Universality of Polynomial Positivity and a Variant of Hilbert's 17th Problem

Grant Olney Passmore and Leonardo de Moura
{g.passmore@ed.ac.uk, leonardo@microsoft.com}

LFCS, University of Edinburgh and Microsoft Research

Abstract. We observe that the decision problem for the $\exists$ theory of real closed fields (RCF) is simply reducible to the decision problem for RCF over a connective-free $\forall$ language in which the only relation symbol is a strict inequality. In particular, every $\exists$ RCF sentence φ can be settled by deciding a proposition of the form "polynomial p (which is a sum of squares) takes on strictly positive values over the reals," with p simply derived from φ. Motivated by this observation, we pose the goal of isolating a syntactic criterion characterising the positive definite (i.e., strictly positive) real polynomials. Such a criterion would be a strictly positive analogue to the fact that every positive semidefinite (i.e., non-negative) real polynomial is a sum of squares of rational functions, as established by Artin's positive solution to Hilbert's 17th Problem. We then prove that every positive definite real polynomial is a ratio of a Real Nullstellensatz witness and a positive definite real polynomial. Finally, we conjecture that every positive definite real polynomial is a product of ratios of Real Nullstellensatz witnesses and examine an interesting ramification of this conjecture[1].

1 Motivation

Real polynomial (non-strict) positivity is a classically studied topic in real algebraic geometry with many applications to mainstream mathematics, theoretical computer science, engineering, and the natural sciences. For example, the termination of rewriting systems [5], the construction of Lyapunov functions for proving the stability of dynamical systems [3][7], and the distiguishing between separable and entangled quantum states [1] are problems that can be in many cases solved by proving the non-negativity of certain associated polynomials in $\mathbb{R}[\boldsymbol{x}]$.

[1] We are extremely grateful to a number of helpful anonymous referees. In particular, the first referee pointed out that our main conjecture (Conjecture 1) is in fact known to be true, and follows as a simple corollary of the Krivine-Stengle Positivstellensatz. This referee then even took the time to construct an original proof of this conjecture, given that the original references were not easily accessible. We must express our true appreciation for this amazingly generous referee. We will attach this referee's proof as an appendix to our paper.

The work in this paper is motivated primarily by the wish for improved decision methods for the quantifier-free fragment of the elementary theory of real closed fields. In particular, we observe that the satisfiability of any boolean combination of polynomial equations and inequalities over $\mathbb{R}^n$ can be reduced to the strict positivity of an associated polynomial that is itself a sum of squares of real polynomials. Wishing to make use of this observation in practice, we then ask: What form must a strictly positive real polynomial have?

Artin's positive solution to Hilbert's 17th Problem established a syntactic criterion for the non-negativity of a real polynomial, namely that every non-negative real polynomial is a sum of squares of real rational functions. Is there an analogous, sharper criterion for the strictly positive real polynomials?

2 Preliminaries

In the sequel, let $\mathbb{R}[\boldsymbol{x}]$ denote the polynomial ring $\mathbb{R}[x_1, \dots, x_n]$, $\mathbb{R}^+$ the set of strictly positive reals, $\mathcal{L}$ the elementary language of ordered rings, and $QF_{\mathcal{L}}$ the collection of quantifier-free $\mathcal{L}-$formulæ. We first recall some basic real algebraic preliminaries and then observe that the decision problem for the existential fragment of RCF is simply reducible to the problem of whether or not a sum of squares of real polynomials is positive definite.

Definition 1. *A polynomial $p \in \mathbb{R}[\boldsymbol{x}]$ is positive definite (resp. semidefinite) iff $\forall \boldsymbol{r} \in \mathbb{R}^n (p(\boldsymbol{r}) > 0)$ (resp. $\forall \boldsymbol{r} \in \mathbb{R}^n (p(\boldsymbol{r}) \geq 0)$). We say p is PD (resp. PSD) if p is positive definite (resp. semidefinite).*

Definition 2. *A set $S \subseteq \mathbb{R}^n$ is semialgebraic iff $S = \{\boldsymbol{r} \in \mathbb{R}^n \mid \langle \mathbb{R}, +, -, *, <, 0, 1 \rangle \models \varphi(\boldsymbol{r})\}$ for some $\varphi \in QF_{\mathcal{L}}$.*

Definition 3. *A real algebraic variety is the locus of real zeros of a finite system of real polynomials. That is, given $p_1, \dots, p_m \in \mathbb{R}[\boldsymbol{x}]$,*

$$\begin{aligned} \mathcal{V}_{\mathbb{R}}(p_1, \dots, p_m) &= \{\boldsymbol{r} \in \mathbb{R}^n \mid p_1(\boldsymbol{r}) = 0 \ \wedge \dots \wedge \ p_m(\boldsymbol{r}) = 0\} \\ &= \mathcal{V}(p_1, \dots, p_m) \ \cap \ \mathbb{R}^n \end{aligned}$$

where $\mathcal{V}(p_1, \dots, p_m)$ is the (complex) algebraic variety of classical algebraic geometry.

Observe that every real algebraic variety is semialgebraic.

Definition 4. *The projection $\Pi_X : 2^{\mathbb{R}^n} \rightarrow 2^{\mathbb{R}^{n-k}}$ of a semialgebraic set $S \subseteq \mathbb{R}^n$ onto a lower-dimensional Euclidean space w.r.t. a collection of eliminated coordinates (wlog) $X = \{1, \dots, k\}$ $(1 \leq k \leq n)$ is defined as follows:*

$$\Pi_X(S) = \{\langle r_{k+1}, \dots, r_n \rangle \in \mathbb{R}^{n-k} \mid \langle r_1, \dots, r_n \rangle \in S\}.$$

As every semialgebraic set $S \subseteq \mathbb{R}^n$ is of the form $S = \{\boldsymbol{r} \in \mathbb{R}^n \mid \langle \mathbb{R} \rangle \models \varphi(\boldsymbol{r})\}$ for some $\varphi \in QF_{\mathcal{L}}$, we can describe the geometric operation of projection strictly in terms of operations upon formulæ:

$$\Pi_X(S) = \{\langle r_{k+1}, \dots, r_n \rangle \in \mathbb{R}^{n-k} \mid \langle \mathbb{R} \rangle \models \exists x_1 \dots \exists x_k \varphi(x_1, \dots, x_k, r_{k+1}, \dots, r_n)\},$$

where $\langle\mathbb{R}\rangle$ *is an abbreviation for* $\langle\mathbb{R},+,-,*,<,0,1\rangle$.

And so we see that the geometric operation of projection corresponds to the logical operation of existential quantification. Surprisingly, adding a projection operator to $QF_{\mathcal{L}}$ does not increase the expressive power of the language w.r.t. the collections of real vectors that can be defined. The following important result is what ultimately allows the theory of real closed fields to admit elimination of quantifiers.

Theorem 1 (Tarski-Seidenberg). *The collection of semialgebraic sets is closed under projection.*

It is a marvelous fact that quantifier-free equivalents of all $\mathcal{L}-$formulæ can be found algorithmically [6], though infeasibly.

3 Universality of Polynomial Positivity

We now use the well-known Rabinowitsch encoding to observe the folklore[2] result that every $\exists$ RCF sentence is equivalent to the $\exists-$closure of a single polynomial equation. We phrase the result geometrically in terms of projection. We then observe that with a simple application of the Intermediate Value Theorem, which holds over every RCF, we can reduce the truth of any $\exists$ RCF formula to (the falsity of) a statement proclaiming the strict positivity of a derived polynomial which is a sum of squares of real polynomials.

Theorem 2. *Every semialgebraic set is the projection of a real algebraic variety.*

Proof. Let $S \subseteq \mathbb{R}^n$ *be given as* $S = \{\boldsymbol{r} \in \mathbb{R}^n \mid \langle\mathbb{R},+,-,*,<,0,1\rangle \models \varphi(\boldsymbol{r})\}$ *for some* $\varphi \in QF_{\mathcal{L}}$. *By induction on* φ *(which is quantifier-free) we obtain an equivalent RCF formula* Ψ *whose quantifier-free matrix consists of a single polynomial equation. This is done by using the Rabinowitsch equivalences (where* z *is a fresh variable):*

$$\begin{aligned}
(p \neq 0) &\iff \exists z(pz-1)=0,\\
(p \leq q) &\iff \exists z(q-p-z^2=0),\\
(p < q) &\iff \exists z(q-p)z^2-1=0,\\
\bigwedge_{i=1}^{v} p_i = 0 &\iff \sum_{i=1}^{v}(p_i)^2=0,\\
\bigvee_{i=1}^{v} p_i = 0 &\iff \prod_{i=1}^{v} p_i = 0.
\end{aligned}$$

[2] This observation appears already in 1954 in Seidenberg's seminal paper [4]. We are grateful to an anonymous reviewer for pointing this out.

Note that the obtained Ψ is quantifier-free iff φ is a negation-free boolean combination of polynomial equations. In that case, the projection used to obtain S from the real algebraic variety defined by Ψ is the trivial projection, and thus S is itself a real algebraic variety. Otherwise, $\Psi = \exists \boldsymbol{x} \exists \boldsymbol{z}(p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ for some $p \in \mathbb{R}[\boldsymbol{x}, \boldsymbol{z}]$ s.t. $\boldsymbol{z} = \langle z_1, \ldots, z_k \rangle$ and k is the number of inequality symbols appearing in φ.

The following immediate corollary places an upper-bound on the dimension of the ambient Euclidean space containing a real algebraic variety whose projection is S.

Corollary 1. *If $S \subseteq \mathbb{R}^n$ is semialgebraic, then $S = \Pi_Z(T)$ where $T \subseteq \mathbb{R}^{n+k}$ is a real algebraic variety s.t. $k = |Z|$ is the total number of inequality and negated-equality symbols appearing in a defining $QF_{\mathcal{L}}$ formula for S.*

In fact, by a difficult construction of Motzkin [2], the following stronger result is known:

Theorem 3. *If $S \subseteq \mathbb{R}^n$ is semialgebraic, then $S = \Pi_{\{z\}}(T)$ where $T \subseteq \mathbb{R}^{n+1}$ is a real algebraic variety. Note that in this construction, T is defined by an equation with only one more variable (z) than appear in a $QF_{\mathcal{L}}$ formula defining S.*

With these results in hand, we are ready to make the following simple observation which motivates the rest of the work in this article:

Theorem 4. *The decision problem for the $\exists$ theory of RCF is simply reducible to the decision problem for RCF over a connective-free $\forall$ language in which the only relation symbol is a strict inequality. In particular, every $\exists$ RCF sentence φ can be settled by deciding a proposition of the form "polynomial $\mathbb{P}$ takes on strictly positive values over the reals," where $\mathbb{P}$ is simply derived from φ.*

Proof. We show that any $\exists$ $\mathcal{L}-$sentence φ can be either trivially decided by ground evaluation or by deciding a statement of the form "polynomial p takes on strictly positive values over $\mathbb{R}$." Let Ψ be the sentence obtained from φ via the inductive process in Theorem 2 s.t. $(\varphi \iff \Psi) \in RCF$. Note that $\Psi = \exists \boldsymbol{x} \exists \boldsymbol{z}(p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ for some $p \in \mathbb{R}[\boldsymbol{x}, \boldsymbol{z}]$ s.t. $\boldsymbol{z} = \langle z_1, \ldots, z_k \rangle$. Let $\theta(p)$ be the degree zero constant term of p and let $\mathbf{0}$ be the zero vector in $\mathbb{R}^{n+k}$. If $\theta(p) = 0$ then $p(\mathbf{0}) = 0$ and so Ψ (and hence φ) holds. Otherwise, we have either $\theta(p) > 0$ or $\theta(p) < 0$. Let Ψ' be s.t. $\Psi' = \Psi$ if $\theta(p) > 0$ and $\Psi' = \exists \boldsymbol{x} \exists \boldsymbol{z}((-1) * p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ otherwise. Denote the resulting LHS polynomial in Ψ' as $\mathbb{P}$. As the Intermediate Value Theorem holds over every real closed field, we now have

$$\neg \varphi \iff \forall \boldsymbol{x} \forall \boldsymbol{z}(\mathbb{P}(\boldsymbol{x}, \boldsymbol{z}) > 0).$$

And so the truth of φ can be settled by deciding the strict positivity of $\mathbb{P}(\boldsymbol{x}, \boldsymbol{z})$ and negating the result.

The following corollary makes it clear that a method for deciding whether or not a sum of squares of real polynomials is PD is sufficient for the $\exists$ theory of RCF.

Corollary 2. *Strict polynomial positivity for sums of squares of real polynomials is complete for the $\exists$ theory of the reals.*

Proof. This is immediate, as the formula $\Psi = \exists \boldsymbol{x} \exists \boldsymbol{z}(p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ obtained in the inductive construction of Theorem 2 is either already of the form $\exists \boldsymbol{x} \exists \boldsymbol{z}(\sum (p_i(\boldsymbol{x}, \boldsymbol{z}))^2 = 0)$ (e.g., by top-level applications of the encoding of conjunction: $(p = 0) \wedge (q = 0) \iff p^2 + q^2 = 0$), or it is of the form $\exists \boldsymbol{x} \exists \boldsymbol{z}(p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ where p is not a sum of squares of real polynomials. In the latter case, note that $\exists \boldsymbol{x} \exists \boldsymbol{z}(p(\boldsymbol{x}, \boldsymbol{z}) = 0)$ is equivalent to $\exists \boldsymbol{x} \exists \boldsymbol{z}((p(\boldsymbol{x}, \boldsymbol{z}))^2 = 0)$ and the result follows.

4 A PD Variant of Hilbert's 17th Problem

Recall that a real polynomial is PSD iff it assumes only non-negative values for all real values of its variables. Artin's positive solution to Hilbert's 17th Problem characterises the PSD real polynomials with the following syntactic criterion:

Theorem 5 (Artin's Positive Solution to Hilbert's 17th Problem). *Every PSD real polynomial is a sum of squares of rational functions.*

The allowance of *rational functions* above is necessary to obtain a complete characterisation, as there are real polynomials (such as the dehomogenized bivariate Motzkin form, $x^4y^2 + x^2y^4 - 3x^2y^2 + 1$) that are PSD but not sums of squares of real polynomials. By the results in the previous section, we know that the truth of any $\exists$ RCF sentence φ can be settled by deciding if a certain real polynomial derived from φ is PD. Thus, we are interested in obtaining a syntactic criterion characterising the class of PD polynomials. Such a criterion for PD polynomials would be analogous to that of PSD polynomials that is given in Hilbert's 17th Problem. Indeed, it should have the property that every real polynomial meeting the criterion is PD, just as every real polynomial meeting the criterion of being a sum of squares of rational functions is PSD.

In working to obtain a syntactic criterion for PD polynomials, a natural first attempt might take the following form: Every PD polynomial p is PSD, so by Artin's Theorem p is a sum of squares of rational functions. But, as p never obtains 0, p must have a positive constant term. Thus, we have

$$p \;=\; \sum_{i=1}^{k} \left(\frac{q_i}{s_i}\right)^2 \;=\; \mathfrak{p} + c$$

s.t. $q_i, s_i \in \mathbb{R}[\boldsymbol{x}]$ and (i) $\mathfrak{p}(\boldsymbol{0}) = 0$, (ii) $c \in \mathbb{R}^+$, and (iii) $\forall \boldsymbol{r} \in \mathbb{R}^n$ $(\mathfrak{p}(\boldsymbol{r}) > -c)$. All of these requirements would certainly be met if p was of the form

$$p \;=\; \left(\sum_{i=1}^{k} \left(\frac{q_i}{s_i}\right)^2\right) + r$$

with $r \in \mathbb{R}^+$. And so it is natural to ask the following question.

Question 1. Is every PD real polynomial a sum of a sum of squares of rational functions and a positive constant?

We will construct a simple example showing that this is not true in general.

Definition 5. *Let* $(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+) = \{(\sum_{i=1}^{m}(p_i)^2) + c \mid p_i \in \mathbb{R}[\boldsymbol{x}] \mid c \in \mathbb{R}^+ \mid m \in \mathbb{N}\}$, *and* $(\sum(\mathbb{R}(\boldsymbol{x}))^2 + \mathbb{R}^+) = \{(\sum_{i=1}^{m}(\frac{p_i}{q_i})^2) + c \mid p_i, q_i \in \mathbb{R}[\boldsymbol{x}]$ *s.t.* $q_i \neq 0 \mid c \in \mathbb{R}^+ \mid m \in \mathbb{N}\}$.

Lemma 1. $\sum(\mathbb{R}(\boldsymbol{x}))^2 + \mathbb{R}^+$ *does not contain every PD real polynomial.*

Proof. Let $\varphi \in QF_{\mathcal{L}}$ *be the formula* $(x = 0 \ \wedge \ x \neq 0)$. *Using the transformation in Theorem 2 we have* $\exists x(\varphi(x)) \iff \exists x \exists z((xz-1)^2 + x^2 = 0)$. *Let* $p(x,z) = (xz-1)^2 + x^2$. *As* φ *is unsatisfiable over* $\mathbb{R}$, *we have* $\forall x \forall z(p(x,z) \neq 0)$. *But as the constant term of* p *is* 1, *we have by Theorem 4 that* $\forall x \forall z(p(x,z) > 0)$. *We now observe that* $p(x,z) \notin (\sum(\mathbb{R}(\boldsymbol{x}))^2 + \mathbb{R}^+)$. *Suppose otherwise. Then, we must have* $\forall x \forall z(p(x,z) > k)$ *for some* $k \in \mathbb{R}^+$. *Let* $\frac{1}{\epsilon} \in \mathbb{R}$ *be s.t.* $0 < \frac{1}{\epsilon} < k$. *But then* $p(\frac{1}{\sqrt{2\epsilon}}, \sqrt{2\epsilon} + 1) = \frac{1}{\epsilon}$. *Contradiction.*

So we see that even in the bivariate case, there are PD real polynomials that are not simply sums of a sum of squares of rational functions and a positive constant. The situation is altogether more subtle. We now introduce Stengle's Real Nullstellensatz and exploit it to isolate one interesting syntactic criterion for PD real polynomials.

4.1 Stengle's Real Nullstellensatz and a PD Criterion

Stengle's Real Nullstellensatz guarantees the existence of an algebraic proof object certifying the unsatisfiability of a system of polynomial equations over $\mathbb{R}^n$. The result takes the following form.

Theorem 6 (Stengle's Real Nullstellensatz). *Let* $S = \{p_1 = 0, \ldots, p_k = 0\}$ *be a system of real polynomial equations. Then,* S *is unsatisfiable over* $\mathbb{R}^n$ *iff*

$$\exists \mathbb{P} \in \mathcal{I}(p_1, \ldots, p_k) \ \textit{s.t.}\ \mathbb{P} = \left(\sum_{i=1}^{m}(q_i)^2\right) + 1,$$

where $\mathcal{I}(p_1, \ldots, p_k) = \{\sum_{i=1}^{k} p_i r \mid r \in \mathbb{R}[\boldsymbol{x}]\}$ *is the* $\mathbb{R}[\boldsymbol{x}]$*-ideal of* $\{p_1, \ldots, p_k\}$ *and* $q_1, \ldots, q_m \in \mathbb{R}[\boldsymbol{x}]$. $\mathbb{P}$ *is called a* ***Real Nullstellensatz witness****.*

Observe that Stengle's Real Nullstellensatz is presenting another way in which the unsatisfiability of an $QF_{\mathcal{L}}$ formula over $\mathbb{R}^n$ can be reduced to the existence of an associated strictly positive polynomial.

We now use this result to isolate a syntactic criterion for PD real polynomials.

Theorem 7. *Every PD real polynomial is a ratio of a Real Nullstellensatz witness and a PD real polynomial.*

Proof. *Let $p \in \mathbb{R}[\boldsymbol{x}]$ be PD. Then it follows that $\exists \boldsymbol{x}(p(\boldsymbol{x}) = 0)$ is unsatisfiable over $\mathbb{R}^n$, and thus by Stengle's Real Nullstellensatz it follows that $\exists q \in \mathcal{I}(p)$ s.t. $(pq = \left(\sum_{i=1}^{m}(q_i)^2\right) + 1)$ for some $q_1, \ldots, q_m \in \mathbb{R}[\boldsymbol{x}]$. But as $pq = \left(\sum_{i=1}^{m}(q_i)^2\right) + 1$, it follows that pq is itself PD, and so q must be PD as well. Thus, it then follows that $p = \frac{\left(\sum_{i=1}^{m}(q_i)^2\right)+1}{q}$.*

Note that the process involved in the proof of Theorem 7 can be iterated. That is, given that p and q are both PD with $p = \frac{\left(\sum_{i=1}^{m}(q_i)^2\right)+1}{q}$, it then follows again by Stengle's Real Nullstellensatz that $\exists r \in \mathcal{I}(q)$ s.t. $(qr = \left(\sum_{i=1}^{m'}(r_i)^2\right) + 1)$ for some $r_1, \ldots, r_{m'} \in \mathbb{R}[\boldsymbol{x}]$. So as it then follows that r must be PD and therefore $q = \frac{\left(\sum_{i=1}^{m'}(r_i)^2\right)+1}{r}$ and thus

$$p = \frac{\left(\left(\sum_{i=1}^{m}(q_i)^2\right) + 1\right) r}{\left(\sum_{i=1}^{m'}(r_i)^2\right) + 1}$$

where r is PD. But then by the same argument, we have

$$p = \frac{\left(\left(\sum_{i=1}^{m}(q_i)^2\right) + 1\right)\left(\left(\sum_{i=1}^{m''}(s_i)^2\right) + 1\right)}{\left(\left(\sum_{i=1}^{m'}(r_i)^2\right) + 1\right) s}$$

where s is PD, and so on.

Based upon this observation, we make the following conjecture.

Conjecture 1. Every PD polynomial is a finite product of ratios of Real Nullstellensatz witnesses.

Finally, we observe that if this conjecture holds, then it follows that every PD polynomial is in fact a ratio of only two polynomials in $\left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$. This proof is assisted by the following lemmata.

Lemma 2. *If $p, q \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$, then $p + q \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$.*

Proof. *Immediate.*

Lemma 3. *If $p, q \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$, then $pq \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$.*

Proof. *Let* $p, q \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$ *s.t. (wlog)* $p = \sum_{i=1}^{m}(p_i)^2 + k_1,\ q = \sum_{i=1}^{n}(q_i)^2 + k_2$ *for some* $p_i, q_i \in \mathbb{R}[\boldsymbol{x}]$ *and* $k_1, k_2 \in \mathbb{R}^+$. *Then,*

$$\begin{aligned} pq &= \left(\sum_{i=1}^{m}(p_i)^2 + k_1\right)\left(\sum_{i=1}^{n}(q_i)^2 + k_2\right) \\ &= \left(\sum_{i=1}^{m}(p_i)^2\right)\left(\sum_{i=1}^{n}(q_i)^2\right) + k_1\left(\sum_{i=1}^{n}(q_i)^2\right) + k_2\left(\sum_{i=1}^{m}(p_i)^2\right) + k_1k_2 \\ &= \left(\sum_{i=1}^{m}\sum_{j=1}^{n}(p_i)^2(q_j)^2\right) + k_1\left(\sum_{i=1}^{n}(q_i)^2\right) + k_2\left(\sum_{i=1}^{m}(p_i)^2\right) + k_1k_2 \\ &= \left(\sum_{i=1}^{m}\sum_{j=1}^{n}(p_iq_j)^2\right) + \left(\sum_{i=1}^{n}\left(\sqrt[2]{k_1}q_i\right)^2\right) + \left(\sum_{i=1}^{m}\left(\sqrt[2]{k_2}p_i\right)^2\right) + k_1k_2. \end{aligned}$$

Clearly, $\sum_{i=1}^{n}\left(\sqrt[2]{k_1}q_i\right)^2, \sum_{i=1}^{m}\left(\sqrt[2]{k_2}p_i\right)^2$, *and* $k_1k_2 \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$. *By Lemma 2, it suffices to show* $\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(p_iq_j)^2\right) \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$. *But* $\sum_{j=1}^{n}(p_cq_j)^2 \in \left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$ *for each fixed* $(1 \leq c \leq n)$, *and so by Lemma 2 the result follows.*

Theorem 8. *If a real polynomial p is a finite product of ratios of Real Nullstellensatz witnesses, then* $p = \frac{\left(\sum_{i=1}^{m}(q_i)^2\right)+k_1}{\left(\sum_{i=1}^{m'}(r_i)^2\right)+k_2}$ *for some* $q_1, \ldots, q_m, r_1, \ldots, r_{m'} \in \mathbb{R}[\boldsymbol{x}]$, *and* $k_1, k_2 \in \mathbb{R}^+$.

Proof. *Immediate by Lemmas 2 and 3.*

5 Conclusion

In conclusion, we have observed a simple reduction from the ∃ theory of RCF to a restricted theory in which every sentence is of the form "polynomial p (which is a sum of squares) is strictly positive over the reals." Motivated by this observation, we posed the question of isolating syntactic criterion for PD real polynomials analogous to that given by Artin's positive solution to Hilbert's 17th Problem for PSD polynomials. We then found one such criterion, namely that every PD real polynomial is a ratio Real Nullstellensatz witness and a PD real polynomial. Finally, we conjectured that every PD real polynomial is a finite product of ratios of Real Nullstellensatz witnesses and proved that if this holds, then every PD real polynomial is in fact a ratio of two polynomials in $\left(\sum(\mathbb{R}[\boldsymbol{x}])^2 + \mathbb{R}^+\right)$.

References

1. A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88(18):187904, Apr 2002.

2. T. S. Motzkin. The real solution set of a system of algebraic inequalities. 1970.
3. Pablo A. Parrilo. Semidefinite programming relaxations for semialgebraic problems, 2001.
4. A. Seidenberg. A new decision method for elementary algebra. *The Annals of Mathematics*, 60(2), 1954.
5. Joachim Steinbach. Proving polynomials positive. In *Proceedings of the 12th Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 191–202, London, UK, 1992. Springer-Verlag.
6. Alfred Tarski. A decision method for elementary algebra and geometry. Technical report, Rand Corporation, 1948.
7. A. Tiwari. Abstractions for hybrid systems. *Formal Methods in Systems Design*, 32:57–83, 2008.

APPENDIX

We now present a proof of Conjecture 1 constructed by the aforementioned generous and much appreciated anonymous referee.

Theorem 9. *Every PD polynomial is a finite product of ratios of Real Nullstellensatz witnesses. In fact, every PD polynomial is a ratio of two Real Nullstellensatz witnesses.*

Proof. Assuming $p > 0$*, then* $-p \geq 0$ *is inconsistent, so by the usual PSatz (e.g. Theorem 4.6 in the Parrilo reference [3]), there are two sums of squares of polynomials S1 and S2 such that*

$$-p * S_1 + S_2 = -1.$$

Now the trick is to use the algebraic identity

$$\begin{aligned} 4p &= (p+1)^2 - (p-1)^2 \\ &= (p+1)^2 + (-1)(p-1)^2 \\ &= (p+1)^2 + (S_2 - S_1 p)(p-1)^2. \end{aligned}$$

Let $S_1' = S_1(p-1)^2$*, and* $S_2' = S_2(p-1)^2$*, both obviously still sums of squares of real polynomials. Then,*

$$\begin{aligned} 4p &= (p+1)^2 + S_2' - S_1' p \\ (4 + S_1')p &= (p+1)^2 + S_2' \\ (4 + S_1')p &= p^2 + 2p + 1 + S_2' \\ (2 + S_1')p &= 1 + p^2 + S_2' \end{aligned}$$

and therefore as desired

$$p = \frac{1 + p^2 + S_2'}{2 + S_1'}.$$

Observe that $2 + S_1'$ *is a Real Nullstellensatz witness as* $2 + S_1' = 1 + (1 + S_1')$ *with* $1 + S_1'$ *clearly a sum of squares of real polynomials.*

That this result unconditionally subsumes Theorem 8 is readily seen.