HILBERT'S 17TH PROBLEM

STEVEN CREECH

ABSTRACT. Hilbert's 17th problem asks if every $f \in \mathbb{R}[x_1, x_2, ..., x_n]$ that is a positive semi-definite (PSD) can be written as a sum of squares of rational functions. In this paper, we take a look at some of the tools developed to answer this question. In particular, we examine the deep connection between orders and being positive semi-definite. We finish by providing a proof due to Emil Artin [Art27].

1. INTRODUCTION

In 1900, David Hilbert created a list of 23 problems to inspire mathematical work for the next century [Hil02]. His 17th problem asked if $f(x) \in \mathbb{R}[x_1, .., x_n]$ is a positive semi-definite polynomial, then $f(x)$ is sum of square in $\mathbb{R}(x_1, .., x_n)$. In this section, we shall give the motivation behind this problem. First, we shall show that the converse of Hilbert's 17th problem is quite natural that is if $f \in \mathbb{R}[x_1, ..., x_n]$ can be written as a sum of squares, then f is PSD. Recall that $f(x) \in \mathbb{R}[x_1, ..., x_n]$ is said to be *positive semi-definite* if for all $c_1, .., c_n \in \mathbb{R}$, we have that $f(c_1, .., c_n) \geqslant 0$

Lemma 1.1. *If $f \in \mathbb{R}[x_1, .., x_n]$ is a sum of squares, then f is PSD.*

Proof. Let us write $f = \sum_{i=1}^{n} (g_i)^2$ where $g_i \in \mathbb{R}[x_1, .., x_n]$. Now for any $c_1, ..., c_n \in \mathbb{R}$, we have that $(g_i(c_1, ..., c_n))^2 \geqslant 0$; hence, $f(c_1, ..., c_n) = \sum_{i=1}^{n} (g_i(c_1, ..., c_n))^2 \geqslant 0$. □

It is not too hard to extend the above proof to the case where f is a sum of squares of rational functions. However, one might wonder why we need to extend to sums of squares of rational functions as compared to that of the polynomial ring. As it is true in the single variable case, we can take the sum of squares to just be sums of squares of polynomials rather than rational functions. However, David Hilbert showed in [H$^+$93] that for $n \geqslant 2$ that there are PSD polynomials which cannot be written as a sum of squares. However, Hilbert did not have an explicit example. It wasn't until 1965 when Motzkin came up with an explicit example of a polynomial which cannot be written as a sum of squares [Mot67].

Example 1.2. Consider the Motzkin polynomial $M(x, y) = 1 + x^2y^4 + x^4y^2 - 3x^2y^2 \in \mathbb{R}[x, y]$, a quick exercise in calculus shows that M has a minimum value of 0 obtained at $(\pm 1, \pm 1)$. Using Newton polytopes, one can show that if the Motzkin polynomial is a sum of squares, then it has to be a sum of square terms of the form $(ax^2y + bxy^2 + cxy + d)^2$. However, no such polynomial will have a negative x^2y^2 coefficient. Thus, the Motzkin polynomial is not a sum of squares.

The remainder of the paper will be organized as follows. In section 2, we shall introduce the concept of preorders and orders and describe their relation to sums of squares via the Artin-Schreier Theorem. In section 3, we prove a theorem due to Artin which reduces

Date: April 24, 2020.

Hilbert's problem to a problem about orderings. In section 4, we shall introduce the concept of real closures. In section 5, we prove Hilbert's 17th problem.

2. Orderings

We shall begin this section with some definitions and notion. Firstly, we shall use K to denote a field. Furthermore, for a commutative ring R we shall let $\sum R^2 = \{x \in R : x \text{ is a sum of squares in } R\}$ and $(\sum R^2)^\times = \sum R^2 \backslash \{0\}$. In particular, we are interested in *formally real fields* which are fields in which -1 cannot be written as a sum of squares that is $-1 \notin \sum K^2$. One easily makes the following observations $\sum R^2$ is closed under addition and multiplication, K is formally real if and only if $-1 \notin \sum K^2$. We now will define a preordering of a commutative ring R and we shall see that it has a connection with $\sum R^2$. However, we shall primarily be interested in the case when R is a field.

Definition 2.1. A subset P of a R is called a *preorder* of R if:

$$P + P \subseteq P,\ P \cdot P \subseteq P,\ \Sigma R^2 \subseteq P,\ -1 \notin P$$

We call a preordering P an *order* of R if in addition for $x \neq 0$ we have that:

$$x \in P \text{ or } -x \in P$$

this is equivalent to having

$$P \cup -P = R,\ P \cap -P = \{0\}$$

We note that by definition we have that either $-1 \in \sum R^2$ or $\sum R^2$ is a preorder of R. The notion of order should be analogous to our preperceived notion of the total order $\leqslant$ on $\mathbb{R}$. In general for an order P we shall write that $a \leqslant_P b$ whenever $b - a \in P$ (we may omit the P if the order is understood). We note that this gives a total order on R which is compatible with the operations of the ring. For an example of an ordering see 2.2 and 2.3 where we also show how one can construct a new ordering from a previous ordering.

Example 2.2. Let $K = \mathbb{Q}(\sqrt{2})$. Thinking of K as a subset of $\mathbb{R}$, we have that the natural order ($\leqslant$) on $\mathbb{R}$ restricted to K gives an order on K. We shall construct a new order ($\preceq$) as follows for $a + b\sqrt{2} \preceq c + d\sqrt{2}$ if and only if $a - b\sqrt{2} \leqslant c - d\sqrt{2}$. We note that $\preceq$ is an order as $\phi : K \to K$ given by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism. Thus, as sums and products are preserved this will be a new order. We can generalize this construction given any ordered field $(K, \leqslant)$ and an automorphism ϕ, we can construct a new ordering $(K, \preceq)$ in the analogous fashion.

Example 2.3. Consider $\mathbb{R}(x)$ the rational functions in one-variable, we can define

$$P_\infty^+ = \{\text{all polynomials with positive leading coefficients}\} \cup \{0\}$$

on $\mathbb{R}[x]$. In this order we have declare that $c < x$ for every $c \in \mathbb{R}$; thus, this is the order where $t^k > t^l$ for $k > l$. We can then extend this to $\mathbb{R}(x)$ by having $\frac{g(x)}{h(x)} \in P_\infty^+$ whenever the quotient of the leading coefficients of g and h is positive.

We now define P_∞^- have the property that $f(x) >_{P_\infty^-} > 0$ whenever $f(-x) >_{P_\infty^+} 0$.

Now we note that $t \mapsto t^{-1}$ is an automorphism of $\mathbb{R}(x)$, so we define P_0^+ to be the corresponding order. In P_0^+ we have that $0 < x$, but $x < c$ for every $c \in \mathbb{R}$. We can think of this as x being infinitesimally close to 0 on the right. We analogously have P_0^- which have x being infinitesimally close to 0 on the left.

Furthermore, we can analogously define P_c^+ and P_c^- for any $c \in \mathbb{R}$ to be the order where $f(x) \in P_c^+$ if and only if $f(x-c) \in P_0^+$. We can think of this order as simply shifting where x to be infinitesimally close to c.

Now we now state two lemmas which will allow us to say that formally real fields are exactly the fields which have an order.

Lemma 2.4. *Let P be a preorder of R and let $a, b \in R$. If $ab \in P$, then $P + aP$ or $P - bP$ is a preorder of R.*

Proof. It is easy to check that $P + aP$ and $P - bP$ are closed under addition, multiplication, and contain $\sum R^2$. Thus, we need to show that $-1 \notin P + aP$ or $-1 \notin P - bP$. Assume for sake of contradiction that $-1 \in P + aP \cap P - bP$, then we can write $-1 = x + ay = z - bw$ for some $x, y, z, w \in P$. Then $(ay)(-bw) = (-1 - x)(-1 - z) = 1 + x + z + xz$. Subtracting 1 and adding $abwy$ to both sides yields $-1 = x + z + xz + (ab)yw$. As every summand on the righthand side in P, we have that $-1 \in P$, but this contradicts the fact that P is a preorder. □

Lemma 2.5. *Let P be a maximal preorder of R. Then $P \cup -P = R$ and $P \cap -P = \mathfrak{p}$ is a prime ideal of R. If $R = K$ is a field, then $\mathfrak{p} = 0$ and P is an order of K.*

We shall omit the proof of this lemma as it requires some case analysis; however, the idea of the proof is to let $a = b$ and apply Lemma 2.4. For details of proof see Lemma 1.5 of [Pfi95]. A nice corollary of the lemma is Artin-Schriere theorem:

Theorem 2.6. *(Artin-Schreier) K is a formally real field if and only if K has an order P*

Proof. For the forward direction, if K is formally real, we know that $\sum K^2$ is a preorder on K. Thus, lemma 2.5 tells us that a maximal preorder is an order (note that such a maximal preorder exists by Zorn's Lemma). The backwards direction follows trivially from the definition of order. □

Remark 2.7. Thus, the study of formally real fields is equivalent to the study of ordered fields. However, ordered fields must have characteristic 0; thus, all formally real fields must contain a copy of $\mathbb{Q}$. Furthermore, as we can construct an order on $\mathbb{R}(x_1, .., x_n)$ in an analogous way to that of Example 2.3 by inducting on the number of variables and noting that $\mathbb{R}(x_1, .., x_n) \cong \mathbb{R}(x_1, ..., x_{n-1})(x_n)$. Thus, we have that $\mathbb{R}(x_1, .., x_n)$ is formally real.

3. Artin's Reduction

The goal of this section is to prove the following theorem due to Emil Artin:

Theorem 3.1. *(Artin)*
If K is a formally real field, then K has an ordering and

$$\sum K^2 = \bigcap_{P \text{ ordering of } K} P$$

This result relies on the subsequent two lemmas.

Lemma 3.2. *Say P is a preorder of K, for $a \in K$, define $P[a] := P + aP$. $P[a]$ is a preorder if and only if $-a \notin P$.*

Proof. $-1 \in P[a]$ if and only if $-1 = x + ay$ for some $x, y \in P$. That is $-1 \in P[a]$ if and only if $-ay = 1 + x$; thus, $-a = y^{-1}(1 + x) \in P$. We note that this is in P as $y^{-1}(1 + x) = (y^{-1})^2(y(1 + x))$, and as $(y^{-1})^2, y(1 + x) \in P$.

Thus, we see the forward direction via the contrapositive as $-a \in P$ if and only if $-1 \in P[a]$; however, -1 cannot be in a preorder, so $P[a]$ is not a preorder.

We then get the backwards direction via the contrapositive, and noting that $-1 \notin P[a]$ if and only if $-a \notin P$. Furthermore, it is easy to see that $P[a]$ is closed under addition and multiplication and contains $\sum K^2$. □

Lemma 3.3. *If T is a preorder of K, then:*

$$T = \bigcap \{P : P \text{ is an order on } K \text{ and } T \subseteq P\}$$

Proof. We note that $\subseteq$ inclusion is trivial as each set on the right hand side contains T by definition. Thus, let us show the inclusion $\supseteq$ to do this we shall show that for $a \notin T$, then $a \notin \cap P$ that is there is some order P which contains T such that $a \notin P$. Assume that $a \notin P$, then by Lemma 3.3 we have that $T[-a]$ is a preorder with $-a \in T[-a]$; hence, we know by Zorn's Lemma that $T[-a]$ is contained in some maximal preorder P, and by Lemma 2.5 the maximal preorder P is an order. Thus, P is an order with $-a \in P$, so $a \notin P$. □

Remark 3.4. We note that $\sum K^2$ is the minimal preorder that is every order must contain $\sum K^2$, so the above lemma implies Theorem 3.1. We now have a really nice reduction of Hilbert's 17th problem. Recall that given $f \in \mathbb{R}[x_1, .., x_n]$ which is PSD, we want to prove that $f = \sum_{i=1}^{n} g_i^2$ for $g_i \in \mathbb{R}(x_1, ..., x_n)$ that is we want $f \in \sum \mathbb{R}(x_1, .., x_n)^2$. Thus, given a PSD polynomial if we can show that $f \geqslant_P 0$ for all orderings P on $\mathbb{R}(x_1, ..., x_n)$, then

$$f \in \bigcap_{P \text{ ordering of } \mathbb{R}(x_1, ..., x_n)} P = \sum \mathbb{R}(x_1, ..., x_n)^2$$

4. Real Closure

We now will introduce the concept of real closed fields. A *real closed* field K is a formally real field that has no algebraic extension that is formally real. Our goal will be to show that real closed fields have the nice property that there exists a single order on a real closed field namely K^2 the set of squares is the unique order. We start out by proving a lemma about quadratic extensions of ordered fields.

Lemma 4.1. *Let (K, P) be an ordered field, let $K' = K(\sqrt{\alpha})$ for some $\alpha \in K$, then there is an order P' on K' whose restriction to K is P if and only if $\alpha \in P$.*

Proof. The forward direction is easy as α is a square in K'; hence, for every order P' on K', $\alpha \in P'$. Thus, as P' restricts to P on K, and $\alpha \in K$, we have that $\alpha \in P$.

Now for the backwards direction, let us assume $\alpha \in P$ and $\alpha \notin K^2$ as the case were α is a square is trivial. Now we note that the set of sums of the form $\sum c_i x_i^2$ is a preorder where $c_i \in P$ and $x_i \in K'$. This preorder contains P as a set, and can thus be extended to an order. □

This lemma allows us to show that there is a unique ordering on a real closed field K.

Theorem 4.2. *If K is a real closed field, then K^2 is the only order of K.*

Proof. Let P be an order of K, then for $\alpha \in P$, by Lemma 4.1 we have that $K(\sqrt{\alpha})$ has an order P' that extends P. However, as K is real closed, we know that there is no ordered extension. Hence, we have that $K(\sqrt{\alpha}) = K$ and $P' = P$. Namely $\alpha \in K^2$; thus, we have that $K^2 = P$ is the unique order on K. □

Now we shall define the real closure of a formally real field. The concept of the real closure is analogous to an algebraic closure in that it shall be the largest algebraic extension which is an ordered field. Artin actually used the concept of the real closure to give a generalized proof of Hilbert's 17th problem dealing with polynomials over real closed fields rather than just $\mathbb{R}$ (which is real closed).

Definition 4.3. Let (K, P) be an ordered field. A real closed field R is called the *real-closure* of (K, P) if R is an algebraic extension of K and $R^2 \cap K = P$ that is the restriction of the squares of R (which is the only order on R) to K is exactly the order P.

Theorem 4.4. *Every ordered field has a real closure. Furthermore, two real closures are unique up to isomorphism.*

Proof. We omit the proof; however, a proof can be found in [San91]. □

5. Solution to Hilbert's 17th Problem

We are finally ready to prove Hilbert's 17th problem. Recall we have reduced the problem to showing that if $f \in \mathbb{R}[x_1, ..., x_n]$ is PSD, then we want to show that $f \geqslant_P 0$ for every order P on $\mathbb{R}(x_1, .., x_n)$. We shall first state the Artin-Lang Homomorphism Theorem which shall be used in the proof. We shall omit the proof of this theorem, but a proof can be found in [Lor97].

Theorem 5.1. *Artin-Lang Homomorphism Theorem Let K be a real closed field, let $A = K[x_1, ..., x_n]$ be a finitely generated K-algebra which has no zero divisors (the x_is may satisfy some relations as in the $\mathbb{R}$-algebra in the proof of Hilbert's 17 problem) such that the quotient field $K(x_1, ..., x_n)$ is formally real. Then there exists a K-algebra homomorphism*

$$\phi : K[x_1, ..., x_n] \to K$$

We now state Artin's generalization of Hilbert's 17th problem in terms of real closures. We will only prove the case for $\mathbb{R}$, the general case can be found in [Pfi95].

Theorem 5.2. *Let $(K_0, P_0 = K_0^2)$ be a real closed field. Let $K = K_0(x_1, ..., x_n)$ be the rational function field in n variables over K_0 and let $f \in K$ be a rational function such that $f(a) = f(a_1, ..., a_n) \geqslant 0 \in K_0$ for all $a = (a_1, ..., a_n) \in K_0^n$ where $f(a)$ is defined. Then there exists finitely many $p_i \in P_0 \subseteq K_0$ and $f_i \in K$ such that $f = \sum p_i f_i^2$. Since $P_0 = \sum K_0^2$ is the only order of K_0, then the p_i are sums of squares in K_0 and f is a sum of squares in K.*

We shall simply present the proof when $K_0 = \mathbb{R}$, and $P_0 = \mathbb{R}_{\geqslant 0}$ as this will simplify some of the steps. We note that as $\mathbb{R}$ is a real closed field, we have that $\mathbb{R}_{\geqslant 0}$ is the unique order on $\mathbb{R}$.

Proof. First let us define $T = \{\sum p_i f_i^2 : p_i \in \mathbb{R}_{\geqslant 0}, f_i \in \mathbb{R}(x_1, .., x_n)\}$. Now T is a preorder, our goal is to show that for a PSD polynomial f, we have that $f \in T$. We note by remark 3.4 that showing $f \in T$ is analogous to showing $f \in P$ for every order P on $\mathbb{R}(x_1, .., x_n)$ such that $T \subseteq P$.

Let $f \in \mathbb{R}(x_1, ..., x_n)$ be a PSD rational function. Now let us assume for sake of contradiction that there exists an order P on $\mathbb{R}(x_1, ..., x_n)$ such that $T \subseteq P$ such that $f \notin P$. Thus, we have that $-f \in P$. Now let R be a real closure of $(\mathbb{R}(x_1, ..., x_n), P)$. Then we have that $-f$ is a square in R, so $-f = \omega^2$ for some $\omega \in R$.

Now fix $f = \frac{g}{h}$ for $g, h \in \mathbb{R}[x_1, ..., x_n]$ as a quotient of two polynomials. Now for the $\mathbb{R}$-algebra, $A = \mathbb{R}[x_1, ..., x_n, \frac{1}{g}, \frac{1}{h}, \omega, \frac{1}{\omega}] \subseteq R$ we can apply the Artin-Lang Homomorphism Theorem to give us a homomorphism $\phi : A \to \mathbb{R}$. Now denote $a_i = \phi(x_i)$. Thus, we have that:

$$\phi(f) = \phi(\frac{g}{h}) = \frac{g(a_1, ..., a_n)}{h(a_1, ..., a_n)} = f(a_1, ..., a_n)$$

We have that this is well-defined as $\phi(\frac{1}{h})$ is defined, then $\phi(h) \neq 0$, as $\phi(\frac{1}{h})\phi(h) = \phi(1) = 1$. Similarly, we have that $\phi(\omega) \neq 0$ and $\phi(g) \neq 0$ as we have that $\frac{1}{\omega}, \frac{1}{g} \in A$. Hence, we can say that $\phi(f) \neq 0$. Now, we use the equation that $-f = \omega^2$. Then:

$$f(a_1, ..., a_n) = \phi(f) = -\phi(\omega)^2 < 0$$

However, this contradicts the fact that f is PSD. Thus, no order P of $\mathbb{R}(x_1, .., x_n)$ exists were $f \notin P$, so as $f \in \cap P$, $f \in T$ which consists of elements which are sums of squares. □

Remark 5.3. The proof we gave worked due to the fact that $\mathbb{R}$ is a real closed field. We note that for any real closed field K, the PSD rational functions with coefficients in K can be written as a sum of squares using the exact same proof.

References

[Art27] Emil Artin. Über die zerlegung definiter funktionen in quadrate. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 5, pages 100–115. Springer, 1927.

[H+93] David Hilbert et al. Über ternäre definite formen. *Acta Mathematica*, 17:169–197, 1893.

[Hil02] David Hilbert. Mathematical problems. *Bulletin of the American Mathematical Society*, 8(10):437–479, 1902.

[Lor97] Falko Lorenz. *Einführung in die Algebra II*, volume 2. Spektrum Akademischer Verlag, 1997.

[Mot67] Theodore Samuel Motzkin. The arithmetic-geometric inequality. *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, pages 205–224, 1967.

[Pfi95] Albrecht Pfister. *Quadratic forms with applications to algebraic geometry and topology*. London Mathematical Society lecture note series ; 217. Cambridge University Press, Cambridge ; New York, 1995.

[San91] Tomas Sander. Existence and uniqueness of the real closure of an ordered field without zorn's lemma. *Journal of pure and applied algebra*, 73(2):165–180, 1991.

Email address: screech6@math.gatech.edu

School of Mathematics, Georgia Institute of Technology, USA