A Model Theoretic Approach to Hilbert's 17th Problem

Pesara Amarasekera

April 2025

1 History and Overview

Hilbert became interested in what functions can be represented as a sum of squares (SS), due to a conjecture by Minkowski. At Minkowski's PhD desertation, he conjectured that there existed real polynomials which are nonnegative on the whole $\mathbb{R}^n$ and cannot be written as finite sums of square of real polynomials.[1]

As Hilbert was an official opponent of the PhD defense, he tried arguing the opposite, yet "was convinced by Minkowski's exposition that already for $n = 3$ there may well be such remarkable forms, which are so stubborn as to remain positive without allowing themselves to submit to a representation as sums of squares of forms." [2] Hilbert proved a special case for Minkowski conjecture that stated there existed a real polynomial in two variable of degree six which is nonnegative on $\mathbb{R}^2$ but not a SS of real polynomials, using some basic results of algebraic curves. Howevever the first example of such a function is due to Motzkin [1]:

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

Called the Motzkin polynomial discovered in 1967.

Now because Hilbert himself proved that a polynomial functions could not expressed as a SS, he changed the original problem thus:

> Given a multivariate polynomial that takes only non-negative values over the reals, can it be represented as a sum of squares of rational functions?

In this paper we will use the following definition we state the problem as intended by Hilbert:

Definition 1. Positive Semi-definite (PSD): Let F be a field and $f(\overline{X}) \in F(X_1, \ldots, X_n)$ be a rational function. We say that f is *positive semi-definite* if $f(\overline{a}) \geq 0$ for all $\overline{a} \in F^n$. [3]

Hence the problem becomes:

Hilbert's 17th problem: Is it true that if f is a PSD rational function over a real closed field F , then f is a sum of squares of rational functions?

This helps isolate a useful property, write more clear arguments, and still captures Hilbert's original questions as posed in his list of 23 problems.

The first person to solve this problem was Emil Artin and he presented his positive solution as a theorem in 1926 [4], to do so he developed the theory of Real Closed Fields (RCF) himself along

with Schreier, specifically to answer this problem. Artin's proof essentially showed the result would still hold if $\mathbb{R}$ is replaced by any field admitting a unique ordering, compatible with addition and multiplication.

Artin's proof employed Sturm's Theorem and the theory of ordered fields. Later, Serge Lang in 1953, revised Artin's proof, in which he used the theory of *real places*[4].

In 1955, Abraham Robinson building on the work of Artin used a model theoretic approach and obtained a completely novel solution. He proved the more general *Artin-Lang's Theorem* as a consequence of the *Quantifier elimination Theorem* for real closed fields, discovered by Tarski [4]. We will present Robinson's proof as it appears in [3], with theorems of RCF [3], as well as some discussion regarding Robinson's result.

Our proof will first begin with representing the theory of real closed fields, then we shall discuss the model theoretic techniques and finally conclude the proof.

This proof hinges on two things; the theory of ordered fields and quantifier elimination (QE).

2 Mathematical Framework and Proof

2.1 The Theory of Real Closed Fields

We will first develop the theory of real closed fields. Note we use the language of ordered fields (called $\mathcal{L}_{or}$ [RL1], which is for ordered rings to which we append) in order to access QE, this is expanded in the model theory section. Our results are mainly algebraic and are mainly due to Artin and Schreier [3] the proofs are available in [3] and [5], We present some of them here.

Definition 2. We say a field F is *orderable* if there is a linear order $<$ making $(F, <)$ into an ordered field.

Definition 3 (Ordered Field)**.** Field F is *ordered* with order $<_F$ (or "$<$" if clear) when

1. $\forall x, y, z \in F x < y \implies x + z < y + z$ (implies $\text{char}(F) = 0$);
2. $\forall x, y, z \in F, (x < z \text{ and } 0 < z) \implies xz < yz$ (implies $x^2 > 0$ for $x \neq 0$).

Definition 4 (Real Closed Field)**.** A *real closed field* is an ordered field $(F, <_F)$ such that:

1. Every positive element of F has a square root in F
2. Every odd degree polynomial of F has a square root in F.

Using these definition we attempt to show that the following hold. Note this proof is due to algebra.

Lemma 1: If -1 and $b \in F$ are not sums of squares in a field F then -1 is not a sum of squares (SS) in $F(\sqrt{-b})$.

Proof. This Algebraic Proof is available in the Appendix [RC1] □

We give the following useful definition:

Definition 5 (Formally Real)**.** A field F is formally real if -1 is not a sum of squares

If all squares are non-negative then the field orderable. Hence, consider the following Theorem:

Theorem 1. *If F is a formally real field, then F is orderable. Indeed, if $a \in F$ and $-a$ is not a sum of squares of elements of F,then there is an ordering of F where a is positive. [3]*

Proof. We construct a set of fields $\mathbf{F} = \{K : F(\sqrt{-b}) \subset K \subset \bar{F}$ and -1 is not SS in $K\}$, apply Zorn's Lemma on this. So we say that $\mathbf{F}$ has a maximal element K. By Lemma 1, if c is not a SS in K, then $K(\sqrt{-c}) \in \mathbf{F}$. By maximality, $\sqrt{-c} \in \mathbb{K}$. We order $\mathbb{K}$ as follows:

$$x < y \iff y - x \neq 0 \text{ and } y - x \text{ is a square in } K$$

This is well-defined. Then both $F(\sqrt{-b})$ and F inherit this order as subfields and $-b = (\sqrt{-b})^2 > 0$ so $b < 0$. □

The converse is also true, in any ordered field all squares are nonnegative. Thus, every orderable field is formally real.
Corollary 1 A field F can be ordered if and only if -1 is not a sum of squares in F

Proof. By Mutual implication, Forwards by noting $1 = 1^2 > 0 \iff -1 < 0$.
Backwards by applying Theorem 1. □

Definition 6. A field F is *real closed* if it is formally real with no proper formally real algebraic extensions

Theorem 2. *Let F be a formally real field. The following are equivalent*

1. *F is real closed*
2. *$F(i)$ is algebraically closed (where $i^2 = -1$).*
3. *For any $a \in F$, either a or $-a$ is a square and every polynomial of odd degree has root.*

Although we can axiomatize real closed fields in the language of rings ($\mathcal{L}_r$), QE is not available in this language. However by [P3.3.8] we do not lose definable sets.

Definition 7. We let RCF be the the $\mathcal{L}_{or}$-theory axiomatized by the axioms for real closed fields and ordered fields [RCF1]

Definition 8. If F is a formally real field, a *real closure* of F is a real closed algebraic extension of F.

Lemma 3 If $(F, <)$ is an ordered field,$0 < x \in F$ and x is not a square in F, then we can extend F to an ordered field $F(\sqrt{x})$

Proof. We can extend the order to $F(\sqrt{x})$ by $0 < a + b\sqrt{x}$ iff $(b = 0$ and $a > 0) \vee (b > 0$ and $(a > 0$ or $x > \frac{a^2}{b^2})) \vee (b < 0$ and $(a < 0$ and $x < \frac{a^2}{b^2}))$ □

Corollary 2

1. If $(F, <)$ is an ordered field there is a real closure R of F, such that the canonical ordering of R extends the ordering on F.

2. The set of all sentences true for any Model of RCF ($RCF_\forall$) is the theory of ordered integral domains [3]

Proof. in Appendix [Prf3.3.12] □

Although a formally real field may have nonisomorphic real closures, if $(F, <)$ is an ordered field there will be a unique real closure compatible with the ordering of F. [3]

2.2 Model Theory

Definition 9 (Algebraically Prime Model)**.** We say that a theory T has *algebraically prime models* if for any $\mathcal{A} \models T_\forall$ (all sentences true for any model of T) there is $\mathcal{M} \models T$ and an embedding $i : \mathcal{A} \to \mathcal{M}$ such that for all $\mathcal{N} \models T$ and embeddings $j : \mathcal{A} \to \mathcal{N}$ there is $h : \mathcal{M} \to \mathcal{N}$ such that $j = h \circ i$.

Corollary 3 RCF has algebraically prime models [3].

Proof. Let $(D, <)$ be an ordered domain, and let $(R, <)$ be the real closure of the fraction field compatible with the ordering of D. Let $(F, <)$ be any real closed field extension of $(D, <)$. Let $K = \{\alpha \in F : \alpha \text{ is algebraic over the fraction field of } D\}$. By Theorem 2, it is easy to see that K is real closed. Because the ordering of K extends $(D, <)$, by [Th3.3.13] there is an isomorphism $\phi : F \to K$ fixing D. □

2.2.1 Quantifier Elimination

Note [C3.1.12] and [Th3.2.2] from Marker regarding the theory of algebraically closed fields (ACF) in $\mathcal{L}_r$ (the language of rings). ACF is useful for us when proving results about real closed fields which is governed by RCF.

Theorem 3. *The First Order Logic (FOL) theory of Real closed fields (RCF) admits QE in* $\mathcal{L}_{or}$*.*

Proof. Because RCF has algebraically prime models, by [C3.1.12], we need only show that $F \prec_s K$ (for $\prec_s$ check [C3def]) when $F, K \models \text{RCF}$ and $F \subseteq K$. Let $\phi(v, \bar{w})$ be a quantifier-free formula and let $\bar{a} \in F$, $b \in K$ be such that $K \models \phi(b, \bar{a})$. We must find $b' \in F$ such that $F \models \phi(b', \bar{a})$.

Note that

$$p(X) \neq 0 \leftrightarrow (p(X) > 0 \vee -p(X) > 0)$$

and

$$p(X) \not> 0 \leftrightarrow (p(X) = 0 \vee -p(X) > 0).$$

With this in mind, we may assume that ϕ is a disjunction of conjunctions of formulas of the form $p(v, \bar{w}) = 0$ or $p(v, \bar{w}) > 0$. As in Theorem 3.2.2, we may assume that there are polynomials $p_1, \ldots, p_n$ and $q_1, \ldots, q_m \in F[X]$ such that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge_{i=1}^{n} p_i(v) = 0 \wedge \bigwedge_{i=1}^{m} q_i(v) > 0.$$

If any of the polynomials $p_i(X)$ is nonzero, then b is algebraic over F. Because F has no proper formally real algebraic extensions, in this case $b \in F$. Thus, we may assume that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge_{i=1}^{m} q_i(v) > 0.$$

The polynomial $q_i(X)$ can only change signs at zeros of q_i and if all zeros of q_i are in F. Thus, we can find $c_i, d_i \in F$ such that $c_i < b < d_i$ and $q_i(x) > 0$ for all $x \in (c_i, d_i)$. Let $c = \max(c_1, \ldots, c_m)$ and $d = \min(d_1, \ldots, d_m)$. Then, $c < d$ and $\bigwedge_{i=1}^{m} q_i(x) > 0$ whenever $c < x < d$. Thus, we can find $b' \in F$ such that $F \models \phi(b', \bar{a})$. □

2.2.2 Model Completeness

Note that RCF with $\mathcal{L}_r$ (language of rings) does not admit quantifier elimination, but RCF with $\mathcal{L}_{or}$ (ordered rings) does.

Lemma 5 If a theory T has QE, then T is model complete (MC)

Proof. It suffices to show that for a formula $\psi(v_0, \ldots, v_n)$ is quantifier free and $\mathcal{M} \subseteq \mathcal{N}$ then

$$\mathcal{M} \models \psi(a_0, \ldots, a_n) \Longleftrightarrow \mathcal{N} \models \psi(a_0, \ldots, a_n)$$

for all $a_0, \ldots, a_n \in M$. This fact is proven by induction on the length of ψ [5]. □

Theorem 4. *RCF is MC*

Proof. If a theory T admits QE then it's MC. As a consequence of this we know that RCF is also MC. Which means that the rational numbers are embedded in every real closed field. Ergo the real closure of the rationals $\mathbb{R}_{alg}$ is a subfield of any real closed field. Hence, for any real closed field R,

$$\mathbb{R}_{alg} \prec R$$

hence

$$R \equiv \mathbb{R}_{alg} \equiv \mathbb{R}$$

□

2.3 Solution to Hilbert's 17th Problem

Theorem 5 (Solution to Hilbert's 17th Problem)**.** *If f is a positive semi-definite rational function over a real closed field F , then f is a sum of squares of rational functions.*

Proof. Suppose that $f(X_1, ..., X_n)$ is a positive semi-definite rational function over F that is not a sum of squares. By Theorem 1, there is an ordering of $F(\bar{X})$ so that f is negative. Let R be the real closure of $F(\bar{X})$ extending this order. Then

$$R \models \exists \bar{v} f(\bar{v}) < 0$$

because $f(\bar{X}) < 0$ in R. By MC

$$F \models \exists \bar{v} f(\bar{v}) < 0$$

, contradicting the fact that f is PSD. □

3 Robinson's Result

In fact Robinson proved a stronger theorem than Artin [4]

Theorem 6 (Artin-Lang Theorem)**.** *Let R be the real closure of the ordered field (E, P) (P is a unique ordering on E) and let $E_n := E(x_1, \ldots, x_n)$ be the field of rational functions with coefficients in E. Let Q_n be an ordering in E_n with $Q_n \cap E = P$, and $f_1, \ldots, f_r \in Q_n \setminus \{0\}$. Then, there exists $x \in R^n$ such that each rational function is defined in x and $f_i(x) > 0$ in R.*

This showed a great insight into the use of model theory in solving problems across other domains in mathematics, and enhanced the fields of Real Algebra and Real Geometry [4].

Bibliography

[1] Konrad Schmüdgen. *Around Hilbert's 17th Problem*. URL: https://www.kurims.kyoto-u.ac.jp/EMIS/journals/DMJDMV/vol-ismp/61_schmuedgen-konrad.pdf.

[2] Safdar Quddus. *Positive polynomials - Hilbert's 17th problem*. URL: https://www.isibang.ac.in/~sury/hilbert17.pdf.

[3] David Marker. *Model Theory: An Introduction*. Springer, 2002.

[4] J. Manuel Gamboa José F. Fernando. *REAL ALGEBRA FROM HILBERT'S 17th PROBLEM*. URL: https://www.mat.ucm.es/~josefer/articulos/rgh17.pdf.

[5] Aaron Crighton. *Hilbert's 17th Problem for Real Closed Fields 'a la Artin*. URL: https://www.math.utoronto.ca/undergrad/projects-undergrad/MAT477in2014byAaronCrightonHilbert17.pdf.

Appendix

RL1 Note the first order language $\mathcal{L}_{or}$ contains the following symbols [5]

RC1 *Proof.* For the case when $\sqrt{-b} \in F$, by definition it will be in $F(\sqrt{-b})$. For the case $\sqrt{-b} \notin F$ suffices, equivalently $\dim_F F(\sqrt{-b}) = 2$. Then

$$-1 = \sum_{i=1}^{m}(x_i + y_i\sqrt{-b})^2 \Rightarrow b = \frac{1 + \sum_i x_i^2}{\sum_i y_i^2} = \sum_i w_i^2$$

since

$$(\sum_i y_i^2)^{-1} = \sum_i (y_i / \sum_j y_j^2)^2$$

contrary to the assumption. □

(a) The binary functions $+, -$ and $\times$.

(b) The binary relation $<$

(c) The constant symbol 0 and 1

P3.3.8 **Proposition 3.3.8 [3]** If F is a real closed field and $X \subseteq F^n$ is definable by an $\mathcal{L}_{\text{or}}$-formula, then X is definable by an $\mathcal{L}_{\text{r}}$-formula.

Proof. Replace all instances of $t_i < t_j$ by $\exists v(v \neq 0 \wedge v^2 + t_i = t_j$, where t_i and t_j are terms occurring in the definition of X (see Ex 1.4.15 of [3]) □

C3def We write $\mathcal{M} \prec_s \mathcal{N}$ if for any quantifier free formula $\phi(\bar{v}, w)$ and any $\bar{a} \in M$, if $\mathcal{N} \models \exists w\, \phi(\bar{a}, w)$ then so does $\mathcal{M}$.

C3.1.12 **Corollary 3.1.12 [3]** Suppose that T is an $\mathcal{L}$-theory such that

i) T has algebraically prime models and

ii) $\mathcal{M} \prec_s \mathcal{N}$ whenever $\mathcal{M} \subseteq \mathcal{N}$ are models of T.

Then, T has quantifier elimination.

Th3.2.2

Theorem 7 (Theorem 3.2.2 [3])**.** *ACF has QE.*

Prf3.3.12 *Proof.* i) By successive applications of Lemma 3.3.11, we can find an ordered field $(L, <)$ extending $(F, <)$ such that every positive element of F has a square root in L. We now apply Zorn's Lemma to find a maximal formally real algebraic extension R of L. Because every positive element of F is a square in R, the canonical ordering of R extends the ordering of F.

ii) Clearly, any substructure of a real closed field is an ordered integral domain. If $(D, <)$ is an ordered integral domain and F is the fraction field of F, then we can order F by

$$\frac{a}{b} > 0 \Leftrightarrow a, b > 0 \text{ or } a, b < 0.$$

By i), we can find $(R, <) \models \text{RCF}$ such that $(F, <) \subseteq (R, <)$.

□

Th3.3.13

Theorem 8 (3.3.13)**.** *If $(F, <)$ is an ordered field, and R_1 and R_2 are real closures of F where the canonical ordering extends the ordering of F, then there is a unique field isomorphism $\phi : R_1 \to R_2$ that is the identity on F.*