LOGIC AND INVARIANT COMPUTATION FOR ANALYTIC GEOMETRY*

WALTER WHITELEY†

Abstract. Some results from the invariant theory of first-order formulas are summarized and connected to the problems of symbolic computation in analytic geometry and analytic translations of synthetic geometry. Special emphasis is given to projective geometry over algebraically closed fields and over real closed fields. Properties initially expressed with first order algebraic formulas, which are invariant for appropriate geometric transformations, are transformed into a precise invariant form. First-order proofs of theorems in these properties are also transformed in a standard invariant pattern which is accessible to synthetic interpretation.

Synthetic geometric theorems and constructions fit within first-order logic. That is, they can be written with quantified formulas formed with a finite pattern of disjunctions, conjunctions and negations of polynomial equations, with the quantifiers restricted to variables for numbers or fixed length vectors (points, lines, planes etc. of fixed types). This assumption excludes statements such as "there exists a non-algebraic number" or "there exists a polynomial such that ..." which would require other quantifiers for higher order objects (such as general polynomials), or an infinite number of simpler polynomial equations.

Given such a first-order formula \( F \), we can restate Klein’s Erlanger program for geometry as follows (Whiteley 1974): A formula is "geometric" if the set of values which make \( F \) true is invariant under the corresponding "geometric transformations". As a general setting for this invariance, we select a set of mathematical (algebraic) models which we wish to describe, and the collection (category) of transformations either within a particular model, or between these models, which should preserve the truth of these geometric formulas. This pattern includes the classical invariant theory for groups of transformations within a fixed model, as well as some separate logical work on invariance under embeddings etc...

1. The First Fundamental Theorem.

The "First Fundamental Theorem" for the classical invariant theory of a vector space and a group of morphisms will characterize all polynomials in the coordinates of the vectors which are relative invariants of the morphisms:

\[
p(T(a_1) \ldots T(a_m)) = g(T) p(a_1, \ldots, a_m) \quad \text{for all } a_1, \ldots, a_m
\]

*Work supported, in part, by grants from NSERC (Canada) and FCAR (Québec), and a short term visit at the I.M.A., University of Minnesota

†Champlain Regional College, 900 Riverside Drive, St. Lambert, Québec, J4P-3P2, CANADA, and Centre de recherches mathématiques, Université de Montréal, Montréal, Québec, H3C-3J7, CANADA
The characterization will give a standard form for all these invariants, if possible as a finitely generated ring of polynomials, for a finite set of variables [4,16]. While this is not always possible, such a theorem will hold for the classical groups we encounter.

The "First Fundamental Theorem" for the invariant theory of a category of models and morphisms will again characterize the invariant formulas by their syntax, i.e. the way they are written [19,21]. The principle is to find a form of writing which guarantees the invariance, and then prove that all invariant formulas are equivalent to statements in this invariant language.

Example 1.1. For the category of vector spaces of dimension \( n \) over fields, with non-singular linear transformations as the morphisms, the \( n \)-bracket \( [a_1 \ldots a_n] \), which is interpreted as the determinant, is a relative algebraic invariant:

\[
[T(a_1) \ldots T(a_n)] = \det(T(a_1) \ldots T(a_n)) = (\det[T]) \cdot \det(a_1 \ldots a_n) = (\det[T]) \cdot [a_1 \ldots a_n]
\]

As a result, any polynomial \( p(a_1, \ldots, a_n) \) in the \( n \)-brackets which is homogeneous in the total degree \( k \) for all monomials is a relative invariant [16]:

\[
p(T(a_1), \ldots, T(a_n)) = (\det[T])^k \cdot p(a_1, \ldots, a_n)
\]

In terms of first order formulas:

\[
p(T(a_1), \ldots, T(a_n)) = 0 \iff (\det[T])^k p(a_1, \ldots, a_n) = 0 \iff p(a_1, \ldots, a_n) = 0
\]

Thus homogeneous polynomial equations in the \( n \)-bracket are invariant formulas. The first fundamental theorem says the converse is true.

Theorem 1.2. [19] A first-order formula \( F \) in the language of integral domains (using addition, subtraction, multiplication, equality of terms, plus logical connectives and quantifiers) 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 \( F \) is equivalent to a formula \( G \) written with the \( n \)-brackets \( [a_1 \ldots a_n] \), and the operations of integral domains, with each equation homogeneous in the brackets.

As a computational technique, the translation to brackets runs as follows. For a new "basis" \( e_1, \ldots, e_n \), the \( i \)-th coordinate \( a_j^i \) of a point \( a_j \) is replaced by the bracket \( [e_1 \ldots e_{i-1} a_j e_{i+1} \ldots e_n] \) and a universal quantifier \( (\forall e_1 \ldots e_n) \) is added. If any of the equations are not homogeneous, they are replaced by a conjunction of their homogeneous pieces. The result is an invariant formula.

In some, but not all, formulas, the new variables \( e_1, \ldots, e_n \) can be eliminated as follows. For a given equation \( q(\ldots, a_j, \ldots) = 0 \), the above transformation gives a new polynomial \( q^*(\ldots, e_1, \ldots, e_n) \) in the brackets \( [e_1 \ldots e_{i-1} a_j e_{i+1} e_n] \). This polynomial is now straightened (see [17]) with \( e_1, \ldots, e_n \) as lexicographically first elements. If the
original polynomial was invariant, then the result is a formula \([c_1 \ldots c_n] \cdot B(a_1, \ldots, a_m)\), with no occurrences of the new variables in \(B(a_1, \ldots, a_m)\).

In general this translation will leave some of the new universally quantified variables. Consider, for example, the formula which says that two points \(x = (x_1, x_2, x_3)\) and \(y = (y_1, y_2, y_3)\) coincide in the projective plane:

\[
x_1 y_2 - x_2 y_1 = 0 \& x_1 y_3 - x_3 y_1 = 0 \& x_2 y_3 - x_3 y_2 = 0 \iff (\forall z) [xyz] = 0
\]

Without the variable \(z\), this cannot be written using the basic invariants \([abc]\).

The same general result holds if we restrict to the vector spaces over a particular infinite field, or fields of a particular characteristic. \(\square\)

**Example 1.3.** For the study of projective geometry, we add the transformations which multiply a single vector by a non-zero scalar. A single bracket remains invariant, as does a polynomial which is homogeneous in each of the points (vectors). The converse is also true.

**Theorem 1.4.** [21] A first-order formula \(F\) in the language of integral domains (using addition, subtraction, multiplication, equality of terms, plus logical connectives and quantifiers) is invariant for the category of projective spaces of dimension \(n - 1\) over fields, with non-singular linear transformations and homogeneous multiplication as the morphisms, if and only if \(F\) is equivalent to a formula \(G\) written with the \(n\)-brackets \([a_1 \ldots a_n]\), and the operations of integral domains, with each equation homogeneous in each of the points. \(\square\)

We recall another example of invariance drawn from first-order logic.

**Example 1.5.** For the category of models of a first order theory, with embeddings of models as the morphisms, open formulas (with no quantifiers) and purely existential formulas are invariant. That is, "there exists \(X\)" is invariant under embedding or adding new points to the model, but "for all \(X\)" is not, in general, invariant under embedding. Conversely all invariant formulas are equivalent to such first-order formulas which are at most existential in prenex form (see Section 3b) [22]. \(\square\)

**Example 1.6.** Consider the category of vector spaces of dimension \(n\) over ordered fields extending the rationals, with orthogonal matrices as the transformations. There are two simple invariants: the brackets \([x_1 \ldots x_n]\) and the inner products \((x_1 x_2)\). The algebraic First Fundamental Theorem says that all relative polynomial invariants are either polynomials \(p\) in the inner products or have the form \([x_1 \ldots x_n] \cdot p\) for such a polynomial [4,16]. (We could allow products of two brackets, but such products are equivalent to a polynomial in the inner products. As a result any product of brackets is equivalent to a polynomial of the above forms).

**Theorem 1.7.** A first order formula \(F\) in the language of integral domains (using addition, subtraction, multiplication, equality of terms, plus logical connectives and quantifiers)
is invariant for the category of orthogonal transformations over vector spaces extending a field if and only if \( F \) is equivalent to a formula \( G \) written with inner products.

To complete the characterization of Euclidean geometry, we must add translations. We believe that these invariants can be characterized in terms of distances [7], but we have not seen this explicitly written out. 

In closing this section, we recall a geometric example where such a theory has not yet been completed.

**Example 1.8.** 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. However, for formulas larger than a single polynomial equation, I know of no proof that all invariant formulas for this category can be rewritten in this form.

If we consider projective geometry over the complex numbers, all field automorphisms induce collineations (line and intersection preserving transformations). All synthetic constructions can be written with the rational numbers (see [12]) and it would be nice to show that these synthetic geometric formulas coincide with the invariant geometric formulas for the category of all collineations. This is needed to complete the "metatheorem" that synthetic projective geometry and analytic projective geometry over the complex numbers are equivalent (see [12]).

In summary, for projective geometry, and many other geometries, we have an explicit language for expressing geometric theorems and geometric constructions. These formulas are broader than the restricted language of algebra and ideals, but the basic invariant components are the same. The logical "First Fundamental Theorems" show that formulas in the basic algebraic invariants give all of the first-order geometric theorems.

2. **The Second Fundamental Theorem.**

The Second Fundamental Theorem for a classical group of transformations gives a finite set of generators (the "syzygies") for the ideal of relative invariant polynomials which are identically zero [4,16].

The Second Fundamental Theorem for a category of models and morphisms gives an explicit set of axioms (traditionally the same syzygies) for the invariant forms such that all true invariant formulas can actually be proven in first-order logic using only the invariant language [20].

**Example 2.1.** For the category of vector spaces of dimension \( n \) over fields, with non-singular linear transformations as the morphisms, we have the invariant language of the \( n \)-brackets. The classical Grassmann–Plücker syzygies give the essential axioms for these
invariants.

\[
[y\ldots] = 0, \quad [y_1y_2\ldots y_iy_{i+1}\ldots y_n] = -[y_1y_2\ldots y_{i+1}y_i\ldots y_n]
\]
\[
[x_1x_2\ldots x_n][y_1y_2\ldots y_n] = \sum_{i=1}^{n}[x_1x_2\ldots x_{i-1}y_1x_{i+1}\ldots x_n][x_iy_2\ldots y_n]
\]

We add the usual axioms for equality, and for integral domains extending a fixed field \( K \):

for all terms \( s, t, u \) (polynomials with coefficients in \( K \))

\[
t = t, \quad s = t \Rightarrow t = s, \quad s = t \& t = u \Rightarrow s = u,
\]
\[
s = t \& s' = t' \Rightarrow s + s' = t + t', \quad s = t \& s' = t' \Rightarrow s \cdot s' = t \cdot t', \quad s = t \Rightarrow -s = -t,
\]
\[
t + s = s + t, \quad s + (t + u) = s + (t + u), \quad t + (-t) = 0, \quad t + 0 = t,
\]
\[
t \cdot s = s \cdot t, \quad s \cdot (t \cdot u) = s \cdot (t \cdot u), \quad t \cdot 1 = t, \quad s \cdot (t + u) = s \cdot t + s \cdot u,
\]
\[
s \cdot t = 0 \Rightarrow s \in 0 \lor t = 0,
\]

for all constants \( k_1, \ldots, k_n \) (for elements in \( K \)):

\[
t(k_1, \ldots, k_m) = s(k_1, \ldots, k_m) \text{ whenever this is true in } K,
\]
\[
t(k_1, \ldots, k_m) \neq s(k_1, \ldots, k_m) \text{ whenever this is true in } K.
\]

Together with the usual axioms for propositional logic (see below), these give invariant proofs (proofs with all formulas invariant) for all open invariant theorems (without quantifiers) which hold over all extensions of \( K \) [18,20].

If we add quantifiers, the axioms must be extended as follows:

\[
[t \oplus t' \ldots] = [t \ldots] + [t' \ldots], \quad [s \cdot t' \ldots] = s[t \ldots]
\]

\textbf{Axioms for division}

and \((\exists z_1, \ldots, z_n)([z_1\ldots z_n] \neq 0)\)

With these extensions, any invariant formula true in all the models will have an invariant proof.

Since the basic syzygies are homogeneous, any proof for the homogeneous formulas of projective geometry can be restricted to homogeneous invariant formulas throughout [20]. □

\textbf{Example 2.2}. For the invariants of the orthogonal group, we have a similar set of axioms. To the axioms for equality and for ordered fields, we add the syzygies:

\[
\begin{bmatrix}
(x_0y_0) & (x_0y_1) & \cdots & (x_0y_n) \\
(x_1y_0) & (x_1y_1) & \cdots & (x_1y_n) \\
\vdots & \vdots & \ddots & \vdots \\
(x_ny_0) & (x_ny_1) & \cdots & (x_ny_n)
\end{bmatrix} = 0
\]

42
where the brackets indicate a determinant and \( n \) is the dimension. With these axioms, we can give an orthogonal-invariant proof for any theorems true over ordered extensions of the reals, or over real-closed fields (see below).

If we switch to Euclidean-invariant theorems, we believe that the required axioms will be the Cayley–Menger conditions \([5,7]\) but we have not seen a proof of this. □

A symbolic computation is a type of first-order logical proof. This is an underlying principle of the computer language PROLOG (PROgramming in LOGic). Thus the above logical result guarantees that all symbolic computations can be carried out within the invariant language, with the syzygies as added rules.

3. **Proofs over Algebraically Closed Fields.**

3 a) **Open or universal theorems.**

Consider any open (quantifier free) formula \( M \), built from the basic equations with \( \& \) (and) \( \lor \) (or) \( \Rightarrow \) (implication) and \( \sim \) (negation). We can replace an implication \( (F \Rightarrow G) \) by the equivalent formula \( (\sim F \lor G) \). We can distribute \( \sim \) over \( \& \) and \( \lor \), and distribute \( \lor \) over \( \& \):

\[
\sim (F \& G) \leftrightarrow (\sim F \lor \sim G) \quad \text{and} \quad (F \lor G) \leftrightarrow (\sim F \& \sim G)
\]

\[F \lor (G \& H) \leftrightarrow (F \lor G) \& (F \lor H)\]

After repeated applications, any quantifier free formula assumes a conjunctive normal form:

\[(\sim F_1 \lor \cdots \lor \sim F_m \lor G_1 \lor \cdots \lor G_n) \& \cdots \& (\sim F_p \lor \cdots \lor \sim F_q \lor G_r \lor \cdots \lor G_t)\]

where \( F_i \) and \( G_j \) are atomic formulas. In all our cases the atomic formulas are polynomial equations \( s_i = t_i \) or equivalently \( s_i - t_i = 0 \). Thus every quantifier free formula can be written in the standard form:

\[
(f_1 \neq 0 \lor \cdots \lor f_m \neq 0 \lor g_1 = 0 \lor \cdots \lor g_n = 0) \& \cdots
\]

\[
\cdots \& (f_p \neq 0 \lor \cdots \lor f_q \neq 0 \lor g_r = 0 \lor \cdots \lor g_s = 0)
\]

Equivalently, every such formula can be written:

\[
(f_1 = 0 \& \cdots \& f_m = 0 \Rightarrow g_1 = 0 \lor \cdots \lor g_n = 0) \& \cdots
\]

\[
\cdots \& (f_p = 0 \& \cdots \& f_q = 0 \Rightarrow g_r = 0 \lor \cdots \lor g_s = 0)
\]

For algebraically closed fields, we have an additional result which simplifies such statements: Hilbert’s nullstellensatz.
Theorem 3.1. A formula of the form:

\[ f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \lor \ldots \lor g_m = 0, \]

is true over an algebraically closed field if and only if there are polynomials \( a_i \) and integers \( n(j) \) such that \( \sum a_i f_i = \Pi(g_j^{n(j)}) \) as polynomials.

There is a logical form of this result as a metatheorem about proofs of such formulas.

Theorem 3.2. A first-order proof of a formula of the form

\[ M \Rightarrow N : f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \lor \ldots \lor g_m = 0, \]

from axioms for an algebraically closed field, or fields extending a fixed field \( K \), gives an explicit construction for the corresponding Hilbert equation

\[ h(M \Rightarrow N) : \sum a_i f_i = \Pi(g_j^{n(j)}). \]

Without presenting the full proof of this metatheorem, we will illustrate the process. We first note that the axioms for equality, integral domains, etc., give immediate Hilbert equations. For example:

\[
\begin{align*}
    h(t = t) & : (t - t) = 0; \\
    h(s = t \Rightarrow t = s) & : (t - s) = -(s - t) \\
    h(s = t & t = u \Rightarrow s = u) & : (s - t) + (t - u) = (s - u); \\
    h(s = t & s' = t' \Rightarrow s + s' = t + t') & : (s - t) + (s' - t') = (s + s' - (t + t')); \\
    h(s = t & s' = t' \Rightarrow s \cdot s' = t \cdot t') & : s'(s - t) + t(s' - t') = (s \cdot s' - t \cdot t').
\end{align*}
\]

We now give some "natural rules" for logical proofs of such formulas (based on Gentzen style natural deductions), and showing how to read the Hilbert equation through these steps. In the following, imagine a vertical "proof tree", with axioms at the top of each branch, and the desired theorem at the bottom. Each solid line represents a proof rule, from the higher formula(s) to the logically equivalent lower formula.

\[
\begin{align*}
    F_1 \& \ldots \& F_m & \Rightarrow G_1 \lor \ldots \lor G_p \\
    F_1 \& \ldots \& F_m & \Rightarrow G_1 \lor \ldots \lor G_p
\end{align*}
\]

\[
\begin{align*}
    \sum_{i=1}^{m} a_i f_i &= \prod_{j=1}^{p} g_j^{n_j} \\
    \sum_{i=1}^{m} a_i f_i + 0 \cdot f_0 &= \prod_{j=1}^{p} g_j^{n_j}
\end{align*}
\]

\[
\begin{align*}
    F_1 \& \ldots \& F_m & \Rightarrow G_1 \lor \ldots \lor G_p \\
    F_1 \& \ldots \& F_m & \Rightarrow G_1 \lor \ldots \lor G_p \lor G_0
\end{align*}
\]

\[
\begin{align*}
    \sum_{i=1}^{m} a_i f_i &= \prod_{j=1}^{p} g_j^{n_j} \\
    \sum_{i=1}^{m} g_0 a_i f_i &= g_0 \prod_{j=1}^{p} g_j^{n_j}
\end{align*}
\]

44
Consider the more complex "cut" rule (a variant of modus ponens)

\[ F_1 \& \ldots \& F_m \& \& E \Rightarrow G_1 \lor \cdots \lor G_p, \quad F_{m+1} \& \& \ldots \& \& F_n \Rightarrow G_{p+1} \lor \cdots \lor G_q \lor E \]

\[ F_1 \& \ldots \& F_m \& \& F_{m+1} \& \& \ldots \& \& F_n \Rightarrow G_1 \lor \cdots \lor G_p \lor G_{p+1} \lor \cdots \lor G_q \]

with the following Hilbert equations for the top pieces:

\[ \sum_{i=1}^{m} a_i f_i + a_e e = \prod_{j=1}^{p} g_j^n, \quad \sum_{i=m+1}^{n} a_i f_i = c^n \prod_{j=p+1}^{q} g_j^n \]

We solve the first equation for \( a_e e \), and multiply the second equation by \( a_e^n \). We now substitute for \( a_e e \) in the modified second equation to obtain the required Hilbert equation, with a complex multiplier \( k \) formed from the pieces of the first equation:

\[ (k \prod_{j=p+1}^{q} g_j^n) \sum_{i=1}^{m} a_i f_i + \sum_{i=m+1}^{n} a_i^n a_i f_i = \prod_{j=1}^{p} g_j^n a_i f_i = \prod_{j=p+1}^{q} g_j^n \]

Other rules allow us to collapse duplications among the \( F_i \) and the \( G_i \), and this is reflected by the obvious additions and multiplications of the equal polynomials in the Hilbert equation.

Our logical rules will include rules for adding quantifiers:

\[
\begin{align*}
M \& F(w) & \Rightarrow N \\
M \& (\exists x) F(x) & \Rightarrow N \\
M \Rightarrow N \lor G(t) \\
M \Rightarrow N \lor (\exists x) G(x)
\end{align*}
\]

\[
\begin{align*}
M \& F(t) & \Rightarrow N \\
M \& (\forall x) F(x) & \Rightarrow N \\
M \Rightarrow N \lor G(w) \\
M \Rightarrow N \lor (\forall x) G(x)
\end{align*}
\]

where \( w \) does not occur as a free (unquantified) variable in the formulas of \( M \) or \( N \). We do not have to work out Hilbert equations for such rules because we can eliminate all quantified formulas from the proof of an open statement. In proof theory this is done by "cut reduction" - eliminating all uses of the cut rule on quantified formulas, a process which works when all axioms are quantifier free [6,18]. This holds for the axioms systems described above - including the theories of fields extending a fixed field \( K \). We return to this theme in Section 4.

We interpret this Hilbert equation \( h(F) \) as an algebraic proof of the formula \( F \). Thus the theorem says: any logical proof yields an algebraic proof. Notice that there is a simple transition from this Hilbert equation back to the original formula. In general this Hilbert equation gives a superior presentation of the algebraic (and geometric) information in such a theorem. For example, we can see all variations in the assumptions, and there are no "hidden" hypotheses.
Example 3.3. If a matroid of rank $n$ can be coordinatized, the coordinates satisfy a first-order formula:

$$(\exists x_1 \ldots x_k) \left( [x_1 \ldots x_n] = 0 \& \ldots \& [x_j \ldots x_m] = 0 \& [x_s \ldots x_t] \neq 0 \& \ldots \& [x_d \ldots x_r] \neq 0 \right)$$

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

$$\sim (\exists x_1 \ldots x_k) \left( [x_1 \ldots x_n] = 0 \& \ldots \& [x_j \ldots x_m] = 0 \& [x_s \ldots x_t] \neq 0 \& \ldots \& [x_d \ldots x_r] \neq 0 \right)$$

i.e. $$(\forall x_1 \ldots x_k)([x_1 \ldots x_n] \neq 0 \vee \ldots \vee [x_j \ldots x_m] \neq 0 \vee [x_s \ldots x_t] = 0 \vee \ldots \vee [x_d \ldots x_r] = 0)$$

In the logical structure outlined above, this is equivalent to a single Hilbert equation:

$$a[x_1 \ldots x_n] + \ldots + c[x_j \ldots x_m] = [x_s \ldots x_t]^p \ldots [x_d \ldots x_r]^q$$

In this context of representing matroids, the polynomial part of this equation, $a[x_1 \ldots x_n] + \ldots + c[x_j \ldots x_m] - [x_s \ldots x_t]^p \ldots [x_d \ldots x_r]^q$, has been called the “final polynomial” of the proof by Bokowski and Sturmfels (see [1,11] for this alternate description).

![Diagram](image)

**Figure 1. The Fano plane**

Consider the example of the Fano plane (Figure 1). Since this is a projective plane configuration, we use 3-brackets. We assume that $[xbc] = 0$, $[ayc] = 0$, $[abz] = 0$, $[axp] = 0$, $[byp] = 0$, $[cyp] = 0$, and $[xyz] = 0$. We also assume that all other brackets are non-zero (no other triples are collinear). 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 to be zero:

\[
2 [pbc][apc][abp][axc][aby][zbc] = \\
+ [pbc][apc][abp][axc][ybc][abx] + [pbc][apc][abp][axb][zbc][acy] \\
- [pbc][abp][ybc][axc][abc][apx] - [pbc][abp][axc][abc][ayb] \\
- [pbc][abp][axc][aby][abc][pzc] + [pbc][apc][abp][abc][xycz] \\
- [pbc][apc][abp][abc][ayz][xbc]
\]

Since we assumed that \( [axc] \neq 0, [abp] \neq 0, [pbc] \neq 0, [apy] \neq 0, [zbc] \neq 0, [apc] \neq 0 \), the configuration cannot be coordinatized unless \( 2 = 0 \). \( \square \)

We showed, above, that any unquantified formula is equivalent to a formula in conjunctive normal form:

\[
\{ f_1 = 0 \land \ldots \land f_m = 0 \} \Rightarrow g_1 = 0 \lor \ldots \lor g_n = 0 \}
\]

If this is a theorem over the complex numbers (or any algebraically closed field), each of the pieces in this conjunction has a Hilbert equation, so the result is recorded by the conjunction:

\[
h(f_1 = 0 \land \ldots \land f_m = 0 \Rightarrow g_1 = 0 \lor \ldots \lor g_n = 0) \land \ldots
\]

If the formulas are invariant, then we can make all formulas in the proof invariant, and therefore make all terms of the Hilbert equations invariant. Thus this result reinforces the role of such basic identities, or syzygies, in the invariant proofs of open theorems. Translated into computer terms, the metatheorem suggests that a little extra bookkeeping in any computer proof will give these Hilbert equations - and more information than any other proof. Thus we propose that the computer proof of such a theorem should be recorded as a conjunction of Hilbert equations, or final polynomials.

3b) Quantifiers over Algebraically Closed Fields.

For some mathematical theories, such as the theory of algebraically closed fields, or the theory of real-closed fields (see below) we have a process of quantifier elimination [9,10].

Every first order formula \( F \) is equivalent to a quantifier-free formula \( G \).

However, quantifier elimination may destroy the invariant form of the formula. Recall from Example 1.1:

\[
x_1 y_2 - x_2 y_1 = 0 \land x_1 y_3 - x_3 y_1 = 0 \land x_2 y_3 - x_3 y_2 = 0 \quad \iff \quad (\forall z) [xyz] = 0
\]

47
For this reason, we will not use quantifier elimination.

We will use a more subtle theory which breaks down the proofs of general formulæ from open (unquantified) theories, such as the theory of fields of a fixed characteristic. The basic ideas are simple. First we pull all quantifiers to the front of the formula, putting it in "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. At most this involves changing the names of some variables in the basic pieces (equations).

Next, we reorder the use of the logical rules, placing all the quantifier rules at the bottom of the proof, in the simplified form:

$$\frac{M_1 \lor \cdots \lor M_i(t) \lor \cdots \lor M_n}{M_1 \lor \cdots \lor (\forall x)M_i \lor \cdots \lor M_n} \quad \frac{M_1 \lor \cdots \lor M_i(w) \lor \cdots \lor M_n}{M_1 \lor \cdots \lor (\exists x)M_i \lor \cdots \lor M_n}$$

where $t$ is a variable which is not free in other $M_i$. In the last layer we also keep a simplified rule for collapsing duplicate formulæ:

$$\frac{M_1 \lor \cdots \lor M_n \lor M_n}{M_1 \lor \cdots \lor M_n}$$

All other rules come higher up in the proof tree. Just above the highest quantifier rule in this pattern, we have a middle, quantifier free formula, called the Herbrand formula. Assume that the final theorem has the prenex form:

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

The Herbrand formula then has the form:

$$M_1 \lor \cdots \lor M_2$$

where each $M_i$ is the basic open formula $M$ with the existential quantifiers replaced by terms in the language (polynomials in our case), and universal quantifiers replaced by variables which do not replace quantifiers to the left in the prenex form. Again, the passage from the Herbrand disjunction to the prenex formulæ actually reduces the information - by removing the construction of terms which are existentially quantified.

If the final formulæ, and the axioms, are invariant, all equations in the Herbrand disjunction can also be made invariant - giving a completely invariant proof.

Any first-order proof of a first-order theorem about such fields can be organized in a four stage sequence:

(i) all formulæ of the top section are conjunctions of equations (the Hilbert equations);
(ii) second stage operations are substitutions into equations of the form \( \Pi(g_j)^n(j) = \sum a_i f_i \) to give conjunctions of the formulas of the form:

\[
f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \lor \ldots \lor g_m = 0,
\]
or similar pieces which are equivalent under the usual propositional rules on “and, or, not” etc.;

(iii) third stage operations rearrange the equations of conjunctive normal form into the Herbrand disjunction;

(iv) final stage operations insert quantifiers and collapse pieces which are identical after quantification.

We offer a simple example to illustrate the stages of such a proof.

**Example 3.4.** Recall 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 \( bc \), then either \( d \) and \( e \) are coplanar with \( a, b, \) and \( c \), or the point of intersection \( b \) lies on \( de \).

We must first translate the theorem into analytic geometry. This is a projective theorem, so we will write it in the invariant language of 4-brackets. The statement that line \( de \) intersects \( ab \) is written \([abde] = 0\). (This is actually a more general projective statement, including the possibility that the lines are parallel.) Similiarly for \( bc \) and \( de \) we have the assumption \([bcde] = 0\). The conclusion that \( d \) and \( e \) are coplanar with \( abc \) is written as \([abcd] = 0 \& [abce] = 0\). Thus the entire theorem translates as:

\[
([abde] = 0 \& [bcde] = 0) \Rightarrow ([abcd] = 0 \& [abce] = 0) \lor (\forall x)([debx] = 0)
\]

In prenex form the theorem is:

\[
(\forall x) \{ ([abde] = 0 \& [bcde] = 0) \Rightarrow ([abcd] = 0 \& [abce] = 0) \lor ([debx] = 0) \}
\]

Since there are no existential quantifiers, the Herbrand disjunction is a single substitution:

\[
([abde] = 0 \& [bcde] = 0) \Rightarrow ([abcd] = 0 \& [abce] = 0) \lor ([debx] = 0)
\]

To place this in disjunctive normal form we translate the implication:

\[
([abde] \neq 0 \lor [bcde] \neq 0) \lor ([abcd] = 0 \& [abce] = 0) \lor ([debx] = 0)
\]

After distributing the conjunction we have:

\[
( [abde] \neq 0 \lor [bcde] \neq 0 \lor [abcd] = 0 \lor [debx] = 0 ) \&
( [abde] \neq 0 \lor [bcde] \neq 0 \lor [abce] = 0 \lor [debx] = 0 )
\]
These come from the conjunction of two Hilbert equations:

\[[abcd][debx] = [abde][bcdx] + [abxd][bcde] \quad \& \quad [abce][debx] = [abde][bcex] + [abxe][bcde]\]

Summarizing, this gives us the following four stages for the proof:

(i) From the axioms of rings and the syzygies for the brackets, we have two Hilbert equations

\[[abcd][debx] = [abde][bcdx] + [abxd][bcde], \quad [abce][debx] = [abde][bcex] + [abxe][bcde],\]

which we combine as a conjunction.

(ii) Substitution produces the disjunctive normal form

\[([abde] \neq 0 \lor [bcde] \neq 0 \lor [abcd] = 0 \lor [debx] = 0) \quad \& \quad ([abde] \neq 0 \lor [bcde] \neq 0 \lor [abce] = 0 \lor [debx] = 0)\]

(iii) The Herbrand formula is obtained by simple propositional rules.

\[([abde] = 0 \land [bcde] = 0) \implies ([abcd] = 0 \land [abce] = 0) \lor ([debx] = 0)\]

(iv) The proof is completed by introducing the quantifiers

\[(\forall x) \{([abde] = 0 \land [bcde] = 0) \implies ([abcd] = 0 \land [abce] = 0) \lor ([debx] = 0)\}\]

Notice that the conjunction of Hilbert equations in (i) is open to other interpretations. For example, we could select alternative substitutions – to give the theorem:

\[[bcdx] = 0 \land [abxd] = 0 \land [bcex] = 0 \land [abxe] = 0 \implies ([abcd] = 0 \land [abce] = 0) \lor ([debx] = 0)\]

This, in turn, can be read as:

If the lines \(xd\) and \(xe\) each intersects the lines \(ab\) and \(bc\), then either the points \(d\) and \(e\) are coplanar with \(abc\), or the points \(b, x, d\) and \(e\) are coplanar.

Thus the single conjunction of Hilbert equations embodies many geometric connections.

\[\Box\]

In summary, we have the following “metatheorems” about first-order proofs, including computer proofs, for geometric theorems over algebraically closed fields:

(a) a conjunction of Hilbert equations (or final polynomials) plays a crucial primary role in a “natural” proof of such first-order formulas;

(b) for invariant formulas, all these stages can be carried out within the invariants;

(c) the maximum information is available in the stage of these Hilbert equations.
4. Extensions to Real Closed Fields.

The logical results on Hilbert equations and Herbrand disjunctions depended on open axioms (axioms without quantifiers). Consider the theory of real closed fields, such as the real algebraic numbers and the real numbers, or elementary geometry [2,3,14]. This theory requires a critical existential axiom. One form of this axiom is:

\[ p(x) < 0 \& p(y) > 0 \& x < y \Rightarrow (\exists z) \, p(z) = 0 \]

where \( p(x) \) is a polynomial. When placed in prenex form, this formula is existential:

\[ (\exists z) \{ p(x) < 0 \& p(y) > 0 \& x < y \Rightarrow p(z) = 0 \} \]

A result about ordered fields which follows from this axiom, which we will need below, is the squares principle:

\[ \sum (a_i)^2 = 0 \Rightarrow a_1 = 0 \& \ldots \& a_m = 0 \]

There is a real nullstellensatz for formulas over real closed fields (see [11] for an alternate version).

**Theorem 4.1.** [8] A formula of the form:

\[ f_1 = 0 \& f_2 = 0 \& \ldots \& f_k = 0 \Rightarrow g_1 = 0 \lor \ldots \lor g_m = 0, \]

is true over a real closed field if and only if there are polynomials \( a_i, b_j \) and integers \( n(j) \) such that \( \sum a_i f_i = \Pi(g_j^{2n(j)}) + \sum (b_j)^2 \) as polynomials.

**Example 4.2.** We illustrate this difference between algebraically closed fields and real closed fields with a simple example.

\[ x^2 + y^2 + 1 = 0 \Rightarrow 1 = 0 \]

is true over the real numbers, but false over the complex numbers. Clearly there is no Hilbert equation in the sense of Section 3.1:

\[ a_1(x^2 + y^2 + 1) = 1 \]

is impossible. However,

\[ (x^2 + y^2 + 1) = 1^2 + (x^2 + y^2) \]

is a correct decomposition - and the squares principal gives an immediate deduction for:

\[ x^2 + y^2 + 1 = 0 \Rightarrow 1 = 0 \]

over a real closed field \( \square \)
PROBLEM 4.3. Does a logical metatheorem hold? That is, does any "natural" first-order proof, or computer proof, of such a formula generate an explicit construction, as an intermediate stage, of this single equation, from which the theorem results by simple substitutions?

Example 4.4. An explicit case of this problem is presented by Sturm sequences [15, pp. 220-222]. Assume that a univariate polynomial \( p(x) \), and its derivative \( p'(x) \) are relatively prime. We establish a sequence of polynomials:

\[
f_0(x) := p(x), \quad f_1(x) := p'(x), \ldots, f_i(x) := q_i(x)f_{i-1}(x) - f_{i-1}(x), \ldots
\]

with degree \( f_i < \) degree \( f_{i-1} \), using the Euclidean algorithm. We 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

\[
w(\infty) := \# \text{sign changes in } S(\infty); \quad \text{and } w(-\infty) := \# \text{sign changes in } S(-\infty).
\]

Sturm's theorem says that the number of real roots of \( p(x) \) is \( w(-\infty) - w(\infty) \). In particular, if there are not real roots, then we must have:

\[
p(x) = \sum_i \left[ \frac{q_i(x)}{r_i(x)} \right]^2 + \epsilon \quad \text{for some polynomials } q_i, r_i \text{ and a rational number } \epsilon > 0.
\]

How does this sequence (or the proof that the theorem holds) generate these polynomials \( q_i(x), r_i(x) \)? \( \square \)

We note that Sturm sequences are a crucial part of the computer algorithms for real algebraic geometry [2]. Thus we have the general question: does a verification of an open theorem over the reals using Collins' cylindrical decomposition algorithm [2] actually encode the construction of such real-nullstellensatz equations?

We close with three remarks.

(i) Expressing any open theorem through such "real Hilbert equations" or "real final polynomials" [11] will continue to give the maximum available information on the underlying geometry.

(ii) Quantifier elimination holds for the theory of real closed fields, but will continue to destroy the invariant nature of the simple equations in an invariant formula.

(iii) The logic of these geometric and algebraic theories is subtle. For example, there are theoretical decision procedures for the theories of real projective geometry, and of complex projective geometry. However the theory of projective geometry over unspecified fields is not decidable [13,14].

52
REFERENCES


[17] N. White, Multilinear Cayley factorization, this volume.


