Hillar-Nie 2006

Jasper Ty

What is this?

This are notes I took while reading "An elementary and constructive solution to Hilbert's 17th Problem for matrices" by Christopher J. Hillar and Jiawang Nie [HN06].

This was for the class "Positive Polynomials and Sums of Squares" I took Winter 2024.

Contents

Notation

Let $\mathbf{x} = (x_1, \ldots, x_m)$ be a collection of indeterminates, and let $F[\mathbf{x}]$ and $F(\mathbf{x})$ denote the polynomial ring and the ring of rational functions with coefficients in the field F respectively.

For any subset S of a commutative ring R, let ΣS^2 denote the **sums of squares** of S, i.e

$$\Sigma S^2 := \left\{ \sum_{i=1}^{k} r_i^2 : r_1, \ldots, r_k \in S \right\}.$$

Similarly, let R^2 denote the **squares** of R.

Let $R^{d\times d}$ denote the set of $d\times d$ matrices in the ring R. And, let $\operatorname{Sym}_d(R)$ denote the subset of $R^{d\times d}$ consisting of symmetric matrices.

If A is a matrix and $J \subseteq \{1,\ldots,n\}$, let $A[J]$ denote the principal submatrix with indices picked out by J.

1 Introduction

We seek to exposit the proof given in [HN06] of the following result:

Theorem 1 (Procesi-Schacher, Gondard-Ribenboim)**.** Let $A \in \mathbb{R}^{d\times d}[\mathbf{x}]$ be symmetric. Let $A(\mathbf{x}_0)$ denote A with all entries evaluated at $\mathbf{x}_0 \in \mathbb{R}^d$. If $A(\mathbf{x}_0)$ is positive semidefinite for all choices of $\mathbf{x}_0 \in \mathbb{R}^m$, then A is a sum of squares of

This generalizes Artin's celebrated, classical result on nonnegative polynomials with real coefficients.

Theorem 2 (Artin's solution to Hilbert's 17th Problem)**.** Let $f \in \mathbb{R}[\mathbf{x}]$. The following are equivalent:

(i) $f(\mathbf{x}) \geq 0$ for all $\mathbf{x}$.

(ii) $f \in \Sigma\mathbb{R}(\mathbf{x})^2$.

We will prove the more general statement, which proves Theorem 1 with the help of Theorem 2.

Theorem 3. Let F be a real field, and let $A \in \operatorname{Sym}_d(F)$ such that $\det A[J] \in \Sigma F^2$ for all $J \subseteq \{1,\ldots,n\}$. Then $A \in \Sigma\left[\operatorname{Sym}_d(F)\right]^2$.

Proof that Theorem 3 implies Theorem 1. Let $A \in \operatorname{Sym}_d(\mathbb{R}[\mathbf{x}])$.

We will first show that all principal minors of A are in fact non-negative polynomials. We note that for all matrices $H \in \mathbb{R}[\mathbf{x}]^{d\times d}$, $(\det H)(\mathbf{x}_0) = \det\left(H(\mathbf{x}_0)\right)$ and $H[J](\mathbf{x}_0) = H(\mathbf{x}_0)[J]$ for all $J \subseteq [n]$. In other words, *taking determinants and taking submatrices commutes with evaluation*. So, if $J \subseteq [n]$,

$$\left(\det A[J]\right)(\mathbf{x}_0) = \det\left(A[J](\mathbf{x}_0)\right) = \det\left(A(\mathbf{x}_0)[J]\right) \geq 0,$$

for all $\mathbf{x}_0 \in \mathbb{R}^d$ supposing that $A(\mathbf{x}_0)$ is positive semidefinite for all $\mathbf{x}_0 \in \mathbb{R}^d$. Then we may apply Theorem 2 to $\det A[J] \in \mathbb{R}[\mathbf{x}]$, to conclude that $\det A[J] \in \Sigma\mathbb{R}(\mathbf{x})^2$.

Now, take A to live in $\mathrm{Sym}_d(\mathbb{R}(\mathbf{x}))$, where we are simply extending the inclusion of $\mathbb{R}[\mathbf{x}]$ into $\mathbb{R}(\mathbf{x})$, then we can apply Theorem 3, with $F = \mathbb{R}(\mathbf{x})$, to say that $A \in \Sigma\left[\mathrm{Sym}_d(\mathbb{R}(\mathbf{x}))\right]^2$. □

2 Review of real algebra

We will recover basic results in the theory of real symmetric matrices in the more general context of real closed fields.

First, a small digression about ordering. The data involving the order in an ordered field can be encoded as a set that names all the positive elements.

Definition 4. Let P be a subset of F. We say that P is a **ordering** of F if

(a) $P + P \subseteq P$,

(b) $P \cdot P \subseteq P$,

(c) $F^2 \subseteq P$,

(d) $-1 \notin P$, and

(e) $P \cup -P = F$.

If one has an ordered field F, then one has an ordering P by considering all the elements $p \in F$ such that $p \geq 0$. Conversely, if one has a field and an ordering P and a field F, one can make F an ordered field by putting $p \geq 0$ for all $p \in P$.

Now, we discuss real closed fields.

Definition 5. The **first order language of ordered fields** OrdField consists of well-formed sentences involving the usual logical symbols and connectives, as well as the non-logical symbols $+, \cdot, 0, 1, {}^{-1}, \leq$.

A **real closed field** is an ordered field for which a sentence ψ in OrdField is true if and only if it is true over $\mathbb{R}$.

This is not the usual definition of a real closed field. We will discuss a few important, equivalent definitions.

Theorem 6 (Artin-Schreier 1926)**.** Let F be a field. The following are equivalent:

(i) $-1 \notin \Sigma F^2$, and $-1 \in \Sigma G^2$ for any nontrivial algebraic extension G of F.

(ii) F^2 is an ordering of F, and every odd degree polynomial with coefficients in F has a root in F.

(iii) $F \neq F[\sqrt{-1}]$, and $F[\sqrt{-1}]$ is algebraically closed.

Proof. See Theorem 1.2.9 in [N] □

Theorem 7 (Tarski 19??). Let F be a field. The following are equivalent:

(i) F is real closed.

(ii) F satisfies any of the statements in Theorem 6.

Proof. We will define RCF to be the **theory of real closed fields**, to be the field axioms adjoined with (the correct encoding of) statement (ii) in Theorem 6.

One can prove **quantifier elimination** is possible in RCF, and moreover algorithmically possible, hence RCF is a decidable theory. Moreover, one can show that RCF can prove or disprove any quantifier free statement in OrdField, hence RCF is complete. Lastly, $\mathbb{R} \models$ RCF, so by basic model theory, if $R \models$ RCF, R and $\mathbb{R}$ are elementarily equivalent, i.e, they agree on all sentences in OrdField. □

With the logic out of the way, we can begin to glean some properties of real closed fields.

Proposition 8 (The ordering on RCFs). In a real closed field R, the set R^2 identifies all the positive elements.

Proof. Consider the OrdField sentences

$$\forall y(y^2 \geq 0)$$

and

$$\forall x\Big(x \geq 0 \iff \exists y(x = y^2)\Big),$$

which are evidently true in $\mathbb{R}$. □

Proposition 9 (Characterizations of PSD matrices over an RCF). Let R be a real-closed field and let $A \in \mathrm{Sym}_d(R)$. The following are equivalent

(i) All the principal minors of A are nonnegative.

(ii) $\mathbf{x}^T A\mathbf{x} \geq 0$ for all $\mathbf{x} \in R^d$.

(iii) A is diagonalizable with nonnegative eigenvalues.

Proof. If we fix d, we may completely encode the statement (i) $\implies$ (ii) in OrdField, hence its truth in R coincides with its truth in $\mathbb{R}$.

As an example, put $d = 2$. Then our statement in the first order language of ordered fields is

$$\forall a, b, c, d$$
$$\Bigg[\underbrace{\Big(a \geq 0 \wedge d \geq 0 \wedge ad - bc \geq 0\Big)}_{\text{nonnegative principal minors}} \implies \underbrace{\forall x, y \Big(ax^2 + (b+c)xy + dy^2 \geq 0\Big)}_{\text{positive-semidefiniteness}}\Bigg].$$

Similarly, we may do (ii) $\implies$ (iii).

The statement "$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is diagonalizable with nonnegative eigenvalues", in the $d = 2$ case, is [1]

$$\exists e, f, g, h$$
$$\Big[eh - fg = 1 \wedge e^2 b + efd - fea + f^2 c = 0 \wedge g^2 b + ghd - hga + h^2 c = 0$$
$$\wedge\ hea + hfc - geb - gfd \geq 0 \wedge egb + ehd - fga - fhc \geq 0\Big]$$

The point is, we can encode the whole theorem for a fixed d entirely as a sentence in OrdField. Then, we use the fact that the theorem is true for real symmetric matrices. □

Next, we discuss weaker objects than real closed fields, which we will need.

Definition 10. A **real field** is a field F in which $-1 \notin \Sigma F^2$.

Proposition 11. All real fields F have at least one ordering $\leq$ such that $(F, \leq)$ is an ordered field. Moreover, when equipped with such an order, there exists an ordered field R such that R is real closed, R is algebraic extension of K, and the order on R extends the order on F. We call R a **real closure** of F.

Proof. Theorem 1.4.2 in [N]. □

[1] Trust me

3 Proof of the theorem

We will need the following lemma.

> **Lemma 12.** Let F be a real field and suppose A satisfies the hypotheses of Theorem 3; $A \in \mathrm{Sym}_d(F)$ such that $\det A[J] \in \Sigma F^2$ for all $J \subseteq \{1, \dots, n\}$.
>
> Then the minimal polynomial $m(t) \in F[t]$ of A is of the form:
>
> $$m(t) = \sum_{i=0}^{k} (-1)^{k-i} a_i t^i = t^k - a_{k-1} t^{k-1} + \cdots + (-1)^k a_0.$$
>
> where $a_i \in \Sigma F^2$ for all i. Moreover, $a_1 \neq 0$.

Proof. This proof happens fairly quickly in [HN06]. We will spend some more detail on this.

Step 1 CHARACTERIZE SUMS OF SQUARES IN TERMS OF NONNEGATIVITY IN REAL CLOSURES

Sums of squares play a special role in real fields K. We have that

$$\Sigma K^2 = \bigcap_{\substack{P \text{ is an} \\ \text{ordering of } K}} P. \qquad \text{([N] Theorem 1.1.16)}$$

One can interpret this as saying that they are the elements that will *always* be positive regardless of the order one realizes on K. So, if $x \in \Sigma F^2$, that means that $x \geq 0$ in *any* ordering of F. In fact, if $x \geq 0$ in any real closure, then this means that $x \in \Sigma K^2$, as $x \geq 0$ in a real closure R means that $x \in P$ in some ordering P of F which R extends. We conclude:

If $x \geq 0$ in all real closures of F, then $x \in \Sigma F^2$, and conversely.

Then the path ahead is clear: *we want to show that $a_i \geq 0$ in all real closures R of F.*

Step 2 SHOW THAT A HAS NONNEGATIVE EIGENVALUES IN EVERY REAL CLOSURE

If R is a real closure of F, all the principal minors $\det A[J]$ of A are nonnegative in R, as, by the hypothesis, they are sums of squares in F, hence they are sums of squares in R, and the nonnegative elements of R are precisely the squares (Theorem 8), so $\det A[J]$ is a sum of nonnegative elements of R.

Then, we have the following:

In any real closure of F, all the principal minors of A are nonnegative.

Now, combined with 9, this statement reads

In any real closure of F, A is diagonalizable with nonnegative eigenvalues.

Step 3 Prove the lemma

Each a_i is a sum of products of eigenvalues of A. (Specifically, it is an elementary symmetric polynomial in the distinct eigenvalues of A, since A is diagonalizable).

Then a_i is nonnegative in every real closure R of A, as we have shown that its eigenvalues in R are nonnegative. But, as we have noted, this means that a_i is a sum of squares in F! This completes the proof of the first statement.

Finally, we complete the theorem by proving the second statement.

Since A is diagonalizable, $m(t)$ has no repeated roots, hence 0 can only appear at most once. This means that there is exactly 1 term in a_1, the $k-1$th elementary symmetric polynomial in the roots of $m(t)$, that avoids this zero and is hence positive, hence $a_1 \neq 0$. □

There is a formula in [H&J] that expresses the characteristic polynomial directly in terms of principal minors, and I'm sure it simplifies this proof, but I haven't had the time to try it.

We are now ready to prove the main theorem.

Proof of Theorem 3. Let F be a real field and let $A \in \mathrm{Sym}_d(F)$ be a matrix whose principal minors are all nonnegative.

Let $m(t) = t^k - a_{k-1}t^{k-1} + \cdots + (-1)^k a_0$ be the minimal polynomial of A.

Then, by Cayley-Hamilton, $m(A) = 0$, so by splitting the even and odd degree terms,

$$(A^{k-1} + a_{k-2}A^{k-3} + \cdots + a_1 I)A = a_{m-1}A^{k-1} + a_{m-3}A^{m-3} + \cdots + a_0 I.$$

Now put $B = A^{k-1} + a_{k-2}A^{k-3} + \cdots + a_1 I \in \mathrm{Sym}_d(F)$. B is invertible, since $a_1 = 0$, hence it does not have 0 as an eigenvalue. Moreover, B's inverse is also symmetric, i.e $B^{-1} \in \mathrm{Sym}_d(F)$.

Then, $B^{-1} = B \cdot B^{-2} = B \cdot (B^{-1})^2$, so

$$A = B\Big(a_{k-1}B^{-2}A^{k-1} + a_{k-3}B^{-2}A^{k-3} + \cdots + a_0 B^{-2}\Big).$$

Everything "in sight" is a sum of squares.

- All coefficients $a_i \in F$ appearing are sums of squares; $a_i \in \Sigma F^2$.
- Each A^{k-2l} term is a square, as k is odd; $A^{k-2l} \in \left[\mathrm{Sym}_d(F)\right]^2$.
- B itself is a sum of squares, as $B = A^{k-1} + a_{k-2}A^{k-3} + \cdots + a_1 I$, and k is odd; $B \in \Sigma\left[\mathrm{Sym}_d(F)\right]^2$
- And finally, $B^{-2} = (B^{-1})^2 \in \left[\mathrm{Sym}_d(F)\right]^2$.

So, in all, $A \in \Sigma\left[\mathrm{Sym}_d(F)\right]^2$. The k even case is similarly argued. □

References

[H&J] Roger Horn, Charles Johnson, *Matrix Analysis*.

[N] Tim Netzer, *Real Algebra and Geometry*, Universität Innsbruck, https://www.uibk.ac.at/mathematik/algebra/media/teaching/ragen.pdf.

[S] Markus Schweighofer, *Real Algebraic Geometry, Positivity and Convexity*, Universität Konstanz, https://cloud.uni-konstanz.de/index.php/s/3bcgdnT2eXR9EKF.

Also available as arXiv:2205.04211.

[HN06] Christopher Hillar and Jiewang Nie, *An elementary and constructive solution to Hilbert's 17th Problem for Matrices*, Proc. Amer. Math. Soc. **136** (2008), 73-76.

https://doi.org/10.1090/S0002-9939-07-09068-5.

Also available as arXiv:math/0610388v3.