Rational Certificates of Positivity on Compact Semialgebraic Sets

Victoria Powers *

February 3, 2011

Abstract

Let $\mathbb{R}[X]$ denote the real polynomial ring $\mathbb{R}[X_1, \dots, X_n]$ and write $\sum \mathbb{R}[X]^2$ for the set of sums of squares in $\mathbb{R}[X]$. Given $g_1, \dots, g_s \in \mathbb{R}[X]$ such that the semialgebraic set $K := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \text{ for all } i\}$ is compact, Schmüdgen's Theorem says that if $f \in \mathbb{R}[X]$ such that $f > 0$ on K, then f is in the preordering in $\mathbb{R}[X]$ generated by the g_i's, i.e., f can be written as a finite sum of elements $\sigma g_1^{e_1} \dots g_s^{e_s}$, where σ is a sum of squares in $\mathbb{R}[X]$ and each $e_i \in \{0, 1\}$. Putinar's Theorem says that under a condition on the set of generators $\{g_1, \dots, g_s\}$ (which is a stronger condition than the compactness of K), any $f > 0$ on K can be written $f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_s g_s$, where $\sigma_i \in \sum \mathbb{R}[X]^2$. Both of these theorems can be viewed as statements about the existence of certificates of positivity on compact semialgebraic sets. In this note we show that if the defining polynomials $g_1, \dots, g_s$ and polynomial f have coefficients in $\mathbb{Q}$, then in Schmüdgen's Theorem we can find a representation in which the σ's are sums of squares of polynomials over $\mathbb{Q}$. We prove a similar result for Putinar's Theorem assuming that the set of generators contains $N - \sum X_i^2$ for some $N \in \mathbb{N}$.

1 Introduction

We write $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{Q}$ for the set of natural, real, and rational numbers. Let $n \in \mathbb{N}$ be fixed and let $\mathbb{R}[X]$ denote the polynomial ring $\mathbb{R}[X_1, \dots, X_n]$. We denote by $\sum \mathbb{R}[X]^2$ the set of sums of squares in $\mathbb{R}[X]$.

For $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[X]$, the *basic closed semialgebraic set* generated by S, denoted K_S, is

$$\{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \dots, g_s(x) \geq 0\}.$$

Associated to S are two algebraic objects: The *quadratic module generated by* S, denoted M_S, is the set of $f \in \mathbb{R}[X]$ which can be written

$$f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_s g_s,$$

*Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322. Email: vicki@mathcs.emory.edu.

where each $\sigma_i \in \sum \mathbb{R}[X]^2$, and the *preordering generated by* S, denoted T_S, is the quadratic module generated by all products of elements in S. In other words, T_S is the set of $f \in \mathbb{R}[X]$ which can be written as a finite sum of elements $\sigma g_1^{e_1} \dots g_s^{e_s}$, where $\sigma \in \mathbb{R}[X]$ and each $e_i \in \{0, 1\}$.

A polynomial $f \in \sum \mathbb{R}[X]^2$ is obviously globally nonnegative in $\mathbb{R}^n$ and writing f explicitly as a sum of squares gives a "certificate of positivity" for the fact that f takes only nonnegative values in $\mathbb{R}^n$. (Note: To avoid having to write "nonnegativity or positivity" we use the term "positivity" to mean either.) More generally, for a basic closed semialgebraic set K_S, if $f \in T_S$ or $f \in M_S$, then f is nonnegative on K_S and an explicit representation of f in M_S or T_S gives a certificate of positivity for f on K_S.

In 1991, Schmüdgen [6] showed that if the semialgebraic set K_S is compact, then any $f \in \mathbb{R}[X]$ which is strictly positive on K_S is in the preordering T_S. A preordering or quadratic module is *archimedean* if it contains $N - \sum X_i^2$ for some $N \in \mathbb{N}$. We note that if M_S is archimedean, then it follows immediately that K_S is compact, however the converse is not true in general. In 1993, Putinar [5] showed that if M_S is archimedean then any $f \in \mathbb{R}[X]$ which is strictly positive on K_S is in M_S. In other words, these results say that under the given conditions a certificate of positivity for f on K_S exists.

Recently, techniques from semidefinite programming combined with Schmüdgen's and Putinar's theorems have been used to give numerical algorithms for applications such as optimization of polynomials on semialgebraic sets. However since these algorithms are numerical they might not produce exact certificates of positivity. With this in mind, Sturmfels asked whether any $f \in \mathbb{Q}[X]$ which is a sum of squares in $\mathbb{R}[X]$ is a sum of squares in $\mathbb{Q}[X]$. In [2], Hillar showed that the answer is "yes" in the case where f is known to be a sum of squares over a totally real field K. The general question remains unsolved.

It is natural to ask a similar question for Schmüdgen's Theorem and Putinar's Theorem: If the polynomials defining the semialgebraic set and the positive polynomial f have rational coefficients, is there a certificate of positivity for f in which the sums of squares have rational coefficients? In this note, we show that in the case of Schmüdgen's Theorem the answer is "yes". This follows from an algebraic proof of the theorem, originally due to T. Wörmann [9]. In the case of Putinar's Theorem, we show that the answer is also "yes" as long as the generating set contains $N - \sum X_i^2$ for some $N \in \mathbb{N}$. This follows easily from an algorithmic proof of the theorem due to Schweighofer [8]. For Lasserre's method for optimization of polynomials on compact semialgebraic sets, see [3], in concrete cases it is usual to add a polynomial of the type $N - \sum X_i^2$ to the generators in order to insure that Putinar's Theorem holds. Thus our assumption in this case is reasonable.

2 Rational certificates of for Schmüdgen's Theorem

Fix $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[X]$ and define K_S and T_S as above.

Theorem 1. *(Schmüdgen) Suppose that K_S is compact. If $f \in \mathbb{R}[X]$ and $f > 0$ on K_S, then $f \in T_S$.*

In this section we show that if f and the generating polynomials $g_1, \ldots, g_s$ are in $\mathbb{Q}[X]$, then f has a representation in T_S in which all sums of squares σ_ϵ are in $\sum \mathbb{Q}[X]^2$. This follows from T. Wörmann's algebraic proof of the theorem using the classical Abstract Positivstellensatz, and a generalization of Wörmann's crucial lemma due to M. Schweighofer.

The Abstract Positivstellensatz. The Abstract Positivstellensatz is usually attributed to Kadison-Dubois, but now thought to be proven earlier by Krivine or Stone. For details on the history of the result, see [4, Section 5.6]. The setting is preordered commutative rings.

Let A be a commutative ring with $\mathbb{Q} \subseteq A$. A subset $T \subseteq A$ is a *preordering* if $T + T \subseteq T$, $T \cdot T \subseteq T$, and $-1 \notin T$. For $S = \{a_1, \ldots, a_k\} \subseteq A$, we define the *preordering generated by* S, T_S, exactly as for $A = \mathbb{R}[X]$.

An *ordering* in A is a preordering P such that $P \cup -P = A$ and $P \cap -P$ is a prime ideal. Any $a \in A$ has a unique sign in $\{-1, 0, 1\}$ with respect to a fixed ordering P and we use the notation $a \geq_P 0$ if $a \in P$, $a >_P 0$ if $a \in P \setminus (P \cap -P)$, etc.

Fix a preordered ring (A, T) and denote by Sper A the real spectrum of (A, T), i.e., the set of orderings of A which contain T. Then define

$$H(A) = \{a \in A \mid \text{ there exists } n \in \mathbb{N} \text{ with } n \pm a \geq_P 0 \text{ for all } P \in \text{Sper } A\},$$

the *ring of geometrically bounded elements in* (A, T), and

$$H'(A) = \{a \in A \mid \text{ there exists } n \in \mathbb{N} \text{ with } n \pm a \in T\},$$

the *ring of arithmetically bounded elements in* (A, T). Clearly, $H'(A) \subseteq H(A)$. The preordering T is *archimedean* if $H'(A) = A$.

The following version of the Abstract Positivstellensatz is [7, Theorem 1]:

Theorem 2. *Given the preordered ring (A, T) as above and suppose $A = H'(A)$. For any $a \in A$, if $a >_P 0$ for all $P \in$ Sper A, then $a \in T$.*

Consider the case where $A = \mathbb{R}[X]$ and $T = T_S$ for $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$. Let $K = K_S$, then K embeds densely in Sper A and hence $H(A) = \{f \in \mathbb{R}[X] \mid f$ is bounded on $S\}$. If S is compact, this implies $H(A) = A$ and Schmüdgen's Theorem follows from the following lemma [1, Lemma 1]:

Lemma 1. *With A, T, and S as above, if $H(A) = A$ then $H'(A) = A$.*

Our result follows from a generalization of Lemma 1, which is [7, Theorem 4.13]:

Theorem 3. *Let F be a subfield of $\mathbb{R}$ and (A, T) a preordered F-algebra such that $F \subseteq H'(A)$ and A has finite transcendence degree over F. Then*

$$A = H(A) \Rightarrow A = H'(A).$$

We can now prove the existence of rational certificates of positivity in Schmüdgen's Theorem. The argument is exactly that of the proof of the general theorem above.

Theorem 4. *Given $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{Q}[X]$ and suppose $K_S \subseteq \mathbb{R}^n$ is compact. Then for any and $f \in \mathbb{Q}[X]$ such that $f > 0$ on K_S, there is a representation of f in the preordering T_S,*

$$f = \sum_{e \in \{0,1\}^s} \sigma_e g_1^{e_1} \ldots g_s^{e_s},$$

with all $\sigma_e \in \sum \mathbb{Q}[X]^2$.

Proof. Let T be the preordering in $\mathbb{Q}[X]$ generated by S. Since K_S is compact, every element of $\mathbb{Q}[X]$ is bounded on K_S. Then K_S dense in Sper A implies that $H(\mathbb{Q}[X]) = \mathbb{Q}[X]$, hence by Theorem 3 we have $\mathbb{Q}[X] = H'(A)$. Note that the condition $F \subseteq H'(A)$ holds in this case since $\mathbb{Q}^+ = \sum \mathbb{Q}^2$. The result follows from Theorem 2. □

3 Rational certificates for Putinar's Theorem

Given $S = \{g_1, \ldots, g_s\}$, recall that the quadratic module generated by S, M_S, is the set of elements in the preordering K_S with a "linear" representation, i.e.,

$$M_S = \{\sigma_0 + \sigma_1 g_1 + \ldots \sigma_s g_s \mid \sigma_i \in \sum \mathbb{R}[X]^2\}.$$

In order to guarantee representations of positive polynomials in the quadratic module, we need a condition stronger than compactness of K_S, namely, we need M_S to be archimedean.

The quadratic module M_S is archimedean if all elements of $\mathbb{R}[X]$ are bounded by a positive integer with respect to M_S, i.e., if for every $f \in \mathbb{R}[X]$ there is some $N \in \mathbb{N}$ such that $N - f \in M_S$. It is not too hard to show that M_S is archimedean if there is some $N \in \mathbb{N}$ such that $N - \sum X_i^2 \in M_S$. Clearly, if M_S is archimedean, then K_S is compact; the polynomial $N - \sum X_i^2$ can be thought of as a "certificate of compactness". However, the converse is not true, see [4, Example 6.3.1]. The key to the algebraic proof of Schmüdgen's Theorem from the previous section is showing that in the case of the preordering generated by a finite set of elements from $\mathbb{R}[X]$, the compactness of the semialgebraic set implies that the corresponding preordering is archimedian.

In 1993, Putinar [5] showed that that if the quadratic module M_S is archimedean, then we can replace the preordering T_S by the quadratic module M_S.

Theorem 5. *(Putinar) Suppose that the quadratic module M_S is archimedean. Then for every $f \in \mathbb{R}[X]$ with $f > 0$ on K_S, $f \in M_S$.*

Lasserre's method for minimizing a polynomial on a compact semialgebraic set, see [3], involves defining a sequence of semidefinite programs corresponding to representations of bounded degree in M_S whose solutions converge to the minimum. In this context, if M_S is archimedean then Putinar's Theorem implies the convergence of the semidefinite programs. In practice, it is not clear how to decide if M_S is archimedean for a given set of generators S, however in concrete cases a polynomial $N - \sum X_i^2$ can be added to the generators if an appropriate N is known or can be computed.

Using an algorithmic proof of Putinar's Theorem due to M. Schwieghofer [8] we can show that rational certificates exist for the theorem as long as we have a polynomial $N - \sum X_i^2$ as one of our generators

Theorem 6. *Suppose* $S = \{g_1, \dots, g_s\} \subseteq \mathbb{Q}[X]$ *and* $N - \sum X_i^2 \in M_S$ *for some* $N \in \mathbb{N}$. *Then given any* $f \in \mathbb{Q}[X]$ *such that* $f > 0$ *on* K_S, *there exist* $\sigma_0 \dots \sigma_s, \sigma \in \sum \mathbb{Q}[X]^2$ *so that*

$$f = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s + \sigma(N - \sum X_i^2).$$

Proof. The idea of Schweighofer's proof is to reduce to Pólya's Theorem. We follow the proof, making sure that each step preserves rationality.

Let $\Delta = \{y \in [0,\infty)^{2n} \mid y_1 + \cdots + y_{2n} = 2n(N + \frac{1}{4})\} \subseteq \mathbb{R}^{2n}$ and let C be the compact subset of $\mathbb{R}^n$ defined by $C = l(\Delta)$, where $l : \mathbb{R}^{2n} \to \mathbb{R}^n$ is defined by

$$y \mapsto \left(\frac{y_1 - y_{n+1}}{2}, \dots, \frac{y_n - y_{2n}}{2} \right)$$

Scaling the g_i's by positive elements in $\mathbb{Q}$, we can assume that $g_i \leq 1$ on C for all i. The key to Schweighofer's proof is the following observation [8, Lemma 2.3]: There exists $\lambda \in \mathbb{R}^+$ such that $q := f - \lambda \sum (g_i - 1)^{2k} g_i > 0$ on C. Since we can always replace λ by a smaller value, we can assume $\lambda \in \mathbb{Q}$.

We have $q := f - \lambda \sum (g_i - 1)^{2k} g_i > 0$ on C, where $q \in \mathbb{Q}[X]$. Write $q = \sum_{i=1}^d Q_i$, where $d = \deg q$ and Q_i is the homogeneous part of q of degree i. Let $Y = (Y_1, \dots, Y_{2n})$ and define in $\mathbb{Q}[Y]$

$$F(Y_1, \dots, Y_{2n}) := \sum_{i=1}^d Q_i \left(\frac{Y_1 - Y_{n+1}}{2}, \dots, \frac{Y_n - Y_{2n}}{2} \right) \left(\frac{Y_1 + \cdots + Y_{2n}}{2n(N + 1/4)} \right)^{d-i}.$$

Then F is homogenous and $F > 0$ on $[0,\infty)^{2n} \setminus \{0\}$. By Pólya's Theorem, there is some $k \in \mathbb{N}$ so that $G := \left(\frac{Y_1 + \cdots + Y_{2n}}{2n(N+1/4)} \right)^k F$ has nonnegative coefficients as a polynomial in $\mathbb{R}[Y]$. Furthermore, since $F \in \mathbb{Q}[Y_1, \dots, Y_{2n}]$, it is easy to see that $G \in \mathbb{Q}[Y]$.

Define $\phi : \mathbb{Q}[Y_1, \dots, Y_{2n}] \to \mathbb{Q}[X]$ by

$$\phi(Y_i) = N + \frac{1}{4} + X_i, \quad \phi(Y_{n+i}) = (N + \frac{1}{4}) - X_i, i = 1, \dots, n$$

and note that $\phi(G) = q$ and

$$\phi(Y_i) = (N + \frac{1}{4}) \pm X_i = \sum_{j \neq i} X_j^2 + (X_i \pm \frac{1}{2})^2) + (N - \sum X_j^2) \in \sum \mathbb{Q}[X]^2 + (N - \sum X_j^2).$$

Thus $\phi(G) = q$ implies there is a representation of q of the required type and then, since $f = q + \lambda \sum (g_i - 1)^{2k} g_i$ with $\lambda \in \mathbb{Q}$, we are done. □

Remark 1. In the preordering case (Schmüdgen's Theorem), as noted above if the semialgebraic set K_S is compact, then it follows that the preordering T_S in $\mathbb{Q}[X]$ is archimedean. However it is more subtle in the quadratic module case since it is not always clear how to decide if M_S is archimedean for a given set of generators S. Thus an open question is the following: Suppose $S \subseteq \mathbb{Q}[X]$ is a finite set of polynomials and M_S is archimedean as a quadratic module in $\mathbb{R}[X]$. Is it true that M_S is archimedean as a quadratic module in $\mathbb{Q}[X]$? To put it more concretely, suppose $S = \{g_1, \dots, g_s\} \subseteq \mathbb{Q}[X]$ and we know that there is some $N \in \mathbb{N}$ such that

$$N - \sum X_i^2 = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s,$$

with $\sigma_i \in \sum \mathbb{R}[X]^2$. Does there exist a representation with $\sigma_i \in \sum \mathbb{Q}[X]^2$? Equivalently, does there exist $N \in \mathbb{N}$ such that for each $i = 1, \dots, n$ we can write

$$N \pm X_i = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s,$$

with $\sigma_i \in \sum \mathbb{Q}[X]^2$?

References

[1] R. Berr and T. Wörmann, *Positive polynomials on compact sets*, Manuscripta Math. **104** (2001), 135–143.

[2] C. Hillar, *Sums of polynomial squares over totally real fields are rational sums of squares*, Proc. Amer. Math. Soc. **137** (2009), 921–930.

[3] J.-B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optimization **11** (2001), no. 3, 796–817.

[4] A. Prestel and C.N. Delzell, *Positive Polynomials – From Hilbert's 17th Problem to Real Algebra*, Springer Monographs Series, Berlin, 2001.

[5] M. Putinar, *Positive polynomials on compact semi-algebraic sets*, Indiana Univ. Math. J. **42** (1993), no. 3, 969–984.

[6] K. Schmüdgen, *The K-moment problem for compact semi-algebraic sets*, Math. Ann. **289** (1991), 203–206.

[7] M. Schweighofer, *Iterated rings of bounded elements and generalizations of Schmüdgen's theorem*, Ph.D. thesis, Universität Konstanz, Konstanz, Germany, 2002.

[8] ———, *Optimization of polynomials on noncompact semialgebraic sets*, SIAM J. Optimization **15** (2005), no. 3, 805–825.

[9] T. Wörmann, *Strikt positive polynome in der semialgebraischen geometrie*, Ph.D. thesis, Universität Dortmund, 1998.