HILBERT'S 17^{th} PROBLEM

HYTHAM FARAH,
SIDDHARTH GURUMURTHY,
TORIN CAREY

The following notes will provide the necessary background for, and the solution of, Hilbert's 17^{th} problem. Emil Artin was the first to solve the problem in 1927 in the affirmative [Art27], resulting in the following theorem:

Theorem 1 (Hilbert's 17^{th} problem)**.** *If f is a positive semidefinite rational function over a real closed field F, i.e. $f(a_1, \ldots, a_n) \geq 0$ for all $a_1, \ldots, a_n \in F$, then f is a sum of squares of rational functions.*

Though Artin was the first to prove this theorem, we shall present Abraham Robinson's proof in this document. His proof made heavy use of model theory techniques, particularly, by exploiting the model theoretic properties of the theory of real closed fields, which we shall henceforth denote by RCF. The proof follows as an almost immediate consequence of the model-completeness of RCF and an algebraic theorem about the ordering of real fields. These notes draw heavily from David Marker's Model Theory [Mar00].

1. Model Completeness of RCF

Before we provide a precise definition of RCF, we note that they key model theoretic property we need for the proof is model completeness.

Definition 2 (Model Completeness)**.** An $\mathcal{L}$-theory T is model-complete, if $M \prec N$ whenever $M \subseteq N$ and $M, N \models T$.

Equivalently, T is model-complete whenever all embeddings are elementary embeddings. We recall that if a theory has quantifier elimination then it is model complete, though the converse need not hold. Unfortunately, unlike the theory of ACF, RCF does not have quantifier elimination in the language of rings $\mathcal{L}_r = (+, -, \cdot, 0, 1)$.

Theorem 3. $\text{Th}(\mathbb{R})$ *does not have quantifier elimination in $\mathcal{L}_r$.*

To prove the theorem we need a definition and some technical lemmas:

Definition 4. An $\mathcal{L}$-theory T is *strongly minimal* if for any $M \models T$ every definable subset of M is either finite or cofinite.

Date: April 2021.

This definition is particularity useful for our purposes because of the following lemma:

Lemma 5. *Any field with quantifier elimination is strongly minimal.*

Proof. Any atomic $\mathcal{L}_r$-formula is of the form $p(x) = 0$ for a polynomial $p(x)$ which is satisfied by finitely many elements of the field. The set of elements satisfying $p(x) \neq 0$ is cofinite, so any quantifier free $\mathcal{L}_r$-formula is satisfied by a finite or cofinite set of elements from the field. Thus if the field has quantifier elimination, every set is algebraic and therefore the field is strongly minimal. □

But $\mathbb{R}$ is not strongly minimal as $\phi(x) = \exists z\ (z^2 = x)$ defines an infinite co-infinite definable set. Hence, by the Lemma, $\mathbb{R}$ cannot have quantifier elimination.

In fact, $\phi(x)$ is itself an instance of a formula that cannot be expressed without quantifiers. However, if we expand our language by adding an order relation to $\mathcal{L}_{or} = \mathcal{L}_r \cup \{<\}$, we immediately see that:

$$(\exists z\ z^2 = x \wedge z > 0) \equiv (x > 0)$$

dissolving the quantifier. It turns out, that quantifier elimination is impeded solely by statements which can be expressed by $<$ instead. Fortunately, expanding the language, does not add any new definable sets since:

$$(\exists z\ z \neq 0 \wedge x + z^2 = y) \equiv (y > x)$$

So any condition expressible in $\mathcal{L}_r$ is expressible in $\mathcal{L}_{or}$

Hence the strategy will be to show that the theory of $\mathbb{R}$ in $\mathcal{L}_{or}$ does have quantifier elimination.

2. Formal Real Closed Fields and Orderings

We begin with a purely algebraic characterization of real fields:

Definition 6. A field F is:

- *formally real* or just *real* if -1 is not a sum of squares.
- *real closed* if it is formally real with no proper formally real algebraic extensions.

Examples of formally real fields include $\mathbb{Q}$ and $\mathbb{R}$, of which only $\mathbb{R}$ is closed. We define the notation $\Sigma F^2 := \{\sum f_i^2, f_i \in F\}$ to be the subset of F which can be written as sum of squares in F.

Note that being *formally real* implies the field has characteristic 0.

Definition 7. An *ordered field* is a field F with a total order $<$ such that the axioms

$$\forall x \forall y\ (x > 0 \wedge y > 0) \to (xy > 0)$$

and

$$\forall x \forall y \forall z \ (x < y) \to (x + z < y + z)$$

hold. Note that $x^2 \geq 0$ for any $x \in F$ as this follows for if $x \geq 0$ or $x \leq 0$. Therefore in any ordering we must have $\Sigma F^2 \setminus \{0\}$ as positive and $-\Sigma F^2 \setminus \{0\}$ as negative.

Lemma 8. *Let F be real and $a \in F$ such that $-a \notin \Sigma F^2$. Then $F(\sqrt{a})$ is real.*

Proof. We may assume $\sqrt{a} \notin F$ otherwise it is trivial. Suppose $F(\sqrt{a})$ is not real, then we have

$$-1 = \sum_i (b_i + c_i\sqrt{a})^2 = \sum_i b_i^2 + 2\sqrt{a}\sum_i b_i c_i + a\sum_i c_i^2$$

with $\sum_i b_i c_i = 0$ as $F(\sqrt{a})$ is an F-vector space and $\sum_i c_i^2 \neq 0$ as F is real. Thus

$$-a = \frac{\sum_i b_i^2 + 1}{\sum_i c_i^2} = \left(\sum_i c_i^2\right)\left(\frac{1}{\sum_i c_i^2}\right)^2\left(\sum_i b_i^2 + 1\right) \in \Sigma F^2$$

which is a contradiction. □

A key property of real fields that we will need for the proof of Hilbert's 17$^{\text{th}}$ theorem is about the ordering of real fields. If F is real closed, it has a unique ordering thanks to the following lemma.

Lemma 9. *Let $a \in F \setminus \{0\}$. If F is real, then at most one of a and $-a$ is a square. If F is real closed, then exactly one of a and $-a$ is a sum of squares.*

Proof. Suppose both of $a, -a \in \Sigma F^2$ are a sum of squares, then

$$-1 = \frac{-a}{a} = a(-a)\left(\frac{1}{a}\right)^2 \in \Sigma F^2$$

is a sum of squares, which is a contradiction to F being real. Suppose F is real closed and neither of a or $-a$ are a sum of squares, then we have the proper algebraic extension $F \subset F(\sqrt{a})$ of real fields, which contradicts F being real closed. □

With this property, supposing F is real closed, we can define a unique ordering as follows:

$$x < y \iff y - x \text{ is a non-zero sum of squares} \tag{1}$$

Lemma 9 tells us that $\Sigma F^2 \cup -\Sigma F^2 = F$, therefore the order is unique.

For real fields which are not closed, we will show that there are still orderings, however, they are not unique. This will prove useful, since, to a certain extent we can control our order relationship on real fields, as seen in the following theorem:

Theorem 10 (Ordering of Real Fields)**.** *Let F be a formally real field. If $a \in F$ and $-a \notin \Sigma F^2$ then there is an ordering of F where $a > 0$*

To prove this theorem we will use the following lemma:

Lemma 11. *Let F be a real field. There there is an $R \supseteq F$ a real closed algebraic extension which we call a real closure of F.*

Proof. Denote by $\mathcal{F} \ni F$ the poset[1] of real algebraic extensions of F with inclusion. Given any chain $F_0 \subseteq F_1 \subseteq \cdots$, we have an algebraic extension $\cup F = \bigcup_i F_i$ of $\mathcal{F}$. Suppose $\cup F$ were not real, then there would exist $f_i \in \cup F$ such that $f_1^2 + \cdots + f_n^2 = -1$, which would contradict F_N being real for some F_N containing $f_1, \ldots, f_n$. Therefore by Zorn's lemma there exists maximal fields R in $\mathcal{F}$. Such a maximal field is real closed since by maximality we cannot extend it properly to a real field. □

Corollary 12. *Every real field F has an ordering.*

Proof. By Lemma 11, there exists a real closure $R \supseteq F$ with embedding $i : F \to R$. We may define an order on F with $x < y$ if and only if $i(x) < i(y)$, where R is ordered with the unique order on real closed fields. □

Now we can prove the desired theorem:

Proof of the Ordering of Real Fields. Since $-a$ is not a sum of squares, we may use Lemma 8 to obtain the inclusion of real fields $i : F \hookrightarrow F(\sqrt{a})$. By the above Corollary, $F(\sqrt{a})$ has an ordering, but all such orderings must have $a > 0$ since a is a square in this field. By pulling-back the ordering to F, we obtain an order on F with $a > 0$. □

Remark 13. Let F be a real closed field. The rational function field $F(x)$ is real since for any $f \in F(x) \setminus F$ we have $f^2 \notin F$. What might an ordering on $F(x)$ look like? It would suffice to describe what the ordering of x is with respect to all other elements of F. We may consider downards closed sets $A \subseteq F$ where if $a < b$ and $b \in A$, then $a \in A$. We may then define $a < x$ if $a \in A$ and $x < a$ is $a \in F \setminus A$. Consider $F = \mathbb{R}$. In the case of $A = (-\infty, 0] \subset \mathbb{R}$, we may consider x as a positive infinitesimal element, since such an element would be less than all positive reals. Likewise in the case of $A = \mathbb{R}$, we may consider x as an infinite element.

As we saw earlier, real fields admit adjoining roots of elements in some cases. We may infact adjoin any elements of odd degree.

Lemma 14. *Let F be a field and α such that $[F(\alpha) : F]$ is odd. Then $F(\alpha)$ is real.*

Proof. Suppose not. Let $a_1, \ldots, a_n \in F(\alpha) \setminus \{0\}$ be such that $a_1^2 + \cdots + a_n^2 = -1$. Let $m(x)$ be the minimal polynomial of α. We may consider a_i as polynomials $a_i(x)$ with $\deg a_i(x) < \deg m(x)$ from the F-algebra isomorphism $F[x]/\langle m \rangle \cong F(\alpha)$. In $F[x]$ we have $\sum_{i=1}^n a_i^2(x) = -1 + h(x)m(x)$ where $\deg h(x) \leq \max(\deg a_i^2(x)) - \deg m(x) < \deg m(x)$ and with $\deg h(x)$ odd. Let $h(x) = k(x)\ell(x)$ where $k(x)$ is

[1]We can make this a set by constructing these extensions manually by successively adding roots of polynomials to get extensions via transfinite induction.

irreducible of odd degree, then $\sum_{i=1}^{n} \overline{a_i(x)} = -1$ in $F[x]/\langle k(x)\rangle$. Let β be a root of $k(x)$, then for $a_i(x) \mapsto a_i$ under the F-algebra isomorphism $F[x]/\langle k(x)\rangle \cong F(\beta)$ we have $a_1^2 + \cdots + a_n^2 = -1$. Since $[F(\beta) : F]$ is odd and strictly less than $[F(\alpha) : F]$, we may repeat this process finitely many times to obtain $c_1, \ldots, c_n \in F$ with $c_1^2 + \cdots + c_n^2 = -1$, contradicting that F is real. □

The definition of real closed fields given above is not conducive to model theoretic techniques. To axiomatize real closed fields in first order logic, we need the following characterization, whose proof is quite technical and thus we won't give a complete proof.

Theorem 15 (Artin)**.** *The following are equivalent:*

(1) *F is real closed;*
(2) *$F(i)$ is algebraically closed;*
(3) *For every $a \in F\backslash\{0\}$ exactly one of a or $-a$ is a square and every polynomial of odd degree has a root in F.*

The main part of the Theorem which we utilise is (1) ⇔ (3), we can prove one direction of this. The proof of (3) ⇒ (1) goes through (2).

Proof (1) ⇒ (3). Suppose F is real closed. Lemma 9 already tells us that for every $a \in F \setminus \{0\}$, exactly one of a or $-a$ is a square. Let $f(x) \in F[x]$ be an odd degree polynomial. Let α be a root of $f(x)$, then the algebraic extension $F(\alpha) \supseteq F$ is real. Since F is closed, we must have $\alpha \in F$ for which proves $f(x)$ has a root in F. □

We now formally define RCF as the theory in the language $\mathcal{L}_{or}$ axiomatized by:

(1) Ordered field axioms
(2) for each $n \geq 1$ the axiom: $\forall x_1 \ldots \forall x_n \; x_1^2 + ... + x_n^2 + 1 \neq 0$
(3) $\forall x \; x > 0 \implies \exists y \; y^2 = x$
(4) for each $n \geq 0$ the axiom: $\forall x_0 ... \forall x_{2n} \exists y \; y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0$, that is, every odd degree polynomial has a root.

Of course, for any $F \models$ RCF we have that F is a formally real closed field since 1 and 2 imply F is a real field with 3 and 4 implying that F is real closed by Theorem 15.

3. Quantifier Elimination of RCF

We begin with the following definitions:

Definition 16. We say that a theory T has algebraically prime models if for any $A \models T_\forall$ there is $M \models T$ and an embedding $i : A \longrightarrow M$ such that for all $N \models T$ and embeddings $j : A \longrightarrow N$ there is $h : M \longrightarrow N$ such that $j = hi$.

Definition 17. If $M, N \models T$ and $M \subseteq N$, we say that M is simply closed in N and write $M \prec_s N$ if for any quantifier free formula $\phi(\bar{v}, w)$ and any $\bar{a} \in M$, if $N \models \exists w\, \phi(\bar{a}, w)$ then so does M.

To show that RCF has quantifier elimination we will make use of the following test:

Theorem 18. *Suppose that T is an L-theory such that: i) T has algebraically prime models and ii) $M \prec_s N$ whenever $M \subseteq N$ are models of T. Then, T has quantifier elimination.*

To prove that RCF has quantifier elimination it is therefore sufficient to check that properties i) and ii) hold for RCF.

Let's start working towards the proof of *i).*

Lemma 19. *If $(F, <)$ be an ordered field and $0 < x \in F$ be a non-square. Then we can extend the order to $F(\sqrt{x})$.*

Proof. The order we want is essentially what we would expect for $F = \mathbb{Q}$. Essentially,

$0 < a + b\sqrt{x}$ iff ($b = 0$ and $a > 0$) OR ($b > 0$ and ($a > 0$ or $x > \frac{a^2}{b^2}$)) OR ($b < 0$ and $a > 0$ and $x < \frac{a^2}{b^2}$).

□

We have talked about real closures of real fields, and now we want to discuss real closures in the context of ordered fields (which are automatically real).

Lemma 20. *a) If $(F, <)$ is an ordered field, then we can get a real closure R of F which extends the order.*
b) $RCF_\forall$ is the the theory of ordered integral domains.

Proof of a). Construct $(L, <)$ an extension of F which has square roots of all positive elements of F. To do this construction, we use transfinite induction: for each successor ordinal add square roots and for each limit ordinal take unions.
Use the construction in *Lemma 11* to construct a real closure R of L. The order on R extends the order on F since every positive element of F is a square in R. □

Proof of b). It is enough to show that each model of $\mathrm{RCF}_\forall$ embeds is a domain and that each ordered domain embeds into a real closed field.
Consider $A \models \mathrm{RCF}_\forall$. Then there is an embedding $A \hookrightarrow (F, <)$, where F is a real closed field. So, A is a substructure of M and hence is a domain.
For the other direction, consider a domain $(D, <)$. It embeds into it's field of fractions $(F, <)$ where the order is given by the natural condition

$$\frac{a}{b} > 0 \text{ iff a and b have the same sign.}$$

We can extend $(F,<)$ to a real closure R. $(D,<)$ embeds into R and thus is a model of $\mathrm{RCF}_\forall$. □

Much like the case for algebraically closed fields, the real closure of an ordered field is unique. Moreover, it is unique up to a unique isomorphism. We have elected to not give a proof as it is too technical.

Lemma 21. *Let $(F,<)$ be an ordered field. Let R_0 and R_1 be real closures of F such that $(R_i,<)$ is an ordered field extension of $(F,<)$. Then, R_0 is isomorphic to R_1 over F and the isomorphism is unique:*

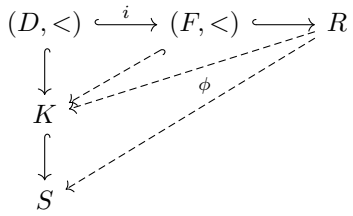
Thus we can talk about "the" real closure of an ordered field.

Proof of i) RCF has algebraically prime models.
Let $(D,<) \models \mathrm{RCF}_\forall$ with an embedding into a real closed field S. We may take $(F,<)$ to be the field of fractions of D, with an embedding $i : A \hookrightarrow F$. Take R to be the real closure of $(F,<)$. Thus we get an embedding $D \hookrightarrow R$. We claim that this is the embedding we want.

The field F satisfies the universal property that if $j : A \hookrightarrow K$ is an embedding into a field, then there exists $h : F \to K$ such that $j = hi$.

If we want a map from R into S, the image has to be algebraic over F. So consider $K = \{\alpha \in S : \alpha \text{ is algebraic over } F\}$. K is real closed by the (3) $\Leftrightarrow$ (1) direction of *Theorem 15.*

By *Lemma 21*, we have an isomorphism $\phi : R \to K$ which fixes F. We can compose this with the embedding $K \hookrightarrow S$ which gives us the required map.



□

Proof of ii) RCF is model complete. Let $F, K \models \mathrm{RCF}$, $F \subset K$, $\bar{a} \in F$ $b \in K$, ϕ is a quantifier free formula and suppose:

$$K \models \phi(b, \bar{a}) \tag{2}$$

We must show that there exists a $b' \in F$ such that $F \models \phi(b, \bar{a})$.

To begin we note that since ϕ is quantifier free, we may write it in disjunctive normal form:

$$\phi(x, \bar{a}) \equiv \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \theta_{ij}(x, \bar{a}) \tag{3}$$

Where θ_{ij} are $\pm$ atomic formulas. By (2), we know $K \models \bigwedge_{j=1}^{m} \theta_{ij}(x, \bar{a})$ for some i, hence it is sufficient to consider formulas of this form, namely, conjunctions of $\pm$ atomic formulas.

We know that the only atomic formulas in $\mathcal{L}_{or}$ are:

$$p(x, \bar{a}) = 0 \qquad p(x, \bar{a}) > 0 \tag{4}$$

where $p(x, \bar{y}) \in \mathbb{Z}[X, \bar{Y}]$. We may write $p(x) = p(x, \bar{a}) \in F[X]$, dropping the $\bar{a}$ argument.

Negations of atomic formulas can be rewritten as follows:

$$(p(x) \neq 0) \equiv (p(x) > 0 \vee p(x) > 0)$$
$$(p(x) \not> 0) \equiv (p(x) = 0 \vee -p(x) > 0)$$

and since each K must satisfy one the two formulas in each of the disjunctions, we can restrict our attention to formulas of the form:

$$\bigvee_{i=1}^{n} p_i(x) = 0 \wedge \bigwedge_{i=1}^{m} q_i(x) > 0 \tag{5}$$

If $p_i \neq 0$, b is algebraic over F, and hence $b \in F$ as F is real closed i.e. has no proper real closed extension. Then, letting $b' = b$, we are done.

Hence we may consider formulas of this form:

$$\bigwedge_{i=1}^{m} q_i(x) > 0$$

First note that each q_i only changes signs at roots. We may list every root of each of the q_i's in order $r_1 < \cdots < r_k$ for national convenience we let $r_0 = -\infty$, $r_{k+1} = \infty$. We know for some $j = 0, ..., k$

$$r_j < b < r_{j+1}$$

We note that the roots of these polynomials are elements of F. If $j = 0$ we may take $b' := r_{j+1} - 1 \in F$, and if $j = k$, we may take $b' := r_k + 1$. Otherwise, let $b' := \frac{r_j + r_{j+1}}{2} \in F$. For each i, since q_i only changes signs at roots, and $q_i(b) > 0$, we conclude that $q_i(b') > 0$ completing the proof. □

4. Resolution of Hilbert's 17th

Since we have shown that RCF has quantifier elimination, it is model-complete. The proof of Hilbert's 17th problem is an immediate consequence of model completeness and the ordering theorems we proved for real fields. For the reader's convenience, we restate the problem:

Theorem 22 (Hilbert's 17th problem)**.** *If f is a positive semidefinite rational function over a real closed field F, i.e. $f(a_1, \ldots, a_n) \geq 0$ for all $a_1, \ldots, a_n \in F$, then f is a sum of squares of rational functions.*

Proof. Suppose that $f(X_1, \ldots, X_n)$ is a positive semidefinite rational function over F that is not a sum of squares. By the ordering theorem, there is an ordering of $F(X_1, \ldots, X_n)$ so that f is negative. Let R be the real closure of $F(X_1, \ldots, X_n)$ extending this order. Then

$$R \models \exists v_1, \ldots, v_n \, f(v_1, \ldots, v_n) < 0$$

because $f(X_1, \ldots, X_n) < 0$ in R. By model-completeness:

$$F \models \exists v_1, \ldots, v_n \, f(v_1, \ldots, v_n) < 0,$$

contradicting the fact that f is positive semidefinite. □

References

[Art27] Emil Artin. "Über die Zerlegung definiter Funktionen in Quadrate". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* (1927).

[Mar00] David Marker. *Model Theory: An Introduction*. Graduate Texts in Mathematics. Seven volumes planned. Springer Verlag, 2000.