMA Volumes in Mathematics and its Applications, Springer, to appear.

Scarpellini, B. (1969). On the metamathematics of rings and integral domains, *Trans. A.M.S.* **138**, 71-96.

Seidenberg, A. (1956). Some remarks on Hilbert's Nullstellensatz, *Arch. Math.* **7**, 235-246.

Sturmfels, B. (1991). Computational synthetic geometry of projective configurations, *J. Symbolic Computation***11**, 595-618.

Sturmfels, B., White, N. (1989). Gröbner bases and invariant theory, *Advances in Math.* **76**, 245-259.

Sturmfels, B., Whiteley, W. (1991). Synthetic factoring of invariant equations, *J. Symbolic Computation***11**, 439-453.

Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry*, 2nd ed. Berkeley University Press.

Takeuti, G. (1975). *Proof Theory*, North Holland, Amsterdam.

van der Waerden, B.L. (1953). *Modern Algebra*, English translation, Ungar, New York.

Weyl, H. (1946). *The Classical Groups*, Princeton University Press, Princeton N.J..

White, N (1988). An implementation of the straightening algorithm, in the *Proceedings of the Workshop on Invariant Theory and Tableaux*, Institute for Mathematics and Its Applications, University of Minnesota, Minneapolis, Minnesota 55455.

White, N (1991). Multilinear Cayley factorization, *J. Symbolic Computation***11**, 421-438.

White, N., Whiteley, W. (1983). The algebraic geometry of stresses in frameworks, *S.I.A.M. J. Algebraic and Discrete Methods* **4**, 481-511.

White, N , Whiteley, W. (1987). The algebraic geometry of motions in bar and body frameworks, *S.I.A.M. J. Algebraic and Discrete Methods* **8**, 1-32.

Whiteley, W. (1971). Logic and invariant theory, PhD thesis, MIT, Cambridge Mass..

Whiteley, W. (1973). Logic and invariant theory I: invariant theory of projective spaces, *Trans. A.M.S.* **177**, 121-139.

Whiteley, W. (1977). Logic and invariant theory III: axiom systems and syzygies *J. London Math Soc.* **(2) 15**, 1-15.

Whiteley, W. (1978). Logic and invariant theory II: homogeneous coordinates, the introduction of higher quantities and structural geometry, *J. Algebra* **50**, 380-394.

Whiteley, W. (1979). Logic and invariant theory IV: invariants and syzygies in combinatorial geometry *J. Comb. Theory* **B 26**, 251-267.

Whiteley, W. (1982). Motions, stresses and projected polyhedra, *Structural Topology* **7**, 13-38.

Whiteley, W. (1983). Cones infinity and 1-story buildings, *Structural Topology* **8**, 53-70.

Whiteley, W. (1984). Infinitesimal motions of a bipartite framework, *Pac. J. Math.* **110**, 233-255.

Whiteley, W. (1987a). Rigidity and polarity I: statics of sheetworks; *Geometriae Dedicata* **22**, 329-362.

Whiteley, W. (1989). A matroid on hypergraphs, with applications in scene analysis and geometry, *Discrete Computational Geom.* **4**, 75-95.

Whiteley, W. (1991). The combinatorics of bivariate splines, in *Applied and Discrete Geometry, the Victor Klee Feischrift*, to appear.